ENCYKLOPEDIA BEZPIECZEŃSTWA

TOM 1

ENCYKLOPEDIA BEZPIECZEŃSTWA

TOM 1

A–C

REDAKCJA NAUKOWA

OLGA WASIUTA, SERGIUSZ WASIUTA

© Copyright by Authors & Wydawnictwo Libron
Kraków 2021

ISBN 978-83-66269-49-1

Recenzenci:
prof. dr hab. Wojciech Jakubowski (Uniwersytet Warszawski)
prof. dr hab. Bogusław Pacek (Uniwersytet Jagielloński)

Redakcja:
Michał Pranke

Korekta:
Joanna Kłos

Projekt okładki i skład:
LIBRON

Publikacja sfinansowana przez Uniwersytet Pedagogiczny
im. Komisji Edukacji Narodowej w Krakowie

Wydawnictwo LIBRON – Filip Lohner
al. Daszyńskiego 21/13
31-537 Kraków
tel. 12 628 05 12
e-mail: office@libron.pl
www.libron.pl

SPIS TREŚCI

6 WSTĘP
12 WYKAZ HASEŁ
17 HASŁA

Połączenie sił to początek,
pozostanie razem to postęp,
wspólna praca to sukces.

HENRY FORD

„Wiedza - to ta część naszej niewiedzy, którą uporządkowaliśmy i skatalogowaliśmy"
Ambrose Gwinnet Bierce

WSTĘP

„Bezpieczeństwo międzynarodowe musi opierać się na zobowiązaniu do wspólnego przetrwania, a nie na groźbie wzajemnego zniszczenia". Te słowa sprzed ponad 40 lat zostały opublikowane w raporcie *„Wspólne bezpieczeństwo: program rozbrojenia"* z 1982 r. Niezależną Komisja ds. Rozbrojenia i Bezpieczeństwa, pod przewodnictwem premiera Szwecji Olofa Palme, i stanowią wyraźne przypomnienie, że przetrwanie ludzkości nie jest przesądzone. Kontynuacja ludzkiej egzystencji w XXI wieku, na planecie liczącej prawie osiem miliardów ludzi, to kolosalna misja globalna. Jest to przedsięwzięcie, które opiera się na zaangażowaniu we współpracę, a nie na unicestwienie. Wyzwania stojące przed naszym współzależnym społeczeństwem globalnym wymagają współpracy i partnerstwa, a nie izolacji i braku zaufania.

Współczesny świat rozwija się w warunkach bezprecedensowej konwergencji międzynarodowych zagrożeń i konfliktów o wysokim stopniu intensywności i niestabilności, które tworzą nowy niespotykany wcześniej poziom i zakres zagrożeń. Przeciwnicy na całym świecie coraz częściej angażują się w wojnę polityczną i informacyjną, praktycznie zniknęła różnica między wojną a pokojem. Dokonując inwazji na Ukrainę, Kreml zamienił zderzenie konkurencyjnych poglądów w śmiertelną rzeczywistość. Czynniki takie jak wojna, zmiany klimatyczne, masowa migracja, eksplozja sztucznej inteligencji, terroryzm i zmieniający się krajobraz geopolityczny oznaczają, że świat stoi przed wieloma problemami, z którymi przywódcy będą musieli się wspólnie uporać, aby zapobiec wzrostowi napięć. Sponsorowani przez totalitarne państwa i grupy terrorystyczne hakerzy przenikają do rządowych, wyborczych, finansowych, gospodarczych energetycznych systemów informacyjnych państw demokratycznych. Autorytarne reżimy oraz prywatne przedsiębiorstwa wojskowe wykorzystują broń niekonwencjonalną, a masowe przesiedlenia ludności oraz przytłaczające kryzysy humanitarne zmieniają zasady i łamią systemy bezpieczeństwa międzynarodowego, które były wynegocjowane z końcem II wojny światowej.

Współczesność przyniosła nowe zagrożenia dla bezpieczeństwa międzynarodowego. Wojna Rosji z Ukrainą stawia nowe wyzwania i problemy dla wielowiekowej tradycji rozumienia pokoju i wojny, a inwazja stała się największym atakiem na kraj europejski od czasu II wojny światowej. Na arenie międzynarodowej widzimy wsparcie dla Ukrainy, ale jednocześnie jest brak zrozumienia pełnej głębi i powagi wydarzeń, z nadzieją na łatwe rozwiązanie konfliktu. Czasami słyszymy zbyt pochopne

wezwania do pokoju, które niestety nie zawsze łączą się z właściwym żądaniem sprawiedliwości.

Nauki o bezpieczeństwie w Polsce obecnie znajdują się na przełomowym etapie kreowania dużego potencjału na licznych polach dydaktyki i nauki w kraju i za granicą. Encyklopedia Bezpieczeństwa – to pierwsze w Polsce tak obszerne specjalistyczne wydanie, celem którego jest rozwinięcie tego potencjału, powielenie i w żądnym przypadku nie zmarnowanie już osiągniętych wspólnie sukcesów badawczych na wielu teoretycznych i praktycznych płaszczyznach działalności.

W trakcie jego przygotowywania Autorzy usystematyzowali terminy z bezpieczeństwa narodowego, międzynarodowego, informacyjnego, społecznego etc., przeprowadzili szereg specjalnych badań naukowych dotyczących uwzględnienia nowych terminów w naukach o bezpieczeństwie, biorąc pod uwagę doświadczenia w przygotowaniu innych publikacji w obszarze szeroko rozumianego bezpieczeństwa w Polsce i za granicą.

Rozwój bezpieczeństwa narodowego i międzynarodowego obecnie, kiedy niektóre autorytarne reżimy w sposób otwarty łamią zasady prawa i uczciwości, musi podążać trudną drogą respektowania istniejącego międzynarodowego prawa, norm i innych regulacji. Zarazem niewątpliwie warto być przygotowanym na nowe niespotykane jak do tej pory wyzwania, kroki przeciwników i rywali cywilizacyjnych, warto wychodzić naprzeciw oczekiwaniom zmieniającej się praktyki. Problematyka ta zyskuje na znaczeniu również w związku z coraz częstszymi licznymi i wieloaspektowymi zagrożeniami oraz konfliktami hybrydowymi, czego rażącym przykładem mogą być współczesne wojny w Ukrainie, Syrii, Libii, Jemenie, Afganistanie etc. Eskalacja konfliktów i nowe ruchy migracyjne w bezpośrednim sąsiedztwie Europy nie pozostaną bez wpływu na jej zbiorowe bezpieczeństwo.

Motywacją przygotowania Encyklopedii Bezpieczeństwa był dotychczasowy brak obszernego, usystematyzowanego zbioru zagadnień terminologicznych dotyczących różnorodnych aspektów narodowego i międzynarodowego bezpieczeństwa. Świat jest coraz bardziej nieprzewidywalny, a zdolność państw do zarządzania ryzykiem związanym z rosnącą przyszłą niepewnością pozostaje zagrożona. Obecnie państwa znajdują się w obliczu szerszej gamy zagrożeń niż w poprzednich dekadach, które stają się bardziej złożone i wzajemnie powiązane.

Spoiwem formalnych i nieformalnych zasad wspólnego bytu państw Sojuszu Północnoatlantyckiego, cywilizacji zachodniej, regulujących kwestie o istotnym wspólnym znaczeniu są wartości polityczne, gospodarcze, społeczne tj. tradycję rozwoju światowej demokracji, społeczeństw obywatelskich, gospodarek rynkowych, praw człowieka, odzwierciedlające troskę wszystkich odpowiedzialnych podmiotów stosunków międzynarodowych, narodowych instytucji o upowszechnienie tego co nas łączy i wyeliminowanie tego, co jest zbędne, utrudnia wspólne zasady technologicznego postępu i społecznego rozwoju.

Współczesne globalne środowisko bezpieczeństwa zmienia się bardzo dynamicznie. Najbardziej kontrowersyjne kwestie bezpieczeństwa dotyczące reżimów autorytarnych i podmiotów niepaństwowych znajdują się w „szarej strefie" na kształt kradzieży własności intelektualnej, wojen cybernetycznych etc., co komplikuje zdolność podmiotów decyzyjnych do wypracowania adekwatnego i skutecznego systemu bezpieczeństwa, co z kolei potrzebuje autentycznego odzwierciedlenia na poziomie pojęciowym i terminologicznym. W związku z powyższym przygotowanie pracy encyklopedycznej ma na celu próbę odpowiedzi na współczesne już istniejące i przyszłe wyzwania i zagrożenia.

W tym kontekście potencjał niniejszej publikacji ściśle wiąże się z codziennością rutynowo wykonywanych obowiązków w wojsku, policji, służbach specjalnych, urzędach państwowych i samorządowych związanych z problematyką bezpieczeństwa i sytuacjami kryzysowymi. Tylko szeroko rozumiana polityka bezpieczeństwa państwa może być odporna na różne niespodzianki, które niewątpliwie czekają na nas w przyszłości.

W związku z powyższym, trzeba dążyć do ułatwienia współpracy międzynarodowej i wewnątrznarodowej poprzez uproszczenie procedur i eliminację biurokracji we wszystkich kluczowych dla bezpieczeństwa rodzajach działalności i procesach. Nabyte dotychczasowe doświadczenia w Polsce i na świecie przekonują, że jest to zadanie wykonalne. Zarazem każdy decydent lub pracownik musi ponosić swoją część konkretnej odpowiedzialności za losy wspólnego bytu.

Możemy i powinniśmy wspólnie kreować mechanizmy adaptacji wobec zaistniałych ostatnio zagrożeń militarnych, paramilitarnych, pandemicznych, radykalnych zmian na arenie międzynarodowej, nie poddawać się względem nich totalnemu sceptycyzmu lub rujnacji tego co łączy państwa zachodnie i demokratyczne, dobrze prezentuje i funkcjonuje. Należy zadbać i pielęgnować elementy solidarności unijnej, europejskiej w obliczu nowych trudnych i niespotykanych wyzwań.

Autorzy niniejszej Encyklopedii Bezpieczeństwa dołożyli maksimum starań żeby zabezpieczyć jej należny poziom naukowy, treść i realia opisywanych procesów i zjawisk bezpieczeństwa. Terminy są ściśle związane z historią kraju, teorią i praktyką bezpieczeństwa narodowego, jednak nie zamykają się w problematyce narodowej. Znacząca liczba terminów odzwierciedla problemy bezpieczeństwa międzynarodowego oraz wybranych państw świata, przede wszystkim sąsiadów, ponieważ zagrożenia dla bezpieczeństwa narodowego są ściśle związane z rozwojem sytuacji w środowisku bezpieczeństwa międzynarodowego, działaniami wojskowymi innych państw, w tym Rosji w pobliżu granic Polski, cyberterroryzmem oraz innymi rodzajami zagrożeń międzynarodowych. Co raz większe znaczenie obecnie odgrywa społeczno-systemowa problematyka - bezpieczeństwo ustrojowe, polityczne, gospodarcze, finansowe, ekologiczne etc. Widać to na tle prób penetracji poszczególnych narodowych instytucji i organów poprzez obce wywiady i inne struktury. Ich celem jest podporządkowanie

polskiego społeczeństwa, zmiana tożsamości narodowej i wartości politycznych obywateli metodami i instrumentami informacyjnymi.

W związku z powyższym zadaniem zespołu Autorów niniejszej pracy była próba uchwycenia i sformułowania fundamentalnych zasad unifikacji koncepcyjnej i terminologicznej jako podstawy dalszego rozwoju teorii i praktyki nauki o bezpieczeństwie, które spełniałoby rolę praktycznego kompendium wiedzy w różnych zakresach współczesnego bezpieczeństwa z uwzględnieniem najnowszych faktów i tendencji. Natomiast głównym celem Encyklopedii Bezpieczeństwa była analiza i wyjaśnienie powszechnie używanych i nowopowstałych terminów bezpieczeństwa narodowego, międzynarodowego, gospodarczego, ekologicznego, technologicznego, energetycznego, społecznego, informacyjnego etc. oraz różnego rodzaju zagrożeń. Duża liczba artykułów i definicji terminologicznych odzwierciedla globalne doświadczenie w zakresie zarządzania aspektami bezpieczeństwa narodowego, tendencje w rozwoju ogólnej teorii bezpieczeństwa, globalizacji, ponieważ zapewnienie bezpieczeństwa narodowego jest złożonym procesem zarządzania państwem, który obejmuje zaangażowanie i wszechstronne wykorzystanie wiedzy wielu nauk.

Rozwój aparatu terminologicznego w każdej sferze działalności zazwyczaj przechodzi przez trzy etapy: pojawienie się podstawowych terminów, formowanie kompleksu najważniejszych terminów i usystematyzowanie terminów w całościowy zespół terminologiczny, stworzenie spójnego systemu terminologicznego. Biorąc pod uwagę, że nauka o bezpieczeństwie jako sfera badań jest wciąż kształtowana i „młoda", jej aparat terminologiczny prawdopodobnie znajduje się na drugim etapie rozwoju. Znakiem tego jest pojawienie się licznych słowników, leksykonów i vademecum bezpieczeństwa[1]. Korzyści płynące z nich oczywiste, ponieważ nie tylko wprowadzają koncepcje w sferę uwagi społeczności naukowej, ale także ich udoskonalają i rozszerzają. Więc, wszystkie terminologiczne słowniki, leksykony, vademecum czy encyklopedie odgrywają ważną rolę w społeczeństwie, a przede wszystkim są integralnym i normatywnym systemem wiedzy. Pełnią w społeczeństwie funkcję integralną, regulacyjną, translacyjną, instytucjonalną, doradczą, a także budują potencjał poznawczo-rozwojowy.

[1] *Słownik terminów z zakresu bezpieczeństwa narodowego*, (red.) W.Łepkowski. Akademia Obrony Narodowej. Warszawa. Wydania 2002-2009; J.Kunikowski, *Słownik terminów wiedzy i edukacji dla bezpieczeństwa*, Wydawnictwo Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach. Wydanie 4, Siedlce 2015; *Leksykon bezpieczeństwa. Wybrane pojęcia,* (red.) K.Dziubińska-Wójcik, R.Niedźwiecki, W.Saletra, A.Zagórska, Wydawnictwo Uniwersytetu Jana Kochanowskiego, Kielce 2016; *Leksykon bezpieczeństwa morskiego. 100 podstawowych pojęć,* (red.) T. Szubrycht. Wydawca: C.H. Beck, Warszawa 2016; *Leksykon bezpieczeństwa wewnętrznego*, (red.) W.Fehler, J.J.Piątek, R.Podgórzańska. Wydawnictwo Naukowe Wydziału Humanistycznego Uniwersytetu Szczecińskiego MINERWA, Szczecin 2017; *Vademecum bezpieczeństwa*, (red.) O.Wasiuta, R.Klepka, R.Kopeć. Wydawnictwo Libron, Kraków 2018; *Vademecum bezpieczeństwa wewnętrznego: społeczny wymiar bezpieczeństwa*, (red.) M. Z. Kulisz. Oficyna Wydawnicza PWSZ w Nysie, Nysa 2019; *Vademecum bezpieczeństwa informacyjnego*. **W 2 tomach**. AT Wydawnictwo -Wydawnictwo Libron, Kraków 2019; *Encyklopedia Bezpieczeństwa*, (red.) O.Wasiuta, S.Wasiuta. **W 6 tomach**, Wydawnictwo Libron. Kraków 2021-2023; *Encyklopedia bezpieczeństwa wewnętrznego*, (red.) A. Misiuk, J. Itrich-Drabarek, M.Dobrowolska-Opała. Wydawnictwo Elipsa, Warszawa 2021.

Baza terminologiczna jest systemem zmiennym pod wpływem rozwoju społecznego i informacyjnego oraz nowych wynikających zagrożeń. Atutem niniejszej publikacji jest fakt, iż w procesie pisania tekstów na temat różnych składowych elementów systemu terminologicznego Autorzy sięgali po różne dane powiązane z bezpieczeństwem z ościennych naukach, które charakteryzują się bogactwem terminów tj. teoria państwa i prawa, nauki o polityce, socjologią, zarządzanie, ekonomią etc. Na uwagę zasługuje także kwestia szerokiego zakresu systemowego bazy terminologicznej, która obejmuje bardzo szeroki przekrój problematyki od rozwoju dziedziny wiedzy naukowej do praktyki konkretnych instytucji.

Całokształt tekstów Encyklopedii Bezpieczeństwa stanowi swego rodzaju punkt widzenia i wyjścia do dalszych dociekań naukowych, konkretyzuje kolejne pytania badawcze. W związku z tym podstawę Encyklopedii Bezpieczeństwa stanowi problemowy trójkąt jako swoisty uniwersalny rdzeń analizy mnogości terminologii, uwzględniający: a) kategorie z obszaru teorii bezpieczeństwa narodowego; b) kategorie z obszaru nauk politycznych, prawniczych, ekonomicznych i wojskowych, a także prawa międzynarodowego w kontekście globalizującego się świata; c) kategorie z obszaru teorii i praktyki działalności administracji publicznej.

Przedstawiona Encyklopedia Bezpieczeństwa została zbudowana z unifikowanych tekstów, niektóre terminy zostały bardziej rozbudowane, co wynika z faktu, iż część pojęć szczególnie istotnych, ważnych, ale słabo opisanych w dostępnej literaturze Autorzy starali się przedstawić w nieco rozszerzonej postaci. Podkreślić należy także, że przygotowana Encyklopedia Bezpieczeństwa ma charakter nie tylko stricte naukowy, ale i praktyczny. Autorzy chcieli dogłębnie pokazać więzi miedzy teorią a praktyką bezpieczeństwa, co z kolei tylko dodaje znaczenia i rozbudowuje możliwości funkcjonowania danej publikacji w realnych procesach społecznych, kiedy potrzebna jest dokładna, precyzyjna i jednoznaczna definicja lub ocena procesu.

Encyklopedia Bezpieczeństwa zawiera prawie 900 terminów (ogółem ponad 300 a.d.). Materiały przedstawione w niej usystematyzowane na podstawie różnych źródeł, które wymagały krytycznej oceny i polemiki merytorycznej wewnątrz autorskiego zespołu, ponieważ miały różny stopień wiarygodności i miarodajności. Na podstawie osobistych doświadczeń Autorów teksty zostały ustrukturyzowane w taki sposób, żeby do pewnego stopnia stworzyć bazę, która jest niezbędna dla wszystkich zainteresowanych w rozwiązywaniu teoretycznych i praktycznych problemów złożonego problemu bezpieczeństwa i które traktowane są jako najważniejsze w literaturze naukowej i publikacjach edukacyjnych.

W przypadku używania określonych fraz przyjmuje się kolejność słów odpowiadającą ich naturalnemu użyciu. Ta obszerna praca obejmuje interdyscyplinarne aspekty bezpieczeństwa, nad którą pracowało prawie pięćdziesiąt twórczych osób - przedstawicieli różnych dyscyplin naukowych, w tym nauk o bezpieczeństwie, o wojskowości, nauk o polityce i administracji, prawnicy, historycy etc.

Ze względów obiektywnych Encyklopedia Bezpieczeństwa nie może przedstawić w sposób wyczerpujący całokształtu obszernej problematyki dotyczącej różnych aspektów bezpieczeństwa, wciąż istnieje wiele nośnych terminów, które nie zostały uwzględnione w Encyklopedii Bezpieczeństwa, co z kolei nie jest wewnętrzną sprzecznością. Autorzy w sposób sukcesywny przeanalizowali najważniejsze pojęcia, uwzględniając bardzo szybki rozwój terminologiczny z zakresu bezpieczeństwa na przestrzeni ostatnich kilku lat. Nowe określenia takie jak: steganografia, wojna kosmiczna, wojna hybrydowa, wojny nowego pokolenia, zielone ludziki już mają swoje stałe miejsce w życiu naukowym i politycznym. Mamy nadzieję, że inne zespoły autorskie uzupełnią niniejsze wysiłki na drodze nowych obszernych publikacji, uwzględniających nowe trendy i realia pojęciowe.

Encyklopedia Bezpieczeństwa jest efektem współpracy zespołu naukowców Instytutu Bezpieczeństwa i Informatyki Uniwersytetu Komisji Edukacji Narodowej w Krakowie. W podobnym gronie autorskim powstało już „Vademecum Bezpieczeństwa" (2018) i „Vademecum Bezpieczeństwa Informacyjnego" (2019), „Encyklopedia bezpieczeństwa" w 6 tomach (2021-2023), które spotkało się ze sporym zainteresowaniem ze strony środowiska naukowego i społeczeństwa.

Autorzy zaproponowanej Czytelnikom Encyklopedii Bezpieczeństwa świadomi tego, że nie jest ona odosobnioną próbą interpretacji szeroko rozumianych aspektów bezpieczeństwa, dlatego przekonani, że niniejsza praca zajmie adekwatne miejsce w kontekście naukowego rozwoju nauk o bezpieczeństwie.

Zachęcając Czytelnika do sięgnięcia po Encyklopedie Bezpieczeństwa, Autorzy liczą, że uzupełni ona już znajdujące się w obiegu naukowym lub dotychczas nietknięte, nowe obszary bezpieczeństwa, w sposób udany będzie odzwierciedlać często odmienne wizje i tematy o różnym stopniu ważności, aktualności i zakresie.

Jesteśmy przekonani, że Encyklopedia Bezpieczeństwa będzie wartościowym przewodnikiem dla wszystkich specjalistów ds. bezpieczeństwa, niezbędnym źródłem informacji w procesach prac referencyjnych, edukacyjnych, analitycznych, eksperckich. Publikacja przyda się każdemu, kto chce opanować najnowszą wiedzę i terminologię naukową z zakresu bezpieczeństwa, okaże się pomocna dla wszystkich zainteresowanych problematyką bezpieczeństwa, zarówno w środowisku akademickim, jak i wśród praktyków, szerokiego grona zainteresowanych.

Jako naukowy zespół jesteśmy świadomi własnej odpowiedzialność. Dlatego z wdzięcznością uwzględnimy wszystkie konstruktywne recenzje, rady, uwagi oraz racjonalne propozycje doskonalenia tej publikacji w kontekście rozwoju nauk o bezpieczeństwie.

Olga Wasiuta, Sergiusz Wasiuta

WYKAZ HASEŁ

Active Shooter 17
Afrykański Trybunał Praw Człowieka i Ludów 20
Agencja Bezpieczeństwa Wewnętrznego 24
Agencja Obrony Przeciwrakietowej 28
Agencja Prasowa 32
Agencja Unii Europejskiej ds. Cyberbezpieczeństwa 57
Agencja Wywiadu (AW) 41
Agencja Zaawansowanych Badań i Rozwoju Departamentu Obrony USA 43
Agent wpływu / agent zagraniczny 49
Agresja 56
Agresja w prawie międzynarodowym 65
Agroterroryzm 69
AI Foundation 74
Al-Dżazira 77
Al-Kaida 82
Alkoholizm 86
Alternacja władzy 92
Ambasada danych 95
Amerykańskie Centrum Badań nad Wojną Nowej Generacji 98
Analiza strategiczna 100
Anarchizm w Polsce 104
Anarchizm w praktyce 109
Anarchizm w teorii 114
Aneksja 118
Antydostępowe zdolności 121
Antyrakietowe systemy 124
Antyterrorystyczna operacja 126
Antyterroryzm 133
Architektura Zero Trust 139
Armia hybrydowa 142
Armia zawodowa 148
Artyleria 153
Asymilacja 162

Atak DDOS 167
Atak informacyjny 172
Atak symultaniczny 176
Attaché obrony 177
Ataszat obrony (wojskowy) 183
Audyt bezpieczeństwa informacji 189
Audyt bezpieczeństwa obiektu 195
Autorytaryzm i neoautorytaryzm 200
Azyl 204
Bańka informacyjna i zjawisko Echo Chamber 209
Barguzin 214
Bariery i zagrożenia w dostępie do informacji 218
Bayraktar 223
Baza lądowa 227
Baza wojskowa 230
Bellingcat 234
Bezpieczeństwo 238
Bezpieczeństwo całościowe 243
Bezpieczeństwo danych osobowych 246
Bezpieczeństwo defensywne 253
Bezpieczeństwo demograficzne 256
Bezpieczeństwo dziecka 261
Bezpieczeństwo ekologiczne 265
Bezpieczeństwo ekonomiczne 271
Bezpieczeństwo energetyczne 278
Bezpieczeństwo euroatlantyckie 287
Bezpieczeństwo europejskie 292
Bezpieczeństwo finansowe 298
Bezpieczeństwo ideologiczne 302
Bezpieczeństwo i higiena pracy (BHP) 310
Bezpieczeństwo informacji niejawnych 314
Bezpieczeństwo informacji wojskowej 321
Bezpieczeństwo informacyjne 330
Bezpieczeństwo klimatyczne 335
Bezpieczeństwo kulturowe 340
Bezpieczeństwo lokalne 344
Bezpieczeństwo ludzkie 345
Bezpieczeństwo medialne 355
Bezpieczeństwo międzynarodowe 360

Bezpieczeństwo militarne 365
Bezpieczeństwo morskie 370
Bezpieczeństwo narodowe 375
Bezpieczeństwo planetarne 382
Bezpieczeństwo polityczne 386
Bezpieczeństwo powszechne i ochrona ludności 392
Bezpieczeństwo pracy 396
Bezpieczeństwo prawne 398
Bezpieczeństwo przesyłu i dystrybucji energii 400
Bezpieczeństwo publiczne 404
Bezpieczeństwo regionalne 411
Bezpieczeństwo rodziny 415
Bezpieczeństwo sanitarno-epidemiologiczne 420
Bezpieczeństwo społeczne 424
Bezpieczeństwo szkolne (bezpieczeństwo w szkole) 429
Bezpieczeństwo teleinformatyczne 435
Bezpieczeństwo ustrojowe 439
Bezpieczeństwo w eksporcie zabytków 444
Bezpieczeństwo w kampaniach wyborczych 448
Bezpieczeństwo w sieci 451
Bezpieczeństwo w tradycyjnych i nowych mediach 456
Bezpieczeństwo wewnętrzne państwa 464
Bezpieczeństwo w zakresie efektywności energetycznej 472
Bezpieczeństwo w zakresie wydobycia surowców energetycznych 478
Bezpieczeństwo zdrowotne 484
Bezpieczeństwo żywności 490
Biała księga bezpieczeństwa narodowego Rzeczypospolitej Polskiej (BK) 496
Biały wywiad 499
Big data 503
Biometria 505
Bioterroryzm 511
Bitwa 515
Bitwa powietrzno-morska 521
Bitwa wieloobszarowa 524
Biuro bezpieczeństwa narodowego RP (BBN) 531
Biuro Informacji i Prasy NATO 535
Blokada morska 536
Blokada zbrojna 538

Botnet 542
BRICS 544
Broń antysatelitarna 549
Broń biologiczna 554
Broń chemiczna (BCh) 559
Broń ekologiczna / broń biosferyczna 562
Broń demograficzna 565
Broń entomologiczna 570
Broń genetyczna 573
Broń geofizyczna 578
Broń hipersoniczna 584
Broń klimatyczna / broń meteorologiczna 591
broń masowego rażenia (BMR) 596
Broń nieśmiercionośna 599
Broń nuklearna 601
Broń orbitalna 604
Broń radiologiczna 607
Broń strzelecka 609
Brytyjska Królewska Marynarka Wojenna 611
Bukaresztańska dziewiątka (B9) 618
Bundeswehra 625
Buriewiestnik 9M730 630
Business Process Management (BPM) 634
C4ISR 646
Cambridge Analytica (CA) 650
Casus Belli 652
CENTO (Central Treaty Organization) 654
Centralne Biuro Antykorupcyjne (CBA) 657
Centralne Biuro Śledcze Policji (CBŚP) 660
Centrum analiz Propagandy i Dezinformacji (CAPD) 666
Centrum Bezpieczeństwa Nowej Ameryki 667
Centrum Doskonalenia Obrony Przed Cyberatakami 672
Centrum Eksperckie NATO ds. Komunikacji Strategicznej 676
Centrum Komunikacji Strategicznej i Bezpieczeństwa Informacji 680
Centrum Kosmiczne NATO 683
Centrum Powiadamiania Ratunkowego (CPR) 685
Centrum Przyszłości Wojny 688
Cenzura 689
Chiński Wielki Podwodny Mur 695

Chmura obliczeniowa 699
Choroby informacyjne 704
Cichociemni 709
Cloud Act 713
COVID-19 (aspekt medyczny) 717
COVID-19 (aspekt społeczny) 721
Crime Mapping 725
Crime Prevention Through Environmental Design (CPTED) 727
Cyberataki 732
Cyberbezpieczeństwo 735
Cyberbroń (broń cybernetyczna) 740
Cybercenzura 744
Cyberdyplomacja 747
Cybergrupy 752
Cyberkonflikt 756
Cyberoperacje 759
Cyberpolityka 763
Cyber Power (potęga cybernetyczna) 768
Cyberprzemoc 773
Cyberprzestępczość 777
Cyberprzestrzeń 784
Cyberstalking 791
Cyberszpiegostwo 795
Cyberterroryzm 799
Cyberwojna 805
Cyberwojska 809
Cyberzagrożenia 813
Cyborg 816
Cyfrowa demencja 818
Cyfrowa konwencja genewska 823
Cyfrowe patologie 827
Cyfrowe prawa człowieka 833
Cyfrowy narcyzm 837
Cyfrowy żołnierz 842
Cyrkon 849
Czynności dochodzeniowo-śledcze 850
Czyn zabroniony 859
Czynności operacyjno-rozpoznawcze 861

A

ACTIVE SHOOTER (z ang. aktywny strzelec) – osoba, której wyłącznym celem jest zabicie jak największej liczby ludzi, najczęściej przy użyciu broni palnej, nierzadko niestabilna psychicznie i emocjonalnie. Początkowo termin był używany jedynie w kręgach służb specjalnych i formacji mundurowych. Do mediów przeniknął dopiero po masakrze w Columbine High School w 1999 r., w czasie której zginęło 15 osób, a 24 zostały ranne. Miejscem ataku przeważnie są miejsca przebywania dużej liczby osób, będące tzw. celami miękkimi (np. szkoły, zakłady pracy czy centra handlowe). Nie istnieje żaden uniwersalny schemat, wg którego wybierane są ofiary aktywnego strzelca (AS). Ataki cechują się przypadkowością, nieprzewidywalnością, dynamiką oraz krótkim czasem akcji – ok. 10–15 min – co nierzadko uniemożliwia przyjazd na czas wyspecjalizowanych jednostek. Mając to na uwadze, każdy człowiek powinien indywidualnie przygotować się na możliwy atak AS. Jest to możliwe poprzez udział w szkoleniach realizowanych zarówno dla funkcjonariuszy służb, jak i dla pracowników czy osób indywidualnych. Ponadto wiele instytucji, organizacji oraz firm wydaje poradniki i broszury poświęcone tej tematyce. W razie wystąpienia ataku AS należy pamiętać o 3 podstawowych zasadach:

- Jeżeli jest to możliwe – uciekaj. W czasie ucieczki pamiętaj o tym, aby nie zabierać ze sobą niepotrzebnych rzeczy (z wyjątkiem telefonu). Jednakże zanim wybierzesz drogę ucieczki, najpierw spróbuj zlokalizować napastnika (np. poprzez odgłosy strzałów czy krzyków). Pomóż w ewakuacji innym tylko wtedy, kiedy jest to możliwe i nie zagrozi to twojemu życiu i zdrowiu. Nie zmuszaj nikogo do ucieczki. W bezpiecznym miejscu zadzwoń pod numer alarmowy.
- Jeżeli nie możesz bezpiecznie uciec – schowaj się. Jeżeli nie wiesz, gdzie znajduje się napastnik, bądź gdy ucieczka jest niemożliwa, pozostań w miejscu, w którym jesteś. Zejdź z pola widzenia strzelca i pozostań bardzo cicho. Wycisz swoje urządzenia elektroniczne i upewnij się, że nie będą wibrować. Jeżeli jest to możliwe, zamknij i zabarykaduj drzwi. Możesz je zastawić ławką, biurkiem czy szafą. Pamiętaj – nadrzędnym celem AS jest pozbawienie życia jak największej liczby osób w jak najkrótszym czasie. Z tego powodu napastnik zazwyczaj nie usiłuje otwierać pomieszczeń, do których dostęp jest utrudniony. Znajdź przedmioty, które mogą być przydatne, jeżeli wystąpi konieczność obrony bądź ataku. Znajdź własne miejsce do ukrycia. Postaraj się komunikować z → p o l i c j ą [t. 3][1] po cichu – na

1 Rozstrzelone słowa stanowią osobne hasła znajdujące się w *Encyklopedii bezpieczeństwa*.

przykład za pośrednictwem wiadomości tekstowych lub umieszczając znak w zewnętrznym oknie. Pozostań na miejscu aż do zakończenia akcji przez funkcjonariuszy i wydania odpowiednich poleceń. Analiza dotychczasowych przypadków wystąpienia ataku AS zwraca uwagę na możliwość wykorzystania → m e d i ó w s p o ł e c z n o ś c i o w y c h [t. 3] (Facebook, Twitter, Instagram) do zaalarmowania służb.

- Jeżeli miejsce ukrycia przestaje być bezpieczne – walcz. W tym przypadku należy pamiętać, że napastnik zazwyczaj dysponuje bronią palną. Priorytetowym celem jest zatem niedopuszczenie do możliwości jej użycia. Najlepszym rozwiązaniem jest zaskoczenie zdecydowanym i dynamicznym atakiem, od razu po wejściu AS do pomieszczenia. Jeżeli przebywasz w grupie – działaj zespołowo. Ustalcie między sobą konkretne zadania, zastanówcie się, co możecie wykorzystać. Pozwoli to na przeprowadzenie ataku w sposób zorganizowany i skuteczny. Jednak warto pamiętać, że nie każdy ma w sobie odwagę, by prowadzić lub podjąć walkę z uzbrojonym przeciwnikiem. Brytyjskie piśmiennictwo zwraca uwagę na prośbę o darowanie życia.

Bezpośrednie działania, jakie podejmują funkcjonariusze służb przybywający na miejsce zdarzenia, ukierunkowane są przede wszystkim na bezzwłoczną eliminację agresora. Należy podkreślić, że w związku z obecnością na miejscu zdarzenia licznych świadków są to czynności, które wymagają ze strony interweniujących funkcjonariuszy zachowania szczególnej ostrożności i rozwagi. Z kolei świadkowie zdarzenia mają obowiązek postępować zgodnie z wydawanymi instrukcjami, a także ewakuować się zgodnie z zaleceniami. W znacznej ilości materiałów analizujących ataki AS w USA występują próby stworzenia profilu psychologiczno-społecznego sprawcy. Jednakże w związku z tym, że w większości przypadków napastnicy popełniają samobójstwo lub tracą życie w wyniku starcia z osobami cywilnymi albo funkcjonariuszami, uzyskanie bezpośrednich → i n f o r m a c j i [t. 2] dotyczących ich motywacji jest trudne. Psycholodzy uważają, że przyczyny działania AS można podzielić na wewnętrzne (takie jak przeżycia, emocje, doświadczenia z dzieciństwa czy młodości) oraz na zewnętrzne (np. niepowodzenia zawodowe, problemy w szkole). Inne czynniki wpływające na działania AS mogą być związane z:

- chorobami psychicznymi oraz zaburzeniami osobowości (zaburzenia afektywne dwubiegunowe);
- poczuciem osamotnienia, izolacją (osoby nieakceptowane i wykluczone społecznie);
- chęcią ukarania niewinnych osób (poczucie wewnętrznej niesprawiedliwości);
- stresem i stanami lękowymi (osoby chorujące na PTSD);
- → k r y z y s e m [t. 2] wartości (brak prawidłowych wzorców społecznych).

Przypadki występowania AS odnotowywane są niemal na całym świecie. W statystykach prowadzonych przez FBI w okresie między 2000 a 2018 r. na terenie USA

doszło do 277 incydentów z udziałem AS, w których zginęły 884 osoby, a 1546 zostało rannych. Do najtragiczniejszych przypadków AS w historii zaliczyć można następujące zdarzenia:

- Ch. Whitman, Uniwersytet Teksański, 1 sierpnia 1966 r. Strzelając z wieży na terenie kampusu, zabił 14 osób, a 31 ranił. Wcześniej zamordował żonę i matkę. Zginął w czasie interwencji policji. W czasie badania ciała w zakładzie medycyny sądowej w mózgu Whitmana znaleziono złośliwego guza w okolicach ciała migdałowatego, które odpowiada za odczucia → a g r e s j i i lęku. Pierwszy atak AS w historii.
- E. Harris i D. Klebold, Columbine High School, 20 kwietnia 1999 r. 2 uczniów objętych programem dla wybitnie uzdolnionych w czasie 50-minutowego ataku zabiło 15 osób, a 24 raniło. Sprawcy ataku w czasie interwencji popełnili samobójstwo. Masakra w Columbine zyskała szeroki odzew w kulturze masowej. Powstały filmy: *Zabawa z bronią* (*Bowling for Columbine*, reż. M. Moore), *Kwietniowe łzy* (*April Showers*, reż. A. Robinson); zespół Foster the People nagrał utwór *Pumped up Kicks*.
- J. Holmes, Kino Century 16 w miejscowości Aurora, 20 lipca 2012 r. W czasie nocnej premiery filmu *Mroczny rycerz powstaje* (*The Dark Knight Rises*, reż. Ch. Nolan) kupił bilet na premierę, po czym w trakcie seansu wyszedł na parking po broń. Zabił 12 osób, 58 ranił. Pierwsze wezwania pod numer alarmowy 911 wykonano po minucie od pierwszych strzałów, natomiast pierwszy patrol dotarł na miejsce po 90 sek. Znalezione zostały 3 sztuki broni oraz puste magazynki. Holmesa aresztowano na parkingu przed kinem. Był pod wpływem vicodinu.
- R. Steinhauser, gimnazjum w Erfurcie, 26 kwietnia 2002 r. 17 zabitych, 7 rannych. Wzorował się na sprawcach masakry w Columbine. Główną przyczyną jego ataku były problemy z nauką, ze szkoły został usunięty ze względu na dostarczenie fałszywego zwolnienia. Popełnił samobójstwo.
- A. Breivik, 22 lipca 2011 r., Oslo i wyspa Utoya, 77 zabitych, 319 rannych. Pierwsza część działań polegała na zdetonowaniu ładunku wybuchowego w centrum Oslo (bomba saletrowa), w drugiej doszło do ataku na wyspie Utoya, gdzie odbywał się zjazd młodzieżówki Partii Pracy. Główną przyczyną tragedii był jego światopogląd skrajnie prawicowy i nacjonalistyczny opisany przez sprawcę w zbiorze tekstów *2083 – Europejska Deklaracja Niepodległości*. Breivik mówił o sobie, że jest najdoskonalszym rycerzem od czasów II wojny światowej oraz regentem Norwegii.
- Omar Ismail Mostefai, Samy Amimour, Foued Mohamed-Aggad i 4 innych sprawców, Francja, teatr Bataclan, St. Denis, 2015 r. ok. 138 zabitych, ponad 430 rannych. Ataki miały miejsce w dniu 13 listopada 2015 r. Było to połączenie ataku AS z samobójczymi zamachami bombowymi w formie ataku symultanicznego.
- S. Paddock, 1 października 2017 r. Sprawca schował się w oknie na 32. piętrze hotelu Mandalay Bay Resort and Casino. W czasie prowadzonego ostrzału rannych zostało 851 osób, a 59 zginęło. Był to najkrwawszy atak AS w historii USA.

W związku z rozwijającymi się → zagrożeniami bezpieczeństwa [t. 4] personalnego zalecane jest, aby pracownicy instytucji społecznych, edukacyjnych i firm posiadali niezbędną wiedzę i umiejętności na temat tego, jak należy postępować podczas tego typu → zagrożenia [t. 4]. Ataki AS wydarzają się niemal w każdym rejonie świata. Przykładem godnym naśladowania dla Polski w aspekcie profilaktyki mogą być m.in. USA, Czechy i Wielka Brytania. Podstawowe programy profilaktyczne realizowane w tamtejszych szkołach obejmują symulowane scenariusze, w których odgrywa się atak AS. Podobnie jak w przypadku ćwiczeń przeciwpożarowych przeprowadzane są z udziałem funkcjonariuszy różnych służb. W szkołach odbywają się również szkolenia teoretyczne dla uczniów, kadry pedagogicznej oraz pracowników technicznych, w czasie których omawiane są zasady postępowania w trakcie tego typu ataków. Ponadto w wielu ze szkół zadecydowano o zatrudnieniu pracowników ochrony. Prowadzone są rejestry osób wizytujących szkoły, a także montowane wykrywacze metalu, których zadaniem jest niedopuszczenie do wniesienia broni na teren szkoły. Część placówek utworzyła również specjalne zespoły oszacowywania zagrożenia, których zadaniem jest identyfikowanie zachowań takich jak zaburzenia psychiczne, alkoholizm, narkomania oraz innych zachowań autodestrukcyjnych występujących wśród uczniów.

W Polsce dostrzeżono potrzebę szkoleń w zakresie procedur antyterrorystycznych, w tym celu została powołana specjalna komórka → Agencji Bezpieczeństwa Wewnętrznego – Centrum Prewencji Terrorystycznej. W grudniu 2019 r. rozpoczęło pierwszą kampanię społeczną zwiększającą świadomość dotyczącą zagrożeń AS. Warto byłoby w tym celu wykorzystać lekcje → edukacji dla bezpieczeństwa [t. 2], organizować spotkania z przedstawicielami służb mundurowych czy specjalnych. Bardzo ważnym elementem edukacji powinno być także szkolenie służb w zakresie koordynacji i współpracy na miejscu zdarzenia oraz wyposażenie ich w środki niezbędne do prawidłowego zabezpieczenia poszkodowanych.

Andrzej Ziarko, Magdalena Bubak

R. Częścik, *Active shooter*, „Kultura Bezpieczeństwa. Nauka – Praktyka – Refleksje" 2013, nr 14; J.A. Fox, *Quit abusing 'active shooter' term*, 6.04.2014, eu.USAToday. com (dostęp 22.01.2020); Healthcare and Public Health Sector Coordinating Council, *Active Shooter. Planning and Reponse*, 2017, JointCommision.org (dostęp 23.01.2020); T. Małysa, *Konfrontacja z aktywnym strzelcem*, „e-Terroryzm.pl" 2012, nr 7; J. Peterson, J. Densley, *Op-Ed: We Have Studied Every Mass Shooting Since 1966. Here's What We've Learned about the Shooters*, 4.08.2019, LATimes. com (dostęp 23.01.2020); Tomek, *Active shooter (1)*, „Komandos" 2011, nr 5 (214); U.S. Department of Homeland Security, *Active Shooter – How to Respond*, DHS. gov, 2008 (dostęp 23.01.2020); A. Wicik, *First responder – po dramacie w Norwegii*, „Policja 997" 2011, nr 8 (77).

AFRYKAŃSKI TRYBUNAŁ PRAW CZŁOWIEKA I LUDÓW (tzw. Trybunał Afrykański) powołano na mocy art. 1 Protokołu do Afrykańskiej Karty Praw Człowieka i Ludów o ustanowieniu Afrykańskiego Trybunału Praw Człowieka i Ludów (tzw.

Protokół do Karty Afrykańskiej). Protokół ten został przyjęty w Wagadugu (Burkina Faso) 9 czerwca 1998 r. przez Zgromadzenie Szefów Państw i Rządów Organizacji Jedności Afrykańskiej (obecna →U n i a A f r y k a ń s k a , UA), a wszedł w życie 25 stycznia 2004 r. Swoją działalność Trybunał Afrykański rozpoczął w 2006 r. Jego siedziba od 2007 r. jest w Aruszy (Tanzania). Wcześniej znajdowała się ona w Addis Abebie (Etiopia). W latach 2006–2008 Trybunał Afrykański zajmował się przede wszystkim sprawami organizacyjnymi i administracyjnymi, takimi jak rozwój biura, przygotowywanie budżetu, opracowywanie regulaminu przejściowego.

Głównym celem powołania Trybunału było uzupełnienie mandatu ochronnego Afrykańskiej Komisji Praw Człowieka i Ludów (tzw. Komisja Afrykańska), która została utworzona w 1981 r. jako quasi-sądowy organ Karty Afrykańskiej. Trybunał Afrykański wraz z Komisją Afrykańską dążą do tego, by stworzyć całościowy mechanizm nadzoru pozwalający ustalić, czy państwa strony Karty Afrykańskiej wprowadzają w życie postanowienia zawarte w tym dokumencie, dochowując tym samym zobowiązań prawnomiędzynarodowych. Obie instytucje wypowiadają się także na temat roszczeń dotyczących naruszeń → p r a w c z ł o w i e k a [t. 3] przez poszczególne państwa.

W skład Trybunału wchodzi 11 sędziów wybieranych przez Zgromadzenie Szefów Państw i Rządów Unii Afrykańskiej spośród kandydatów zgłaszanych przez państwa członkowskie Unii Afrykańskiej. Należy zaznaczyć, że państwa mogą nominować maksymalnie 3 kandydatów, przy czym 2 z nich musi pochodzić z państwa zgłaszającego kandydatury. Kandydaci na sędziego muszą mieć stosowne kompetencje i kwalifikacje, takie jak uznana praktyka sądowa lub akademicka, a także doświadczenie w zakresie ochrony praw człowieka, oraz prezentować odpowiedni poziom moralny. Sędziowie są wybierani w głosowaniu tajnym. Członkowie Zgromadzenia Szefów Państw i Rządów Unii Afrykańskiej, dokonując ich wyboru, biorą również pod uwagę to, by przyszli sędziowie reprezentowali główne regiony geograficzne Afryki oraz różne kultury prawne. Istotna jest także zasada równości płci kandydatów. Sędziowie są niezależni i niezawiśli. Ich kadencja trwa 6 lat, mogą jednak zostać wybrani na jeszcze jedną kadencję. Mandat 4 sędziów wygasa po upływie 2 lat, a 4 kolejnych po 4 latach. Po pierwszych wyborach dokonywane jest losowanie, które ma stwierdzić, jak długa będzie kadencja wybranych sędziów.

Trybunał nie jest organem pełnoetatowym, lecz sesyjnym. Co roku zwoływane są 4 sesje zwyczajne. Trwają one 4 tygodnie i najczęściej odbywają się w marcu, maju, we wrześniu i w listopadzie. Jeśli zaistnieje konieczność, Trybunał może zostać zwołany na sesje nadzwyczajne. Sędziowie Trybunału pełnią swoje funkcje w niepełnym wymiarze godzin. Tylko prezes Trybunału pracuje w pełnym wymiarze czasu w siedzibie w Aruszy.

Trybunał Afrykański ma kompetencje zarówno sporne, jak i doradcze. W ramach tych pierwszych sprawuje jurysdykcję nad wszystkimi przedłożonymi mu sprawami, które dotyczą interpretacji i stosowania Karty Afrykańskiej, Protokołu do Karty Afry-

kańskiej oraz wszelkich innych instrumentów dotyczących ochrony praw człowieka ratyfikowanych przez dane państwo Unii Afrykańskiej. Podmiotami uprawnionymi do wszczęcia postępowania przed Trybunałem Afrykańskim są: Komisja Afrykańska,państwo strona, które złożyło skargę lub przeciwko któremu złożono skargę w Komisji, państwo strona, którego obywatele są ofiarami łamania praw człowieka. Dodatkowo przed Trybunałem mogą występować organizacje pozarządowe i osoby fizyczne. Pełnią one jednak funkcję obserwatora. Należy podkreślić, że obserwatorzy mają prawo do składania wniosków do Trybunału Afrykańskiego w toczącym się postępowaniu. Dostęp do Trybunału jest jednak ograniczony. Oznacza to w praktyce, że zarówno osoby fizyczne, jak i organizacje pozarządowe nie mogą się do niego zwracać bezpośrednio. W celu wszczęcia postępowania podmiotyte muszą uzyskać zezwolenie od Trybunału Afrykańskiego. Dodatkowo państwo pozwane o naruszenie jednego z międzynarodowych praw człowieka musi przyjąć jurysdykcję Trybunału.

Kartę Afrykańską ratyfikowały 54 państwa z 55 należących do UA (z wyjątkiem Maroka). Jednakże tylko 34 państwa członkowskie UA ratyfikowały Protokół do Karty Afrykańskiej. Spośród nich jedynie 8 państw zaakceptowało kompetencje Trybunału, zgodnie z którymi jednostki i organizacje pozarządowe mogą wnosić sprawy bezpośrednio do Trybunału. Postępowanie przed Trybunałem powinno zostać poprzedzone procedurą polubownego zakończenia sprawy. Szczegóły przeprowadzenia postępowania są określone w jego regulaminie. Posiedzenia Trybunału mają charakter publiczny. Strony w postępowaniu mają prawo do reprezentacji przez wyznaczonego pełnomocnika. W określonych sytuacjach mogą one zostać zwolnione z opłat. Trybunał Afrykański ma rozpatrywać wnioski składane przez strony postępowania. Przeprowadza on dochodzenie, jeśli tylko uzna je za konieczne. Wówczas strony postępowania są zobowiązane do udzielenia wszelkiej pomocy w celu wyjaśnienia sprawy. Świadkowie lub przedstawiciele stron postępowania mają prawo do korzystania z ochrony na podstawie zasad prawa międzynarodowego.

Trybunał Afrykański przyjmuje dowody w formie pisemnej, ustnej, jak i opinie biegłych.

W celu rozpoznania sprawy przed Trybunałem wymagane jest kworum, które wynosi 7 sędziów. Jest to wymóg istotny, gdyż jeśli na początku posiedzenia nie osiągnięto kworum, lub w trakcie posiedzenia zostanie ono zerwane, to prezes Trybunału decyduje o odroczeniu posiedzenia. Orzeczenia zapadają większością głosów członków Trybunału w ciągu 90 dni od zakończenia postępowania.

Jeśli zostanie stwierdzone naruszenie praw i wolności człowieka, Trybunał przygotowuje zalecenia. Mają one skutkować usunięciem naruszeń. W zaleceniach widnieje również decyzja co do wypłaty odszkodowania lub zadośćuczynienia. Jeśli Trybunał orzekł o poważnym naruszeniu praw człowieka, to w celu uniknięcia nieodwracalnej szkody na osobie może on zadecydować o zastosowaniu stosownych środków tymczasowych. Sędziowie, którzy nie zgadzają się z wyrokiem, mogą zgłosić zdanie

odrębne. Po zapadnięciu wyroku Trybunał Afrykański powiadamia strony postępowania, członków Unii Afrykańskiej, Afrykańską Komisję Praw Człowieka i Ludów. Informacja o wyroku zostaje również przesłana do Rady Ministrów Unii Afrykańskiej, która monitoruje jego wykonanie w imieniu Zgromadzenia Unii.

Obowiązkiem Trybunału jest również przygotowanie corocznego sprawozdania ze swojej działalności. Zawiera ono informacje dotyczące niezastosowania się państw do konkretnych wyroków i jest przedkładane Zgromadzeniu Unii. Trybunał może dokonać rewizji swojego orzeczenia oraz jego wykładni.

Pierwsze postępowanie przed Trybunałem Afrykańskim odbyło się w 2008 r. Skarga z 11 sierpnia 2008 r. przeciwko Senegalowi została zwieńczona wyrokiem po upływie 16 miesięcy. Trybunał stwierdził brak jurysdykcji do orzekania w tej konkretnej sprawie. Pierwszy wyrok natury merytorycznej zapadł w Trybunale Afrykańskim 14 czerwca 2013 r. Sprawa dotyczyła procesu demokratycznego w wyborach prezydenckich w Tanzanii. Trybunał stwierdził naruszenie przez Tanzanię przepisów Karty Afrykańskiej, gdyż zakaz kandydowania niezależnych kandydatów w wyborach wynikający z konstytucji Tanzanii łamał postanowienia Karty. W 2014 r. Trybunał Afrykański po raz pierwszy rozpatrzył wniosek o interpretację i rewizję wydanego wcześniej przez siebie wyroku. W tym samym roku wydał także pierwsze orzeczenie w sprawie odszkodowań. Uruchomił również system pomocy prawnej w celu sfinansowania przez ewentualnych skarżących kosztów związanych z wynajęciem adwokata czy z podróżą. W 2017 r. w Trybunale Afrykańskim zapadł przełomowy wyrok w sprawie ludu Ogiek. Było to pierwsze orzeczenie Trybunału dotyczące traktowania ludności rdzennej i jej praw. Stwierdzono, że rząd Kenii naruszył prawa ludu Mau Ogiek, gdy eksmitował jego członków z ich rodowej ziemi. Opierając się na wcześniejszych decyzjach Komisji Afrykańskiej, które odnosiły się do podobnych spraw, Trybunał Afrykański stwierdził naruszenie praw do: niedyskryminacji, kultury, religii, własności, swobodnego dysponowania dobrami i zasobami naturalnymi oraz gospodarczego i społecznego rozwoju. W 2018 r. w zapadł pierwszy wyrok dotyczący praw kobiet i dzieci w Afryce. Trybunał nałożył na państwa zobowiązanie do utrzymania międzynarodowych standardów praw człowieka w sferze prawa rodzinnego, nawet w sytuacji, gdy wymagać to będzie odejścia od prawa religijnego i zwyczajowego.

Jeśli chodzi o kompetencje doradcze Trybunału Afrykańskiego, to na wniosek któregokolwiek z państw członkowskich Unii Afrykańskiej, jej organów lub organizacji afrykańskiej (zarówno rządowej, jak i pozarządowej) uznanej przez UA, Trybunał może wydawać opinie dotyczące każdej kwestii prawnej związanej z Kartą Afrykańską lub innym dokumentem w zakresie praw człowieka, jeśli jej przedmiot nie jest związany z kwestią rozpatrywaną przez Komisję Afrykańską.

Należy również wspomnieć o działalności pozasądowej Trybunału Afrykańskiego. Polega ona na współpracy z takimi organizacjami jak Unia Europejska, Fundacja

Konrada Adenauera, Duński Instytut Praw Człowieka, Fundacja MacArthura. Trybunał prowadzi także akcje promującejego statutową działalność.

Paulina Szeląg

African Charter on Human and Peoples' Rights, Nairobi, 27 June 1981, UNTS, vol. 1520, No. 26363; *African Court on Human and Peoples' Rights*, *Basic Information*, https://www.african-court.org/wpafc/basic-information/ (dostęp 10.05.2023); M.I. Andrzejewski, M. Cios, *Rola i przyszłość Afrykańskiego Trybunału Praw Człowieka i Ludów w regionalnym systemie ochrony praw człowieka*, [w:] *Ochrona praw człowieka w wymiarze regionalnym*, M. Marcinko (red.), Ośrodek Międzynarodowego Prawa Humanitarnego i Praw Człowieka WPiA UJ, Kraków 2012; A. Dąbrowski, *Dwudziesta rocznica utworzenia Afrykańskiego Trybunału Praw Człowieka i Ludów – przegląd działalności*, „Studia Prawnicze" 2019, nr 1; W. Kilarski, *Afrykański system międzynarodowych organów sądowych*, „Przegląd Prawa i Administracji" 2011, t. LXXXV; Protocol to the African Charter on Human and Peoples' Rights on the Establishment of an African Court on Human And Peoples' Rights, Ouagadougou, 9 June 1998, OAU Doc. OAU/LEG/EXP/AFCHPR/PROT (III).

AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO – organ państwa właściwy w sprawach ochrony jego → b e z p i e c z e ń s t w a wewnętrznego i porządku konstytucyjnego. Utworzony na mocy Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. 2002, nr 74, poz. 676), zastępuje działający od 1990 r. → U r z ą d O c h r o n y P a ń s t w a [t. 4]. Obecnie jest to najważniejsza instytucja odpowiedzialna za ochronę bezpieczeństwa wewnętrznego państwa. Spoczywa na niej wyłączny obowiązek stania na straży porządku konstytucyjnego Rzeczypospolitej Polskiej, co zostało określone *expressis verbis* w art. 5 ust. 1 pkt 1 cyt. ustawy. Wskazuje on, iż podstawowym celem działań Agencji Bezpieczeństwa Wewnętrznego (ABW) jest rozpoznawanie, zwalczanie i niedopuszczanie do → z a g r o ż e ń [t. 4] wymierzonych w → b e z p i e c z e ń s t w o w e w n ę t r z n e p a ń s t w a oraz jego porządek konstytucyjny, a w szczególności godzących w tak ważne wartości jak:

- → s u w e r e n n o ś ć [t. 4] i międzynarodowa pozycja Polski;
- niepodległość i nienaruszalność jej terytorium;
- obronność.

Funkcjonowanie demokratycznego państwa prawnego jest uwarunkowane przestrzeganiem – zarówno przez organy władzy państwowej, partie polityczne, jak i obywateli – norm zawartych w ustawie zasadniczej. Stąd wszelkie niekonstytucyjne działania wymagają szybkiej i zdecydowanej reakcji ze strony państwa. Szczególnie groźne są te zmierzające do obalenia lub niezgodnej z prawem zmiany ustroju państwowego bądź zakłócenia jego normalnego funkcjonowania. W tym zakresie ABW spełnia ten obowiązek poprzez aktywność kontrwywiadowczą (art. 5 ust. 1 pkt 2 lit. a) cyt. ustawy). W ramach tych działań ABW monitoruje instytucjonalną i cudzoziemską aktywność na terenie Polski pod kątem rozpoznania realizacji zadań na rzecz obcych służb specjalnych. Prowadzi także ofensywne rozpracowywanie obcych służb specjalnych

i rozpoznanie osób oraz innych podmiotów współpracujących z tymi służbami. ABW organizuje też szkolenia prewencyjne dla kadry urzędniczej, wskazując na niebezpieczeństwa, z jakimi może się ona spotkać w trakcie wykonywanych obowiązków. Z badań wynika, iż często właśnie brak wiedzy i czujności są głównymi przyczynami powstawania zagrożeń o charakterze kontrwywiadowczym. Ważnym wyzwaniem dla ABW jest zapewnienie państwu → b e z p i e c z e ń s t w a e k o n o m i c z n e g o (art. 5 ust. 1 pkt 2 lit. b), c) i d) cyt. ustawy). Procesowi globalizacji oraz postępującej integracji gospodarczej towarzyszy stała redukcja barier polityczno-prawnych sprzyjająca nieskrępowanemu przepływowi osób, towarów i kapitału. To pozytywna tendencja rozwojowa, ale rolą służb specjalnych, a zwłaszcza ABW, jest niedopuszczenie do sytuacji, gdy na skutek zaistnienia niepożądanych działań gospodarka nie będzie w stanie samodzielnie się rozwijać lub jej funkcjonowanie zostanie zakłócone przez negatywne czynniki o charakterze wewnętrznym bądź zewnętrznym.

Zewnętrzne zagrożenia ekonomiczne są efektem procesów zachodzących w gospodarce światowej, czyli globalizacji, oraz wzajemnych współzależności. Mogą tu jednak wystąpić symptomy nieprzewidywalności i chaotyczności światowego rynku, ale także świadome działania obcych państw, których celem jest wywarcie wpływu na sytuację gospodarczą innego kraju. Mogą do tego wykorzystywać własne → s ł u ż b y s p e c j a l n e [t. 4] i powiązane z nimi podmioty gospodarcze. Zagrożeniami ekonomicznymi wewnętrznymi są niezgodne z prawem działania rodzimych i zagranicznych przedsiębiorców prowadzone na rynku krajowym. Mogą to być próby nielegalnego wzbogacenia się poprzez oszustwa podatkowe, defraudacje państwowych lub zagranicznych dotacji czy spekulację. Tym działaniom często towarzyszy → k o r u p c j a [t. 2] urzędników, zarówno szczebla rządowego, jak i samorządowego. → P r z e s t ę p c z o ś ć [t. 3] ekonomiczna zwana też przestępczością „białych kołnierzyków" coraz częściej ma charakter zorganizowany i międzynarodowy i wykazuje związki z → t e r r o r y z m e m [t. 4], którego zwalczanie jest kolejnym ważnym aspektem działań ABW – określonym w art. 5 ust. 1 pkt 2 lit. a) cyt. ustawy. Jest to zadanie trudne do realizacji wtedy, gdy przeciwnikiem staje się tzw. samotny wilk (ang. *lone wolf*), czyli sprawca dokonujący aktów terroru w pojedynkę, odizolowany i pozbawiony powiązań z grupami terrorystycznymi, nad którym nie ma żadnego dowództwa. Środki do przeprowadzania zamachów zdobywa lub produkuje indywidualnie. Mikroterroryści często posługują się improwizowanymi ładunkami wybuchowymi (IED, ang. *Improvised Explosive Device*), korzystając ze stosunkowo łatwego dostępu do komponentów umożliwiających ich skonstruowanie. Jako narzędzia ataku wybierają także broń białą (noże, maczety), a nawet pojazdy samochodowe, którymi taranują osoby uczestniczące w masowych zgromadzeniach.

W taktyce działania terrorystów pojawiły się też zamachy symultaniczne, podczas których w tym samym czasie dochodzi do skoordynowanych ataków w różnych miejscach, na obszarze tego samego miasta. Taki właśnie charakter miały ataki

np. w 2004 r. na pociągi w Madrycie, w 2005 r. na metro i autobus w Londynie czy w 2015 r. na lokale publiczne w Paryżu. Nowym zagrożeniem jest → c y b e r t e r r o r y z m , który w Rządowym Programie ochrony cyberprzestrzeni Rzeczypospolitej Polskiej rozumiany jest jako cyberprzestępstwo mające charakter terrorystyczny. Atak z wykorzystaniem instrumentów informatycznych jest tani i trudny do wykrycia, a jego konsekwencje mogą stanowić poważne zagrożenie dla → i n f r a s t r u k t u r y k r y t y c z n e j [t. 2] państwa. W 2007 r. w Estonii → h a k e r z y [t. 2] posłużyli się formą ataku DDoS (od ang. *distributed denial of service*), polegającą na uniemożliwieniu działania systemu komputerowego czy usługi poprzez zajęcie ich wszystkich wolnych zasobów. Ten atak doprowadził do przeciążenia i zablokowania pracy serwerów, co spowodowało paraliż całego kraju, zwłaszcza jego systemów bankowych, informacyjnych i policyjnych. Estonia uznała ten atak za akt → a g r e s j i ze strony Rosji i domagała się reakcji sojuszniczej ze strony państw członkowskich NATO. Wskazane zmiany we współczesnym terroryzmie znacznie komplikują proces wykrywczy, zwłaszcza że pozyskanie źródeł osobowych w hermetycznym środowisku, np. ekstremistów islamskich, jest wyjątkowo trudne.

Kolejne zadanie ABW związane jest z kwestią proliferacji → b r o n i m a s o w e g o r a ż e n i a . Zwiększone zagrożenie pojawiło się w wyniku rozpadu bloku wschodniego, spowodowanego upadkiem ZSRR oraz likwidacją Układu Warszawskiego. Wielu naukowców i ekspertów z dziedziny produkcji broni masowego rażenia zostało wówczas pozyskanych przez służby specjalne i różnego rodzaju organizacje terrorystyczne, które były zainteresowane wykorzystaniem ich wiedzy do własnych celów. W polu zainteresowania tych podmiotów znalazły się również materiały potrzebne do wytworzenia tego rodzaju broni, a także jej wojskowe składy i magazyny zlokalizowane na obszarze byłego ZSRR. W dalszym ciągu mogą one stanowić przedmiot kradzieży bądź transakcji dokonywanych na tzw. czarnym rynku. Obecnie → i n f o r m a c j e [t. 2] o sposobach skonstruowania broni masowego rażenia, zwłaszcza chemicznej (→ b r o ń c h e m i c z n a) i biologicznej (→ b r o ń b i o l o g i c z n a), można znaleźć w internecie czy w poradnikach przygotowywanych dla terrorystów przez ISIS (zob. → P a ń s t w o I s l a m s k i e [t. 3]). O tym, że zagrożenia te mają charakter realny, świadczą akcje przeprowadzone w Japonii przez sektę Najwyższa Prawda, której liderem był Shōkō Asahara. W czerwcu 1994 r. w Matsumoto członkowie sekty rozpylili sarin z pojemnika zamontowanego w samochodzie ciężarowym. Zwiększenie temperatury pojemnika skutkowało uwolnieniem się oparów substancji, która przybrała postać gazowej chmury. Prądy konwekcyjne przeniosły ją na osiedle mieszkaniowe, doprowadzając do zatrucia 500 osób, spośród których 7 zmarło. Rok później terroryści z tej samej sekty przeprowadzili swą najgroźniejszą akcję, rozpylając sarin w 5 pociągach tokijskiego metra. Sposób rozpylenia aerozolu był wyjątkowo prymitywny, gdyż polegał na przekłuciu plastikowych opakowań. Na skutek zamachu śmierć poniosło 12 osób, a blisko 5,5 tys. zostało rannych. W marcu 2002 r. terrorysta

Hamasu usiłował rozpylić cyjanowodór w budynku hotelu Park, a w 2004 r. iracki odłam Al-Kaidy przygotowywał w Jordanii detonację za pomocą IED 20 ton chemikaliów, czego skutkiem mogła być śmierć ok. 20 tys. ludzi. Wówczas jordańskie służby bezpieczeństwa udaremniły ten atak. Nadal jednak zagrożenie ma charakter realny, co podnoszą eksperci zwłaszcza w kontekście konieczności zapewnienia bezpieczeństwa wielkopowierzchniowym obiektom handlowym.

Wskazane wyżej zadania ABW realizuje poprzez funkcję analityczno-informacyjną zapisaną w art. 5 ust. 1 pkt 4 cyt. ustawy, który stanowi, że do ABW należy uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć duże znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego. W → s p o ł e c z e ń s t w i e i n f o r m a c y j n y m [t. 4] warunkiem sprawnego funkcjonowania systemu bezpieczeństwa wewnętrznego państwa jest zagwarantowanie mu stałego dopływu informacji z różnych źródeł, ich bieżącej analizy oraz przetwarzania. Pozwala to organom państwa na prawidłowe wnioskowanie oraz wykorzystywanie pozyskanych danych w podejmowanych procesach decyzyjnych.

ABW spełnia także funkcję procesową, która definiuje szczególne uprawnienia funkcjonariuszy tej służby, określone w art. 23 ustawy. Należą do nich: zatrzymanie osób; przeszukanie osób i pomieszczeń; legitymowanie osób; stosowanie → ś r o d k ó w p r z y m u s u b e z p o ś r e d n i e g o [t. 4]; prawo użycia broni czy kontrola osobista. Działania w tym obszarze prowadzone są przez ABW na podstawie przepisów kodeksu postępowania karnego.

Funkcję kontrolno-ochronną ABW realizuje według zapisu w art. 5 ust. 1 pkt 3 cyt. ustawy, który określa, że do zadań tej służby należy wykonywanie, w granicach jej właściwości, zadań służby ochrony państwa oraz pełnienie funkcji krajowej władzy bezpieczeństwa, w zakresie ochrony → i n f o r m a c j i n i e j a w n y c h [t. 2] w stosunkach międzynarodowych. Wiąże się to z procesem przeciwdziałania ujawnianiu informacji poufnych oraz sprawdzania stanu ich zabezpieczenia. Zadanie to nabrało szczególnego znaczenia w sytuacji członkostwa Polski w UE i NATO. Funkcję kontrolno-ochronną ABW realizuje w 3 obszarach:

- bezpieczeństwa osobowego – poprzez prowadzenie postępowań sprawdzających, czy dana osoba daje rękojmię zachowania tajemnicy;
- bezpieczeństwa przemysłowego – poprzez prowadzenie postępowań sprawdzających wobec przedsiębiorców starających się o zawarcie umowy, z którą łączy się dostęp do informacji niejawnych;
- kontroli ochrony informacji niejawnych – poprzez sprawdzanie przestrzegania przepisów w zakresie ochrony informacji niejawnych we wszystkich organach władzy publicznej, bankach państwowych i innych państwowych jednostkach organizacyjnych.

Funkcję operacyjno-rozpoznawczą ABW spełnia poprzez niejawne i niekonwencjonalne działania ukierunkowane na uzyskanie, sprawdzenie i wykorzystanie informacji o pozostających w ich prawnie uzasadnionym zainteresowaniu osobach, miejscach bądź zdarzeniach. Podstawowe → c z y n n o ś c i o p e r a c y j n o - r o z p o z n a w c z e prowadzone przez ABW to:

- kontrola operacyjna (art. 27 cyt. ustawy) polegająca na kontrolowaniu zawartości korespondencji i przesyłek oraz stosowaniu środków technicznych do uzyskania w sposób poufny informacji i dowodów o przestępstwie oraz ich utrwalenia;
- przesyłka kontrolowana (art. 30 cyt. ustawy) polegająca na niejawnym nadzorowaniu wytwarzania, przemieszczania, przechowywania przedmiotów przestępstwa i obrotu nimi celem jego udokumentowania, ustalenia tożsamości osób w nim uczestniczących lub przejęcia przedmiotów przestępstwa;
- prowokacja (art. 29 cyt. ustawy) polegająca na niejawnym nabyciu bądź przejęciu przedmiotów pochodzących z przestępstwa, albo których wytwarzanie, posiadanie czy którymi handel są zabronione. Może polegać także na wręczeniu lub przyjęciu korzyści majątkowej przez funkcjonariusza ABW celem sprawdzenia uzyskanych wcześniej wiarygodnych informacji o przestępstwie oraz wykrycia sprawców i uzyskania dowodów na potrzeby planowanej bądź toczącej się sprawy.

Andrzej Czop

M. Bożek, K. Walczuk, *Agencja Bezpieczeństwa Wewnętrznego – organizacja i funkcjonowanie na tle uwarunkowań prawnych*, Kancelaria Adwokacka Paulina Walczuk, Warszawa 2014; A. Czop, *Agencja Bezpieczeństwa Wewnętrznego*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; tenże, *System bezpieczeństwa publicznego Rzeczypospolitej Polskiej ze szczególnym uwzględnieniem prywatnego sektora ochrony*, Wyższa Szkoła Bezpieczeństwa Publicznego i Indywidualnego „Apeiron" w Krakowie, Kraków 2016; *Leksykon bezpieczeństwa wewnętrznego*, W. Fehler, J.J. Piątek, R. Podgórzańska (red.), Wydawnictwo Naukowe Wydziału Humanistycznego US Minerwa, Szczecin 2017; M. Piotrak, *Rola i zadania szefa Agencji Bezpieczeństwa Wewnętrznego w zarządzaniu kryzysowym i ochronie infrastruktury krytycznej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016, nr 15; Ł. Skoneczny, *Rola Agencji Bezpieczeństwa Wewnętrznego w systemie bezpieczeństwa Rzeczypospolitej Polskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2009, nr 1; M. Świderski, *Bezpieczeństwo wewnętrzne i jego uwarunkowania*, [w:] *Bezpieczeństwo państwa. Wybrane problemy*, K. Wojtaszczyk, A. Materska-Sosnowska (red.), ASPRA-JR, Warszawa 2009; *Urząd Ochrony Państwa 1990–2002*: *25 lat UOP ABW, 6 kwietnia 2015*, Z. Nawrocki (red.), Agencja Bezpieczeństwa Wewnętrznego, Centralny Ośrodek Szkolenia im. gen. Stefana Roweckiego „Grota", Warszawa 2015; Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu Dz. U. 2010, nr 29, poz. 154 z późn. zm.

AGENCJA OBRONY PRZECIWRAKIETOWEJ (ang. *Missile Defense Agency*, MDA) – funkcjonująca jednostka organizacyjna Departamentu Obrony Stanów Zjednoczonych zajmująca się opracowywaniem, badaniem oraz nabywaniem środków obrony antybalistycznej. Statutowym celem MDA jest stworzenie systemu umożliwiającego obronę terytorium Stanów Zjednoczonych, sił zbrojnych przebywa-

jących poza granicami kraju oraz sojuszników przed atakami, do których mogą zostać wykorzystane wszelkie rodzaje ataków rakietowych.

Początki rozwoju obrony przeciwrakietowej Stanów Zjednoczonych (ang. *Ballistic Missile Defense*, BMD) wiążą się z wyścigiem zbrojeń, a tym samym – z polityką → o d s t r a s z a n i a [t. 3] wykorzystującą produkcję rakiet balistycznych uzbrojonych w głowice nuklearne. Taka polityka spowodowała, że zagadnienia związane z obroną przeciwrakietową wpisano w 1958 r. do zadań US Army. W 1972 r., kiedy doszło do podpisania między USA a ZSRR porozumienia o ograniczeniu systemów obrony przeciwrakietowej (ang. *ABM Treaty*), Stany Zjednoczone rozwijały kilka programów obrony przeciwrakietowej, tj. Nike-X, Sentinel oraz Safeguard. MDA jest silnie powiązana z programem Strategic Defense Initiative (SDI), który w celu opracowania obrony przeciwrakietowej niebazującej na broni jądrowej zapoczątkował w 1983 r. prezydent Ronald Reagan. SDI powstało z połączenia wielu programów obrony przeciwrakietowej realizowanych przez kilka agencji rządowych i bazowało na idei stworzenia spójnego programu pod kierownictwem Organizacji na rzecz Inicjatywy Obrony Strategicznej (SDIO). Zadania SDIO, oparte pierwotnie na budowie systemu obrony przed strategicznymi głowicami nuklearnymi ZSRR, zostały zmodyfikowane, gdy okres → z i m n e j w o j n y [t. 4] dobiegł końca. W 1994 r. SDIO oficjalnie zmieniła nazwę na Organizację na rzecz Obrony Antybalistycznej (BMDO), a nowe → z a g r o ż e n i a [t. 4] związane z rozwojem technologii balistycznej w krajach takich jak Korea Północna (wystrzelenie w sierpniu 1998 r. nad Japonię pocisku o potencjale międzykontynentalnym Taepo Dong 1) przyczyniły się do uchwalenia w 1999 r. ustawy o narodowej obronie antyrakietowej (*National Missile Defense Act* of 1999). Zgodnie z jej założeniem finansowanie operacji mających na celu utrzymywanie oraz ulepszanie skutecznego, wielopoziomowego systemu obrony przeciwrakietowej bazuje na corocznym budżecie oraz środkach przeznaczanych na Krajową Obronę Przeciwrakietową. Wystąpienie Stanów Zjednoczonych z traktatu antyrakietowego (ABM) w 2002 r. sprawiło, że możliwe stało się wdrożenie programów opracowujących i testujących nowe technologie antybalistyczne. W tym samym czasie doszło do przemianowania BMDO na MDA – agencję funkcjonującą po dziś dzień.

Kadrę MDA stanowią urzędnicy służby cywilnej zatrudnieni przez amerykański rząd, → ż o ł n i e r z e [t. 4] oraz podwykonawcy działający w różnych obszarach Stanów Zjednoczonych. Podczas działań podejmowanych przez agencję i mających na celu opracowanie, testowanie i wdrażanie zintegrowanego systemu obrony przeciwrakietowej, MDA współpracuje z dowództwami bojowymi (np. z Dowództwem Pacyfiku czy z Dowództwem Północnym), korzystającymi z takiego systemu, aby zapewnienić pełną ochronę terytorium Stanów Zjednoczonych, narodowych sił zbrojnych oraz sojuszników przed wrogimi atakami rakietowymi. MDA w swoich działaniach podejmuje inicjatywy mające na celu rozwój współpracy międzynarodowej, umożli-

wiającej wsparcie wzajemnych interesów → b e z p i e c z e ń s t w a [t. 1] w zakresie obrony przeciwrakietowej.

Do najważniejszych celów strategicznych realizowanych przez MDA należą:

- rozwój i wdrażanie zintegrowanego systemu obrony przeciwrakietowej w celu obrony kraju i regionu;
- prowadzenie testów umożliwiających weryfikację skuteczności obrony przeciwrakietowej;
- wsparcie żołnierzy USA oraz ich sojuszników;
- współpraca z krajowymi uniwersytetami oraz przedsiębiorcami, ukierunkowana na wdrożenie innowacyjnych rozwiązań umożliwiających dalszy rozwój zintegrowanego systemu obrony przeciwrakietowej;
- wdrażanie założeń → s t r a t e g i i b e z p i e c z e ń s t w a n a r o d o w e g o [t. 4] poprzez współpracę międzynarodową w zakresie obrony przeciwrakietowej.

Intensyfikacja współpracy MDA z dowódcami sił zbrojnych ma na celu między innymi opracowanie wydajnej technologii warstwowego Systemu Obrony Przeciwbalistycznej (ang. *Ballistic Missile Defense System* – BMDS), która zgodnie z założeniami sprosta wyzwaniom stwarzanym przez stale zmieniające się zagrożenia. Technologia warstwowego Systemu BMDS, wdrożona przez MDA, składa się ze złożonych elementów bazowych oraz wspomagających. Na te drugie składają się:

- **program testowy,** pozwalający na uzyskanie danych określających skuteczność systemu obrony przeciwrakietowej oraz jego poszczególnych elementów. Testy naziemne oraz przeprowadzone w powietrzu określają możliwości systemu oraz dostarczają danych pozwalających na kompleksowe modelowanie i przewidywanie działań umożliwiających zwiększenie wydajności technologii obrony przeciwrakietowej;
- **Agencja ds. Celów i Środków Zaradczych**, której celem jest nadzorowanie, projektowanie, rozwój oraz produkcja i integracja rozwiązań dostosowanych do specyfiki zagrożenia rakietowego mających wejść w skład systemu obrony przeciwrakietowej. W celu usprawnienia rozwoju systemu agencja przeprowadza analizę zarówno testów wstępnych, jak również wyników uzyskanych po przeprowadzonych testach;
- **zaawansowana technologia**, pozwalająca na opracowanie nowych koncepcji systemu i kluczowych jego komponentów, umożliwiających dostosowanie systemu obrony przeciwrakietowej do dynamicznie zmieniających się zagrożeń;
- **Centrum Integracji i Operacji**, wspierające badania i rozwój, przeprowadzające testy oraz weryfikacje, a także organizujące szkolenia w zakresie obrony przeciwrakietowej.

Technologia obrony przeciwrakietowej opracowywana, testowana oraz wdrażana przez Stany Zjednoczone ma na celu przeciwdziałanie atakom z wykorzystaniem pocisków balistycznych o różnym zasięgu – krótkim, średnim i dalekim. Ponieważ po-

ciski balistyczne różnią się prędkością lotu, zasięgiem czy specyfiką działania, system obrony przed rakietami balistycznymi musi stanowić zintegrowaną, wielopłaszczyznową architekturę umożliwiającą niszczenie pocisków oraz ich głowic, zanim dotrą one do celu. Integracja tak wielu elementów umożliwia wydajną, wielopoziomową obronę przed wrogimi pociskami we wszystkich etapach lotu. Trajektorie pocisków balistycznych są zwykle podzielone na 3 fazy lotu: start, kurs pośredni oraz przygotowanie do detonacji. Każda z nich wymusza zastosowanie innych technik obronnych:

- **Faza startu** – obrona w fazie startu pozwala unieszkodliwić niemal wszystkie pociski balistyczne, również międzykontynentalne rakiety balistyczne (ICBM), tyle że to najtrudniejsza faza, w której można zaatakować pocisk.
- **Kurs pośredni** – obrona w fazie odpalonego pocisku lecącego w kierunku celu. Zestrzelenie pocisku spowoduje, że wszelkie szczątki pozostałe po przechwyceniu spłoną w momencie wejścia w kontakt z atmosferą. Element naziemny systemu GMD (ang. *Ground-Based Midcourse Defense*), mający chronić terytorium Stanów Zjednoczonych przed atakami zewnętrznymi, jest dostosowany wyłącznie do zwalczania rakiet balistycznych krótkiego i dalekiego zasięgu (obecnie wdrażany na Alasce i w Kalifornii). Morskim odpowiednikiem przeznaczonym do obrony przed rakietami balistycznymi krótkiego i średniego zasięgu jest komponent obrony przeciwrakietowej AEGIS BMD (ang. *Balistic Missile Defense*), który wykorzystuje istniejące krążowniki i niszczyciele uzbrojone w pociski przechwytujące.
- **Przygotowanie do detonacji** – faza występująca w ostatnim momencie, kiedy możliwe jest przechwycenie pocisku, zanim dotrze on do celu. Margines błędu okazuje się zatem niewielki. Elementy przechwytujące w omawianej fazie obejmują Terminal High Altitude Area Defense (THAAD), który znajduje się obecnie na wyposażeniu armii amerykańskiej, Aegis BMD do obrony morskiej z wykorzystaniem pocisków SM-2 Block IV oraz PATRIOT Advanced Capability-3 (PAC-3).

Architektura systemu obejmuje: czujniki połączone w sieć (w tym – czujniki zlokalizowane na orbicie), radary naziemne i morskie (wykrywające i śledzące cele), naziemne i morskie pociski przechwytujące do niszczenia pocisków balistycznych lub wyposażone w głowicę odłamkowo-burzącą, a także sieć dowodzenia, kontroli i łączności zapewniającą dowódcom komunikację między czujnikami a pociskami przechwytującymi. Elementy obrony przeciwrakietowej obsługuje m.in. personel wojskowy należący do Dowództwa Strategicznego Stanów Zjednoczonych, do Dowództwa Północnego, do Dowództwa Pacyfiku, do Sił Zbrojnych Stanów Zjednoczonych stacjonujących w Japonii oraz do Dowództwa Europejskiego. USA współpracują w zakresie rozwoju programu obrony przeciwrakietowej z wieloma sojusznikami, m.in. z Wielką Brytanią, Japonią, Australią, Izraelem, Danią, Niemcami, Holandią, Czechami, Rumunią, Włochami oraz Polską. W skład BMDS, pozostającego pod nadzorem MDA,

wchodzi system uzbrojenia Aegis Ashore. Instalacja 4 elementów radaru SPY-1D(V) oraz podświetlacza celu (wchodzi w skład systemu kontroli ognia) miała miejsce w 2021 r. na terenie amerykańskiej bazy w Redzikowie.

W ramach II i III etapu programu EPAA (ang. *European Phased Adaptive Approach*), poza wspomnianą bazą w Redzikowie, łącznie (czyli z uwzględnieniem rumuńskiej bazy w Devesulu) mają zostać rozmieszczone 24 rakiety przechwytujące typu SM-3 IB i SM-3 IIA, zwalczające cele o zasięgach od krótkiego do pośredniego. Głównym wyposażeniem bazy Aegis Ashore w bazie w Devesulu jest radar SPY-1/D wraz z elementami systemu kierowania i dowodzenia obroną powietrzną Aegis, a także – wyrzutnie pocisków przeciwrakietowych Standard SM-3 Block IB. Podobne elementy wejdą w skład bazy w Redzikowie, gdzie rozlokowane zostaną nowsze pociski typu Standard SM-3 Block IIA. W sierpniu 2021 r., kiedy kierownictwo z ramienia MDA nadzorowało prace inżynieryjne przy integracji systemu uzbrojenia instalacji bazy Redzikowo, Jon Hill, dyrektor MDA, w odniesieniu do stacjonarnych instalacji w Polsce i Rumunii podkreślił potencjał, jaki może w przyszłości przynieść mobilna wersja systemu obrony przeciwrakietowej AAMDS (ang. *Aegis Ashore Missile Defense System*). Uruchomienie obu baz przełoży się na wdrożenie systemu mającego na celu ochronę terytorium europejskich członków → NAT O [t. 3] przed ograniczonym atakiem pociskami balistycznymi spoza obszaru euroatlantyckiego, np. z Bliskiego Wschodu.

Artur Jach-Chrząszcz

Defence 24, *Rumuńska baza przeciwrakietowa NATO zmodernizowana*, https:// www.defence24.pl/rumunska-baza-przeciwrakietowa-nato-zmodernizowana (dostęp 28.10.2021); Defence 24, *System Aegis instalowany w Redzikowie*, https://www. defence24.pl/system-aegis-instalowany-w-redzikowie (dostęp 28.10.2021); A.J. Futter, *The Evolution of the US Ballistic Missile Defence Debate 1989–2010*, https:// etheses.bham.ac.uk/id/eprint/2956/2/Futter_11_PhD.pdf (dostęp 28.10.2021); M. Kowalski, *Obrona przeciwrakietowa Stanów Zjednoczonych*, https://pulaski. pl/wp-content/uploads/2015/02/Pulaski_Policy_Papers_Nr_19_16.pdf (dostęp 28.10.2021); G.N. Lewis, L. Gronlund, *Debunking the Missile Defense Agency's 'Endgame Success' Argument*, https://www.armscontrol.org/act/2002-12/debunking-missile-defense-agency's-endgame-success-argument (dostęp 28.10.2021); Missile Defense Agency, https:// www.mda.mil (dostęp 28.10.2021); Missile Defense Agency, *FY 2004 Annual Financial Statements*, https://comptroller.defense.gov/ Portals/45/documents/cfs/fy2004/FY_2004_MDA_Financial_Report.pdf (dostęp 28.10.2021); R. Muczyński, *MDA optuje za mobilną obroną przeciwrakietową AAMDS*, https://milmag.pl/mda-optuje-za-mobilna-obrona-przeciwrakietowa-aamds/ (dostęp 28.10.2021); L. Welch, D. Briggs, R. Bleach, G. Canavan, *Study on the Mission, Roles, and Structure of the Missile Defense Agency (MDA)*, https:// apps.dtic.mil/sti/pdfs/ADA486276.pdf (dostęp 28.10.2021).

AGENCJA PRASOWA (informacyjna) – wyspecjalizowane przedsiębiorstwo informacyjne (organizacja, firma, centrum) obsługujące media: gazety, czasopisma oraz radiowe i telewizyjne nadawcy. Główną funkcją agencji prasowej jest dostarczanie operacyjnych → i n f o r m a c j i [t. 2] o bieżących wydarzeniach politycznych,

gospodarczych, społecznych i kulturalnych redakcjom gazet, czasopism, telewizji, audycjom radiowym, portalom internetowym, a także innym instytucjom, organizacjom i osobom, które są subskrybentami jej produktów. Agencja koncentruje się na zbieraniu wiadomości. Informacje są oferowane jako gotowe wiadomości w postaci tekstu, materiałów audio lub wideo oraz w formie obrazów dla środków masowego przekazu. Obecnie istnieje ponad 180 agencji informacyjnych na całym świecie. Większość z nich zaopatruje jedynie rynek prasowy we własnym kraju, natomiast 3 globalne agencje informacyjne – Agence France Presse (AFP), Associated Press (AP) i Reuters – mają biura w większości krajów na świecie i obejmują wszystkie obszary informacji. Aby osiągnąć tak szeroką akceptację, agencje unikają jawnej stronniczości, wydawania osądów i unikają wątpliwości i dwuznaczności. Choć ich założyciele nie używali tego słowa, obiektywizm jest filozoficzną podstawą ich przedsięwzięć – ewentualnie, w przypadku braku takiej zasady, powszechnie akceptowana neutralność. Syndykaty prasowe zazwyczaj sprzedają swoje materiały tylko jednemu klientowi w każdym państwie, podczas gdy agencje prasowe dystrybuują artykuły prasowe do wszystkich zainteresowanych stron.

Tradycyjne agencje prasowe – zdaniem R. Piaseckiej-Strzelec – w 1. poł. lat 90. XX w. zaczęły przenosić swoją działalność do → c y b e r p r z e s t r z e n i, a określenie „agencje informacyjne" ewoluowało do sformułowania „internetowe agencje informacyjne".

Funkcjonujące obecnie pojęcie agencji informacyjnych jest wynikiem transformacji z przełomu XIX i XX w. w obrębie agencji prasowych korzystających z drukowanych nośników rozpowszechniania informacji. W tradycyjnym rozumieniu agencje informacyjne traktowane były jako jeden z rodzajów agencji prasowych, który w XX w. sprowadzano wyłącznie do rozpowszechniania wiadomości. Współcześnie w literaturze polskiej i zagranicznej pojęcia „agencja prasowa" oraz „agencja informacyjna" stosuje się często synonimicznie (ang. odpowiedniki: *press agency*, *news agency* czy *information agency*). Stosuje się także zapis „agencje prasowo-informacyjne", podkreślając równorzędność znaczeniową pojęć składowych. Agencja prasowa przez R. Borkowskiego rozumiana jest jako „instytucja, która gromadzi, opracowuje i rozpowszechnia informacje dla potrzeb środków masowego przekazu". Podobną definicję proponuje M. Hamer. Zaznacza on, że zgromadzone informacje rozpowszechniane są w różnych mediach w skali lokalnej, regionalnej, krajowej lub międzynarodowej. Agencje prasowe w swej pierwotnej postaci gromadziły i rozpowszechniały informacje pochodzące z kraju i spoza jego granic. Początkowo agencje te korzystały ze środków masowego przekazu, do których wówczas zaliczano głównie prasę, radio i telewizję, a później także techniki druku, fotografię oraz gazetę elektroniczną. Borkowski określił agencję prasową ogniwem, które pośredniczy „pomiędzy rynkiem informacji obejmującym całą kulę ziemską a rynkiem prasy, który przy dzisiejszym, można już powiedzieć powszechnym, zasięgu środków masowego przekazu obejmuje

praktycznie całą ludzkość". Terminem „agencja prasowa" określano wówczas instytucję, która pozyskiwała informacje oraz przekazywała je redakcjom prasowym na podstawie zawieranych z nimi umów. To właśnie te dwie cechy – gromadzenie oraz rozpowszechnianie informacji – stanowią istotę agencji prasowej i umożliwiają odróżnienie jej od innych instytucji.

Przedmiotem działalności tak rozumianych agencji prasowych są informacje utożsamiane z przekazem słownym, dźwiękowym lub obrazowym. Są one pozyskiwane, a następnie, po ich opracowaniu, tj. selekcji i uzupełnieniu, przekazywane innym instytucjom, upowszechniającym je społeczeństwu. Stąd też pojawiły się określenia informacji agencyjnej wejściowej oraz informacji agencyjnej wyjściowej. Agencja prasowa w tym kontekście odgrywa rolę pośrednika w obrocie informacją.

Agencje prasowe rozwinęły się w krajach kapitalistycznych na przełomie XIX i XX w. Najstarszą agencję prasową założył – zdaniem E. Rudzińskiego – C.-L. Havas w 1835 r. Po 1860 r. oferowała ona swoje informacje 12 gazetom francuskim. Kolejną agencję informacyjną otworzył były pracownik agencji Havasa – J. Reuter w 1851 r. Nawiązał on współpracę z „The Times" oraz „Morning Advertiser" i przesyłał informacje z Paryża do Londynu. Trzecią agencją, konkurującą z Havasem i Reuterem, było niemieckie Biuro Wolffa (Wolff Telegraphisches Bureau), istniejące od 1849 r. Agencje te określano w literaturze jako tzw. wielką trójkę. Konkurowała z nimi amerykańska AP, powstała w 1848 r. Ten układ utrzymał się do 1914 r. Dopiero I wojna światowa przerwała współpracę „wielkiej trójki", powodując jednocześnie wzrost popytu na informacje pochodzące z agencji prasowych USA. Porozumienie o współpracy pomiędzy Havasem i Reuterem zostało odnowione w 1919 r., a rok później do współpracy dołączył niemiecki Wolff.

Dużą rewolucję w funkcjonowaniu agencji prasowych wywołały zmiany w technice przekazywania informacji. Pierwsza wiadomość przesłana w 1919 r. za pomocą radiotelegrafu była słyszana na całym świecie. Na jej przekazanie wystarczyły sekundy. Poprzednie telegramy, przesyłane za pośrednictwem kabla, po kilku minutach docierały zaledwie do jednego adresata. W starciu między telegrafem a radiem zwycięzcą okazało się radio. W latach 30. XX w., gdy do władzy doszedł Hitler, przekaz informacji zaczęto poddawać kontroli państwowej.

Agencje prasowe początkowo (w XIX w.) przekazywały informacje za pośrednictwem gołębi pocztowych, następnie telegrafem świetlnym, później elektrycznym Morse'a. Wraz z upływem czasu ulegał skróceniu okres pomiędzy otrzymaniem przez agencję informacji a jej przekazaniem innym odbiorcom. Źródłem informacji dla agencji prasowych były: prasa krajowa i zagraniczna, serwisy zagranicznych agencji prasowych, radio i telewizja, komunikaty rządowe, placówki zagraniczne, reporterzy i korespondenci czy oddziały krajowe agencji.

Jedną z najstarszych w kraju była Polska Agencja Prasowa Polpress, utworzona 10 marca 1944 r. w Moskwie przez Związek Patriotów Polskich. 18 października

1945 r. w jej miejsce powołano dekretem Rady Ministrów Polską Agencję Prasową (PAP) z siedzibą w Warszawie.

Wśród typów agencji prasowych, wyodrębnianych w latach 70. XX w., Borkowski wskazał agencje telegraficzne (zakładane w XIX i na początku XX w., np. Polska Agencja Telegraficzna – PAT – która powstała w 1918 r.), agencje prasowe (np. Polska Agencja Prasowa – PAP, założona w 1944 r.) oraz agencje informacyjne (np. Allgemeiner Deutscher Nachrichtendienst – ADN). W tradycyjnym ujęciu agencje informacyjne koncentrowały się na rozpowszechnianiu wyłącznie informacji prostych. Rozwój agencji prasowych spowodował ich dalszą specyfikację na agencje informacyjne, publicystyczne, fotograficzne oraz reklamowe (ogłoszeniowe). Informacyjne agencje prasowe pozyskują wiadomości, dokonują ich selekcji i uzupełnienia, a następnie rozpowszechniają je w postaci informacji prostej lub rozszerzonej. Agencje te ze względu na swój zasięg dzielono na agencje krajowe (np. PAP), regionalne oraz światowe (np. Reuter w Wielkiej Brytanii czy AP w USA). Agencje publicystyczne pozyskują, opracowują i rozpowszechniają „korespondencje zagraniczne i krajowe oraz artykuły problemowe z różnych dziedzin życia kraju, reportaże, komentarze, felietony oraz opracowania źródłowe, dokumentacyjne – słowne i obrazowe". W 2. poł. XX w. pełniły także funkcję propagandową (zob. → p r o p a g a n d a [t. 3]), informując o osiągnięciach kraju. W tym okresie dokonał się również podział agencji publicystycznych na agencje: ekonomiczne, finansowe, sportowe, turystyczne, artystyczne (ze względu na tematykę materiałów prasowych), oraz na: np. robotnicze, katolickie czy narodowościowe (ze względu na społeczność, do której kierowano materiał prasowy). Fotograficzna agencja prasowa gromadziła i utrwalała obrazy z życia kraju, które wykorzystywane były przez prasę, kroniki filmowe oraz telewizję. Działy fotografii były także elementem składowym krajowych agencji prasowych (pierwsze takie działy pojawiły się na początku XX w.), ale agencje fotograficzne stanowiły też autonomiczny rodzaj agencji prasowych. Reklamowe agencje prasowe od początku swego funkcjonowania gromadziły ogłoszenia i informacje reklamowe, dokonywały ich opracowania, by uczynić je bardziej atrakcyjnymi dla odbiorcy, oraz udostępniały je dla środków masowego przekazu.

Borkowski i Rudziński dokonali również podziału agencji pod względem ich statusu na oficjalne, półoficjalne i nieoficjalne agencje rządowe, a także agencje prywatne. Oficjalne reprezentowały stanowisko rządu, podczas gdy agencje półoficjalne i nieoficjalne pozostawały pod jego silnym wpływem. To rząd ustalał ich metody działania, skład personalny oraz rozdysponowywał środki finansowe. Zdaniem Borkowskiego agencje te pełniły szereg funkcji, w tym: informacyjną (wtedy gdy zajmowały się pozyskiwaniem i dystrybucją informacji, umożliwiając odbiorcom odpowiedź na pytania: co? gdzie? kiedy? jak? dlaczego?) oraz polityczną (wtedy gdy prezentowały informacje dostosowane „do potrzeb i tendencji ideowo-politycznych środowiska, społeczeństwa, narodu", służąc tym samym różnym grupom społecznym). W tym kontekście

pojawiały się stwierdzenia, że przez wzgląd na realizowane funkcje agencje prasowe „uzależniają od siebie inne środki masowego przekazu". Agencje prywatne – w ujęciu Rudzińskiego – dzieliły się na kilka grup: agencje ogólnoinformacyjne (np. Katolicka Agencja Prasowa, Polska Agencja Agrarna czy Żydowska Agencja Telegraficzna), agencje lokalne (skoncentrowane wokół problematyki charakterystycznej dla danego regionu), agencje zajmujące się problematyką specjalistyczną (dotyczącą np. kwestii gospodarczych, samorządowych, sportowych, rolniczych czy problemów mniejszości narodowych) oraz biuletyny, które publikowały rozmaite instytucje i organizacje naukowe, gospodarcze, polityczne czy społeczne.

Współczesne elektroniczne agencje informacyjne (e-agencje) to takie agencje, które – zdaniem Piaseckiej-Strzelec – wykorzystują „internet do dystrybucji swoich produktów i usług, a także – jako sposób na dotarcie do nowych odbiorców". Agencje informacyjne stosują przekaz wykorzystujący elementy multimedialne, np. dźwięk, obraz, tekst. Współczesne agencje informacyjne to w większości agencje interaktywne, które pozwalają odbiorcy angażować się w odczytywanie i/lub tworzenie materiałów. To zasadnicza różnica, która pozwala odróżnić je od powstałych na przełomie XIX i XX w. agencji prasowych. Do agencji funkcjonujących w cyberprzestrzeni dołączyły jedne z najstarszych polskich agencji. PAP zaczęła wykorzystywać internet w 1994 r., a w 1997 r. zaczęła publikować „Dziennik Internetowy PAP". Był on pierwszą internetową gazetą codzienną w Polsce, która nie posiadała swojego papierowego odpowiednika. Obecnie PAP wykorzystuje łączność satelitarną, internet, kanał RSS i obsługuje portal Interia.pl czy radio RMF.fm. Ogólnopolskie i regionalne media korzystają z Codziennego Serwisu Informacyjnego PAP, który uzupełnia Codzienny Serwis Fotograficzny. Szeroka oferta multimedialna PAP obejmuje także infogalerie, materiały filmowe (np. wywiady), aplikacje przeznaczone dla portali internetowych, telewizji oraz na smartfony. PAP prowadzi również portale internetowe, np. Samorząd.pap.pl, Biznes.pap.pl, NaukaWPolsce.pl czy Dzieje.pl.

Ewelina Włodarczyk

R. Borkowski, *Informacyjne agencje prasowe*, Ośrodek Badań Prasoznawczych RSW „Prasa – książka – ruch", Kraków 1976; T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*, Wydawnictwo Fundacji Postępu Telekomunikacji, Kraków 1999; M. Hamer, *Trading on Trust: News Agencies, Local Journalism and Local Media*, [w:] *Local Journalism and Local Media. Making the Local News*, B. Franklin (ed.), Routledge, London–New York 2006; R. Piasecka-Strzelec, *Metody i techniki upowszechniania informacji przez współczesne polskie agencje informacyjne*, „Studia Medioznawcze" 2014, nr 3 (58); taż, *Przekształcenia i zmiany w agencjach informacyjnych w Polsce*, „Studia Medioznawcze" 2016, nr 3 (66); E. Rudziński, *Informacyjne agencje prasowe w Polsce 1926–1936*, Państwowe Wydawnictwo Naukowe, Warszawa 1979; E. Włodarczyk, *Agencje prasowe,* [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019.

AGENCJA UNII EUROPEJSKIEJ DS. CYBERBEZPIECZEŃSTWA (The European Union Agency for Cybersecurity, ENISA) – centrum eksperckie w dziedzinie bezpieczeństwa cyfrowego. Jest organem Unii Europejskiej i ma osobowość prawną. Siedziba Agencji znajduje się w Atenach, ale Agencja ma ona dodatkowe biura w Heraklionie i Brukseli.

Agencja została utworzona 15 marca 2004 r. na mocy Rozporządzenia (WE) nr 460/2004 Parlamentu Europejskiego i Rady z dnia 10 marca 2004 r. ustanawiającego Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (European Network and Information Security Agency). Powołano ją, aby przyczynić się do zapewnienia wysokiego poziomu bezpieczeństwa sieci i informacji w Unii Europejskiej oraz rozwijania kultury bezpieczeństwa cybernetycznego na rzecz obywateli, konsumentów, przedsiębiorstw oraz administracji publicznej.

Okres działania Agencji modyfikowano kilkakrotnie – początkowo przedłużono jej mandat do marca 2012 r., potem do 13 września 2013 r., a następnie do 19 czerwca 2020 r. W 2019 r. zmieniono nazwę na Agencja Unii Europejskiej ds. Cyberbezpieczeństwa, pozostawiając jej dotychczasowy akronim.

Podstawowym zadaniem Agencji jest wspieranie spójnego wprowadzania odpowiednich ram prawnych, zwłaszcza skutecznego wdrożenia Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii i innych stosownych instrumentów prawnych dotyczących cyberbezpieczeństwa, co ma kluczowe znaczenie dla zwiększenia cyberodporności.

Agencja aktywnie wspiera państwa członkowskie, instytucje, organy i jednostki organizacyjne Unii, a także innych wspólnotowych interesariuszy w poprawie → c y b e r b e z p i e c z e ń s t w a [t. 1]. Jest organem doradczym i ośrodkiem wiedzy fachowej z zakresu bezpieczeństwa cyfrowego. Pomaga w podejmowaniu decyzji, reagowaniu, szczególnie zaś zapobieganiu problemom związanym z bezpieczeństwem sieci i informacji. Opracowuje i wdraża unijną politykę w tej dziedzinie. Buduje zaufanie do produktów, usług i procesów cyfrowych dzięki projektowaniu systemów certyfikacji cyberbezpieczeństwa.

Agencja współpracuje z organizacjami i przedsiębiorstwami, aby zwiększać zaufanie do gospodarki cyfrowej i odporność unijnej infrastruktury, a co za tym idzie – zapewnić obywatelom UE cyberbezpieczeństwo. W tym celu przekazuje wiedzę, szkoli pracowników, buduje struktury i podnosi świadomość na temat bezpieczeństwa sieci i informacji.

Agencja jest zobligowana do wspierania unijnych wysiłków na rzecz współpracy w obszarze cyberbezpieczeństwa z państwami trzecimi, a także organizacjami międzynarodowymi (np. → NAT O [t. 3], → OB W E [t. 5], OECD). Głównym celem tego działania jest wymiana dobrych praktyk oraz wsparcie eksperckie.

Międzynarodowa strategia Agencji, uchwalona w listopadzie 2021 r., wyznacza 7 celów:

- wzmocnienie i zaangażowanie społeczności w całym ekosystemie bezpieczeństwa;
- uczynienie cyberbezpieczeństwa integralną częścią polityki UE;
- efektywną współpracę na wypadek wystąpienia incydentu na masową skalę;
- rozwój kompetencji z zakresu cyberbezpieczeństwa w UE;
- wysoki poziom zaufania do bezpiecznych rozwiązań cyfrowych;
- prognozowanie wyzwań i zagrożeń związanych z cyberbezpieczeństwem;
- zarządzanie wiedzą na temat wydajnego i skutecznego cyberbezpieczeństwa.

Głównymi kierunkami działalności Agencji są:

- udzielanie konsultacji i pomocy Komisji Europejskiej i państwom członkowskim w dziedzinie bezpieczeństwa informacji;
- gromadzenie i analiza danych dotyczących incydentów bezpieczeństwa w Europie i nowych zagrożeń;
- opracowanie metod oceny ryzyka i → z a r z ą d z a n i a r y z y k i e m w celu zwiększenia zdolności UE do reagowania na zagrożenia → b e z p i e c z e ń s t w a i n f o r m a c y j n e g o [t. 1];
- przeprowadzenie ogólnoeuropejskich szkoleń;
- wsparcie współpracy między zespołami powołanymi do reagowania na zdarzenia naruszające → b e z p i e c z e ń s t w o w s i e c i [t. 1] (CERT) w państwach członkowskich;
- podnoszenie wiedzy i współpracy między różnymi podmiotami w dziedzinie bezpieczeństwa informacji.

Agencja pomaga również Komisji Europejskiej we wstępnych pracach technicznych mających na celu aktualizację i ulepszenie europejskiego ustawodawstwa dotyczącego bezpieczeństwa sieci i informacji. W swoich działaniach Agencja opiera się na rocznych planach pracy / programach, które zawierają listę kluczowych priorytetów i celów orazplanowanych działań.

Strukturę administracyjną i kierowniczą Agencji tworzą:

- Zarząd,
- Rada Wykonawcza,
- dyrektor wykonawczy,
- grupa doradcza,
- Sieć Krajowych Urzędników Łącznikowych.

Do Zarządu każde z państw członkowskich powołuje po 1 członku, Komisja Europejska wyznacza 2 osoby. Prawo głosu przysługuje wszystkimczłonkom Zarządu. Ich kadencja, a także kadencja zastępców, trwa 4 latai jest ona odnawialna.

Zarząd wspierany jest przez Radę Wykonawczą. W jej skład wchodzi5 osób powołanych spośród członków Zarządu na czteroletnią kadencję. Rada:

- przygotowuje decyzje do przyjęcia przez Zarząd;
- wraz z Zarządem zapewnia odpowiednie działania następcze w związku z ustaleniami i zaleceniami wynikającymi z dochodzeń przeprowadzanych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (European Anti-Fraud Office, OLAF) oraz z różnych sprawozdań z kontroli i ocen, zarówno wewnętrznych, jak i zewnętrznych;
- doradza dyrektorowi wykonawczemu.

Agencją kieruje dyrektor wykonawczy, który zachowuje niezależność podczas wypełniania swoich obowiązków. Odpowiada on przed Zarządem. Od 2019 r. funkcję tę sprawuje Juhan Lepassaar.

Zarząd, działając na wniosek dyrektora wykonawczego, ustanawia grupę doradczą, która składa się z uznanych ekspertów z branży ICT, przedstawicieli małych i średnich przedsiębiorstw, grup konsumenckich, dostawców sieci lub usług łączności elektronicznej dostępnych publicznie, operatorów usług kluczowych, ekspertów akademickich w dziedzinie cyberbezpieczeństwa, a także nominowanych przedstawicieli z europejskich organizacji normalizacyjnych, organów ścigania i organów nadzorujących ochronę danych. Zarząd stara się zapewnić odpowiednią równowagę płci i geograficzną, a także równowagę między poszczególnymi grupami interesariuszy.

Zarząd powołuje również Sieć Krajowych Urzędników Łącznikowych, w jej skład wchodzą przedstawiciele wszystkich państw członkowskich (krajowi urzędnicy łącznikowi). Posiedzenia Sieci mogą odbywać się w różnych konfiguracjach eksperckich. Ma ona szczególnie ułatwiać wymianę informacji między Agencją a państwami członkowskimi i wspierać Agencję w promowaniu jej działalności, ustaleń i zaleceń wśród odpowiednich interesariuszy w całej Unii Europejskiej.

Agencja ściśle współpracuje z → E u r o p o l e m [t. 2] i Europejskim Centrum Cyberprzestępczości (European Cyber Crime Centre), a także wspiera inne instytucje UE, w tym Agencję Unii Europejskiej ds. Szkolenia w Dziedzinie Ścigania (European Union Agency for Law Enforcement Training, CEPOL), Organ Europejskich Regulatorów Łączności Elektronicznej (Body of the European Regulators of Electronic Communications, BEREC), Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice, eu-LISA), Agencję Unii Europejskiej ds. Bezpieczeństwa Lotniczego (European Union Aviation Safety Agency, EASA).

Agencja zarządza ogólnoeuropejskim programem Cyber Europe. Jest to seria ćwiczeń związanych z → c y b e r p r z e s t ę p c z o ś c i ą [t. 1] i → z a r z ą d z a n i e m k r y z y s o w y m [t. 4] na szczeblu UE dla sektora publicznego i prywatnego państw członkowskich. Są to symulacje incydentów, których nasilenie grozi cyberkryzysami. Ćwiczenia realizują scenariusze prawdziwych wydarzeń opracowanych przez

europejskich ekspertów w dziedzinie bezpieczeństwa cyfrowego. Zapewniają one uczestnikom doświadczenia edukacyjne i umożliwiają analizę zaawansowanych technicznych środków bezpieczeństwa cybernetycznego oraz rozwiązywanie problemów związanych z → s y t u a c j a m i k r y z y s o w y m i [t. 4].

Agencja rokrocznie organizuje Europejski Miesiąc Cyberbezpieczeństwa (European Cyber Security Month, ECSM), czyli cykliczną kampanię, której celem jest podnoszenie świadomości na temat bezpieczeństwa w świecie cyfrowym oraz dzielenie się dobrymi praktykami dotyczącymi tego, jak unikać → c y b e r z a g r o ż e ń [t. 1] i radzić sobie z nimi. W październiku każdego roku państwa UE jednoczą się pod hasłem „Cyberbezpieczeństwo to wspólna odpowiedzialność" i razem występują przeciwko zagrożeniom cybernetycznym.

Agnieszka Warchoł

About ENISA, https://www.enisa.europa.eu/about-enisa (dostęp 25.04.2019); *Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA*), https://european-union.europa. eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-andbodies/enisa_pl (dostęp 10.05.2023); J. Balcewicz, *Międzynarodowa Strategia ENISA*, 2.03.2022, https://cyberpolicy.nask.pl/miedzynarodowa-strategia-enisa/ (dostęp 10.05.2023); *ENISA*, https://www.enisa.europa.eu/ (dostęp 10.05.2023); Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz.Urz. UE L 194 z 19.07.2016; Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r., ustanawiającą Europejski kodeks łączności elektronicznej, Dz.Urz. UE L 321 z 17.12.2018; ENISA, Decision No MB/2023/02/ of the Management Board of the European Union Agency for Cybersecurity (ENISA) setting up an Advisory Group for the period 2023–2025, https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/management-board-decisions/mb-decision-2023-02setting-up-enisa-advisory-group-for-period-2023-2025.pdf (dostęp 30.06.2023); *ENISA Programming Document 2018–2020*, 2017, https://www.enisa.europa.eu/ publications/corporate-documents/enisa-programming-document-2018-2020 (dostęp 25.04.2019); *ENISA Strategy*, https://www.enisa.europa.eu/publications/ corporate/enisastrategy (dostęp 25.04.2019); *European Union Agency for Network and Information Security (ENISA)*, https://www.diplomatie.gouv.fr/IMG/pdf/aesri_ directeur_executif_enisa_com-2018-20032_ad14_heraklion_cle0fe364.pdf (dostęp 25.04.2019); Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie), Dz.Urz. UE L 151 z 7.06.2019; Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 526/2013 w sprawie Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz uchylające rozporządzenie (WE) nr 460/2004, Dz.Urz. UE L 165 z 18.06.2013; Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 580/2011 z dnia 8 czerwca 2011 r. zmieniające rozporządzenie (WE) nr 460/2004 ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji w zakresie okresu jej działania, Dz.Urz. UE L 165 z 24.06.2011; Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1007/2008 z dnia 24 września 2008 r. zmieniające rozporządzenie (WE) nr 460/2004 ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji w zakresie okresujej działania, Dz.Urz. UE L 293 z 31.10.2008; Rozporządzenie (WE) nr 460/2004 Parlamentu Europejskiego i Rady z dnia 10 marca 2004 r. ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji, Dz.Urz. UE L 77 z 13.03.2004.

AGENCJA WYWIADU (AW) – to polska → służba specjalna [t. 4], właściwa w sprawach ochrony → bezpieczeństwa zewnętrznego państwa, realizująca zadania kontrwywiadowcze w obszarze → wywiadu [t. 4] cywilnego oraz strategicznego wywiadu wojskowego.

Została utworzona w 2002 r. w wyniku reformy cywilnych służb specjalnych. Po zlikwidowanym wówczas → Urzędzie Ochrony Państwa [t. 4] (UOP) przejęła zadania wywiadowcze, a od Wojskowych Służb Informacyjnych (WSI), które odpowiadały w tym czasie za wywiad i → kontrwywiad [t. 2], dodatkowo zadania z zakresu strategicznego wywiadu wojskowego, stając się tym samym narodową agencją wywiadu strategicznego.

Podstawą prawną jej działania jest Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, która w art. 6 wymienia następujące jej zadania:

- uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom → informacji [t. 2] mogących mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej oraz jej potencjału ekonomicznego i obronnego;
- rozpoznawanie → zagrożeń [t. 4] zewnętrznych godzących w bezpieczeństwo, obronność, niepodległość i nienaruszalność terytorium Rzeczypospolitej Polskiej i przeciwdziałanie im;
- ochrona zagranicznych przedstawicielstw Rzeczypospolitej Polskiej i ich pracowników przed działaniami obcych służb specjalnych i innymi działaniami mogącymi przynieść szkodę interesom Rzeczypospolitej Polskiej;
- zapewnienie ochrony kryptograficznej łączności z polskimi placówkami dyplomatycznymi i konsularnymi oraz poczty kurierskiej; rozpoznawanie międzynarodowego → terroryzmu [t. 4], ekstremizmu oraz międzynarodowych grup → przestępczości zorganizowanej [t. 3];
- rozpoznawanie międzynarodowego obrotu bronią, amunicją i materiałami wybuchowymi, środkami odurzającymi i substancjami psychotropowymi oraz towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także rozpoznawanie międzynarodowego obrotu bronią masowej zagłady i zagrożeń związanych z rozprzestrzenianiem tej broni oraz środków jej przenoszenia;
- rozpoznawanie i analizowanie zagrożeń występujących w rejonach napięć, → kryzysów [t. 2] i →konfliktów międzynarodowych [t. 2], mających wpływ na bezpieczeństwo państwa, oraz podejmowanie działań, których celem jest eliminowanie tych zagrożeń;
- rozpoznawanie zdarzeń o charakterze terrorystycznym wymierzonych przeciwko obywatelom lub mieniu Rzeczypospolitej Polskiej poza granicami państwa, z wyłączeniem zdarzeń o charakterze terrorystycznym wymierzonych przeciwko

personelowi bądź mieniu →Sił Zbrojnych Rzeczypospolitej Polskiej [t. 4], a także przeciwdziałanie i zapobieganie im;
- prowadzenie wywiadu elektronicznego;
- podejmowanie innych działań określonych w odrębnych ustawach i umowach międzynarodowych.

W zakresie realizowanych zadań funkcjonariusze AW wykonują → czynności operacyjno-rozpoznawcze oraz analityczno-informacyjne. Składają się one przede wszystkim na podstawową funkcję tej służby w systemie bezpieczeństwa państwa, czyli funkcję informacyjną, polegającą na pozyskiwaniu, gromadzeniu, analizie, opracowywaniu, a następnie przekazywaniu najważniejszym organom państwa informacji fundamentalnych dla jego bezpieczeństwa, niezakłóconego funkcjonowania i rozwoju. Funkcja ta ma również bardzo duże znaczenie w przedmiocie przeciwdziałania tzw. → zagrożeniom globalnym [t. 4] i wymiany informacji sojuszniczych w tym zakresie. Podkreśleniem podstawowej, informacyjnej roli AW było umiejscowienie jej w centrum rządowych → procesów informacyjnych [t. 3] w latach 2002–2004, gdy szef AW odpowiedzialny był za koordynację wymiany informacji o najważniejszych zagrożeniach dla bezpieczeństwa zewnętrznego oraz międzynarodowej pozycji Polski między organami administracji rządowej. Co do zasady, AW realizuje swoje zadania poza granicami RP, natomiast działalność na własnym terytorium musi mieć związek z działalnością prowadzoną poza granicami państwa, przy czym w zakresie realizacji czynności operacyjno-rozpoznawczych na terytorium RP korzystać musi z pośrednictwa → Agencji Bezpieczeństwa Wewnętrznego (ABW).

Agencja Wywiadu jest urzędem administracji rządowej obsługującym jej Szefa, który stoi na jej czele i kieruje jej pracą. Szef AW jest centralnym organem administracji rządowej i podlega bezpośrednio Prezesowi Rady Ministrów, a jego działalność kontrolowana jest przez Sejm RP. Działalność AW jest finansowana z budżetu państwa, natomiast w stosunku do działań niejawnych prowadzonych przez AW nie mają zastosowania przepisy o finansach publicznych, rachunkowości i zamówieniach publicznych. Działalność w tym zakresie finansowana jest ze specjalnie utworzonego w tym celu funduszu operacyjnego.

Organizacja wewnętrzna AW określana jest w jej statucie nadawanym w drodze zarządzeń przez Prezesa Rady Ministrów. Po ostatnich zmianach w tym przedmiocie z 2018 r. struktura organizacyjna AW przedstawia się następująco:
- Departament Operacyjny;
- Departament Informacyjny;
- Departament Techniczny;
- Biuro Bezpieczeństwa;
- Biuro Finansowo-Administracyjne;
- Biuro Kadr i Szkoleń;

- Biuro Prawne;
- Gabinet Szefa;
- Samodzielny Wydział ds. Zarządzania Kryzysowego.

Piotr Swoboda

M. Gałka, *Reformy służb specjalnych III RP*, „Poliarchia" 2013, nr 1; T. Kosobudzki, *Bezpieka w MSZ. Służby specjalne w polityce zagranicznej RP w latach 1989–1997*, Dom Wydawniczy Elipsa, Kielce–Warszawa 1998; D. Laskowski, *Prawne podstawy funkcjonowania służb specjalnych z perspektywy potrzeb obronnych państwa*, „Obronność. Zeszyty Naukowe" 2014, nr 2 (10); Ł. Roman, G. Winogrodzki, *Służby specjalne w systemie bezpieczeństwa państwa*, Wydawnictwo Wyższej Szkoły Gospodarki Euroregionalnej im. Alcide De Gasperi w Józefowie, Józefów 2016; *Służby specjalne w systemie bezpieczeństwa państwa. Przeszłość – teraźniejszość – przyszłość. Materiały i studia*, t. 1, A. Krzak, D. Gibas-Krzak (red.), Wojskowe Centrum Edukacji Obywatelskiej, Szczecin–Warszawa 2012; P. Swoboda, *Wywiad i kontrwywiad w Polsce w procesie przemian systemowych (1989–2007)*, Avalon, Kraków 2016; Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, t.j. Dz. U. 2020, poz. 27; Zarządzenie nr 106 Prezesa Rady Ministrów zmieniające zarządzenie w sprawie nadania statutu Agencji Wywiadu, M.P. 2018, poz. 660; A. Żebrowski, *Ewolucja polskich służb specjalnych. Wybrane obszary walki informacyjnej. (Wywiad i kontrwywiad w latach 1989–2003)*, Oficyna Wydawnicza Abrys, Kraków 2005.

AGENCJA ZAAWANSOWANYCH BADAŃ I ROZWOJU DEPARTAMENTU OBRONY USA (ang. Defense Advanced Research Projects Agency, DARPA) – rządowa agencja zajmująca się rozwojem zaawansowanych technologii, działająca w strukturach Departamentu Obrony USA, od dekad będąca źródłem innowacyjnych rozwiązań, które w przyszłości staną się powszechnym standardem. W latach 1958–1972 i 1993–1996 działała pod nazwą Advanced Research Projects Agency – ARPA (Agencja Zaawansowanych Projektów Badawczych). **Działalność DARPA jest częściowo tajna.** Lista aktywnych i archiwalnych projektów DARPA jest dostępna na stronie agencji. Uporządkowane → i n f o r m a c j e [t. 2] o niektórych kontraktach i projektach DARPA też są publicznie dostępne. Ze względu na szybkie tempo pracy agencji programy stale zaczynają się i kończą z uwzględnieniem potrzeb rządu USA.

Agencję utworzył 7 lutego 1958 r. prezydent Dwight D. Eisenhower w celu tworzenia i realizacji projektów badawczo-rozwojowych poszerzających granice technologii oraz nauki i mogących wykraczać daleko poza bezpośrednie wymagania wojskowe. Była to odpowiedź na sowieckie wystrzelenie pierwszego sztucznego satelity – Sputnika – w 1957 r. USA, świadome, że ZSRR rozwinął zdolność do szybkiego wykorzystania technologii wojskowej, zobowiązały się, że od tego czasu to one staną się inicjatorem, a nie – ofiarą strategicznych niespodzianek technologicznych. Początkowe finansowanie ARPA wyniosło 520 mln dolarów.

Nowa organizacja koordynowała prace badawcze nad przełomowymi obszarami niezbędnymi dla Departamentu Obrony USA. Aby zapobiec pojawianiu się takich

przykrych niespodzianek w przyszłości, a jednocześnie osiągnąć przewagę technologiczną USA na świecie, na polecenie prezydenta Eisenhowera powołano tę agencję.

Misją DARPA jest inwestowanie w technologie przełomowe dla → b e z p i e c z e ń s t w a n a r o d o w e g o [t. 1], przekształcanie rewolucyjnych koncepcji (a nawet – pozornych niemożliwości) w praktyczne możliwości. Naukowcy z DARPA futurystyczne wizje czynią realnymi – to ich zasługą stały się internet, mysz komputerowa, nawigacja GPS, asystent głosowy Siri w iPhone'ach. To oni tworzyli pierwsze autonomiczne auta czy egzoszkielety poprawiające siłę mięśni.

W latach 1958–1965 ARPA koncentrowała się na głównych kwestiach narodowych, takich jak przestrzeń kosmiczna, obrona przeciwrakietowa i wykrywanie prób jądrowych. W 1960 r. wszystkie cywilne programy kosmiczne przeniesiono do Narodowej Agencji Aeronautyki i Przestrzeni Kosmicznej (NASA), a wojskowe programy kosmiczne – do poszczególnych służb. To pozwoliło ARPA skoncentrować wysiłki na programach Project Defender (obrona przed rakietami balistycznymi) oraz Project Vela (wykrywanie testów jądrowych), jak również rozpocząć prace nad przetwarzaniem komputerowym, naukami behawioralnymi i materiałoznawstwem. Programy stanowiły podstawę badań i rozwoju w zakresie nadzoru i ukierunkowanej energii, zwłaszcza w badaniach nad radarami, nad wykrywaniem podczerwieni czy promieniowania rentgenowskiego. Program TRANSIT, sponsorowany przez → m a r y n a r k ę w o j e n n ą [t. 3] i opracowany pod kierownictwem dr. Johnsa Hopkinsa, był pierwszym systemem pozycjonowania satelitarnego.

Pod koniec lat 60., wraz z przeniesieniem tych programów do innych instytucji, ARPA przedefiniowała swoją rolę i skoncentrowała się na zróżnicowanym zestawie stosunkowo małych, zasadniczo odkrywczych programów badawczych. Agencję przemianowano na Agencję Zaawansowanych Projektów Badawczych Obrony (DARPA) w 1972 r., i właśnie na początku lat 70. kładła ona nacisk na programy bezpośredniej energii, na przetwarzanie informacji i na technologie taktyczne.

Na zlecenie Departamentu Obrony w 1967 r. rozpoczęła projekt budowy zdecentralizowanej sieci komputerowej, którą nazwano później ARPANET, oraz Packet Radio Network, Packet Satellite Network, który zapoczątkował rozwój internetu oraz badań w dziedzinie sztucznej inteligencji rozpoznawania mowy i przetwarzania sygnałów, w tym – części robota Shakey. DARPA nigdy nie prowadziła badań samodzielnie: zajmowała się finansowaniem wyższych uczelni, instytucji komercyjnych i innych organizacji non-profit.

W latach 1976–1981 główne projekty DARPA były zdominowane przez technologię powietrzną, lądową, morską i kosmiczną, wysokoenergetyczną technologię laserową do obrony przeciwrakietowej w kosmosie, zaawansowane pociski manewrujące i zaawansowane, programy opancerzenia taktycznego i przeciwpancernego, wykrywania podczerwieni do nadzoru w przestrzeni kosmicznej, zwalczania okrętów podwodnych.

W 1981 r. DARPA założyła grupę ekspertów – ICCB (ang. Internet Configuration Control Board), której zadaniem stało się zarządzanie przebiegiem prac badawczych prowadzonych w związku ze stworzeniem internetu. W 1984 r. agencja przekształciła ICCB w IAB (ang. Internet Activities Board), która to grupa została podzielona na grupy robocze, zajmujące się zastosowaniem, współdziałaniem, → b e z p i e c z e ń - s t w e m [t. 1] i testowaniem. Na koniec IAB przekształcono w IETF (ang. Internet Engineering Task Force) oraz w IRTF (ang. Internet Research Task Force). Te grupy te odpowiedzialne za rozwój konstrukcji internetu i za badania nad rozwojem w tej dziedzinie.

Agencja rozwija w ramach FCS (ang. *Future Combat Systems*) program przyszłościowych systemów pola walki analizowany przez armię amerykańską, obejmujący m.in: egzoszkielet wspomagany, UAV różnej wielkości i lądowe pojazdy autonomiczne. W latach 80. uwaga agencji koncentrowała się na przetwarzaniu informacji i programach związanych z samolotami i badaniami naddźwiękowymi. Ponadto DARPA zaczęła opracowywać nowe koncepcje małych, lekkich satelitów i kierowała nowymi programami dotyczącymi produkcji obronnej, technologii okrętów podwodnych i opancerzenia oraz broni przeciwpancernej.

DARPA prowadzi badania, rozwija technicznie i koordynuje podwzględem naukowym program globalnej obrony antybalistycznej USA.

„The Economist" nazwał DARPA agencją, która ukształtowała współczesny świat, ponieważ wynalazła satelity pogodowe, GPS, → d r o n y [t. 2], technologie stealth, interfejsy głosowe, komputery osobiste i internet. Jej sukcesy stały się inspiracją dla rządów na całym świecie do uruchomienia podobnych agencji badawczo-rozwojowych.

W latach 2014–2016 DARPA prowadziła pierwszy konkurs ekspertów ds. bezpieczeństwa komputerowego w celu wyszukiwania luk w zabezpieczeniach, wykorzystywania ich i tworzenia poprawek, które łatają te luki w sposób w pełni zautomatyzowany.

W czerwcu 2018 r. liderzy DARPA zademonstrowali szereg nowych technologii, opracowanych w ramach programu GXV-T. Celem tego programu jest stworzenie lekko opancerzonego pojazdu bojowego o niezbyt dużych gabarytach, który dzięki zwrotności i zwinności może z powodzeniem oprzeć się nowoczesnym systemom uzbrojenia przeciwpancernego. We wrześniu 2020 r. DARPA i Siły Powietrzne USA ogłosiły, że koncepcja hipersonicznej broni – manewrujących pocisków szybujących – jest gotowa do testów w locie swobodnym. Pociski poruszają się z prędkością wielokrotnie większą niż dotychczasowe rakiety i są praktycznie niewykrywalne dla radarów.

Instytucja nigdy nie prowadziła swoich przedsięwzięć samodzielnie – do projektów angażowane były komercyjne instytucje i uczelnie wyższe. Mimo że DARPA zajmuje się projektami związanymi z technologią militarną, wiele rozwiązań znalazło zastosowanie w sektorze komercyjnym. Jest to bezpośrednio związane z koncepcją istnienia

DARPA, która bada wszelkie, nawet najbardziej fantastyczne obszary technologii pod kątem wykorzystania ich w siłach zbrojnych. Ciągłe zmiany struktury agencji, elastyczność, kreatywność i fluktuacja kadr to znaki szczególne tej innowacyjnej instytucji.

Dzięki współpracy ze środowiskiem akademickim, przemysłem i partnerami rządowymi DARPA opracowuje i realizuje projekty badawczo-rozwojowe mające na celu poszerzenie granic technologii i nauki, często pozabezpośrednie wymagania wojskowe USA. Agencja opracowała i przekazała programy technologiczne obejmujące szeroki zakres dyscyplin naukowych, odpowiadające na pełne spektrum potrzeb bezpieczeństwa narodowego.

DARPA jest niezależna od innych wojskowych prac badawczo-rozwojowych i podlega bezpośrednio kierownictwu wyższego szczebla Departamentu Obrony. Zatrudnia ok. 240 pracowników rządowych, w tym prawie 100 kierowników programów, którzy wspólnie nadzorują ok. 250 programów badawczo-rozwojowych. Jednocześnie bezpośrednio kontroluje budżet ok. 2 mld dolarów. Składa się z 6 biur badawczych i kilku biur organizacyjnych. Biuro Technologii Taktycznych zajmuje się pracami w zakresie platform powietrznych, kosmicznych, lądowych i morskich, systemów bezzałogowych, systemów laserowych, systemów broni precyzyjnej. Za prace w zakresie tworzenia czujników i systemów sterowania odpowiada Biuro Wykorzystania Informacji. Biuro Technologii Strategicznych zajmuje się rozwojem sensorów kosmicznych, strategicznych i taktycznych sieci informacyjnych, systemów i technologii dla bezpieczeństwa chemicznego i biologicznego oraz operacji morskich. Biuro Nauk Obronnych jest ukierunkowane na badania z zakresu fizyki, materiałów, biologii, matematyki itp. Biuro Technologii Przetwarzania Informacji odpowiada za wysokowydajne technologie obliczeniowe, kognitywne systemy tłumaczenia maszynowego itp.

DARPA dokłada wszelkich starań, aby zidentyfikować, rekrutować i wspierać doskonałych menedżerów programów – specjalistów w swojej dziedzinie. Menedżerowie programów mierzą się z wyzwaniami w szerokim zakresie: od głębokiej nauki, przez systemy, po możliwości, ale ostatecznie kieruje nimi chęć dokonania zmian. Kierownicy programówpodlegają dyrektorom biur DARPA i ich zastępcom, którzy są odpowiedzialni za wyznaczanie kierunków technicznych ich biur, zatrudnianie kierowników programów i nadzorowanie realizacji programu. Kadrę techniczną wspierają również eksperci z dziedziny bezpieczeństwa, zagadnień prawnych i kontraktowych, finansów, zasobów ludzkich i komunikacji. To ludzie, dzięki którym menedżerowie programów mogą osiągnąć bardzodużo podczas stosunkowo krótkiej kadencji.

Na poziomie agencji Dyrektor i Zastępca Dyrektora DARPA zatwierdzają każdy nowy program i przeglądają bieżące programy, ustalają priorytety dla całej agencji i zapewniają zrównoważony portfel inwestycyjny. **Wiele współczesnych projektów DARPA utajniono. Kilka ciekawych przedsięwzięć ujrzało jednak światło dzienne.** Głównym projektem agencji jest FCS (ang. *Future Combat Systems*, ‘przyszłościowe systemy walki), który ma być tak rewolucyjny, jak wynalezienie prochu strzelniczego.

FCS został zainicjowany w 1999 r. i powinien zostać zakończony w 2040 r. Projekt obejmuje wiele modułów związanych z innowacyjnymi systemami łączności, → t a k t y k i , rozpoznania, ale także z powstaniem nowych bezzałogowych pojazdów, inteligentnej amunicji oraz z nowatorskimi systemami wyposażenia → ż o ł n i e r z y [t. 4].

Do pojazdów bezzałogowych obecnie projektowanych przez DARPA zalicza się roboty RUV na kołach lub gąsienicach (wersja szturmowa i zwiadowcza), mule (bezzałogowy pojazd wielozadaniowy) oraz SUGV – niewielkie, kilkunastokilogramowe roboty przeznaczone do penetracji trudnodostępnych miejsc i do neutralizowania pocisków minowych.

Bezzałogowce to jeden z głównych tematów podejmowanych przez DARPA. Agencja prowadzi np. zaawansowane prace nad pływającymi dronami. Od końca 2016 r. trwają próby w ramach projektu SeaHunter. Chodzi o autonomiczny statek zwiadowczy przeznaczony do zwalczania okrętów podwodnych. Agencja bada też możliwość wdrożenia tzw. morskiego pociągu, czyli grupy autonomicznych małych statków transportowych łączących się niczym wagony w jeden duży okręt zdolny do samodzielnego pokonywania tysięcy mil bez konieczności tankowania. Jednym z głównych modułów FCS jest system broni elektromagnetycznej EGS (Electromagnetic Gun System), który jest obecnie testowany w bezzałogowym śmigłowcu Dragonfly DP-4X. Docelowo produktami ECS mają być pistolet elektromagnetyczny oraz działo elektromagnetyczne, wystrzeliwujące wojskowe satelity na orbitę ziemską. Obecnie trwają też zaawansowane prace nad stworzeniem miękkiego egzoszkieletu – kombinezonu, który miałby wspomóc żołnierza na polu walki poprzez ułatwienie dźwigania ciężkiego wyposażenia wojskowego. Jednocześnie egzoszkielet DARPA pełniłby funkcję ochronną.

Innym ciekawym projektem, na który w DARPA przewidziano spory budżet w 2021 r., jest Gunslinger: program stworzenia efektywnego systemu uzbrojenia do przenoszenia broni klasy powietrze – powietrze oraz powietrze – ziemia. Z pewnością Gunslinger będzie powiązany z innym innowacyjnym projektem tej agencji, czyli z bezzałogowym statkiem powietrznym LongShot, który ma szansę podejść do celu jeszcze bliżej niż załogowa jednostka bojowa. Podstawową zaletą bezzałogowca LongShot jest to, że chroni on życie pilota – nie ma go w kokpicie podczas ataku. Ochrona życia żołnierzy na polu walki jest zawsze celem nadrzędnym: takie przesłanie przyświecało też projektowi „Żelaznej Kurtyny" – Iron Curtain. Jest to system aktywnej ochrony pojazdów militarnych, składający się z zaawansowanego radaru, z czujników wykrywających → z a g r o ż e n i e [t. 4] oraz z układu balistycznego, który ma je odeprzeć. System sam podejmuje decyzję, jakie przeciwdziałanie militarne będzie skuteczne do obrony przed atakiem, i docelowo rakieta jest niszczona przed osiągnięciem celu. Iron Curtain ma budowę modularną i w teorii może aktywnie chronić każdą powierzchnię.

Tak innowacyjna organizacja jak **DARPA stała się obiektem wielu insynuacji i → teorii spiskowych** [t. 4]. Część z nich dotyczy programu HAARP (ang. *High-frequency Active Auroral Research Program)*, obejmującego wiele badań dotyczących jonosfery w zakresie działania systemów telekomunikacyjnych i nadzoru elektronicznego. W tym celu używa się rozmaitych urządzeń nadawczych, mających symulować zmiany w jonosferze. W 2005 r. opublikowano informację o wytworzeniu sztucznej zorzy polarnej – już nawet to wydarzenie świadczy o powadze projektu i o jego możliwościach technologicznych. Mimo że większość prowadzonych badań jest jawna, program HAARP stał się przedmiotem wielu teorii spiskowych, które rzekomo mają być odpowiedzią na niewyjaśnione dotąd zjawiska. Niektóre teorie spiskowe argumentują nawet, że stanowi on zagrożenie dla całej ludzkości. Istnieje hipoteza, która mówi, że urządzenia HAARP mogą wywoływać niekontrolowane trzęsienia ziemi, tsunami i cyklony lub nawet sterować myślami i nastrojami ludzi. Wystarczy wspomnieć też o tym, że jedna z teorii spiskowych potwierdzających rzekomy udział DARPA odnosi się do wyłączenia prądu w całym Nowym Jorku.

Nie jest też tajemnicą, że DARPA pracuje nad podskórnym czipem wstrzykiwanym pod skórę, stale analizującym skład krwi pacjenta i natychmiast wykrywającym zakażenie koronawirusem. Jest to kontynuacja innego, militarnego programu DARPA, który miał na celu opracowanie substancji monitorującej krew żołnierza pod kątem zagrożeń → bronią chemiczną [t. 1] i → bronią biologiczną [t. 1], zanim jeszcze wystąpią pierwsze objawy. Agencja oficjalnie uspokaja zwolenników teoriispiskowych – DARPA nie przewiduje instalować pod skórą obywateli Stanów Zjednoczonych żadnych urządzeń śledzących.

Kolejnym przedmiotem teorii spiskowych odsyłających do DARPA jest projekt ADAPTER (ang. *Advanced Acclimation and Protection Tool for Environment Readiness)*, docelowo przeznaczony dla żołnierzy w podróży. Adapter podróżny, wszczepiany pod skórę lub przyjmowany z pożywieniem, ma mieć na celu zmniejszenie dolegliwości związanych z długimi przelotami samolotem i ze zmianą strefy czasowej, a także pomóc w walce z biegunką. ADAPTER mógłby mieć zastosowanie również poza środowiskiem wojskowym, co wzbudza uzasadnione obawy. Nie zapominajmy jednak o tym, że obecnie powszechne są już inne urządzenia wszczepiane pod skórę – np. elektrostymulatory pracy serca (rozruszniki) czy systemy dostarczania leków w dawkach określonych przez lekarza. Wszystko to pokazuje dość jednoznacznie, że projekty rozwijane przez DARPA mogą wpłynąć na naszą rzeczywistość w wielu różnych obszarach.

Ponad 70 lat doświadczenia agencji było niezwykle satysfakcjonujące. Na jej liście osiągnięć znalazły się systemy bezzałogowe, technologie redukcji sygnatury radarowej, globalne systemy pozycjonowania i wreszcie technologia globalnego internetu, której prototypem był ARPANET, stworzony przez agencję. Praca DARPA ma na celu przewidywanie przyszłych potrzeb w sferze wojskowej i przyśpieszenie rozwoju w niektórych obszarach. Tym samym agencja nie tylko zapewnia wojsku niezbędne

systemy, lecz także tworzy nową wizję możliwości wykorzystania zaawansowanych technologii do celów wojskowych.

Od początku istnienia ta organizacja była wyjątkowa w swojej formie. Początkowo podlegała bezpośrednio Sekretarzowi Obrony USA. Ściśle współpracuje z innymi organizacjami badawczymi Departamentu Obrony USA, ale zachowuje całkowitą niezależność od nich. Pod względem struktury oraz organizacji różni się od wszystkich innych organizacji badawczych Departamentu Obrony USA.

Sergiusz Wasiuta

About DARPA, https://www.darpa.mil/about-us/about-darpa (dostęp 11.10.2021); *Avengers oraz Gremliny wspomogą armię USA. Zaskakujące projekty*, 05.01.2021, https://cyfrowa.rp.pl/innowacje/art18284231-avengers-oraz-gremliny-wspomoga-armie-usa-zaskakujace-projekty (dostęp 22.11.2021); L. Blain, *DARPA Demonstrates 6 New Technologies Behind the Agile Combat Vehicles of Tomorrow*, 25.06.2018, https://newatlas.com/darpa-gxv-t-demonstration-military-vehicle-technology/55198/ (dostęp 14.10.2021); B. Charzyński, *Czym jest DARPA? Najważniejsze informacje o Agencji Zaawansowanych Projektów Badawczych*, 22.08.2021, https://scroll.morele.net/technologia/czym-jest-darpa-najwazniejsze-informacje/ (dostęp 11.10.2021); M. Hołowacz, *Projekty DARPA są jakby wyrwane z książki SF. Te podobają mi się najbardziej*, 21.08.2017, https://antyweb.pl/darpa-warrior-web-alias (dostęp 11.10.2021); *Inventing the Future. A Growing Number of Governments Hope to Clone America's DARPA*, 3.06.2021, https://www.economist.com/science-and-technology/2021/06/03/a-growing-number-of-governments-hope-to-clone-americas-darpa (dostęp 12.10.2021); M. Kamiński, *Najciekawsze bieżące projekty DARPA* [cz. 1], https://gadzetomania.pl/3889,najciekawsze-biezace-projekty-darpa-cz-1 (dostęp 14.10.2021); R. Richard, H. Van Atta, S.G. Reed, S.J. Deitchman, *DARPA Technical Accomplishments Volume I. An Historical Review Of Selected DARPA Projects*, April 1991, https://apps.dtic.mil/dtic/tr/fulltext/u2/a241725.pdf (dostęp 11.10.2021); M.A. Dennis, *Defense Advanced Research Projects Agency*, United States government, https://www.britannica.com/topic/Defense-Advanced-Research-Projects-Agency (dostęp 15.10.2021); S. Weinberger, *The Imagineers of War. The Untold Story of DARPA, the Pentagon Agency That Changed the World*, Alfred A. Knopf, New York 2017.

AGENT WPŁYWU / AGENT ZAGRANICZNY (z łac. *agens* – działający; ang. *agent of influence*; niem. *Agent des Einflusses*) – osoba lub organizacja, która znajduje się w jednym kraju, ale systematycznie realizuje cele polityki państwa obcego, korzystając z zaufania społeczeństwa; działacz społeczny, aktywista, prowadzący politykę partii lub organizacji w środowisku nienależącym do tych struktur.

Termin ma kilka znaczeń, w tym „przedstawiciel zagranicznego agenta" i „szpieg". Zagraniczni agenci to osoby fizyczne lub prawne reprezentujące interesy (najczęściej finansowe, handlowe) agenta za granicą. W niektórych krajach nazywają się tak organizacje lub osoby, które angażują się w krajową działalność polityczną w interesie obcego państwa. W przestrzeni rosyjskojęzycznej określa się tak również szpiegów, redukując nazwę „agent obcego → w y w i a d u [t. 4]" do jej pierwszego członu, dlatego nawet neutralna koncepcja – np. termin finansowy „agent zagraniczny" – w Rosji i innych krajach postsowieckich ma negatywny wydźwięk. Natomiast w przestrzeni anglojęzycznej ten termin nie ma takiego nacechowania.

Agent wpływu to osoba, która prowadzi systematyczną działalność w interesie konkretnego środowiska politycznego. Rolę agentów wpływu zwykle odgrywają społeczni i polityczni aktywiści, którzy korzystają z zaufania społeczeństwa, w którego obrębie operują. Praktyka infiltracji agentów wpływu znana jest od czasów starożytnych. Na przykład Aleksander Macedoński w 328 r. p.n.e., po zdobyciu Sogdiany (krainy w Azji Środkowej leżącej nad rzeką Zarafszan, przez którą biegł jedwabny szlak; obecnie tereny te leżą na terytorium Uzbekistanu i Tadżykistanu i mają charakter pustynny), wezwał z Macedonii i Grecji 100 chłopców z wyższych sfer społecznych i zmusił ich do ożenku z dziewczętami z miejscowej szlachty. Akcja ta zdawała się aktem pojednania dawnych wrogów i umocnienia przyjaźni między nimi. Jednocześnie dzięki tej operacji zdobywca utworzył potężną strukturę władzy nowej szlachty, która gwarantowała bezpieczeństwo podstawowych interesów imperium Aleksandra.

Agent zagraniczny jest w swoich działaniach podobny do lobbysty i może wykonywać różne zadania bezpośrednio lub pośrednio związane z polityką. Może również promować ekonomiczne, kulturalne i informacyjne interesy rządu innego państwa.

Głównym celem agenta wpływu jest pomoc agresorowi, najeźdźcy (innemu państwu) w ich destrukcyjnej działalności przeciwko temu państwu, w którym znajduje się agent wpływu. Jego możliwości zmniejszają się albo zanikają podczas pobytu poza państwem, przeciwko któremu działa. Innymi celami agenta są:

- formowanie korzystnej dla agresora (okupanta) → o p i n i i p u b l i c z n e j [t. 3] w danym państwie,
- wpływ na osoby podejmujące decyzje zarządcze w państwie, korzystne dla okupanta (agresora),
- destabilizacja sytuacji politycznej prowadząca do utraty kontroli państwa w celu zwiększenia wpływu agresora (okupanta),
- poszerzanie konfliktowych tematów w społeczeństwie,
- sabotaż władzy (bezczynność) dla osłabienia państwa na rzecz agresora (okupanta).

Obecnie agenci wpływu z reguły nie są wdrażani z zewnątrz, lecz są ludźmi już funkcjonującymi w środowisku wybieranym jako sfera oddziaływania. W tym celu można wykorzystywać różne konferencje międzynarodowe, stowarzyszenia, towarzystwa przyjaźni, wizyty, kontakty osobiste. Agentami wpływu często stają się intelektualiści, pracownicy rządowi, którzy mają dostęp do → i n f o r m a c j i [t. 2] tajnych, właściciele dużych banków lub firm, pracownicy wykonujący różne usługi pomocnicze, członkowie rodzin najważniejszych w państwie osób, przychylni interesom innego środowiska politycznego, które jest zainteresowane ich wykorzystaniem. Agenci wpływu mogą się różnić pod względem pozycji, form i metod działania. Nierzadko działają legalnie, lobbując na rzecz obcych interesów w organach ustawodawczych, wykonawczych i sądowniczych, w dziedzinie nauki, technologii, ekonomii i mediów.

Aktywność agentów wpływu przejawia się w tworzeniu atmosfery sprzyjającej podejmowaniu decyzji, którymi jest zainteresowany obcy podmiot.

Charakterystyczne cechy agentów wpływu to: zdolność do wpływania na społeczną świadomość; obiektywna orientacja ich działań w celu ułatwienia osiągnięcia określonych celów; przynależność do grupy funkcjonariuszy publicznych niższego stopnia, którzy pozostają w cieniu osób na wyższych stanowiskach („szare eminencje"). W ramach długoterminowej strategicznej kombinacji operacyjnej agentura wpływu dzieli się na rzeczywistą (taką, która odgrywa przypisaną jej rolę na pewnym etapie) i perspektywiczną (taką, która powinna zastąpić pierwszą po jej zdyskredytowaniu). Istnieją 2 zasadniczo różne podejścia do pojęcia agentów zagranicznych. Pierwsze – amerykańskie – miało na celu przeciwdziałanie rozprzestrzenianiu się nazizmu i → k o m u n i z m u [t. 2]. Stopniowo amerykańska ustawa została zmodyfikowana, w USA prowadzi się raczej rejestr organizacji lobbujących na rzecz obcych rządów. W rzeczywistości celem modelu amerykańskiego nie jest kontrola samych organizacji, lecz kontrola polityków, z którymi takie organizacje współdziałają. Bardzo rzadko podejście to obejmuje media.

Drugim podejściem do statusu zagranicznych agentów jest podejście rosyjskie. Rosja nie podnosi kwestii kontroli nad politykami i posłami, ustawa o agentach zagranicznych dotyczy wyłącznie organizacji publicznych, które korzystają z funduszy międzynarodowych i – zdaniem rządu rosyjskiego – wpływają na proces decyzyjny w kraju. Model rosyjski polega na tym, że wszystkie materiały informacyjne i działania organizacji znajdujących się w rejestrze agentów zagranicznych powinny być oznaczone jako wyprodukowane przez organizację opatrzoną statusem agenta zagranicznego. Jest to praktyka często służąca podważaniu zaufania do tych organizacji i wywieraniu na nie presji.

W USA Ustawa o rejestracji agentów zagranicznych (Foreign Agents Registration Act, FARA) została przyjęta w 1938 r. Była przede wszystkim reakcją na wzmocnienie lobbingu i → p r o p a g a n d y [t. 3] ze strony państw uważających Amerykę za jednego z potencjalnych wrogów.

Ustawa była wymierzona głównie w stronę narodowo-socjalistycznych Niemiec, które przez kilka lat przed II wojną światową usilnie starały się wpłynąć na kształtowanie opinii publicznej w USA. Swoją działalność prowadziły np. poprzez German-American Bund (niem. Amerikadeutscher Volksbund) lub America First Committee, utworzony w celu zorganizowania kampanii przeciwko zaangażowaniu USA w → w o j n ę [t. 4].

Później, w 1966 r., FARA została zmieniona, a jej uwaga przesunęła się z propagandy politycznej na lobbing polityczny działający w interesie innych państw. Prawo zobowiązywało agentów zagranicznych do dostarczania sprawozdań finansowych, a także do ujawniania ich pracy. Ponadto po latach 50. XX w., gdy wielu Amerykanów na całym świecie zauważało coraz większe wpływy komunistyczne w USA, prawna

definicja agentów zagranicznych stała się węższa. Zaliczano do nich osoby i organizacje, które działają tylko poprzez bezpośredni wpływ zagranicznych władz lub organizacji. W kontrowersyjnych przypadkach władze amerykańskie musiały udowodnić, że cel rzekomych agentów rzeczywiście miał wpływ na politykę USA. Ten ostatni warunek doprowadził do tego, że kara za naruszenia FARA stała się bardzo rzadka.

W teorii agentom zagranicznym, czyli politycznym lobbystom obcego rządu, którzy się nie zarejestrowali, grozi do 5 lat pozbawienia wolności i grzywna do 10 tys. USD. Każda z dwóch kar może być również stosowana niezależnie od siebie. Według amerykańskiego Departamentu Sprawiedliwości w ciągu ostatnich 50 lat wydano jedynie 7 wyroków za naruszenie FARA. Po dojściu do władzy D. Trumpa FARA trafiała na pierwsze strony gazet głównie z powodu rzekomych naruszeń tego prawa przez osoby z najbliższego otoczenia amerykańskiego prezydenta. Tak np. były szef kampanii wyborczej Trumpa P. Manafort musiał przyznać, że wbrew wymogom prawa nie ujawnił swoich dawnych powiązań z administracją byłego prezydenta Ukrainy W. Janukowycza. M. Flynn został zwolniony ze stanowiska doradcy Trumpa ds. bezpieczeństwa, próbując ukryć relacje łączące go z władzami rosyjskimi. Później okazało się, że w 2015 r. otrzymał on od rosyjskich firm ponad 50 tys. USD.

Obecnie jako agentów zagranicznych w USA zarejestrowano ok. 1,7 tys. osób i organizacji. Organizacja, która wpisuje się w definicję agenta zagranicznego, może swobodnie wykonywać swoją pracę po terminowej rejestracji w Departamencie Sprawiedliwości. Jednocześnie FARA nie ma zastosowania wobec niepolitycznego lobbingu oraz propagandy w najszerszym znaczeniu. Rozpowszechnianie informacji do celów komercyjnych, kulturalnych, naukowych i religijnych, a także darowizn nie wiąże się z rejestracją jako agenta zagranicznego.

Wbrew swojej nazwie FARA nie jest skierowana przeciwko szpiegom lub agentom obcych państw, ale przeciwko ludziom i organizacjom, które na polecenie i przy wsparciu finansowym innych krajów starają się wpływać na kształtowanie opinii publicznej w USA. Może to nastąpić np. poprzez lobbing lub rozpowszechnianie pewnych informacji, w tym fałszywych. Sama ustawa i przewidziane przez nią kary w przypadku jej naruszenia mają na celu uczynienie tego typu działalności – jak również jej zleceniodawców – przejrzystymi. Wolność słowa nie jest przy tym ograniczona. Prawo amerykańskie nie nakłada ograniczeń na działalność ani nie dotyczy organizacji zajmujących się nauką, kulturą, edukacją lub religią.

W lipcu 2012 r., po fali protestów antyrządowych w Federacji Rosyjskiej, prezydent W. Putin podpisał, a Duma uchwaliła nowelizację ustawy odnoszącej się do sektora pozarządowego, w której pojawiło się pojęcie agenta zagranicznego. Określono tym mianem organizacje, które otrzymywały środki z zagranicy i zajmowały się „działalnością polityczną". NGO miały same uznać, czy spełniają te kryteria, a jeżeli stwierdzą, że tak, zarejestrować się w specjalnym rejestrze. Ustawa została zaprojektowana, by zablokować, napiętnować i uciszyć krytyczne organizacje pozarządowe.

Przede wszystkim ucierpiały organizacje ochrony → p r a w c z ł o w i e k a [t. 3], ekologiczne oraz ośrodki naukowe i centra socjologiczne.

„Honorowy" tytuł agenta zagranicznego został przyznany organizacjom działającym w różnych dziedzinach: przeciwdziałania dyskryminacji, ochrony praw kobiet i osób LGBT, ochrony zabytków, badań naukowych, reformy wymiaru sprawiedliwości w sprawach karnych i systemie penitencjarnym, prawa konsumentów i ekologii. Starały się one zaangażować opinię publiczną do omawiania polityki państwowej i rozwiązywania problemów, których samo państwo nie chciało rozwiązać.

Organizacje spełniające przesłanki do uznania za zagranicznego agenta w FR zmuszone są co kwartał informować organ rejestrujący o wielkości otrzymanej pomocy i celach, na które zostanie ona spożytkowana, a także prowadzić podwójną księgowość dla krajowych i zagranicznych środków. Nałożono na nie również obowiązek wpisania się na „listę niekomercyjnych organizacji pełniących funkcję zagranicznych agentów". Za działalność bez dopełnienia obowiązku rejestracji oraz rozprzestrzenianie materiałów i informacji w środkach masowego przekazu bez wskazania, że ich źródłem jest zagraniczny agent, nakłada się 100–300 tys. rubli kary na kierownictwo organizacji oraz 300–500 tys. dla samej organizacji.

W ciągu kilku lat na listę agentów zagranicznych trafiło 148 organizacji, z czego 27 zostało zamkniętych. Organizacje te odgrywały ważną rolę w ochronie praw zwykłych ludzi. W wielu przypadkach dostarczały wsparcia, którego państwo nie było w stanie zapewnić, m.in. pomoc prawną i psychologiczną dla ofiar dyskryminacji i → p r z e m o c y [t. 3], zajmowały się także monitoringiem stanu środowiska. Mimo że w świetle prawa „działania na rzecz ochrony flory i fauny" nie powinny być uznawane za „polityczne", do rejestru agentów zagranicznych wpisano co najmniej 21 organizacji ekologicznych. Głównym celem rosyjskich władz było ewidentnie stłumienie rozwoju krytycznego → s p o ł e c z e ń s t w a o b y w a t e l s k i e g o [t. 4] i zastąpienie go podporządkowanymi rządowi zwolennikami jego polityki.

Ustawa o zagranicznych agentach zawiera szeroką definicję politycznej działalności (w czerwcu 2016 r. została ona jeszcze rozszerzona). Jest nią wywieranie wpływu na decyzje władz państwowych, a także na opinię publiczną. Obecnie obejmuje praktycznie każdą formę komentowania polityki lub działań funkcjonariuszy publicznych. Określenie „agent zagraniczny" jest w Rosji bardzo negatywnie nacechowane. Wzmacnia ten efekt propaganda, która często informuje o obcych rządach ingerujących w wewnętrzne sprawy kraju.

W 2015 r. Putin podpisał kolejną ustawę – o organizacjach niepożądanych. Dotyczy ona zagranicznych i międzynarodowych organizacji działających na terenie FR. Ustawa umożliwia zakazanie ich działalności, jeśli stanowi ona → z a g r o ż e n i e [t. 4] dla podstaw ustroju konstytucyjnego lub obronności i bezpieczeństwa państwa. Uznanie organizacji za niepożądaną oznacza, że jej wszelka działalność jest całkowicie zakazana, zakazane jest współpracowanie z taką organizacją – grozi za to do

6 lat pozbawienia wolności. W ustawie o organizacjach niepożądanych, podobnie jak w ustawie o agentach, znajduje się wiele nieprecyzyjnych regulacji i sformułowań – np. „zagrożenie dla bezpieczeństwa" – które służyć mogą władzom dowolnie, wg ich potrzeb.

Pod koniec listopada 2017 r. prezydent Rosji Putin zatwierdził ustawę, zgodnie z którą media zagraniczne są uznawane za agentów zagranicznych. Można za nich uznać media zagraniczne o różnej formie prawnej, zarówno „osoby prawne zarejestrowane na terytorium obcego państwa", jak i „struktury zagraniczne niemające formy osoby prawnej". Chodzi o podmioty „rozpowszechniające dla nieograniczonego kręgu osób materiały i wiadomości drukowane, audiowizualne i inne". Media będą uważane za agentów zagranicznych, jeśli otrzymają „pieniądze i/lub inny majątek od obcych państw, ich organów państwowych, organizacji międzynarodowych i zagranicznych, obywateli innych krajów, bezpaństwowców lub osób przez nie upoważnionych", a także od rosyjskich osób prawnych, „które otrzymują pieniądze i inne mienie z określonych źródeł".

Wobec mediów określonych jako agenci zagraniczni stosowane będą analogiczne zasady, jakie obowiązują w Rosji wobec organizacji pozarządowych mających status agenta zagranicznego. Oznacza to m.in. restrykcyjne wymogi dotyczące sprawozdawczości oraz nakaz oznaczania swoich materiałów informacją o nadanym statusie. W przypadku odmowy rejestracji jako agent zagraniczny media zostaną zamknięte. Uchwalone przepisy nie wymieniają konkretnych mediów. Powodem decyzji był spór między Moskwą a Waszyngtonem, który wybuchł pod koniec października 2017 r.: 19 października rosyjski nadawca zagraniczny → RT [t. 3], wcześniej znany jako Russia Today, zawiadomił, że amerykański Departament Sprawiedliwości zobowiązał go do rejestracji zgodnie z FARA. Podobna rejestracja jest również wymagana od rosyjskiej państwowej agencji informacyjnej Sputnik. Po krótkim oporze nadawca zgodził się zarejestrować w USA jako agent zagraniczny. Ustawa FR została przyjęta jako odpowiedź na działania podjęte wobec działającej tam stacji RT America, kanału rosyjskiej telewizji RT finansowanej ze środków budżetu Rosji.

Przepisy o agentach zagranicznych są sprzeczne z obowiązkami i zobowiązaniami FR w dziedzinie praw człowieka, a rozszerzenie ich zasięgu na zagraniczne media stanowi dodatkowe zagrożenie dla wolności i niezależności mediów i dostępu do informacji, nową próbę okrojenia przestrzeni dla niezależnych głosów w Rosji. Ustawa pogłębiła ograniczenia w korzystaniu z podstawowych praw w Rosji i zahamowała rozwój niezależnego społeczeństwa obywatelskiego.

Raport Amnesty International z 2016 r. *Agenci praw człowieka: Cztery lata ustawy o „zagranicznych agentach" w Rosji* ukazuje wysoką cenę, jaką musi płacić rosyjskie społeczeństwo, gdy niezależne, krytyczne organizacje pozarządowe są zmuszane do zamykania wartościowej działalności i do milczenia. Jest to wyrachowana napaść na wolność słowa.

Nowe poprawki do ustawy o mediach władze rosyjskie nazwały „symetryczną reakcją" na działania Waszyngtonu. Ustawa była krytykowana przez zachodnie rządy i obrońców praw człowieka jako zawierająca niejasne sformułowania i zezwalająca na daleko idące ograniczenia wobec zagranicznych mediów. W grudniu 2017 r. za agentów zagranicznych w FR uznano Voice of America (→ G ł o s A m e r y k i [t. 2]), Radio Swoboda (zob. → R a d i o W o l n a E u r o p a i R a d i o S w o b o d a [t. 3]) oraz szereg innych projektów.

Kiedy ustawa o „zagranicznych agentach" została uchwalona w Rosji w 2012 r., prezydent Putin powiedział, że Moskwa poszła w ślady USA. Jednak przy bliższym spojrzeniu okazuje się, że rosyjskie prawo dotyczące organizacji pozarządowych i amerykańska FARA nie są tym samym. W USA do agentów zagranicznych zalicza się tych bezpośrednio kierowanych lub kontrolowanych przez zagraniczny rząd lub organizację. W Rosji, aby uzyskać ten status, wystarczy zdobyć grant zagraniczny.

Droga do osiągnięcia celu rosyjskiej metody wskazywania agentów zagranicznych przebiega w 3 etapach: 1) utożsamienie organizacji publicznych z lobbystami i przekonanie opinii publicznej, że organizacje pozarządowe są złe, by następnie wprowadzić wobec nich specjalne regulacje, które oddzielą je od „dobrych organizacji"; 2) wprowadzenie kar dla organizacji, uzasadnione tym, że naruszają one ustanowione przepisy; 3) zakazanie działalności organizacji pozarządowych. Rosja nie powiedziała, że organizacje zostały zakazane, są to po prostu niepożądane organizacje, które nie mogą działać w Rosji. W rzeczywistości jednak ich działalność jest zabroniona.

Sergiusz Wasiuta

Federal Law on Introducing Amendments to Certain Legislative Acts of the Russian Federation Regarding the Regulation of Activities of Non-Commercial Organizations Performing the Function of Foreign Agents, CityWatch.org (dostęp 10.04.2019); K. Kurczab-Redlich, *Wowa, Wołodia, Władimir. Tajemnice Rosji Putina*, Wydawnictwo W.A.B., Warszawa 2016; Norwegian Helsinki Comittee, *Russia's Foreign Agent Law: Violating Human Rights and Attacking Civil Society, Norwegian Helsinki Committee*, 21.08.2014, NHC.no (dostęp 10.04.2019); W. Sitarz, *Prawo o zagranicznych agentach i jego znaczenie dla rosyjskiego społeczeństwa obywatelskiego na przykładzie ruchu LGBT*, „Wschodnioznawstwo" 2014, nr 8; A.N. Shulsky, G.J. Schmitt, *Silent Warfare: Understanding the World of Intelligence*, Potomac Books, Washington 2011; *Statement by the Spokesperson on the Russian law allowing the registration of foreign media as „foreign agents",* 26.11.2017, EEAS. Europa.eu (dostęp 10.04.2019); *UE interweniuje w sprawie Rosji. Ustawa o „zagranicznych agentach" zagraża wolności prasy*, 26.11.2017, WPolityce.pl (dostęp 10.04.2019); O. Wasiuta, S. Wasiuta, *Wojna hybrydowa Rosji przeciwko Ukrainie*, Arcana, Kraków 2017; *Агенты народа. Четыре года действия закона «Об иностранных агентах» в России: последствия для общества*, 2016, Amnesty.org. pl (dostęp 10.04.2019); Федеральный закон от 20.07.2012 № 121-ФЗ „О внесении изменений в отдельные законодательные акты Российской Федерации в части регулирования деятельности некоммерческих организаций, выполняющих функции иностранного агента", Publication.Pravo.gov.ru (dostęp 10.04.2019); *Політологічний енциклопедичний словник*, М.П. Требін (ред.), Видавництво Право, Харків 2015.

AGRESJA (ang. *aggression*) – pochodzi od łac. *aggressio* i oznacza napaść. Pojęcie stosowane w psychologii społecznej dla określenia zachowań ukierunkowanych „na zadanie cierpienia innemu człowiekowi, który jest motywowany do jego uniknięcia". B. Wojciszke wskazał 2 rodzaje tak rozumianej agresji: agresję instrumentalną (gdy cierpienie ofiary traktowane jest jako środek do osiągnięcia innego celu) oraz agresję wrogą (wówczas cierpienie ofiary staje się celem samym w sobie). Uznanie danego działania za akt agresji nie wymaga przy tym ani cierpienia ofiary (działanie mogło być nieskuteczne), ani też intencji wyrządzenia krzywdy (nie każdy cel człowiek sobie jest w stanie uświadomić). W zbliżonym tonie utrzymana jest definicja J.M. Ramireza, który rozumie agresję jako „wyuczone, zaobserwowane działanie aktywne lub pasywne, którego świadomym celem jest wyrządzenie komuś zamierzonej lub niezamierzonej szkody, krzywdy psychicznej lub fizycznej względem czegoś, co jest znane, nieznane, ożywione lub nieożywione". A.H. Buss określał agresję jako reakcję jednostki, która dla innego organizmu stanowi źródło szkodliwych bodźców.

W. Szewczuk w tym kontekście pisał o wszelkich działaniach o charakterze fizycznym lub słownym, które zmierzają do krzywdy fizycznej, psychicznej, a także rzeczywistej bądź symbolicznej, wymierzonej przeciw osobie albo rzeczy, która ją zastępuje. Natomiast G. Poraj wspominała o agresji jako zachowaniu, które skierowane jest przeciwko osobom lub rzeczom, które ujawnia się w formie fizycznego lub słownego ataku. Za agresję autorka uznała także myśli i agresywne życzenia, brak działania, zaniechanie udzielenia pomocy, które wywołać może szkodę. W *Słowniku socjologii i nauk społecznych* przez pojęcie agresji rozumie się „akty wrogości, wyrządzania krzywdy, przemocy lub skrajnie gwałtownego zachowania". Należy przy tym podkreślić, że nie każdy akt agresji będzie jednocześnie aktem → p r z e m o c y [t. 3]. Agresja i przemoc są często traktowane synonimicznie, co jest nieuprawnione.

Agresja w stosunku do przemocy jest pojęciem szerszym. W literaturze przedmiotu spotyka się sformułowanie „agresja z przeniesienia", która jest kierowana na jednostki słabsze lub przedmioty (tzw. obiekt zastępczy) wówczas, gdy jednostka ma świadomość, że atak na osobę, która faktycznie stanowi powód frustracji, mógłby spotkać się z karą. Podobny charakter relacji pomiędzy agresją a przemocą opisał także J. Pyżalski. Podkreślił on, że „przy spełnieniu pewnych kryteriów agresja może stać się przemocą", i wskazał semantyczną nadrzędność agresji nad przemocą, a przemocy nad bullyingiem (mobbingiem).

W tradycyjnym ujęciu agresja utożsamiana była z każdą reakcją, która miała na celu dostarczenie innym szkodliwych bodźców. Definicja zawarta w *Encyklopedii pedagogicznej XXI wieku* odnosi pojęcie agresji do zachowań, które ukierunkowane są na wyrządzenie komuś lub czemuś krzywdy, a także spowodowanie zła bądź bólu. Istotą takich zachowań jest szkodliwość i postępowanie, które stoi w opozycji do powszechnie obowiązujących norm społecznych. Agresja w ujęciu encyklopedycznym może dotyczyć działań antyspołecznych (wówczas człowiek chce wyrządzić komuś krzywdę) lub prospołecznych (gdy

motywem działania są cele społeczne, np. przeciwdziałanie krzywdzeniu innych). Ujęcie to akcentuje, że przemoc jest jedną z form agresji, a także że agresja może być skierowana na człowieka, ale również na zwierzę, samego siebie (tzw. autoagresja) oraz przedmiot. Stąd też w zachowaniach agresywnych wyodrębnia się podmiot (osobę agresora) oraz przedmiot oddziaływań (osobę lub rzecz będącą celem działania agresora). Ofiarą określa się natomiast człowieka albo inną żywą istotę, na którą skierowana jest agresja.

Agresja – w pewnych okolicznościach – może pełnić w życiu człowieka funkcję adaptacyjną lub adaptacyjno-obronną, toteż jej konstruktywne skutki należy odróżnić od efektów destruktywnych. Z tej przyczyny w ujęciu pedagogicznym – jak podkreśla G. Miłkowska-Olejniczak – mówi się o „właściwym kanalizowaniu agresji" zamiast o jej całkowitym eliminowaniu z życia społecznego. W psychologii, w odniesieniu do tej prawidłowości, pojawia się podział agresji na:

- agresję negatywną – wrogą;
- agresję pozytywną – usprawiedliwianą, akceptowaną społecznie, np. asertywność.

Podobna typologia, którą opracował Buss, dotyczy podziału na:

- agresję antyspołeczną – skierowaną przeciwko innym;
- agresję prospołeczną – ukierunkowaną na dobro innych ludzi.

W metodologii badań nad zjawiskiem agresji M. Farnicka, H. Liberska i D. Niewiedział proponują analizę 3 aspektów:

- agresji jako przejawu – wówczas badaniom podlegają zachowania;
- agresji jako gotowości – analizuje się cechy osobowości oraz czynniki wywołujące agresję;
- agresji jako sposobu radzenia sobie – przedmiotem badań są cechy sytuacji, interakcji sytuacji i cech osób oraz istotnych dla nich wartości, jak również zachowania w danej jednostce czasu.

Wyjaśnienia przyczyn agresji można podzielić na biologiczne, psychologiczne i socjologiczne. Teorie socjologiczne częściej upatrują przyczyn agresji w relacjach ze środowiskiem, a nieco rzadziej odnoszą się do wyjaśnień genetycznych tego zjawiska. Biologiczne i psychologiczne teorie odwołują się natomiast do podobnych przyczyn, różnie definiowanych przez poszczególnych autorów.

Biologiczne wyjaśnienia przyczyn agresji opisane przez Farnicką, Liberską i Niewiedział odnoszą się do:

- poglądu etologicznego – agresja traktowana jest w kategorii naturalnej cechy, która wiąże się z energią wewnętrzną, kumulowaną w organizmie; jej uzewnętrznienie zależne jest od wystąpienia 2 czynników: ilości tej energii oraz siły bodźców zewnętrznych, które tę energię mogą wyzwolić;
- poglądu socjobiologicznego – agresja jest wytworem ewolucji; zachowania agresywne to działania przystosowawcze, skierowane na eliminację napastników i rywali po to, by dać agresywnym przedstawicielom gatunku szansę na przekazanie własnych genów kolejnym pokoleniom;

- genetyki behawioralnej – skłonność do agresji jest uwarunkowana genetycznie; stwierdzono przy tym, że geny silniej niż wpływy środowiskowe kształtują skłonność do agresji w wieku dorosłym; układ ten jest odwrotny w okresie dojrzewania i w dzieciństwie; pogląd ten jest krytykowany przez genetyków zachowania, którzy wskazują na kluczową rolę czynników środowiskowych w mechanizmach powstawania agresji.

Wśród psychologicznych teorii wyjaśniania agresji Wojciszke oraz R.J. Gerrig i P.G. Zimbardo opisali następujące czynniki:

- genetyczne (agresja jako adaptacja oraz element natury człowieka; uruchamiana za pośrednictwem określonych „wyzwalaczy" i tłumiona dzięki pojawieniu się „kontrwyzwalaczy"; taka agresja ma charakter ewolucyjny i podnosi szanse na przeżycie jednostki);
- socjologiczne (agresja będąca efektem frustracji; w tym rozumieniu tendencja do podejmowania zachowań agresywnych zwiększa się wraz ze wzrostem wartości blokowanego celu, z eskalacją przeszkód, które uniemożliwiają jego osiągnięcie oraz ze wzrostem liczby działań, które ulegają blokowaniu; kumulacja drobnych pobudzeń może w efekcie wywołać wielką frustrację i niewspółmierną reakcję agresywną; frustracja nie zawsze jest przy tym kierowana bezpośrednio na podmiot, który ją wzbudził – wówczas mówimy o przemieszczeniu agresji (tzw. agresji z przeniesienia, gdy jest ona zwrócona w stronę innego obiektu zagrożonego mniejszą karą, lub o zmianie postaci agresji, gdy reakcja jest zastępowana inną, zagrożoną mniejszą karą, np. opowiadanie dowcipów o kobietach);
- teorie uczenia się, które podkreślają związek agresji z:
  - warunkowaniem sprawczym (poprzez system nagród, który powoduje, że jednostka dąży do podejmowania podobnych działań; taką nagrodą może być obserwacja cierpienia osoby, która człowieka denerwuje, sukces, np. przerwanie szkodliwej aktywności, gdy zaczepiana przez innych jednostka zareaguje agresywnie, nagrody materialne, np. po wygranej rywalizacji, albo wzrost samooceny);
  - modelowaniem (poprzez obserwację zachowania innych, czyli na podstawie doświadczeń innych osób; nagradzanie zachowań agresywnych modela skutkuje większą podatnością na naśladowanie go; odwrotna tendencja obserwowana jest w przypadku ukarania modela; działania są jednak pod większą kontrolą poznawczą, co oznacza, że nasze przekonania mają dla nas większą wartość niż ewentualne nagrody i kary; identyfikacja z modelem prowadzi także do tzw. zastępczego warunkowania sprawczego – wówczas emocje modela udzielają się obserwatorowi, np. naśladowanie osób o wysokim statusie społecznym).

W odniesieniu do teorii uczenia się Gerrig i Zimbardo opisali tzw. normy zachowań agresywnych, związane z występowaniem w środowisku zewnętrznym modeli, od których dzieci mogą uczyć się agresji. Modele takie mogą pochodzić ze świata

realnego (np. rodzice, grupa rówieśnicza) bądź też świata wirtualnego (np. gry, filmy, konflikty online).

Socjologiczne teorie wyjaśniające agresję – w ujęciu A. Giddensa – to:

- teorie funkcjonalistyczne – gdy jednostka nie jest w stanie realizować własnych aspiracji za pośrednictwem dostępnych środków, wtedy może pojawić się motywacja dewiacyjna, wynikająca z rozbieżności pomiędzy pragnieniami a ich spełnieniem; w tej grupie wyróżnia się np. teorię anomii (gdy w relacjach międzyludzkich brakuje wskazówek odnośnie do właściwego zachowania, a ludzie czują się zagubieni) lub teorię subkultur (dotyczącą dopasowania się do danej grupy społecznej, w której wewnętrzne normy współżycia mogą być sprzeczne z normami ogólnymi);
- teorie interakcjonistyczne – zakładające, że każda dewiacja jest konstruktem społecznym, co oznacza, że dane zachowanie dopiero w świadomości konkretnej grupy społecznej może być postrzegane w sposób negatywny; wśród nich wyodrębnia się np. teorię etykietowania (gdy dane zachowania są etykietowane przez ludzi, którzy stanowią prawo i porządek; zachowanie dewiacyjne jest wówczas zachowaniem, któremu ludzie przypisali taką „etykietę", np. zabicie człowieka w czasie pokoju w odróżnieniu od zabicia w czasie → w o j n y [t. 4]);
- teorie konfliktu – wskazujące na skłonność do samodzielnego wyboru zachowania dewiacyjnego w odpowiedzi na nierówności społeczne, np. realizm nowej lewicy zakłada, że przyczyną zachowań dewiacyjnych jest przekonanie, że człowiek jest pozbawiony tych przywilejów, do których inni mają swobodny dostęp, co uniemożliwia pełne uczestnictwo w życiu społeczeństwa;
- teorie kontroli – upatrujące przyczyn zachowań przestępczych w dążeniu do równowagi pomiędzy impulsami, które skłaniają do podejmowania tego typu czynów, a mechanizmami kontroli społecznej, które do nich zniechęcają; silne więzi człowieka ze społeczeństwem i prawem powodują wzrost kontroli społecznej i konformizmu, a słabe więzi są przyczyną dewiacji; stąd przestępcami są często osoby o niskim poziomie samokontroli, będącym wynikiem niewłaściwej socjalizacji w domu oraz w szkole; ponieważ → c z y n y z a b r o n i o n e są skutkami decyzji sytuacyjnych – wtedy, gdy pojawia się okazja, kontrolę społeczną gwarantują środki prewencyjne takie jak techniki ochrony obiektów oraz system monitoringu, które dają poczucie → b e z p i e c z e ń s t w a obywatelom, lecz nie rozwiązują przyczyn problemu; takie podejście określa się mianem prewencji sytuacyjnej: nadzór (monitoring) opiera się na pilnowaniu porządku (na podstawie obowiązujących przepisów prawa), instalacji kamer, → s t r a ż y s ą s i e d z k i e j [t. 4], natomiast techniki ochrony obiektów związane są z modyfikacjami w środowisku lokalnym, które utrudniają popełnianie czynów zabronionych.

Wskazując przyczyny agresji, R. Porzak odniósł się do tzw. modelu ekologicznego, w którym wyodrębnił kilka istotnych elementów: jednostkę, jej najbliższe otoczenie,

społeczność lokalną oraz kontekst społeczny. Każdy z tych elementów może – zdaniem autora – być źródłem powstawania agresji oraz jej późniejszego utrwalania w postaci przemocy. Spośród czynników społecznych podłożem dla agresji i przemocy może być: osłabienie więzi społecznych (zanik wsparcia społecznego i mechanizmów kontroli społecznej), wykluczenie, marginalizacja społeczna osób o niskim statusie społeczno-ekonomicznym (osoby marginalizowane przejawiają skłonność do negowania norm społecznych), rozbieżności pomiędzy aspiracjami ludzi a możliwościami ich realizacji (frustracja i przekonanie o braku alternatywy mogą skłonić do przemocowego mechanizmu zaspokajania własnych potrzeb), obecność grupowych norm społecznych, które stoją w opozycji do powszechnie akceptowalnego systemu wartości. Klasyfikacji czynników, które mogą sprzyjać rozwojowi zachowań agresywnych, dokonał także W. Kowalski. Wśród nich znalazły się czynniki makrospołeczne (np. rozpad więzi społecznych, upadek norm i wartości, ograniczenie mechanizmów kontroli społecznej, dezorientacja polityczna, zaniedbania wychowawczej funkcji szkoły, rodziny, negatywny wpływ mediów, zwiększenie skali zjawisk patologicznych, słabość obowiązujących przepisów prawa) oraz mikrospołeczne (np. → k r y z y s [t. 2] rodziny, uczenie się zachowań agresywnych w rodzinie, odrzucenie emocjonalne dzieci, niewłaściwa opieka rodzicielska, alkoholizm, niewłaściwe metody wychowawcze, przemoc w rodzinie, niskie kompetencje wychowawcze rodziców i nauczycieli). Podobne czynniki zostały opisane przez G. Miłkowską-Olejniczak.

Wśród czynników ryzyka zachowań agresywnych uwzględnić można większość tych, które wyodrębnia Z.B. Gaś (zob. → p r o f i l a k t y k a b e z p i e c z e ń s t w a [t. 3]). W tym obszarze Farnicka, Liberska i Niewiedział uwzględniły:

- w grupie czynników ryzyka agresji: obniżony poziom sprawności intelektualnej, niską pozycję w grupie oraz zaniżone poczucie własnej wartości, brak umiejętności interpersonalnych, niedosyt wsparcia społecznego, skłonność do izolacji, „trudne zachowania", np. ADHD, doświadczenie bycia ofiarą przemocy, przynależność do mniejszości społecznej, uwarunkowania kulturowe i społeczne wyrażające się w akceptacji kar fizycznych i przemocy, trudną sytuację ekonomiczną rodziny, „odmienność" postrzeganą w środowisku w sposób negatywny, np. niepełnosprawność;
- w grupie czynników chroniących przed agresją: wysoką sprawność intelektualną, atrakcyjność fizyczną, posiadanie wysokiej pozycji w grupie oraz wysokiej samooceny, umiejętności interpersonalne, wysoki poziom wsparcia społecznego, brak zaburzeń rozwojowych, pozytywne relacje z innymi ludźmi (w tym z rodzicami), terapię w sytuacji bycia ofiarą przemocy, dodatkowe umiejętności wysoko oceniane w społeczeństwie, np. osiągnięcia szkolne i sportowe, uwarunkowania kulturowe wyrażające się w braku akceptacji dla przemocy, dobrą sytuację ekonomiczną rodziny, „odmienność", która jest postrzegana w sposób pozytywny, np. zdolności muzyczne.

Agresja – w ujęciu I. Pospiszyl – w kontekście zmiany społecznej determinowana jest kilkoma prawidłowościami: brutalizacją zachowań, unifikacją grupową (agresja dotyczy wszystkich warstw społecznych, a nie – jak do niedawna uważano – wyłącznie osób pochodzących z marginesu społecznego), unifikacją płciową (agresja rozwija się zarówno w grupie chłopców, jak i dziewcząt), manifestowaniem agresji w miejscach, w których dotychczas nie było na to przyzwolenia (np. szkoła, miejsca publiczne), obniżaniem się wieku sprawców brutalnych zachowań.

Czynniki wywołujące agresję w ujęciu psychologicznym klasyfikowane są przez Wojciszke jako:

- czynniki indywidualne – uwarunkowania genetyczne, płeć, agresywność jako cecha związana z wrogim wzorcem atrybucji (upatrywaniem wrogich intencji innych osób w sytuacjach niejednoznacznych), cechy osobowości skłaniające do zachowań agresywnych (jak impulsywność, podatność emocjonalna, ruminacja, narcyzm);
- czynniki sytuacyjne – prowokacja, pobudzenie emocjonalne, normy i oczekiwania społeczne oraz ograniczenia kulturowe, alkohol, temperatura powietrza, przemoc w mass mediach, która wzmaga zachowania agresywne, stwarza okazję do modelowania agresji, zwiększa obojętność na tego typu zachowania (tzw. desensytyzacja) oraz zmniejsza skłonność do zachowań prospołecznych.

Na podstawie psychologicznych teorii przyczyn można wskazać kilka rodzajów agresji. M. Szpringer wyodrębnia wśród nich:

- agresję frustracyjną – jej przyczyną jest frustracja; wówczas bodźcem hamującym jest kara lub jej groźba;
- agresję naśladowczą – związaną z naśladowaniem modelu, który obecny jest w otoczeniu jednostki; wówczas człowiek może nie być świadom, że zachowuje się agresywnie;
- agresję instrumentalną – gdy agresja jest środkiem do realizacji innych celów;
- agresję patologiczną – wywołaną procesem chorobotwórczym. Badacze przedmiotu wskazują ponadto:
- agresję fizyczną – bezpośrednią napaść, bójkę, pobicie, uderzenie, zabranie przedmiotu, kopanie, duszenie, szczypanie, plucie, ciągnięcie, popychanie, podstawianie nogi itp.;
- agresję werbalną – dotyczącą interakcji takich jak obelgi, wyzwiska, negowanie poleceń wychowawców i przełożonych, dotkliwe słowa mało konstruktywnej krytyki wyartykułowane „twarzą w twarz", groźby, straszenie, naruszenie dobrego imienia, przekazywanie fałszywych → i n f o r m a c j i [t. 2], przezywanie, poniżanie, wyśmiewanie;
- agresję pośrednią – przybierającą formę inną niż bezpośrednia, np. plotki, zniesławianie, odmowa w celu sfrustrowania proszącego, ośmieszanie, podburzanie innych, opuszczenie towarzystwa, by okazać komuś niechęć; może także być

skierowana na obiekt, np. trzaskanie drzwiami, uderzenie w stół, rzucanie przedmiotami lub niszczenie ich.

W pewnych okolicznościach niektóre wskazane rodzaje agresji będą również dotyczyły zachowań o charakterze przemocy. W *Encyklopedii pedagogicznej XXI wieku*, za R.A. Hindem, przyjęto podział na:

- agresję instrumentalną – ukierunkowaną na uzyskanie określonego celu;
- agresję ze złości – bez wyraźnego ukierunkowania na konkretny obiekt lub sytuację;
- agresję obronną – będącą reakcją na atak;
- agresję związaną z grą lub zabawą – nasila się ona w toku rywalizacji o zwycięstwo w grze.

Obszernej klasyfikacji rodzajów agresji w powyższym źródle dokonała Miłkowska-Olejniczak, która wyodrębniła:

- ze względu na kierunek: agresję skierowaną na istoty żywe (w tym samego siebie oraz innych ludzi), agresję ukierunkowaną na przedmioty martwe (niszczenie oraz wandalizm), agresję skierowaną na jednostki oraz agresję ukierunkowaną na grupę;
- ze względu na podmiot: agresję indywidualną (sprawcą jest jednostka) oraz agresję grupową;
- ze względu na formę: agresję bezpośrednią, pośrednią, przemieszczoną, agresję czynną i bierną, bezpośrednią i pośrednią agresję słowną oraz fizyczną, agresję jawną i ukrytą;
- ze względu na złożoność: zachowania agresywne proste i złożone;
- ze względu na sposób realizacji: agresję behawioralną, wyobrażeniową, symboliczną i tematyczną;
- ze względu na warunki zewnętrzne: agresję impulsywną, instrumentalną, frustracyjną, wyuczoną, wywołaną zachowaniem lub wypowiedziami innych, wywołaną własnym niepowodzeniem;
- ze względu na cel: agresję zamierzoną oraz niezamierzoną. Często stosowana jest typologia zachowań agresywnych zaproponowana przez B. Krahe. Opisała ona:
- ze względu na modalność reakcji: zachowania werbalne, związane z napastliwymi, szkodliwymi wypowiedziami oraz zachowania fizyczne, związane z zadawaniem bólu ludziom i zwierzętom lub niszczeniem przedmiotów;
- ze względu na jakość reakcji: działanie i brak działania;
- ze względu na stopień bezpośredniości zachowania: działanie bezpośrednie, skierowane wprost na daną osobę, zwierzę lub przedmiot oraz działanie pośrednie;
- ze względu na widoczność zachowania: działania jawne i ukryte;
- ze względu na sposób wzbudzenia działania: niesprowokowane i odwetowe;
- ze względu na ukierunkowanie na cel: zachowania wrogie, gdy motyw dotyczy chęci wyrządzenia krzywdy, oraz zachowania instrumentalne, gdy agresja jest środkiem do osiągnięcia innych celów;

- ze względu na typ szkody: agresja fizyczna i psychiczna;
- ze względu na stopień trwałości konsekwencji: przejściowe i długotrwałe;
- ze względu na rodzaj zaangażowanego obiektu: działania jednostkowe i grupowe.

Ponadto w literaturze istnieje także określenie tzw. agresji żartobliwej, która zawsze koreluje z pozytywnymi emocjami (np. dowcipy, żartobliwe opowieści).

W klasyfikacji zachowań agresywnych autorstwa Farnickiej, Liberskiej i Niewiedział wyróżnionych zostało 8 typów:

- napastliwość fizyczna – użycie siły fizycznej wobec istot żywych lub przedmiotów;
- napastliwość słowna – negatywne wypowiedzi, np. krzyk, kłócenie się, przekleństwa, obelgi;
- napastliwość pośrednia – tzw. zachowania okrężne, takie jak złośliwe sugestie czy obmawianie, niszczenie własności, rzucanie przedmiotami, trzaskanie drzwiami;
- negatywizm – działania opozycyjne, m.in. przeciw zwierzchnikom lub osobom o wyższym statusie zawodowym, np. poprzez odmowę współpracy czy wykonania prośby/polecenia;
- podejrzliwość – przenoszenie własnej wrogości na innych pod postacią nieufności i przekonania, że inni nam szkodzą;
- uraza – związana z gniewem, złością, zazdrością jednostki skierowaną na innych „za rzeczywiste lub urojone krzywdy";
- drażliwość – dotycząca gwałtownego manifestowania negatywnych uczuć, gdy ich przyczyna jest błaha, np. niecierpliwość, rozdrażnienie, niegrzeczne zachowanie, tzw. zły humor;
- poczucie winy – wyrastające z przeświadczenia, że jednostka jest złym człowiekiem nawet wtedy, gdy jej przewinienie jest nieznaczne; wiąże się ono z „podwyższoną gotowością do doświadczania wyrzutów sumienia i wstydu za siebie"; wówczas, by zminimalizować dyskomfort, człowiek może podjąć próbę samoukarania się, zwaną autoagresją, lub próbować wymierzyć karę innej osobie, szukając tzw. kozła ofiarnego.

Pyżalski dokonał klasyfikacji rodzajów agresji ze względu na 6 kryteriów. Wyodrębnił on kryterium dotyczące bodźca, czyli frustracji, której pojawienie się pozwala mówić o agresji reaktywnej, a nieobecność tego bodźca – o agresji proaktywnej, ukierunkowanej na zadanie drugiemu człowiekowi cierpienia. Kolejne kryterium dotyczy sposobu kontaktu pomiędzy sprawcą a ofiarą. W tym kontekście mówimy o agresji bezpośredniej (ukierunkowanej na konkretną osobę) lub agresji pośredniej (np. związanej z niszczeniem własności ofiary albo obmawianiem jej). Kryterium trzecie odnosi się do rodzajów działań agresywnych, które mogą przybierać powszechnie znaną postać fizyczną (jak bicie) lub werbalną (poprzez obrażanie i wyzwiska). Podstawą czwartego kryterium jest specyfika działań sprawcy. Możemy wówczas mówić o agresji czynnej (np. bicie, wyzywanie) bądź agresji biernej (np. wykluczanie z grupy). Kryterium piąte odnosi się do

intencjonalności działań sprawcy. Rozróżniamy w jego ramach agresję instrumentalną, będącą sposobem osiągnięcia przez sprawcę zakładanego celu, oraz agresję afektywną, wynikającą z trudności w panowaniu nad emocjami. Kryterium ostatnie dotyczy liczby sprawców, gdyż agresor może działać indywidualnie bądź grupowo.

Specyficznym rodzajem agresji jest agresja elektroniczna, która w sposób szczególny rozpowszechniła się w XXI w. za sprawą nowoczesnych → t e c h n o l o g i i i n f o r m a c y j n o - k o m u n i k a c y j n y c h [t. 4]. Definicję cyberagresji prezentuje Grigg, opisując ją jako „umyślną krzywdę wyrządzoną przez korzystanie ze środków elektronicznych osobie lub grupie osób, niezależnie od ich wieku, które postrzegają takie akty jako obraźliwe, uwłaczające, szkodliwe lub niechciane".

Zdaniem Pyżalskiego jej szeroki zasięg zależny jest od: permanentnej dostępności ofiary (praktycznie przez całą dobę), pozornej anonimowości (która pozwala zachowywać się w sposób, w jaki sprawca nigdy nie zachowałby się w kontakcie bezpośrednim, i wprowadza w przekonanie o niemożności wykrycia aktu agresji, a – co z tym związane – perspektywę uniknięcia konsekwencji), niejawności komunikacji online (która wynika z niechęci do informowania dorosłych o własnych problemach – ofiara pozostaje z problemem sama i bezradna), nieograniczonej publiczności (co eskaluje skutki agresji, gdyż informacja ma nieograniczony zasięg i bardzo szybko się rozprzestrzenia), jak również występowania tzw. efektu „kabiny pilota" (fakt, że sprawca nie znajduje się z ofiarą „twarzą w twarz", powoduje, że negatywne emocje są mniejsze, a sprawca agresji zza ekranu komputera nie angażuje empatii, redukującej negatywne zachowania, i nie dostrzega cierpienia swoich ofiar). Do podobnych wniosków dochodzi

A. Andrzejewska, która podkreśla, że w sieci agresja pojawia się znacznie częściej aniżeli w komunikacji bezpośredniej. Dystans pomiędzy rozmówcami, będący cechą komunikacji internetowej, potęguje agresję werbalną. Podobny związek z osłabieniem mechanizmów kontroli społecznej a agresją wskazał także B. Hołyst.

Wieloczynnikowy charakter agresji – zdaniem Wojciszke – skłania do podejmowania złożonych interwencji zmierzających do usuwania czynników, które ją inspirują, oraz dostarczania alternatywnych wzorców zachowania. A zatem działania profilaktyczne ukierunkowane na zmniejszanie agresywnych zachowań muszą uwzględniać zarówno eliminację czynników ryzyka, jak i wzmacnianie czynników chroniących przed → z a g r o ż e n i a m i [t. 4], np. więzi rodzinnych, samoakceptacji, empatii. Koncentracja wyłącznie na profilaktyce defensywnej (negatywnej) połączona z marginalizowaniem profilaktyki ofensywnej (pozytywnej) powoduje niską efektywność podejmowanych działań profilaktycznych.

Ewelina Włodarczyk

A. Andrzejewska, *Dzieci i młodzież w sieci zagrożeń realnych i wirtualnych. Aspekty teoretyczne i empiryczne*, Wydawnictwo Difin, Warszawa 2014; K. Borzucka-Sitkiewicz, K. Kowalczewska-Grabowska, *Profilaktyka społeczna. Aspekty teoretyczno-metodyczne*, Wydawnictwo

Uniwersytetu Śląskiego, Katowice 2013; M. Farnicka, H. Liberska, D. Niewiedział, *Psychologia agresji. Wybrane problemy*, Wydawnictwo Naukowe PWN, Warszawa 2016; R.J. Gerrig, P.G. Zimbardo, *Psychologia i życie*, tłum. E. Czerniawska i in., Wydawnictwo Naukowe PWN, Warszawa 2009; D.W. Grigg, *Cyber-Aggression: Definition and Concept of Cyberbullying*, „Journal of Psychologists and Counsellors in Schools" 2010, vol. 20, iss. 2; W. Kowalski, *Agresja jako problem współczesnej szkoły*, [w:] *Profesjonalna profilaktyka w szkole. Nowe wyzwania*, Z. Gaś (red.), Innovatio Press Wydawnictwo Naukowe Wyższej Szkoły Ekonomii i Innowacji w Lublinie, Lublin 2011; B. Krahe, *Agresja*, tłum. J. Suchanecki, Gdańskie Wydawnictwo Psychologiczne, Gdańsk 2005; G. Miłkowska-Olejniczak, *Agresja*, [w:] *Encyklopedia pedagogiczna XXI wieku*, T. Pilch (red.), Wydawnictwo Akademickie „Żak", Warszawa 2003; R. Porzak, *Profilaktyka przemocy rówieśniczej*, [w:] *Profesjonalna profilaktyka w szkole. Nowe wyzwania*, Z. Gaś (red.), Innovatio Press Wydawnictwo Naukowe Wyższej Szkoły Ekonomii i Innowacji w Lublinie, Lublin 2011; J. Pyżalski, *Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży*, Oficyna Wydawnicza Impuls, Kraków 2012; tenże, *From Cyberbullying to Electronic Aggression: Typology of the Phenomenon*, „Emotional and Behavioural Difficulties" 2012, vol. 17, iss. 3–4; *Słownik socjologii i nauk społecznych*, G. Marshall, M. Tabin (red.), tłum. A. Kapciak i in., Wydawnictwo Naukowe PWN, Warszawa 2008; E. Włodarczyk, *Agresja elektroniczna*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; taż, *Profilaktyka bezpieczeństwa*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; taż, *Profilaktyka zagrożeń wirtualnych w pracy szkoły*, [w:] *Nauki społeczne i ekonomiczne – węzłowe zagadnienia*, J. Żylińska, I. Przychocka (red.), Wydawnictwo Uczelni Techniczno-Handlowej im. Heleny Chodkowskiej, Warszawa 2017.

AGRESJA W PRAWIE MIĘDZYNARODOWYM – oznacza zachowanie państwa, które albo inicjuje → w o j n ę [t. 4] przeciwko innemu państwu, albo prowadzi do sytuacji, w której ofiara jest (lub może być) doprowadzona do wojny. Nigdy nie ustalono, czy → a g r e s j a sama w sobie musi polegać na użyciu siły, czy może przejawiać się w mniejszych czynach, takich jak groźba użycia siły, a nawet w działaniach niezwiązanych z użyciem siły, np. poprzez zmianę przebiegu koryta rzeki.

W stosunkach międzynarodowych pojęcie agresji pojawiło się już przed II wojną światową w takich dokumentach prawa międzynarodowego jak Pakt Ligi Narodów. Jednakże dopiero Karta Narodów Zjednoczonych z 1945 r. (KNZ) redefiniowała kwestię pokojowego współistnienia państw. Przyjęcie KNZ wynikało ze wstrząsu, jakim dla społeczności międzynarodowej była II wojna światowa. To właśnie ten dokument po raz pierwszy zanegował agresję na tak szeroką skalę – przyjęto, że jedyną drogą do zapobieżenia kolejnej wojnie światowej będzie wyrzeczenie się → p r z e m o c y [t. 3] w stosunkach między państwami. Emanacją tego poglądu jest art. 2 ust. 4 KNZ, który stanowi, że:

> państwa w ich stosunkach międzynarodowych powinny powstrzymywać się od stosowania groźby lub użycia siły przeciwko nietykalności terytorium albo niepodległości politycznej któregokolwiek państwa, lub wszelkiego innego sposobu, niezgodnego z zasadami Narodów Zjednoczonych.

Przez wiele lat podejmowano próby zdefiniowania agresji. Dokumentem, w którym po raz pierwszy całościowo opisano zbrodnię agresji, była Deklaracja zasad prawa międzynarodowego dotyczących przyjaznych stosunków i współdziałania państw, będąca rezolucją Zgromadzenia Ogólnego ONZ z 24 października 1970 r. Stanowi ona m.in., że utrzymanie międzynarodowego pokoju i → b e z p i e c z e ń s t w a oraz rozwój przyjaznych stosunków i współdziałania między narodami należą do podstawowych celów Narodów Zjednoczonych.

Zwraca przy tym uwagę na doniosłość utrzymania i umocnienia międzynarodowego pokoju opartego na wolności, równości, sprawiedliwości i poszanowaniu → p r a w c z ł o w i e k a [t. 3] oraz rozwoju przyjaznych stosunków między narodami niezależnie od ich ustroju politycznego, gospodarczego i społecznego lub stopnia ich rozwoju.

Ponadto w świetle rezolucji ścisłe przestrzeganie przez państwa zobowiązania niemieszania się w sprawy jakiegokolwiek innego państwa stanowi podstawowy warunek zapewnienia, że narody będą ze sobą współżyły w pokoju, gdyż stosowanie interwencji w jakiejkolwiek postaci nie tylko narusza ducha i literę KNZ, lecz prowadzi także do powstania sytuacji, które zagrażają międzynarodowemu pokojowi i bezpieczeństwu.

KNZ podkreśla też zakaz agresji w sformułowaniu o konieczności powstrzymania się w swych stosunkach międzynarodowych od wojskowej, politycznej, gospodarczej lub jakiejkolwiek innej postaci przymusu skierowanego przeciw politycznej niepodległości lub integralności terytorialnej jakiegokolwiek państwa.

Państwa powinny rozwiązywać spory środkami pokojowymi zgodnie z KNZ. Deklaracja wprowadzała regulacje, które potwierdzały zakaz agresji w stosunkach międzynarodowych, wskazując m.in.:

> […] że państwa w ich stosunkach międzynarodowych powinny powstrzymać się od groźby lub użycia siły przeciw integralności terytorialnej lub niepodległości politycznej jakiegokolwiek państwa, lub w inny sposób niezgodny z celami Narodów Zjednoczonych,
>
> […] że państwa powinny regulować ich spory międzynarodowe środkami pokojowymi w taki sposób, by pokój międzynarodowy, bezpieczeństwo i sprawiedliwość nie zostały zagrożone,
>
> […] obowiązek państw współdziałania ze sobą zgodnie z Kartą, […] zasadę równouprawnienia i samostanowienia ludów,
>
> […] zasadę suwerennej równości państw,
>
> […] zasadę, wg której państwa powinny wykonywać w dobrej wierze zobowiązania zaciągnięte przez nie zgodnie z Kartą i że takie zapewnienie ich bardziej skutecznego stosowania w ramach wspólnoty międzynarodowej przyczyni się niechybnie do realizacji celów Narodów Zjednoczonych.

Co szczególnie istotne, wg deklaracji:

> […] wojna stanowiąca agresję jest zbrodnią przeciw pokojowi, która powoduje odpowiedzialność na podstawie prawa międzynarodowego.

Deklaracja nakazuje, aby każde państwo wstrzymało się:

> […] od groźby lub użycia siły celem naruszenia istniejących międzynarodowych granic innego państwa lub jako środka rozwiązywania sporów międzynarodowych, włączając w to spory terytorialne i problemy dotyczące granic państw.

Są to kwestie obecnie ważkie w kontekście debaty nad legalnością działań w Ukrainie i Syrii. Zgodnie bowiem z literalnym brzmieniem deklaracji:

> […] państwa mają obowiązek wstrzymania się od aktów odwetu obejmujących użycie siły, [a także – przyp. aut.] powstrzymania się od organizowania lub zachęcania do organizacji sił nieregularnych lub zbrojnych związków, włączając w to najemników, celem wtargnięcia na terytorium innego państwa.

Państwa mają oprócz tego obowiązek:

> […] powstrzymania się od organizowania, podżegania, pomocy lub uczestnictwa w aktach walki wewnątrzpaństwowej lub aktach terrorystycznych w innym państwie lub godzić się ze zorganizowaną na jego terytorium działalnością mającą na celu popełnienie tego rodzaju aktów, gdy wspomniane w tym paragrafie akty obejmują groźbę lub użycie siły.

W odniesieniu do działań rosyjskich na Krymie warto przytoczyć ponadto fragment, który stanowi, że:

> […] terytorium jakiegoś państwa nie może być przedmiotem okupacji wojskowej w wyniku użycia siły wbrew postanowieniom Karty. Terytorium jakiegoś państwa nie może być przedmiotem nabycia przez inne państwo w wyniku groźby lub użycia siły. Żadne nabytki terytorialne wynikające z groźby lub użycia siły nie mogą być uznane za legalne.

Deklaracja potwierdza zasadę suwerennej równości państw. Suwerenność w rozumieniu deklaracji oznacza, że:

a) państwa są równe pod względem prawnym,
b) każde państwo korzysta z praw związanych z pełną suwerennością,
c) każde państwo ma obowiązek szanowania osobowości innego państwa,
d) integralność terytorialna i niepodległość polityczna państwa są nienaruszalne,
e) każde państwo ma prawo swobodnie wybrać i rozwijać swój system polityczny, społeczny, gospodarczy i kulturalny,
f) każde państwo ma obowiązek w pełni stosować się w dobrej wierze do swych międzynarodowych zobowiązań oraz współżyć w pokoju z innymi państwami.

Deklaracja nie ma charakteru wiążącego.

Kolejną próbę zdefiniowania agresji podjęło Zgromadzenie Ogólne ONZ 14 grudnia 1974 r. Przyjęto wówczas rezolucję nr 3314. Jej art. 1 stanowi, że:

> […] agresja jest użyciem siły zbrojnej przeciwko suwerenności, integralności terytorialnej lub niepodległości politycznej innego państwa lub w jakikolwiek inny sposób niezgodny z Kartą Narodów Zjednoczonych.

Zgodnie zaś z art. 2:

> […] użycie siły zbrojnej z pogwałceniem KNZ przez państwo, działające jako pierwsze, stanowi dowód prima facie aktu agresji.

Artykuł 3 podaje przykłady agresji. Są to:

a) inwazja lub zaatakowanie terytorium jednego państwa przez drugie lub jakakolwiek zbrojna okupacja (nawet czasowa), lub włączenie (aneksja) przy użyciu siły terytorium innego państwa lub jego części;
b) bombardowanie przez siły zbrojne lub użycie przez państwo jakiegokolwiek rodzaju broni przeciwko integralności terytorialnej innego państwa;
c) blokada portów i wybrzeży jednego państwa przez siły zbrojne innego państwa;
d) atak sił zbrojnych jednego państwa na terytorium lądowe, morskie lub siły powietrzne, flotę morską lub powietrzną innego państwa;
e) użycie sił zbrojnych jednego państwa stacjonujących na terytorium innego państwa za wcześniejszym porozumieniem w sposób naruszający postanowienia tegoż porozumienia lub jakiekolwiek przedłużenie ich obecności wykraczające poza powyższe porozumienie;
f) wysłanie przez państwo lub w jego imieniu uzbrojonych band lub grup, sił nieregularnych lub najemników, którzy przeciwko innemu państwu przeprowadzają działania zbrojne o ciężarze podobnym do działań wymienionych powyżej, lub znaczące zaangażowanie państwa w takie działania.

Artykuł 4 stanowi, że akty wymienione powyżej nie mają charakteru zamkniętego, Rada Bezpieczeństwa może określić, które działania uznała za agresję zgodnie z postanowieniami KNZ.

W art. 5 zawarto z kolei sformułowanie, że żadne uzasadnienie polityczne, ekonomiczne czy wojskowe nie jest i nie może być usprawiedliwieniem agresji, ponadto agresja jest zbrodnią przeciwko pokojowi, a korzyści terytorialne wynikające z agresji są nielegalne.

W toku prac nad statutem →M i ę d z y n a r o d o w e g o T r y b u n a ł u K a r n e g o [t. 3] (MTK) panowało powszechne przekonanie o konieczności penalizacji zbrodni agresji. Pomimo woli państw, aby ustanowić jej wspólną definicję, pojawiło się tak wiele rozbieżnych propozycji, że ostatecznie zamiar ten przesunięto w czasie. Artykuł 5 ust. 1 statutu MTK z 17 lipca 1998 r. wymienia zbrodnię agresji jako jedną z czterech najpoważniejszych zbrodni, które zostaną objęte jego jurysdykcją. Jednocześnie art. 5 ust. 2 stanowi, że MTK będzie ją sprawował w odniesieniu do zbrodni agresji dopiero wtedy, gdy zostanie przyjęte postanowienie definiujące tę zbrodnię. Ostatecznie definicję agresji przyjęto w toku konferencji rewizyjnej, która odbyła się

w dniach 31.05–11.06 2010 r. w Kampali. Tam też określono kwestię wykonania jurysdykcji nad agresją. Zgodnie z zaproponowanym brzmieniem art. 8 bis zbrodnia agresji oznacza:

1. Planowanie, przygotowywanie, wszczynanie lub prowadzenie przez osobę mogącą efektywnie sprawować kontrolę lub kierownictwo nad działaniami politycznymi lub wojskowymi państwa aktu agresji, który ze względu na swój charakter, ciężar i skalę stanowi oczywiste naruszenie Karty Narodów Zjednoczonych.
2. Dla celów ust. 1 „akt agresji" oznacza użycie sił zbrojnych przez państwo przeciwko suwerenności, integralności terytorialnej oraz politycznej niezależności innego państwa lub każde inne działanie w sposób niezgodny z Kartą Narodów Zjednoczonych. Każdy z poniższych aktów, bez względu na fakt wypowiedzenia wojny, będzie, zgodnie z rezolucją Zgromadzenia Ogólnego Narodów Zjednoczonych 3314 (XXIX) z 14 grudnia 1974 r., zakwalifikowany jako akt agresji.

Wymienione punkty art. 8 bis ust. 2 korespondują z treścią definicji aktów agresji w rezolucji Zgromadzenia Ogólnego ONZ nr 3314.

14 grudnia 2017 r. przyjęto na posiedzeniu państw stron statutu MTK rezolucję, która umożliwia MTK sądzenie spraw z zakresu zbrodni agresji od dnia 17 lipca 2018 r.

Piotr Łubiński

C.N.651.2010.TREATIES-8 [Porozumienie z Kampali], 29.11.2010; Y. Dinsten, *War, Aggression and Self-Defence*, Cambridge University Press, Cambridge 2005; P. Grzebyk, *Odpowiedzialność karna za zbrodnię agresji*, Wydawnictwo Uniwersytetu Warszawskiego, Warszawa 2010; P. Łubiński, *Agresja,* [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; P. Vieri, *Dictionary of the International Law of Armed Conflict*, International Committee of the Red Cross, Geneva 1992; Poprawki do Rzymskiego Statutu Międzynarodowego Trybunału Karnego, sporządzonego w Rzymie dnia 17 lipca 1998 r., Kampala, 10–11.06.2010 r.; Resolution ICC-ASP/16/Res.5 Activation of the jurisdiction of the Court over the crime of aggression, adopted at the 13th plenary meeting on 14 December 2017, ICC-ASP/16/20; Rezolucja Zgromadzenia Ogólnego ONZ z dnia 14 grudnia 1974 r., nr 3314 (XXIX) A/RES/29/3314; Rzymski Statut Międzynarodowego Trybunału Karnego sporządzony w Rzymie dnia 17 lipca 1998 r., Dz. U. 2003, nr 78, poz. 708; Zasady prawa międzynarodowego dotyczące przyjaznych stosunków i współdziałania państw zgodnie z Kartą Narodów Zjednoczonych – Rezolucja Zgromadzenia Ogólnego z dnia 24 października 1970 r. nr 2625 (XXV).

AGROTERRORYZM – szczególny rodzaj →terroryzmu [t. 4], a dokładniej →bioterroryzmu [t. 1]. Może być definiowany jako bezprawne, nielegalne użycie albo groźba użycia patogenów zwierzęcych lub roślinnych przeciwko sektorowi rolniczemu z zamiarem wymuszenia określonego działania bądź zastraszenia rządu, społeczeństwa dla osiągnięcia określonych celów, np. politycznych czy społecznych. Niektórzy badacze definiują agroterroryzm szerzej, wskazując, że to celowe wyrządzanie szkód w rolnictwie bądź przemyśle rolno-spożywczym, w tym intencjonalne

zakażenie zwierząt hodowlanych. Obejmuje on zastosowanie wszystkich możliwych środków → p r z e m o c y [t. 3] wobec rolnictwa (tj. nie będzie ograniczony tylko do środków biologicznych). Atak możedotyczyć rolników, producentów, przetwórców, dystrybutorów, handlu detalicznego, laboratoriów działających na rzecz sektora spożywczego, jak również restauracji i pozostałych punktów gastronomicznych. W ataku na zwierzęta szczególnie niebezpieczne są patogeny wywołujące takie schorzenia jak: wąglik, bruceloza, pryszczyca, gorączka Q, zapalenie mózgu i rdzenia koni, pomór świń, rzekomy pomór drobiu, afrykański pomór świń, gorączka doliny Rift, księgosusz. Z kolei uprawom roślinnym szczególnie zagrażają grzyby.

Rolnictwo jest istotne dla funkcjonowania społeczeństwa. Od początku cywilizacji człowiek był zależny od zwierząt oraz uprawy roślin. Wszelkie choroby pojawiające się naturalnie wśród zwierząt czy roślin stanowiły duże zagrożenie dla bezpieczeństwa żywnościowego i nadal nim są, choć bywa to lekceważone. Bezpieczeństwo żywnościowe według definicji → Or g a n i z a c j i N a r o d ó w Z j e d n o c z o n y c h d o s p r a w W y ż y w i e n i a i R o l n i c t w a [t. 5] to przede wszystkim dostęp do żywności i jej ekonomiczna odpowiedniość w takiej ilości, aby zaspokoić potrzeby żywieniowe ludności niezbędne do prawidłowego odżywiania się i prowadzenia zdrowego, aktywnego stylu życia.

Historia pamięta wiele epidemii w świecie zwierząt, które przyczyniły się do destabilizacji państw i stały się tematem debat o konieczności stworzenia systemowego zabezpieczenia sektora rolniczego i bieżącego rozwiązywania problemów wraz z pojawiającymi się zagrożeniami. Jeśli dojdzie do celowego ataku z wykorzystaniem czynnika biologicznego, będzie to szczególnie niebezpieczne zagrożenie, wymagające użycia dodatkowych sił i środków. Z pewnością atak na rolnictwo mógłby spowodować destabilizację gospodarczą i wywołać strach. Dobrym przykładem jest epidemia pryszczycy w Wielkiej Brytanii w 2001 r. Epidemia pokazała, jak szybko choroba może się rozprzestrzenić i jak trudno walczyć z jej konsekwencjami. Wtedy ustalenie źródła zakażenia pryszczycy i prześledzenie drogi transmisji było niemożliwe, ponieważ handlowano zwierzętami, które były nosicielami wirusa i miały kontakt z wieloma innymi zwierzętami. Niektóre z tych transakcji odbywały się na obrzeżach rynku i nie zostały odnotowane, stąd najważniejszym działaniem i największątrudnością było dotarcie do miejsca pobytu zwierząt, które mogły miećkontakt z zakażonymi stadami. Rząd wprowadził zakaz eksportu, następnie po kilku dniach zakaz handlu na terenie Wielkiej Brytanii. Według danych szacunkowych ustalono, że po terenie kraju mogło przemieścić się ok. 2 mln owiec, a 30 tys. sztuk opuściło kraj i zmieszało się ze stadami w Europie. Potwierdzono przypadki choroby we Francji i w Niemczech. Około 2 miesięcy później epidemia przybrała katastrofalne skutki, zidentyfikowano 1366 ognisk pryszczycy (łącznie przez cały przebieg epidemii odnotowano 1664 ogniska). Do pomocy wysłano wojsko i osoby zajmujące się ubojem zwierząt. Zasada była prosta – potwierdzenie 1 przypadku w gospodarstwie wiązało się z ubojem całego

stada do 24 godzin od wykrycia zakażenia. Programem przymusowego uboju objęto nawet 10 mln zwierząt.

Do dziś nie ustalono jednoznacznie, co było bezpośrednią przyczyną pojawienia się choroby w Wielkiej Brytanii. Sugerowano, że to nielegalnie importowane mięso, które zostało użyte do przygotowania potraw w angielskich restauracjach, a następnie w postaci resztek trafiło do rolników, a ci nakarmili nimi zwierzęta, wywołało epidemię. Teoria ta była kwestionowana, podobnie jak zdanie dr. Harasha Naranga, który twierdził, że przyczyną wybuchu mogło być przypadkowe uwolnienie wirusa z brytyjskiego laboratorium w miejscowości Pirbright. Najbardziej kontrowersyjna wersja została przedstawiona w czerwcu 2001 r. na spotkaniu ekspertów ds. terroryzmu w Edynburgu. Profesor Malcolm Dando z Instytutu Badań nad Pokojem Uniwersytetu Bradford powiedział, że pryszczyca to oczywisty czynnik, który zostałby wykorzystany przez każdego, kto chciałby zaatakować żywy inwentarz danego kraju, gdyż od lat 40. traktuje się ją jako rodzaj potencjalnej → b r o n i b i o l o g i c z n e j [t. 1].

Doświadczenie epidemii przyczyniło się do poszerzenia badań nad chorobami zakaźnymi mającymi wpływ na rolnictwo. Stwierdzono m.in. konieczność zwiększenia kontroli nad importem oraz powstrzymanie skali transportu zwierząt, a także testowanie szczepień, aby w przyszłości nie dochodziło do sytuacji masowej rzezi zwierząt, co mogłoby dodatkowo wywołać masowe protesty przeciwko tak kontrowersyjnym decyzjom rządzących. Epidemia miała katastrofalne skutki dla hodowli w Wielkiej Brytanii. Komisja Europejska na pewien czas zakazała eksportu zwierząt i produktów zwierzęcych z tego kraju. A koszty walki z epidemią oszacowano na ok. 8,5 mld funtów.

W czasie II wojny światowej takie państwa jak Japonia, Niemcy, Wielka Brytania, Stany Zjednoczone, Rosja prowadziły badania nad możliwością wykorzystania czynników biologicznych w ataku, również wymierzonym w sektor rolniczy. Prowadzono prace nad środkami porażającymi zwierzęta i uprawy roślinne, m.in. nad pryszczycą, księgosuszem, zarazą ryżową, rdzą pszenicy czy zarazą ziemniaczaną. Znane są także przypadki użycia patogenów przeciwko sektorowi rolniczemu w atakach terrorystycznych. Według Instytutu Studiów Międzynarodowych w Monterey od 1915 do 2000 r. odnotowano 19 ataków agroterrorystycznych na świecie, m.in. w latach 1982–1984 Związek Radziecki stosował zarazki nosacizny przeciwko mudżahedinom. Skutkiem tych działań było zakażenie koni, które były głównym środkiem transportu w Afganistanie. W latach 1983–1987 Tamilowie niszczyli uprawy herbaty na Sri Lance, wykorzystując do tego środki biologiczne. Powszechne były również groźby agroterroryzmu, jeden z takich incydentów nastąpił, gdy w 1989 r. grupa The Breeders, wcześniej nieznana jednostka, wysłała listy do burmistrza Los Angeles Toma Bradleya, grożąc wypuszczeniem owocanki południówki (*Ceratitis capitata*), inwazyjnej muchy znanej z niszczenia upraw owoców, którą hodowała. Co ciekawe, istnieją pewne przesłanki, że atak mógł zostać przeprowadzony, ponieważ w tym samym roku w południowej Kalifornii wystąpiły nieprawidłowości w populacjach tego owada.

Podane przykłady wskazują na niebezpieczeństwo związane z możliwością wykorzystania czynnika chorobotwórczego przeciwko rolnictwu, co w konsekwencji może mieć znamienne skutki, takie jak: destabilizacja państwa, dezorganizacja życia społecznego, zakłócenia w imporcie i eksporcie żywności, zniszczenie środowiska naturalnego, skutki zdrowotne, ekonomiczne oraz straty w hodowli i uprawie roślin. To z kolei może wpłynąć na bezpieczeństwo żywnościowe przez ograniczenie dostępności produktów spożywczych. Oprócz daleko idących skutków ekonomicznych, jakie może mieć udany atak na rolnictwo, może on również spowodować utratę zaufania do rządu w kwestii ochrony obywateli. Nawet częściowo udany atak może sprawić, że ludzie będą się obawiać o bezpieczeństwo dostaw żywności. Społeczeństwo mogłoby zacząć kwestionować zdolność rządu do ochrony przed bronią masowego rażenia w ogóle.

Przeprowadzenie ataku na przemysł rolniczy może być celem terrorystów z wielu powodów. Armin Elbers i Rickard Knutsson zauważyli, że większość gospodarstw rolnych jest rozproszona geograficznie, obejmują one rozległe obszary, co utrudnia, jeśli nie uniemożliwia, zapewnienie → b e z p i e c z e ń s t w a [t. 1]. Ponadto zwierzęta gospodarskie są zazwyczaj trzymane w bliskiej odległości i w dużych skupiskach, a różne populacje zwierząt są mieszane w transporcie. Zagrożeniem jest również to, że większość hodowli jest zależna od eksportu, a zwierzęta nie są odporne na patogeny, które przeważają w krajach docelowych. Co więcej, kontinuum „od pola do stołu" zwiększa podatność całego przemysłu rolnego na zagrożenia, potęgując tym samym liczbę potencjalnych dróg ataku i zmniejszając zdolność zapobiegania użyciu patogenów przed wprowadzeniem żywności na rynek. Produkcja, przetwarzanie, dystrybucja i przygotowanie są narażone na naturalne i celowe zanieczyszczenia lub zakażenia. Scentralizowana produkcja żywności i rozbudowane systemy dystrybucji produktów stwarzają zwiększone możliwości celowego jej zanieczyszczenia. Ponieważ produkty rolne zarówno przed zbiorami, jak i po nich są bardzo podatne na ataki, terrorystom nie brakuje tu możliwości. Zamachy agroterrorystyczne cechują się tym, że wykorzystywane do nich patogeny są w większości niegroźne dla agresora, a bariery moralne są łatwiejsze do pokonania. Atak taki może być zainicjowany przez kraje działające z motywów militarnych, politycznych, ideologicznych lub gospodarczych, ale też przez korporacje rolnicze z uwagi na konkurencję, zorganizowane grupy przestępcze ze względu na umiejscowienie przemysłu narkotykowego z upraw oraz organizacje terrorystyczne i indywidualne osoby z pobudek osobistych.

W Polsce stosuje się zabezpieczenia zapobiegające przypadkowemu zanieczyszczeniu i wprowadzeniu chorób do upraw i zwierząt gospodarskich. Położono także nacisk na ochronę pozbiorczych produktów rolnych oraz produktów, które są przetwarzane. Do dziś istnieje niewiele środków, które odpowiednio zapobiegałyby celowemu wprowadzaniu chorób do upraw i zwierząt gospodarskich przed ich pozyskaniem. Funkcjonuje jednak system nadzoru i kontroli, jego celem jest wykrycie choroby na

tyle wcześnie, aby zapobiec wybuchowi epidemii i powszechnym stratom. Skuteczność w łagodzeniu wybuchu choroby w obliczu celowego wprowadzenia pozostaje niezbadana. Wśród polskich instytucji odpowiedzialnych za poszczególne obszary funkcjonowania sektora rolniczego, zajmujących się → bezpieczeństwem żywności w kontinuum „od pola do stołu", znajdują się m.in. Państwowa Inspekcja Sanitarna, Inspekcja Weterynaryjna, Inspekcja Handlowa oraz Inspekcja Jakości Handlowej Artykułów Rolno-Spożywczych.

Arsenał broni biologicznej zawiera liczne mikroorganizmy niezagrażające bezpośrednio ludziom, ale mające znamienny wpływ na uprawy rolne i zwierzęta hodowlane, co może doprowadzić do strat ekonomicznych. Szczególne niebezpieczeństwo stanowi handel międzynarodowy produktami roślinnymi oraz organizmy szkodliwe przenoszone między kontynentami na obszary o podobnych warunkach klimatycznych, co może zagrażać uprawom krajów docelowych. Przykładem takiej sytuacji może być zaraza ziemniaczana przeniesiona z Ameryki do Europy. Szacuje się, że z jej przyczyny rocznie globalne straty w uprawach ziemniaka wynoszą 6,7 mld dolarów. Przyglądając się historycznym przykładom zagrożeń, a także opracowanym przez państwa programom broni biologicznej (np. prowadzono prace nad grzybem powodującym rdzę źdźbłową pszenicy lub nad grzybem wywołującym śniedź pszenicy – skutecznie likwidującym uprawy rolne), staje się jasne, że ważnymi celami są zboża i żywy inwentarz. Zagadnienia zwalczania organizmów szkodliwych dla roślin oraz zapobiegania ich rozprzestrzenianiu na poziomie ogólnoświatowym regulują: Międzynarodowa Konwencja Ochrony Roślin, sporządzona w Rzymie dnia 6 grudnia 1951 r., Porozumienie w sprawie stosowania środków sanitarnych i fitosanitarnych oraz Konwencja w sprawie utworzenia Europejskiej i Śródziemnomorskiej Organizacji Ochrony Roślin, podpisana w Paryżu dnia 18 kwietnia 1951 r. Na poziomie krajowym kwestie te reguluje Ustawa z dnia 12 lipca 1995 r. o ochronie roślin uprawnych wraz z późniejszymi nowelizacjami. W ramach zwalczania terroryzmu biologicznego w Europie stosuje się przede wszystkim Europejską konwencję o zwalczaniu terroryzmu, sporządzoną w Strasburgu dnia 27 stycznia 1977 r., oraz uzupełniającą jej zapisy Konwencję Rady Europy o zapobieganiu terroryzmowi, sporządzoną w Warszawie dnia 16 maja 2005 r. Powołano 2 instytucje chroniące bezpieczeństwo żywności: Europejski Urząd ds. Bezpieczeństwa Żywności (European Food Safety Authority, EFSA) oraz System Wczesnego Ostrzegania o Niebezpiecznej Żywności i Paszach (Rapid Alert System for Food and Feed, RASFF).

Należy mieć na uwadze, że zagrożenie jest realne, a przeprowadzony atak w jednym kraju może spowodować skutki w sąsiednich państwach z uwagi na szybkość rozprzestrzeniania się patogenów oraz łatwość komunikacji i handlu międzynarodowego. Samo zwalczanie skutków ataków agroterrorystycznych jest niezwykle trudne i wymaga zaangażowania wielu służb oraz współpracy międzynarodowej. Najbardziej skutecznym środkiem jest rozpoznanie tego typu zamiarów i szybkie reagowanie oraz

zwiększenie nadzoru nad produkcją i dystrybucją w rolnictwie, a także przygotowanie gospodarek na taką ewentualność.

Żaneta Mrożek

Agroterrorism: National Defense Assessment, Strategies, and Capabilities, A. Mauroni, R.A. Norton (eds.), U.S. Air Force Center for Strategic Deterrence Studies, Alabama 2020; Europejska konwencję o zwalczaniu terroryzmu, sporządzona w Strasburgu dnia 27 stycznia 1977 r., Dz.U. 1996, nr 117, poz. 557; N. Hashempour, *Agroterroryzm a niektóre strategie prawne*, Wydawnictwo Nasza Wiedza, Warszawa 2020; Konwencja Rady Europy o zapobieganiu terroryzmowi, sporządzona w Warszawie dnia 16 maja 2005 r., Dz.U. 2008, nr 161, poz. 998; Konwencja w sprawie utworzenia Europejskiej i Śródziemnomorskiej Organizacji Ochrony Roślin, podpisana w Paryżu dnia 18 kwietnia 1951 r., Dz.U. 1959, nr 33, poz. 191; Międzynarodowa Konwencja Ochrony Roślin, sporządzona w Rzymie dnia 6 grudnia 1951 r., Dz.U. 2001, nr 15, poz. 151; P. Moore, *Tajemnicze choroby współczesnego świata. Nowe zagrożenia wirusy, bakterie, zarazki*, tłum. Z. Szachnowska, Bellona, Warszawa 2009; S.C. Perkowski, *America's Food Does Anthrax Pose A Threat?*, Air University Maxwell Air Force Base, Alabama 2002, https://apps.dtic.mil/sti/pdfs/ADA420514. pdf (dostęp 10.05.2023); Porozumienie w sprawie stosowania środków sanitarnych i fitosanitarnych, Dz.Urz. UE L 336 z 23.12.1994; M. Prusakowski, *Bioterror. Jak nie dać się zabić*, Tower Press, Gdańsk 2001; M. Szwejkowska, W. Truszkowski, *Zagrożenie terrorystyczne w sektorze gospodarki rolnej (agroterroryzm) w aspekcie prawa międzynarodowego*, „Studia Prawnoustrojowe" 2016, t. 31; Ustawa z dnia 12 lipca 1995 r. o ochronie roślin uprawnych, Dz.U. 1995, nr 90, poz. 446; A. Zawojska, *Ekonomiczne motywy i skutki agroterroryzmu*, „Roczniki Naukowe Stowarzyszenia Ekonomistów Rolnictwa i Agrobiznesu" 2011, t. 13, nr 5; M. Żuber, *Agroterroryzm – zagrożenie sektora rolniczego*, [w:] *Katastrofy naturalne i cywilizacyjne. Terroryzm współczesny aspekty polityczne, społeczne i ekonomiczne*, M. Żuber (red.), Wyższa Szkoła Oficerska Wojsk Lądowych im. gen. T. Kościuszki, Wrocław 2006; tenże, *Broń masowego rażenia w działalności terrorystycznej*, Difin, Warszawa 2015; J. Bertrandt, *Bioterroryzm żywnościowy – realne zagrożenia użycia patogenów biologicznych w działaniach terrorystycznych*, „Lekarz Wojskowy" 2007, t. 8, nr 1.

AI FOUNDATION – przedsiębiorstwo mające siedzibę w San Francisco, założone w 2017 r. w celu tworzenia zarówno darmowych narzędzi wykorzystujących technologię sztucznej inteligencji (AI), mających na celu zwłaszcza udaremnienie negatywnych skutków jej działania, jak i produktów komercyjnych. Jak wskazują twórcy AI Foundation, misją projektu jest rozwijanie sztucznej inteligencji w służbie ludzkości, przy jednoczesnym przewidywaniu możliwego ryzyka i przeciwdziałaniu mu. AI Foundation tworzy w tym celu własne, oryginalne koncepcje, produkty i idee korzystające ze sztucznej inteligencji oraz przeciwdziała nadużyciom związanym z ich wykorzystaniem przez innych. Start-up współpracuje ze światowymi innowatorami, naukowcami, inżynierami i inwestorami zjednoczonymi wokół idei upowszechniania możliwości sztucznej inteligencji, chroniąc jednocześnie użytkowników przed niebezpieczeństwami, jakie niesie ona za sobą. AI rewolucjonizuje sposób, w jaki ludzie komunikują się ze sobą, żyją i pracują, tworzy wartość dodaną dla tych wszystkich, którzy posługują się jej zdobyczami. Jednocześnie sztuczna inteligencja przynosi wielkie niebezpieczeństwa, których specyfika zależy od tego, kto i jakie cele stawia przed

rozwojem tej technologii. Wśród nich wymienić należy uprzedzenia i manipulacje, a także utratę wspólnej obiektywnej rzeczywistości za sprawą powstawania i działania fake'owych treści. AI może również wywołać rewolucję robotów na skalę, której nie zaobserwowano od rewolucji przemysłowej. Jednocześnie podział zasobów i władzy pomiędzy korzystającymi z dobrodziejstw sztucznej inteligencji i zależnymi od niej może powodować nowe, nieznane dotąd wielkie podziały społeczne. AI stwarza poważne → z a g r o ż e n i a [t. 4], gdy używana jest do manipulowania ludźmi i wprowadzania między nimi podziałów.

Jednym z najbardziej znanych osiągnięć przedsiębiorstwa jest stwo-

rzenie produktu Reality Defender, oprogramowania powstałego w celu wykrywania potencjalnie fałszywych medialnych przekazów znajdujących się w sieci. Podobnie jak ochrona antywirusowa program skanuje każdy obraz, wideo i inne media napotkane przez użytkownika w poszukiwaniu zafałszowanej zawartości, umożliwia zgłaszanie podejrzanych treści i analizuje je za pomocą różnych technik opartych na AI, aby wykrywać przesłanki wskazujące na modyfikację lub sztuczne wygenerowanie danej treści. Reality Defender powstał w ramach współpracy AI Foundation i Human-AI, zaangażowanej we wspólne z twórcami treści prace zmierzające do stworzenia znaku Honest AI, który ma celu wyraźną identyfikację tekstów, obrazów, dźwięków i filmów wygenerowanych przy użyciu technologii sztucznej inteligencji.

Działanie programu opiera się na społeczności użytkowników zgłaszających podejrzane materiały, alarmujących o zafałszowanej zawartości i w ten sposób szkolących agentów sztucznej inteligencji. Twórcy oprogramowania wskazują, że prawie każdy obraz związany z modą w internecie jest zmodyfikowany, jednak o wiele większe zagrożenie to modyfikacja obrazów w materiałach informacyjnych dostępnych w internecie. Ważne pozostaje, jak bardzo obraz lub film zostały zmienione, dlaczego i jakie są konsekwencje tej zmiany w ogólnym kontekście danego newsa. Jednym z najważniejszych twórców Reality Defender jest dr S. Suwajanakorn, autor narzędzia, które – na podstawie odpowiednio dużej ilości danych w postaci filmów i zdjęć – może stworzyć realistyczny fałszywy film naśladujący sposób, w jaki dana osoba mówi. Program czyni to dzięki uważnej obserwacji istniejących ujęć ust i zębów danej postaci, w efekcie tworząc idealną symulację mimiki twarzy wypowiadającego się. Narzędzie to po 14 godz. analizy materiałów wideo z B. Obamą pozwoliło stworzyć algorytm umożliwiający odtworzenie jego wizerunku wypowiadającego dowolny zadany tekst.

Suwajanakorn podkreślał, że aplikacja Reality Defender, która uruchamia się automatycznie w przeglądarkach internetowych, aby wykrywać i oznaczać fałszywe zdjęcia lub filmy, pozwala na eliminację powszechnego wytwarzania wirtualnych wersji wypowiedzi niemal każdego człowieka, którego zdjęcia bądź filmy są w naszym posiadaniu. W tym kontekście można wyobrazić sobie sytuację, w której → w o j n a [t. 4] zostanie wywołana przez fałszywe wideo światowego przywódcy ogłaszającego uderzenie nuklearne. Narzędzie Reality Defender stworzone przez AI Foundation ma

na celu eliminację takich sytuacji. O ile pisanie fałszywych wiadomości może być tanie i łatwe, o tyle trudno jest manipulować nagraniami wideo, nie pozostawiając żadnych śladów ingerencji. Istnieje zatem także możliwość wyszukiwania algorytmów, które pozwalają wychwycić nienaturalność, a więc sztuczny charakter danego filmu.

Najnowszym projektem AI Foundation, który stawia sobie za cel wykorzystanie pozytywnych stron sztucznej inteligencji, jest Personal AI, czyli rodzaj specyficznych awatarów sławnych ludzi. Pierwszym z nich była cyfrowa wersja amerykańskiego pisarza, filozofa i duchowego doradcy Deepaka Chopry. Wirtualna postać Chopry może rozpoznać odbiorcę, odpowiedzieć na jego pytania, a nawet medytować z nim. Wytworzona aplikacja Digital Deepak oparta na zaawansowanej, w pełni spersonalizowanej AI, stawia sobie za zadanie pomaganie ludziom na całym świecie w osiąganiu osobistych celów związanych z samopoczuciem. Cyfrowy Deepak wygląda, mówi i zachowuje się jak światowej sławy pisarz i nauczyciel. Dzięki projektowi Digital Deepak wszyscy mogą otrzymywać spersonalizowane porady od dra Chopry, zadawać mu pytania na temat każdego aspektu dobrego samopoczucia i korzystać z medytacji w dowolnym miejscu i czasie. Sam Chopra uważa, że projekt Digital Deepak jest przyszłością dobrodziejstw wykorzystania sztucznej inteligencji i pokazuje, w jaki sposób postępy w dziedzinie AI mogą uwolnić pełny potencjał ludzkości.

W 2020 r. AI Foundation kontynuowało prace nad możliwościami stworzenia własnej Personal AI, czyli awatara swojego lub osób bliskich, czy to 5-letniego dziecka, czy to rodzica bądź dziadka. Będzie istniała możliwość stworzenia własnej cyfrowej repliki, mającej określony wygląd, potrafiącej mówić, i która będzie stale szkolona przez jej twórcę. Zdjęcie lub film wskazują twórcom awatara, jak ktoś wygląda, i jego wizerunek zostaje zatrzymany w czasie. Do filmu dodaje się również elementy tonu głosu oraz gesty. Dzięki własnemu projektowi można wrócić do momentu, gdy stworzyło się awatar, i porozmawiać z młodszym sobą. Takie osobiste wersje sztucznej inteligencji mogą być też wykorzystywane do rozrywki, nauczania lub stać się przyszłym odpowiednikiem gwiazd YouTube'a. Twórcy koncepcji awatarów znanych ludzi podają dziesiątki przykładów zastosowań nowego narzędzia. Pozwala ono zorganizować wspólne gotowanie w kuchni w towarzystwie nieżyjącej już mistrzyni sztuki kulinarnej J. Child. Nie tylko będzie ona pilnowała przestrzegania szczegółów realizacji przepisu krok po kroku, ale także może efektywnie doradzać w trakcie gotowania, a to dzięki innym elementom sztucznej inteligencji, czujnikom oraz temu, że piekarnik i inne urządzenia są połączone i mogą się ze sobą porozumiewać. Nowe rozwiązanie może w ten sposób prowadzić do radykalnego uproszczenia wielu pozornie trudnych czynności.

Osobiste awatary AI mogą dać każdemu jego własny mówiący i słuchający odpowiednik, który będzie zawsze dostępnym rozmówcą. Zdaniem prezesa AI Foundation awatary Personal AI mogą realizować cele twórcy przez tysiące lat, awatar taki będzie mógł reprezentować wartości swojego realnego odpowiednika i popierać jego dążenia

obecnie oraz w odległej przyszłości. Media osobiste wspierane przez własną sztuczną inteligencję, wg ich twórców, staną się narzędziami, które umożliwią kolejną erę zmian. Twórcy awatarów Personal AI zademonstrowali nową technologię, prezentując 3 przygotowane wcześniej awatary, wykonane przez uczestników One Young World Summit, 4-dniowej konferencji łączącej innowatorów z ponad 190 krajów ze światowymi liderami biznesu i polityki, która odbyła się w dniach 22–25 października 2019 r. w QEII Centre i Westminster Hall, w centrum Londynu. Na 3 umieszczonych obok siebie iPadach przedstawiono twarze 3 prawdziwych ludzi, których głosy i motywacje zostały wbudowane w ich „reprezentacje AI": L. Ulloi, 28-letniej Kolumbijki ocalałej z porwania, G. Hyoka Kima, 27-letniego uchodźcy i aktywisty z Korei Północnej oraz brytyjskiego miliardera i biznesmena R. Bransona. Każdy awatar przedstawił się i wyjaśnił cele swojego działania.

Szczególne wrażenie wywarł na publiczności awatar młodzieńca z Korei, który powiedział, że pracuje nad szerzeniem demokracji w swoim kraju. Twarze na iPadach były w stanie rozmawiać niezależnie od siebie, zadając sobie pytania i słuchając odpowiedzi.

AI Foundation ma rozbudowaną strukturę, na którą składają się liderzy, partnerzy inwestycyjni, Globalna Rada ds. Sztucznej Inteligencji i Rada ds. Działalności Non Profit.

Jakub Idzik, Rafał Klepka

AIFoundation.com (dostęp 17.01.2020); CIO Bulletin, *Google Engineer Designs a Tool to Discern Fake Video and Images*, 13.04.2018, CIOBulletin.com (dostęp 17.01.2020); L. Floridi, *Artificial Intelligence, Deepfakes and a Future of Ectypes*, „Philosophy & Technology" 2018, vol. 31, iss. 3; J. Idzik, R. Klepka, *AI Foundation*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; P. Korshunov, S. Marcel, *DeepFakes: A New Threat to Face Recognition? Assessment and Detection*, 20.12.2018, ArXiv.org (dostęp 17.01.2020); The Star, *Lying Eyes: Google Engineer Developing Tool to Spot Fake Video*, 13.04.2018, TheStar.com.my (dostęp 25.03.2019).

AL-DŻAZIRA – satelitarna stacja telewizyjna założona w 1996 r. Stała się najpopularniejszą telewizyjną siecią informacyjną w świecie arabskim i cieszy się znakomitą renomą. Kanał ten jest powszechnie uznawany za przełomowy w historii telewizji arabskiej poprzez wprowadzenie liberalnego modelu telewizji, który jest w dużej mierze wolny od kontroli rządu w arabskim środowisku medialnym. Sieć została założona przez władcę Kataru, emira Al-Thaniego, który zatrudnił dużą liczbę dziennikarzy z zamkniętego w tym samym roku arabskiego serwisu BBC. Kiedy nowy emir Kataru zakładał Al-Dżazirę, miał nadzieję, że telewizyjna sieć informacyjna poprawi pozycję jego kraju w Zatoce Perskiej, ale nie spodziewał się najprawdopodobniej, że zapoczątkował proces nowego sposobu komunikowania medialnego w świecie arabskim. „Arabska CNN", jak często nazywa się Al-Dżazirę, miała na celu połączenie

amerykańskich formatów wiadomości i programów politycznych z etyką dziennikarstwa BBC dotyczącą neutralności i obiektywności podczas realizacji arabskiego programu informacyjnego.

W pierwszych latach istnienia Al-Dżazira zdobyła ok. 40 międzynarodowych nagród od organizacji takich jak Index on Censorship (Indeks Cenzury). Tym, co sprawiło, że sieć była tak atrakcyjna zarówno dla arabskich widzów, jak i dla międzynarodowych obserwatorów, było częste przełamywanie przez kanał tabu społecznego i politycznego. Tematy takie jak obrzezanie kobiet, → r e ż i m [t. 3] syryjski lub konflikt na Saharze Zachodniej były jednymi z wielu problemów, które Al-Dżazira omawiała przez lata, a o których żadna inna arabska stacja telewizyjna nigdy nie wspomniała. W talk-show takich jak „The Opposite Direction" z moderatorem Faisalem al-Kasimem, programie opartym na modelu „Crossfire", przeciwnicy z różnych obozów ideologicznych, przedstawiciele rządów i sił opozycyjnych bezpośrednio konfrontowali swoje punkty widzenia. Al-Dżazira ożywiła ideę wolności słowa w świecie arabskim.

Sieć jest krytykowana przez prawie wszystkie reżimy arabskie, w większości autorytarne z natury, które obawiają się utraty monopolu telewizyjnego. Wiele biur sieci w krajach arabskich było wielokrotnie zamykanych.

Arabska Unia Nadawców (Arab States Broadcasting Union, ASBU) odmówiła Al-Dżazirze regularnego członkostwa, a wielu reklamodawców bliskich reżimom arabskim z Arabii Saudyjskiej i innych krajów bojkotowało sieć. Rządy zrozumiały jednak również, że taka presja sprawiła, że sieć stała się jeszcze bardziej popularna jako prawdziwy głos świata arabskiego. Chociaż istnieje niewiele wiarygodnych danych, a badania koncentrujące się na wzorcach korzystania z mediów przez widzów stacji są wciąż niedostateczne, Al-Dżazira jest powszechnie uważana za wiodącą sieć informacyjną w świecie arabskim z liczbą regularnych widzów na poziomie od 35 do 45 mln, którzy odbierają kanał przez Arabsat i inne satelity. Pod względem finansowym i organizacyjnym Al-Dżazira jest hybrydą, która nie pasuje do żadnej ze standardowych zachodnich kategorii nadawców państwowych, publicznych ani prywatnych. Bez ochrony i zaangażowania finansowego emira Kataru Al-Dżazira nie istniałaby. Jednak kanał uważa się za niezależny, wpływ na niego ma wyłącznie arabska → o p i n i a p u b l i c z n a [t. 3]. Jest również „prywatny" w tym sensie, że wydaje się, że nie podlega żadnym instytucjonalnym mechanizmom kontroli i równowagi. Co więcej, dotacje państwowe nie są gwarantowane na czas nieokreślony, a sieć często deklarowała potrzebę niezależności handlowej.

Sytuacja finansowa i organizacyjna Al-Dżaziry pozostaje niestabilna i jest podatna na → z a g r o ż e n i a [t. 4].

Bez wiążących ram prawnych kanał mógłby zostać zamknięty z dnia na dzień, chociaż jest to dość mało prawdopodobne, ponieważ wizerunek Kataru ogromnie zyskał dzięki pozycji Al-Dżaziry na całym świecie. Niemniej jednak trudno sobie wyobrazić,

w jaki sposób sieć może zostać przekształcona w zadowalający model telewizji publicznej bez uprzedniej demokratyzacji systemu politycznego Kataru. Państwo może zakazać jakiegokolwiek relacjonowania polityki wewnętrznej Kataru, a naturalny sojusznik sieci, jej widzowie, wymaga ścisłego ukierunkowania stacji na arabską kulturę polityczną – tendencji, którą wielu krytykowało jako prowadzącą do nieobiektywnego nastawienia w relacjonowaniu polityki.

Mówić można o kilku etapach rozwoju stacji. W latach 1996–2001 dominowało otwarcie demokratycznej debaty łamiące dotychczasowe tabu w zakresie sposobu prezentacji polityki w arabskich mediach. Po raz pierwszy w telewizji arabskiej można było usłyszeć izraelskie głosy uzasadniające działania rządu Izraela wobec Palestyńczyków. Po wybuchu drugiej intifady na okupowanych terytoriach w 2000 r., po wydarzeniach z 11 września 2001 r. i amerykańskiej interwencji w Afganistanie dominował stronniczy sposób budowania relacji wymierzony przeciwko Izraelowi i USA. Całodniowa relacja z pochówku szejka Yassina z palestyńskiej organizacji islamistycznej Hamas, regularne pokazy wiodących islamistycznych kaznodziejów takich jak Jusuf Karadawi z jego kontrowersyjnym poparciem dla palestyńskich zamachowców samobójców oraz częste nadawanie filmów z Al-Kaidy ukazujących wiadomości Osamy bin Ladena i innych przyniosły telewizji negatywne oceny jako światowemu głosowi → t e r r o r y z m u i s l a m s k i e g o [t. 4], chociaż zachodnie kanały nierzadko kupowały takie materiały od Al-Dżaziry.

Al-Dżazira obszernie relacjonowała oznaki demokratycznego przebudzenia w świecie arabskim długimi doniesieniami o opozycyjnym ruchu Kefaja w Egipcie lub libańskim powszechnym oporze przeciwko okupacji syryjskiej. Relacje polityczne Al-Dżaziry stanowią połączenie profesjonalnej neutralności dziennikarskiej i zorientowanego na konsumentów populizmu w czasach → k r y z y s u [t. 2], który wydaje się porównywalny ze stylem dużych sieci telewizyjnych w USA. Al-Dżazira zawarła szereg umów o współpracy z CNN, ABC, NBC, Fox i wieloma innymi sieciami zachodnimi w zakresie wymiany programów. W praktyce jednak taka wymiana niejednokrotnie ogranicza się do kwestii materiałów dotyczących terroryzmu, obrazów i filmów wideo, nie zaś treści wiadomości, które mogłyby pomóc zachodniej widowni zrozumieć arabskie poglądy na wydarzenia światowe.

Nie ulega wątpliwości, że niewiele zjawisk w świecie arabskim jest bardziej intrygujących niż sukces Al-Dżaziry. 24-godzinny panarabski satelitarny kanał informacyjny wg raportu z 2002 r. na temat komunikacji na Bliskim Wschodzie opublikowanego przez Spotbeam Communications podkreśla, że Al-Dżazira zajmuje centralne miejsce w modernizacji nadawania w języku arabskim. Sieć nie tylko pozostawiła trwały ślad w nadawaniu w świecie arabskim, ale ma ogromny potencjał w zakresie wywierania wpływu na arabską opinię publiczną i arabską politykę. Jednocześnie Al-Dżazira jest bardzo kontrowersyjna i zarówno w świecie arabskim, jak i poza nim przyjmowana bywa niezwykle sceptycznie.

W oficjalnych kręgach arabskich Al-Dżazira uważana jest za ważne medium zdolne do wywoływania kryzysów dyplomatycznych. Na tym tle mówi się często o istnieniu efektu Al-Dżaziry, który stanowiłby odpowiednik efektu CNN, tłumaczącego siłę oddziaływania mediów na opinię publiczną i polityków w zachodnim świecie. Niewątpliwie istnienie tego rodzaju oddziaływań wynika z siły mediów, w szczególności 24-godzinnych telewizyjnych programów informacyjnych nadających „prawdę przez całą dobę".

Al-Dżazira była jedynym kanałem relacjonującym → w o j n ę [t. 4] na żywo po 11 września, w tym najważniejsze wydarzenia z okresu → i n w a z j i [t. 2] na Afganistan. Podobnie jak w przypadku efektu CNN efekt Al-Dżaziry dotyczy nie tylko tego konkretnego medium, ale szerokiej gamy organizacji medialnych na Bliskim Wschodzie, w tym głównego konkurenta Al-Dżaziry, telewizji Al-Arabija z Dubaju. Efekt Al-Dżaziry przekształca sposób myślenia o świecie poprzez zwiększenie obecności i siły islamskiego sposobu myślenia o rzeczywistości. Wielu badaczy stawia przed stacjami takimi jak Al-Dżazira, Al Arabija i innymi sieciami medialnymi ambitne zadania, mają one zmienić relacje między arabską publicznością medialną a rządami, niszcząc monopole państwowe w zakresie masowej komunikacji i dając nowe możliwości wyboru odbiorcom. Przedefiniowują one region i jego relacje z Zachodem, projektując idee świata arabskiego poza Bliskim Wschodem.

Choć podkreśla się, że Al-Dżazira jest telewizją arabską, to jednym z najtrudniejszych wyzwań, jakie stoją przed nią, pozostaje reprezentowanie głosu tej części świata i jednoczesne poszanowanie zasad dziennikarskiego pluralizmu i bezstronności. Wydaje się to zadaniem niezwykle karkołomnym. Przeciwnicy z Zachodu zawsze uznają Al-Dżazirę za tubę propagandową (zob. → p r o p a g a n d a [t. 3]) świata arabskiego, a rządy państw arabskich za stację, która nie sprzyja interesom regionu. Szczególnie istotna w swoistej walce obrazów pozostaje rola, jaką Al-Dżazira odegrała, prezentując z wielką siłą przekazy, które nie odpowiadały konwencjonalnym wyobrażeniom dominującej zachodniej interpretacji politycznej. Od 2001 r. stacja regularnie emitowała nagrania wideo z udziałem islamskich bojowników i Osamy bin Ladena, które były pokazywane na całym świecie przez inne sieci, stając się częścią debaty na temat „wojny z terroryzmem". Kanał ten rzucił wyzwanie tradycyjnemu pojęciu bezstronności zdefiniowanemu przez środowiska dziennikarskie, które reprezentują świat z perspektywy amerykańskiej lub eurocentrycznej, pokazując głosy i przedstawicieli świata arabskiego, w dużej mierze niewidocznych dla widowni medialnej w sieciach zachodnich. Ze względu na dążenie do prezentacji wielości głosów i opinii Al-Dżazira doświadczyła wrogości zarówno ze strony rządów zachodnich, jak i arabskich, ale to właśnie krytyka amerykańska była najsilniejsza.

Relacje Al-Dżaziry z wojny w Iraku w 2003 r., oskarżanej przez wielu o antyamerykańskie uprzedzenia, pokazywały obrazy ofiar cywilnych i okrucieństw, które były zauważalne mimo ich nieobecności w CNN. Al-Dżazira miała w Iraku

5 korespondentów, z których 2 było ulokowanych wraz z → ż o ł n i e r z a m i [t. 4] USA. W swoich relacjach stacja podkreślała, że dołożyła znacznych starań, aby być bezstronną. M. Massing, który nie przebywał w Iraku jako reporter, ale by monitorować → b e z p i e c z e ń s t w o dziennikarzy dla Komitetu Ochrony Dziennikarzy (Committee to Protect Journalists), powiedział, że nie było tajemnicą, że wojsko amerykańskie jest niezadowolone z Al-Dżaziry, szczególnie z uwagi na nacisk w relacjach tej stacji na ofiary cywilne. W trosce o bezpieczeństwo personelu Al-Dżazira przekazała Pentagonowi współrzędne swojego biura w Bagdadzie z prośbą o to, aby nie było atakowane. Mimo to atak nastąpił, odnotowano ofiary śmiertelne, podobnie jak w przypadku biura w Kabulu podczas wojny w Afganistanie. Pomimo amerykańskich przeprosin i zastrzeżeń wielu obserwatorów nie było całkowicie przekonanych co do tego, że którekolwiek z bombardowań było czysto przypadkowe. Al-Dżazira twierdziła również, że od czasu do czasu sabotowano jej strony internetowe, zastępując je proamerykańskimi materiałami. Rzecznicy sieci nie oskarżali sabotażystów o przynależność do którejś ze stron konfliktu, ale twierdzili, że → h a k e r z y [t. 2] potrzebowaliby do tego znacznego finansowania i wiedzy technicznej.

W programach informacyjnych Al-Dżaziry szczególną uwagę zwraca inny niż w stacjach zachodnich stosunek do tożsamości ofiar oraz skali okrucieństwa wojennego, jakie można pokazywać w mediach. Taśma Al-Dżaziry z uwięzionymi amerykańskimi żołnierzami przesłuchiwanymi przez Irakijczyków była dostępna dla amerykańskich dziennikarzy, ale większość z nich odstąpiła od jej wykorzystania na prośbę Pentagonu o wstrzymanie transmisji ze względu na krewnych, którzy nie są jeszcze świadomi tego, co stało się z ich bliskimi. Ze swojej strony Al-Dżazira uzasadniła wykorzystanie materiału, mówiąc, że konwencja genewska zakazuje pokazywania zdjęć jeńców wojennych tylko rządom, a nie prywatnym mediom. Zbyt wyraźne nagrania ofiar, nawet podczas katastrof niezwiązanych z wojnami, zwykle nie są pokazywane w amerykańskiej telewizji ani w ogólnokrajowych mediach drukowanych. Al-Dżazira postępuje w tym zakresie inaczej, bez oporu publikując obrazy rzezi, krwi i wnętrzności ludzkich, których prezentacja byłaby niedopuszczalna w stacjach zachodnich.

Jakub Idzik, Rafał Klepka

C. Cassara, *Al-Jazeera Remaps Global News Flows*, [w:] *The Handbook of Media and Mass Communication Theory*, R.S. Fortner, P.M. Fackler (eds.), Wiley, Chichester 2014; S. Cherribi, *From Baghdad to Paris: Al-Jazeera and the Veil*, „Harvard International Journal of Press/Politics" 2006, vol. 11, iss. 2; K. Hafez, *Al-Jazeera Television*, [w:] *Encyclopedia of Political Communication*, L.L. Kaid, Ch. Holtz-Bacha (eds.), Sage, Los Angeles 2008; J. Idzik, R. Klepka, *Medialne relacje wojenne*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; K. Rinnawi, *Instant Nationalism: McArabism, Al-Jazeera, and Transnational Media in the Arab World*, University Press of America, Lanham 2006; T. Samuel-Azran, *Al-Jazeera and US War Coverage*, Peter Lang, New York 2010; P. Seib, *The Al-Jazeera Effect: How the New Global Media Are Reshaping World Politics*, Potomac Books, Washington 2008; *The Al Jazeera Phenomenon: Critical Perspectives on New Arab Media*, M. Zayani (ed.), Pluto Press, London 2005; W.L.

Youmans, *Al-Jazeera Effect*, [w:] *Encyclopedia of Social Media and Politics*, K. Harvey (ed.), Sage, Los Angeles 2011.

AL-KAIDA – globalna sunnicka islamistyczna (→ i s l a m i z m [t. 2]) grupa terrorystyczna, organizacja wywodząca się z nurtu Bractwa Muzułmańskiego, założonego w 1928 r. w Egipcie. Była to organizacja postulującakonieczność reformy islamu poprzez powrót do jego źródeł, odrzucenieobcych kulturowo wpływów i literalną egzegezę Koranu oraz Sunny. Ten nurt w islamie nazwano salafizmem i uważa się za przykład → f u n d a m e n t a l i z m u r e l i g i j n e g o [t. 2]. Kolejnymi postulatami była walkaz kolonializmem Zachodu i Żydów, chęć utworzenia państwa rządzącego się prawami religijnymi (szariat) oraz odrzucenie → i d e o l o g i i liberalizmu i przede wszystkim → k o m u n i z m u [t. 2]. Bractwo Muzułmańskie nie było grupą jednolitą: różne odłamy powstawały zwłaszcza w okresie prześladowań ze strony władz Egiptu. Szybko uformował się radykalnyruch uważający → p r z e m o c [t. 3] w imię religii – → d ż i h a d [t. 2] – za uprawnioną metodę pokonania wrogów i ustanowienia władzy szariatu.Za głównego ideologa tej formacji uważa się Sajjida Kutbę.

Po objęciu władzy w Egipcie przez Anwara as-Sadata Bracia Muzułmanie przejęli kontrolę nad uniwersytetem Al-Azhar, a sama organizacja została przywrócona do legalności. USA były zainteresowane wykorzystaniem ruchów fundamentalistycznych dla zabezpieczenia przed wpływami komunistycznymi. Salafici nie zaakceptowali porozumienia w Camp David (1978) i przeprowadzili zamach na prezydenta Egiptu (6 października 1981). Miał go przeprowadzić tzw. Egipski Dżihad (*Tanzim al-Jihad*) kierowany przez Chaida Ahmada Szaukiego al-Istambulego. Efektem stały się liczne aresztowania i – ostatecznie – zdelegalizowanie Bractwa oraz wygnaniejego członków. Część wybrała Europę, inni migrowali przede wszystkim do państw Zatoki Perskiej, a jeszcze inni – do Afganistanu. Mniejwięcej w tym samym czasie Bractwo Muzułmańskie poniosło kolejną porażkę, jaką było nieudane powstanie w Syrii, zakończone pacyfikacją miasta Hama (luty 1982). Miejscem, w którym jego członkowie znaleźli schronienie, okazał się Afganistan: tam przechodzili do walki z najeźdźcą świętej ziemi islamu (*dar al-islam*), czyli ZSRR. Tę akcję wspierały służby przynajmniej kilku państw: USA (osłabiało to ZSRR), Arabii Saudyjskiej(przejęcie inicjatywy w świecie islamu po sukcesie rewolucji islamskiejw Iranie, propagowanie swojej wizji tej religii – wahhabizmu), Pakistanu (osłabienie ZSRR – sojusznika Indii, zabezpieczenie swoich interesów, w tym integralności terytorialnej).

Wśród emigrantów było wielu prominentnych działaczy islamistycznych w tym – Abd Allah Yusuf Azzam, Jordańczyk, wykładowcaz Al-Azhar, nazywany ojcem światowego dżihadu. To on, w myśl ideologii Taqia ad-Din Ahmada Ibn Tajmijji i Sajida Kutby czy Muhammada Abd as-Salam Faradż'a czy Syeda Abula a'la al-Maududiego, wezwał muzułmanów z całego świata do dżihadu. W Afganistanie poznał 2 innych emigrantów: Ajmana az-Zawahiriego, egipskiego lekarza, oraz Usamę ibn Ladina

(znanego jako Osama bin Laden). Pierwszy urodził się w Kairze w 1951 r., pochodził ze znakomitej arabskiej rodzinny, acz już zubożałej. Ze strony matki wywodził się z klanu Al-Azzam (podobno pochodzącej od Proroka, nie był jednak spokrewniony z Abd Yusufem Azzamem), również z Półwyspu Arabskiego. Z egipskiej gałęzi jej rodu wywodził się dziadek Ajmana – Azzam Bej, dwukrotny ambasador Egiptu w Arabii Saudyjskiej, założyciel uniwersytetu w Rijadzie. Azzam Pasza (Abd al-Wahhab Azzam), jego brat, był posłem za czasów Faruka I, króla Egiptu, a później – ambasadorem Egiptu w Arabii Saudyjskiej. Był też pierwszym sekretarzem Ligi Państw Arabskich w latach 1945–1952. Ponadto wydał swoją córkę (kuzynkę matki Ajmana) za księcia Muhammada, najstarszego syna króla Fajsala, założyciela Banku Fajsala, działającego zgodnie z zasadami islamu. Az-Zawahiri zradykalizował się podczas studiów w Kairze, podobno bywał w rodzinnym domu Sajjida Kutby. Po aresztowaniach członków Bractwa Muzułmańskiego i on znalazł się w więzieniu, gdzie go torturowano. Po opuszczeniu więzienia zaangażował się w Czerwonym Półksiężycu i wyjechał do Afganistanu.

Usama ibn Ladin (Usama ibn Mohammed ibn Awad ibn Ladin) nie musiał emigrować. Urodził się w jednej z najbogatszych rodzin Arabii Saudyjskiej, był jednym z 54 dzieci Muhammada ibn Ladina, pochodzącego z Jemenu założyciela Saudi Binladin Group – firmy, której głównym polem działania było budownictwo. Ibn Ladin studiował ekonomięi zarządzanie na King Abdulaziz University w Dżuddzie, tam poznał Muhammada Kutbę – brata Sajjida Kutby. Nie jest do końca jasne, jaksyn tak bogatego ojca postanowił porzucić wygody dostatniego życia i wyjechać, ale faktem jest, że wyjechał do Afganistanu, gdzie poznał Abd Azzama. Razem w 1984 r. założyli Maktab al-Chidamat, znane również jako Maktab al-Chadamat al-Mudżahidin al-'Arab (MAK) lub „Biuro".

Ibn Ladin był pod silnym wpływem Azzama, jego intelektu i zdolności organizacyjnych. „Biuro" szybko zaczęło swoją agitację wśród muzułmanów, zarówno na Bliskim Wschodzie, jak i w USA. Azzam osobiście jeździł po świecie, w 1984 r. odbył serię spotkań na uniwersytetach amerykańskich, udało się otworzyć kilka biur rekrutacyjnych m.in. w Michigan, Georgii, na Florydzie, w Kalifornii, Teksasie, Nowym Meksyku, Arizonie, New Jersey i Tennessee. Główna siedziba mieściła się na Brooklynie (552 Atlantic Avenue), gdzie rezydował Omar Abdul Rahman, zwany z racji swej ułomności Ślepym Szejkiem. Komórki działały ponadto w Bostonie, Atlancie i Chicago.

Ibn Ladin chciał sformować własną jednostkę składającą się wyłącznie z Arabów (tzw. Afgańscy Arabowie), Azzam, który uważał, że Arabowie są zbyt nieliczną grupą, i wolałby, aby wchodzili w skład jednostek afgańskich, w których pełniliby funkcje wychowawcze, ale możeteż i wywiadowcze. Była to różnica wynikająca z celów obu przywódców. Ibn Ladin traktował Afganistan za jedynie wstępny etap czegoś większego – do muzułmańskiej rewolucji, która miała się odbyć dzięki awangardzie. To przekonanie wynikało wprost z kutbyzmu, natomiast Azzam raczej koncentrował

się na sytuacji bieżącej. Nie bez znaczenia było też pojawienie się nowego człowieka: az-Zawahiriego. Ten nie był specjalnie zainteresowany Afganistanem, znalazł się tu raczej przypadkiem. Jego celem był Egipt – i wyzwolenie go spod → r e ż i m u [t. 3] Husniego Mubaraka. Rozbrat między ibn Ladinem a Azzamem zaczął się w 1986 r., na 1988 r. datuje się powstanie samodzielnej organizacji ibn Ladina. Fundamentem stała się jednostka arabska powstała w bazie Dżihad Wel al-Farouq. To jedna z wersji pochodzenia nazwy Al-Kaidy. Druga, bardziej prawdopodobna, to odwołanie do koncepcji awangardy rewolucji skonturowanej przez Kutbę, a przypomnianej na łamach „Al-Dżihad" przez samego Azzama: „Awangarda niesie sztandar dzień za dniem, i trudną drogą, dopóki nie dojdzie do celu. Awangarda tworzy solidną bazę (*al-kaida as sulba*) dla przyszłego społeczeństwa".

Azzam zginął w wyniku zamachu terrorystycznego. Trudno powiedzieć, kto był tegoż autorem – na ogół wymienia się izraelski Mosad, wydaje się, że jednak najbardziej zainteresowani byli sami muzułmanie. Wycofanie się ZSRR z Afganistanu (15 lutego 1989 r.) pokazało tak naprawdę olbrzymie podziały i rywalizację. Dla samych Arabów dłuższe przebywanie w tym rejonie było już bezcelowe. Ibn Ladin znalazł schronienie w Sudanie, az-Zawahiri pozostał z nim w dobrych relacjach, ale nadal to Egipt był dla niego priorytetem, dlatego dalej stał na czele swojej organizacji, czyli Egipskiego Islamskiego Dżihadu (ew. *Tanzim al-Jihad*) – to on zreformował organizację i nadał jej struktury, a potem ten wzór zaadaptowała Al-Kaida. Jednak oficjalnie najważniejsza w EID była Rada Dziewięciu Imamów (*Madżlis asz-Szura*), z siedzibą w Afganistanie. Ponadto funkcjonowała Rada Operacyjna, dzieląca się na liczne komitety: Wewnętrznej Organizacji Cywilnej (odpowiedzialny za monitorowanie sytuacji w Egipcie), do spraw Dokumentacji (logistyka), Komitet Finansowy, Komitet Szariatu oraz Komitet Mediów. Rada miała lokalne filie w wielu państwach: od Albanii, przez Kenię, do USA. Co bardzo istotne, ta struktura była potem kopiowana – funkcjonowała zarówno w Al-Kaidzie, jak i w jej tzw. franczyzach. Ich wspólnymi dziełami były fatwy: *Wojna przeciwko Amerykanom okupującym Ziemię Dwóch Świętych Miejsc* (1996 r.) oraz *Dżihad przeciwko Żydom i krzyżowcom* (1998 r.). Na tej bazie ideologicznej powołano w 1998 r. Światowy Islamski Front Przeciwko Żydom i Krzyżowcom, co stało się tak naprawdę platformą do połączenia Al-Kaidy z innymi organizacjami, a zwłaszcza z Tanzimem, z którego ok. 2000 r. oficjalnie odszedł az-Zawahiri.

Pierwszy poważny atak Al-Kaidy przeprowadzono w Nowym Jorku w 1993 r. – zdetonowano bomby w podziemiach kompleksu World Trade Center. W 2. poł. lat 90. Al-Kaida skupiła się na atakowaniu celów w Arabii Saudyjskiej (1996 r.: zginęło 19 amerykańskich żołnierzy) oraz w Afryce (1998 r.: zamach na amerykańskie ambasady w Nairobi, stolicy Kenii, i w Dar es Salam, w Tanzanii). W odwecie Amerykanie przeprowadzili serię ataków lotniczych na bazy Al-Kaidy w Sudanie i Afganistanie. Zmusili też władze w Chartumie do wydalenia ibn Ladina (koniec tzw. okresu

wygnania sudańskiego i przejście do współpracy z afgańskimi talibami). W 2000 r. zaatakowano amerykański niszczyciel USS „Cole" w Jemenie. Wreszcie – 11 września 2001 r. zniszczono wieżowce World Trade Center i zaatakowano budynek Pentagonu w Waszyngtonie. Dodatkowym czynnikiem wzmacniającym pozycję ibn Ladina była sytuacja w Palestynie – druga Intifada, zwana też Intifadą Al-Aksa. W jej rezultacie na znaczeniu straciła Organizacja Wyzwolenia Palestyny, a swoje pozycje wzmocnili islamiści. Nie bez znaczenia były też wybory w USA, gdzie władzę utracili Demokraci, którzy mocno wspierali OWP w negocjacjach z Izraelem, a nowa administracja zmieniła politykę na Bliskim Wschodzie. Wszystko to ostatecznie spowodowało interwencje zbrojne USA i sojuszników w Afganistanie (2001 r.) i w Iraku (2003 r.).

Mocne uderzenie w Al-Kaidę spowodowało zmianę struktury z budowanej organizacji o silnym przywództwie na formę rozproszoną, często nazywaną nawet systemem franczyzowym. Al-Kaida dawała „brand" i ideologię, a lokalne organizacje w dużej mierze działały samodzielnie. Taka filia powstała też w Iraku, a jej założycielem był Abu Musab az-Zarkawi. Z czasem ewaluowała ona do Państwa Islamskiego w Iraku i Syrii (ISIS) i wreszcie do → P a ń s t w a I s l a m s k i e g o [t. 3].

Po zdobyciu Afganistanu przez siły koalicyjne Al-Kaida w dużej mierze utraciła zdolności operacyjne. Usama ibn Ladin i Ajman az-Zawahiri pełnili, wraz z Radą Szury, funkcje bardziej ideologiczne, a działania operacyjne podejmowały poszczególne jej filie czy organizacje uznające zwierzchność Rady Szury i jej liderów.

Najważniejsze z nich to: Al-Kaida Islamskiego Magrebu (AQIM), Al-Kaida Półwyspu Arabskiego (AQAP, ewentualnie Ansar asz-Szaria), Asz-Szabab, czyli Ruch Młodych Bojowników Świętej Wojny (w skrócie: „Młodzi") czy Boko Haram (→ t e r r o r y z m i s l a m s k i [t. 4]). Po sukcesach ISIS większość organizacji uznających zwierzchnictwo Al-Kaidy złożyła przysięgę wierności (*baia*) kalifowi Państwa Islamskiego.

Po tym jak 1 maja 2011 r. prezydent USA Barack Obama ogłosił, że Usama ibn Ladin został zabity w wyniku operacji specjalnej wojsk amerykańskich, oficjalnie przywódcą Al-Kaidy samodzielnie Ajman az-Zawahiri. Tyle że jego pozycja słabła: najlepszym tego przykładem stała się jego bezsilność w zażegnywaniu podziałów islamistów w Syrii – ostatecznie powstał Dżabath an-Nusra, uznający zwierzchność Al-Kaidy i samodzielne ISIS. Po 2015 r. Al-Kaida firmowała żadnego większego zamachu terrorystycznego na Zachodzie. Najbardziej znanymi agitatorami takich ponownych ataków byli Hamza ibn Ladin (syn Usamy) oraz lider AQAP – Kassim ar-Rimi. W 2020 r. pojawiały się pogłoski o śmierci Ajmana az-Zawahiriego.

Al-Kaida jest uważana za pierwszą globalną organizację terrorystyczną nowego typu. Przyczyn jej sukcesów należy szukać w specyficznej strukturze sieciowej. Sami jej zwolennicy często tłumaczą, że Al-Kaida to bardziej ideologia niż organizacja. Kolejnym *novum* stało się wypracowanie metod samofinansowania: była ona dużo mniej uzależniona od darczyńców, zwłaszcza państwowych. Wreszcie – wytworzyła cały

szereg sił i środków komunikacyjnych, tworzyła własne portale internetowe, czasopisma, kanały komunikacyjne itd. (→ d ż i h a d m e d i a l n y [t. 2]). Jej sukcesy często przypisuje się współpracy z → w y w i a d a m i [t. 4] różnych państw: trudno mieć co do tego wątpliwości w odniesieniu do lat 80. XX w., ale okres po 1989 r. okazuje się co najmniej dyskusyjny. Niemniej wymienia się w tym kontekście służby USA, Arabii Saudyjskiej, Kataru, Rosji czy Pakistanu.

Przemysław Mazur

P.L. Bergen, *Osama Bin Laden. Portret z bliska*, tłum. B. Malarecka, Państwowy Instytut Wydawniczy, Warszawa 2007; R. Coury, *„Arabian Ethnicity" and Arab Nationalism. The Case of Abd al-Rahman Azzam*, „Journal of the American Research Center in Egypt" 1998, vol. 25; R. Jacquard, *Osama bin Laden. Tajne akta terrorysty najbardziej poszukiwanego na świecie*, tłum. zespół, Karto Technika2000, Katowice 2001; G. Kepel, *Fitna. Wojna w sercu islamu*, tłum. K. Pachniak, Wydawnictwo Akademickie Dialog, Warszawa 2006; S. Kosmynka, *Od Boga do terroru. Rola religii w ideologii dżihadyzmu na przykładzie organizacji Al-Kaidy*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2012; A.C. Larroque, *Geopolityka fundamentalistów muzułmańskich*, tłum. K. Sztyler, Dialog, Warszawa 2015; B. Lia, *Al-Qaida's Appeal Understanding its Unique Selling Points*, „Perspectives on Terrorism" 2008, vol. 2, iss. 8; T.W. Lippman, *Hero of the Crossing How Anwar Sadat and the 1973 War Changed the World*, Nebraska Potomac Books, Lincoln 2016; P. Mazur, O. Wasiuta, S. Wasiuta, *Państwo Islamskie ISIS. Nowa twarz ekstremizmu*, Difin, Warszawa 2018; N. Raphaeli, *Ayman Muhammad Rabi' Al-Zawahiri: The Making of an Arch-Terrorist*, „Terrorism and Political Violence" 2010, vol. 14, iss. 4; M. Sageman, *Sieci terroru*, tłum. M. Król, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2008; *Vademecum Bezpieczeństwa*, O.Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; A. Wejkszner, *Globalna sieć Al-Kaidy.Nowe państwo islamskie?*, Difin, Warszawa 2017; J. Zdanowski, *Współczesna muzułmańska myśl społeczno-polityczna. Nurt Braci Muzułmanów*, Wydawnictwo Naukowe ASKON, Warszawa 2009.

ALKOHOLIZM. Jak donosi →Ś w i a t o w a O r g a n i z a c j a Z d r o w i a [t. 4], na całym świecie corocznie z powodów związanych z nadużywaniem alkoholu umiera ok. 3 mln osób, co stanowi ponad 5% spośród wszystkich zgonów, a dodatkowo jest przyczyną licznych chorób i urazów. Regionem, w którym pije się najwięcej alkoholu, jest Europa. Dotyczy to większości mieszkańców tego kontynentu, tylko 15% z nich to abstynenci. W tej drugiej, mniej licznej, grupie przeważają osoby o niższym statusie społeczno-ekonomicznym, ale równocześnie to wśród nich występuje większe prawdopodobieństwo nadużywania alkoholu i uzależnienia od niego. Szacuje się, że 23 mln Europejczyków jest uzależnionych od alkoholu, co stanowi 5% mężczyzn i 1% kobiet (należy zaznaczyć, że we wszystkich badanych kulturach przedstawiciele płci męskiej piją częściej i więcej niż kobiety). Nieco rzadziej niż pozostali upijają się mieszkańcy południowej Europy, ale najniższe wskaźniki ma w tym względzie Szwecja. Średnie spożycie czystego alkoholu na dorosłego mieszkańca Unii Europejskiej wynosi ok. 11 litrów, Polska zazwyczaj plasuje się nieco poniżej tej średniej. Najwięcej konsumuje się piwa, następnie wina, najmniej – napojów spirytusowych.

W Polsce większość konsumentów alkoholu spożywa go w sposób niepowodujący negatywnych konsekwencji dla nich i dla osób z ich otoczenia. Kilkanaście procent

dorosłych Polaków pije jednak alkohol problemowo, w tym ponad 2 mln osób robi to ryzykownie (picie nadmiernych ilości jednorazowo i łącznie w określonym czasie) lub szkodliwie (jeszcze niewystępuje uzależnienie, ale picie powoduje szkody zdrowotne, psychologiczne i społeczne), a ok. 900 tys. Polaków jest uzależnionych.

Niektórzy eksperci nalegają, by w odniesieniu do omawianego zagadnienia stosować szerszą terminologię, związaną z używaniem substancji psychoaktywnych. Argumentują, że alkohol jest jedną z nich, a ponadto pojęcie to nawiązuje do koncepcji diagnozy medycznej zaburzeń używania alkoholu (ang. *alcohol use disorder*). Jednocześnie dopuszczają używanie synonimów o neutralnej wymowie, jak spożywanie, konsumpcja oraz picie alkoholu. Warto podkreślić, że osoby używające alkoholu często wielokrotnie przemieszczają się na kontinuum od abstynencji przez picie o niskim poziomie ryzyka i ryzykowne używanie alkoholu do spożywania go w sposób szkodliwy oraz prowadzący do uzależnienia. Sugeruje się również, by terminem „uzależnienie od alkoholu" zastąpić pojęcia „alkoholizm" czy „choroba alkoholowa", ewentualnie można również stosować określenie „zaburzenia używania alkoholu", jednak jest to szersze pojęcie, zawierające zarówno szkodliwe używanie, jak i uzależnienie. Niektórzy badacze proponują też rezygnację z etykietujących w ich odczuciu określeń związanych z bliskimi osoby borykającej się z nałogiem, jak koalkoholizm, współuzależnienie, syndrom dorosłych dzieci alkoholików, dlatego postulują używanie sformułowania „wsparcie terapeutyczne oferowane bliskim osób z uzależnieniem".

W rozważaniach dotyczących zaburzeń psychicznych wyróżnia się 2 główne systemy klasyfikacyjne: DSM Amerykańskiego Towarzystwa Psychiatrycznego (Diagnostic and Statistical Manual of Mental Disorders) oraz popularniejsze w większości krajów Europy kryteria ICD Międzynarodowej Statystycznej Klasyfikacji Chorób i Problemów Zdrowotnych(International Statistical Classification of Diseases and Related Health Problems), wyznaczone przez Światową Organizację Zdrowia. ICD-11 wyodrębniło wzajemnie wykluczające się diagnozy szkodliwego używania alkoholu oraz uzależnienia, wraz z określeniem ich miejsca w hierarchii zaburzeń, i propozycje oddziaływań terapeutycznych. Powstała w ten sposób swoista piramida – u jej podstawy znalazło się używanie nieskutkujące problemami, w tym wypadku wystarczająca jest profilaktyka pierwszorzędowa, wynikająca ze stosowania programów → z d r o w i a p u b l i c z n e g o [t. 4]. Nad nią umieszczono ryzykowne używanie, generujące potrzebę krótkiej interwencji na ogólnych zasadach. Powyżej umiejscowiono używanie szkodliwe (ewentualnie picie szkodliwe według ICD-10 lub nadużywanie alkoholu według DSM-4), wymagające poszerzonej interwencji terapeutycznej. Ostatni poziom to uzależnienie od alkoholu (zaburzenia używania alkoholu według DSM-5), w którym konieczne jest leczenie specjalistyczne.

W rozwoju uzależnienia od alkoholu ważną rolę odgrywają m.in. uwarunkowania genetyczne (bardziej zagrożone są dzieci rodzica, a zwłaszcza rodziców

nadużywających alkoholu), płeć (kobiety), wiek (łatwiej uzależniają się dzieci i młodzież niż osoby dorosłe) oraz status społeczno-finansowy (niski status częściej wiąże się nie tylko z uzależnieniami, ale także ze zgonami na tle alkoholowym). Istotną funkcję pełnią tu również aspekty psychologiczne czy środowiskowe oraz czynniki → r y z y k a i ochrony.

Według Marka Griffithsa uzależnienie wykazuje kilka właściwości, a mianowicie: wyrazistość emocjonalnego podporządkowania, w którym potrzeba sięgnięcia po alkohol staje się najważniejsza zmiana nastroju – optymalizacja następuje jedynie w czasie zachowania nałogowego, zwiększona tolerancja dawkowania, czyli potrzeba picia coraz większej ilości alkoholu (poza ostatnią fazą), objawy abstynencyjne, konflikty z otoczeniem oraz nawroty choroby. Jednak obraz alkoholizmu może wyglądać różnie w zależności od ilości wypijanego alkoholu i częstotliwości sięgania po trunki wysokoprocentowe, a także od towarzyszących im powodów. Elvin Morton Jellinek wyróżnił 5 typów uzależnienia:

1) Alfa – tzw. życie na rauszu. Psychologiczne uzależnienie od alkoholu występujące wśród osób nieradzących sobie ze stresem czy z trudnymi sytuacjami życiowymi. Towarzyszące mu objawy upośledzonej kontroli nad piciem są w tym wypadku umiarkowane i mogą się utrzymywać przez kilkanaście lat, niekiedy przechodząc w typ gamma.
2) Beta – przeciwieństwo typu alfa: picie nieregularne, ale w dużych ilościach. Jednostka nie wykazuje psychologicznych i fizycznych symptomów uzależnienia, istotne są tu jednak aspekty społeczne czy środowiskowe. Negatywne skutki nadmiernego picia mają głównie charakter somatyczny.
3) Gamma – w tym typie występują psychiczne i fizyczne symptomy uzależnienia, jak również zmiany środowiska społecznego. Pojawia się utrata kontroli nad piciem, wzrost tolerancji na alkohol i głód abstynencyjny. To najbardziej typowy i chroniczny rodzaj omawianej choroby, najczęściej spotykany wśród uczestników terapii AA.
4) Delta – kontrolowanie wypijanych ilości przy jednoczesnej niemożności całkowitego powstrzymania się. Polega na regularnym spożywaniu niskoprocentowego alkoholu w celu utrzymania stałego stężenia we krwi całymi tygodniami, miesiącami, a nawet latami. Osoby takie nie przejawiają wyraźnych objawów intoksykacji, jednak typ ten może prowadzić do uzależnienia fizycznego i psychicznego oraz poważnych następstw zdrowotnych.
5) Epsilon – inaczej dipsomania lub opilstwo okresowe. Występowanie ciągów alkoholowych naprzemiennie z okresami pełnej abstynencji. Pretekstu mogą dostarczyć różne imprezy towarzyskie czy uroczystości rodzinne.

Uzależnienie od alkoholu rozwija się stopniowo. Pierwszym etapem jest prealkoholiczna faza objawowa, zaczynająca się od konwencjonalnego i okazjonalnego stylu picia. Jednostka odkrywa alkohol jako źródło przyjemności i sposób na redukcję

napięcia emocjonalnego. Z czasem jej odporność na stresujące sytuacje może maleć, zaczyna więc pić coraz więcej, czego konsekwencją będzie wzrost tolerancji na alkohol. Początkiem drugiej fazy – zwiastunowej – jest moment, w którym jednostka mimo braku utraty przytomności nie może przypomnieć sobie swojego postępowania oraz okoliczności towarzyszących wypiciu alkoholu. Takie epizody zaburzeń pamięci (tzw. palimpsesty) zaczynają się powtarzać nawet bez większych dawek alkoholu. Uwidacznia się coraz większa koncentracja na alkoholu, szukanie wymówek, by po niego sięgnąć, picie kompulsywne, niekiedy po kryjomu. W fazie trzeciej – krytycznej – dochodzi do utraty kontroli, jednostka odczuwa przymus fizyczny (głód alkoholowy) i pije aż do stanu upojenia. Mimo okresowej zdolności do powstrzymywania się od picia czy prób utrzymania nad nim kontroli przez usiłowanie zmieniania wzorów tej aktywności coraz dotkliwiej odczuwa konieczność stałego uzupełniania stężenia alkoholu w organizmie. Występuje coraz więcej objawów uzależnienia, samooszukiwanie, tworzenie racjonalnych uzasadnień dla swojego postępowania, izolowanie się, zaniedbywanie pracy, zainteresowań i relacji z bliskimi – życiowym priorytetem staje się picie. Charakterystyczne dla fazy czwartej, chronicznej, są okresy wielodniowej intoksykacji, których następstwem jest rozpad zasad moralnych, poważne uszkodzenia procesów myślenia i zdolności do oceny faktów. Pojawiają się epizody picia alkoholi niekonsumpcyjnych oraz zmniejszenie tolerancji na alkohol. Coraz częściej występują stany bezprzedmiotowego lęku oraz drżenie i wyraźne obniżenie sprawności motorycznej, a nawet psychozy.

Rozważając skutki szkodliwego picia alkoholu, należy podkreślić, że negatywne konsekwencje pojawiają się nie tylko w fazie pełnoobjawowego uzależnienia, lecz także przy nadmiernym spożywaniu. Przyczynia się ono bezpośrednio do ponad 60 różnych schorzeń i urazów, także chorób cywilizacyjnych. Toksyczny wpływ na narządy i tkanki powoduje ostre lub przewlekłe zatrucia. Degradacja funkcji odpornościowych jednostki zwiększa podatność na zakażenia patogenami wywołującymi zapalenie płuc i gruźlicę. Stanowi też czynnik wpływający na zwiększone występowanie chorób przenoszonych drogą płciową. Nadużywanie alkoholu może wpływać na rozwój nowotworów jamy ustnej, krtani, gardła, przełyku, jelita grubego, wątrobowokomórkowego oraz piersi, zachorowań przewodu pokarmowego, w tym alkoholowej choroby wątroby, ostrego, przewlekłego zapalenie trzustki, zespołu Mallory'ego-Weisa, ostrej gastropatii krwotocznej. W Polsce systematycznie wzrasta liczba hospitalizacji w wyniku szkodliwego picia alkoholu, do czego przyczyniają się dodatkowo zamierzone i niezamierzone następstwa takiego postępowania jak wypadki drogowe, utonięcia, → p r z e m o c [t. 3] wobec innych czy wobec siebie – samookaleczenia, samobójstwa.

Poza destrukcyjnym wpływem na sferę zdrowotną alkoholizm oddziałuje negatywnie na wiele innych obszarów, szkodzi przez to nie tylko dotkniętej nim jednostce. Dezintegruje i destabilizuje małżeństwo i całą rodzinę, a także relacje z przyjaciółmi.

Może doprowadzać do kłótni, zaniedbywania ważnych dziedzin życia, stwarzać problemy w pracy, a w konsekwencji kłopoty finansowe. W wyniku spożycia alkoholu można uszkodzić przedmioty, ulec wypadkowi lub się zranić. Uzależnienie to sprzyja rozwojowi innych nałogów, a także wielu patologii oraz postawi zachowań aspołecznych.

Picie alkoholu przez kobiety w okresie ciąży naraża ich potomstwo na alkoholowy zespół płodowy (*fetal alcohol syndrome*, FAS), skutkujący niepełnosprawnościami fizycznymi i neurorozwojowymi dziecka, wady wrodzone związane z alkoholem (*alcohol-related birth defects*, ARBD) i zaburzenia neurorozwojowe związane z alkoholem (*alcohol-related neuro-developmental disorder*, ARND). Jeśli chodzi o dzieci pijących rodziców, zwiększa się ryzyko ich wykorzystywania fizycznego lub seksualnego, zaniedbywania, powstawania zachowań antyspołecznych, problemów emocjonalnych i trudności w środowisku szkolnym, a także prawdopodobieństwo wystąpienia w przyszłości szkodliwego używania substancji psychoaktywnych, z powodu czynników zarówno środowiskowych, jak i genetycznych. Młodzi ludzie wychowujący się w rodzinach alkoholików są również bardziej narażeni na niechciane doświadczenia seksualne, bójki i incydenty z udziałem policji, łamanie prawa (np. przez prowadzenie pojazdów pod wpływem alkoholu), przemoc i inne zachowania ryzykowne. Ponieważ mózg nastolatka w porównaniu z mózgiem dorosłego jest podatniejszy na ostre i przewlekłe działanie alkoholu, upijanie się młodzieży może powodować nie tylko zatrucie i utratę przytomności, ale także znaczny negatywny wpływ na ogólną pamięć i funkcjonowanie hipokampu, szczególnie w odniesieniu do gromadzenia → i n f o r m a c j i [t. 2] przeznaczonych do długotrwałego przechowywania, a zatem ma ujemny wpływ na całe jej dalsze funkcjonowanie.

Te i inne niekorzystne implikacje spożywania i nadużywania alkoholu powodują, że kształtowanie polityki społecznej w tym zakresie jest bardzo istotne. Wśród jej fundamentalnych elementów wyróżnia się: tworzenie warunków sprzyjających zabezpieczeniu potrzeb, których zaspokajanie motywuje powstrzymywanie się od spożywania alkoholu, działalność wychowawczą i informacyjną, ustalanie odpowiedniego poziomu i właściwej struktury produkcji napojów alkoholowych przeznaczanych do spożycia w kraju, ograniczanie dostępności alkoholu, leczenie, rehabilitację i reintegrację osób uzależnionych od alkoholu, zapobieganie negatywnym następstwom nadużywania alkoholu i ich usuwanie, przeciwdziałanie przemocy w rodzinie, wspieranie zatrudnienia socjalnego przez finansowanie centrów integracji społecznej.

W Polsce najważniejsze przepisy odnoszące się do powyższych kwestii zawiera Ustawa z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi. Zgodnie nią do inicjowania i doskonalenia działań związanych z profilaktyką i rozwiązywaniem problemów alkoholowych w 1993 r. utworzono Państwową Agencję Rozwiązywania Problemów Alkoholowych (PARPA), która była także odpowiedzialna za współdziałanie z organizacjami pozarządowymi i administracją

samorządową, zobowiązaną do realizowania programów profilaktycznych i naprawczych w społecznościach lokalnych. Zadania te od 1 stycznia 2022 r. przejęło Krajowe Centrum Przeciwdziałania Uzależnieniom (KCPU), które powstało z połączenia Państwowej Agencji Rozwiązywania Problemów Alkoholowych oraz Krajowego Biurads. Przeciwdziałania Narkomanii.

Poza działaniami profilaktycznymi, redukującymi czynniki ryzyka i wzmacniającymi czynniki ochrony, jakie należy podejmować w rodzinie, szkole i środowisku lokalnym, pomocniczą rolę mogą odgrywać również instytucje oświatowe i kulturalne, stowarzyszenia, fundacje i służby (w tym Policja). Użytecznym wsparciem są kampanie medialne, zwiększające świadomość społeczną związaną ze szkodliwością omawianej patologii. Z kolei dla samych osób uzależnionych od alkoholu (oraz ich bliskich) nieocenioną pomocą jest psychoterapia lub farmakoterapia, leczenie w zamkniętych ośrodkach leczenia uzależnień, grupy terapeutyczne, np. Anonimowych Alkoholików (AA), czy grupy wspierające ich rodziny, np. terapia dorosłych dzieci alkoholików (DDA), grupy krewnych i przyjaciół alkoholików Al-Anon, Alateen (dla dzieci i młodzieży, których rodzic / rodzice lub inni bliscy są uzależnieni od alkoholu).

Małgorzata Bereźnicka

P. Anderson, B. Baumberg, *Alkohol w Europie: perspektywa zdrowia publicznego. Raport dla Komisji Europejskiej*, „Alkoholizm i Narkomania" 2006, t. 19, nr 2; M. Bereźnicka, *Alcoholism as a Threat to Social Security and the Issue Among Academic Youth*, „Internal Security" 2021, vol. 13, nr 1; taż, *Problem alkoholizmu jako patologii społecznej zagrażającej różnym wymiarom bezpieczeństwa społecznego*, „Annales Universitatis Paedagogicae Cracoviensis Studia de Securitate" 2022, vol. 12, nr 1; M. Bujalski, J. Klingemann, *Słownik uzależnień*, Instytut Psychiatrii i Neurologii, Warszawa 2021; D.F. Hermens, J. Lagopoulos, *Binge Drinking and the Young Brain: A Mini Review of the Neurobiological Underpinnings of Alcohol-induced Blackout*, „Frontiers Psychology" 2018, vol. 9, https://doi.org/10.3389/fpsyg.2018.00012 (dostęp 16.03.2023); D.H. Jernigan, *Global Status Report: Alcohol and Young People*, WHO, Geneva 2001, https://apps.who.int/iris/bitstream/handle/10665/66795/ WHO_ MSD_MSB_01.1.pdf (dostęp 15.03.2023); D. Kozielewicz, D. Dybowska, W. Halota, *Wybrane aspekty kliniczne nadużywania alkoholu*, „Medical Science Review – Hepatologia" 2011, t. 11; J. Mellibruda, *Alkoholizm i diagnozowanie uzależnienia od alkoholu*, Instytut Psychologii Zdrowia Polskiego Towarzystwa Psychologicznego, http://www.psychologia.edu.pl/czytelnia/50-artykuly/1032alkoholizm-i-diagnozowanie-uzaleznienia-od-alkoholu.html (dostęp 11.03.2023); R. Modrzyński, *Zaburzenia związane z używaniem alkoholu – propozycje zmian w klasyfikacji ICD-11*, „Polskie Forum Psychologiczne" 2019, t. XXIV, nr 3, https:// pfp.ukw.edu.pl/archive/article-full/430/modrzynski_zaburzenia_zwiazane_z_uzywaniem_alkoholu/ (dostęp 11.03.2023); K. Morawska, J. Chodkiewicz, *Alkoholicy wysokofunkcjonujący – odrębny typ? Poszukiwanie wspólnych cech w istniejących typologiach alkoholizmu*, „Psychiatria i Psychologia Kliniczna" 2019, vol. 19, no. 4; Państwowa Agencja Rozwiązywania Problemów Alkoholowych, *Picie ryzykowne i szkodliwe*, https://www.parpa.pl/index.php/szkody-zdrowotne-i-uzaleznienie/ picie-ryzykowne-i-szkodliwe (dostęp 17.03.2023); Ustawa z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi, Dz.U. 1982, nr 35, poz. 230; World Health Organization, *Alcohol. Key facts*, 9.05.2022, https:// www.who.int/news-room/fact-sheets/detail/alcohol (dostęp 21.03.2023).

ALTERNACJA WŁADZY – jest rozumiana jako wymiana elity rządzącej oraz przez pryzmat instytucji cykliczności wyborów parlamentarnych i/lub prezydenckich. Jedną z najważniejszych zasad systemu demokratycznego jest odpowiedzialność władzy przed społeczeństwem, które uzyskało możliwość wymiany rządzących, w szczególności w sytuacji niezadowolenia z ich rządów. Dokonująca się za pomocą wyborów parlamentarnych oraz prezydenckich alternacja władzy jest istotnym elementem konsolidacji procesów demokratycznych. Zasada alternacji władzy często jest rozumiana jako synonim wymiany elity rządzącej lub nakaz oddania władzy przez partię polityczną bądź koalicję partii w konsekwencji porażki wyborczej. B. Michalak alternację władzy definiuje jako zmianę władzy oraz wymianę rządzących. W systemach demokratycznych alternację władzy przeprowadza się za pomocą instytucji wyborów. Sposób ten opisują J.J. Linz oraz W. Wojtasik. Pierwszy określa wybory jako procedurę umożliwiającą obywatelom kandydowanie na urząd, na skutek czego możliwe jest dokonywanie alternacji wtedy, gdy sprawujący władzę przegra wybory i musi przekazać władzę zwycięzcy. Jak zaznacza Wojtasik, za pomocą wyborów kształtuje się podział na tych, którzy władzę otrzymują, i tych, którzy tworzą opozycję. Zdaniem T. Wieciecha pojęcie alternacji władzy należy stosować znacznie szerzej, również w odniesieniu do systemów niedemokratycznych. W tym znaczeniu alternacja władzy określa sytuację, w której następuje zmiana układu politycznego kontrolującego instytucje władzy w państwie, a jej konsekwencją jest zmiana w rządzeniu rozumiana jako realizacja odmiennego projektu politycznego.

Według Wieciecha zasada alternacji władzy może nastąpić zarówno w demokratycznych, jak i niedemokratycznych systemach politycznych, tym samym badacz wyróżnia alternację demokratyczną i niedemokratyczną. Alternację demokratyczną cechuje jej zinstytucjonalizowany charakter, gdyż w systemach demokratycznych wymiana rządzących następuje poprzez regularne stosowanie określonych procedur, które są w równym stopniu dostępne dla wszystkich uczestników procesu rywalizacji o władzę, inaczej mówiąc, nie uprzywilejowuje się żadnego z nich. Natomiast w systemach niedemokratycznych zmiana władzy dokonuje się nieregularnie, w drodze przewrotów, zamachów stanu lub wskutek przesilenia w strukturach rządowych monopartii. Wieciech zwraca również uwagę, że dla systemu demokratycznego ważne jest to, że zmiana personalna na stanowiskach państwowych nie oznacza jeszcze alternacji władzy, gdyż istotne jest, żeby w rezultacie zmiany wyborczej nastąpiła zmiana realizowanej przez władze polityki.

Analizując alternację władzy, należy zwrócić uwagę na różne teorie odnoszące się do wymiany elity. S. Szelenyi, I. Szelenyi i I. Kovach wskazują 3 koncepcje dotyczące tego procesu: teorię reprodukcji elit, teorię krążenia elit oraz teorię odnoszącą się do pozycji klasowej elity. Na uwagę zasługuje koncepcja cyrkulacji (krążenia) elit. V. Pareto uznał, że za sprawą demokracji dokonuje się cyrkulacja elit, która odbywa się między przedstawicielami starej oraz nowej elity. Jednakże trzeba zaznaczyć, że

badacz nie precyzuje, w jaki sposób rozumie cyrkulację elit – czy widzi ją przez pryzmat dynamiki wewnątrz elit, czy jako zastąpienie elity (częściowe bądź całkowite) przedstawicielami z nieelity. Istotnym czynnikiem jest rozgraniczenie wewnętrznej cyrkulacji elity oraz zmiana elity. Ukraiński politolog J. Macijewskyj wyróżnia 2 mechanizmy krążenia elit w społeczeństwie, tj. reprodukcję i cyrkulację. W pierwszym przypadku oznacza to odtworzenie pewnej elity w ramach pewnej grupy społecznej, w drugim zaś – uzupełnienie i zastąpienie elity przedstawicielami innych grup. Za narzędzie cyrkulacji elity w państwach demokratycznych Macijewskyj uznaje wybory, jednakże w państwach, które są na etapie tranzycji, reguła ta nie zawsze ma zastosowanie. Szelenyi i Szelenyi przez cyrkulację elit rozumieją sposób zamiany elit przez przedstawicieli innych grup społecznych, jest to zmiana tych, którzy zajmują naczelne pozycje w kluczowych instytucjach danego społeczeństwa. Według teorii transformacji elity wymiana rządzących może zachodzić na 2 sposoby: pierwszy dotyczy sytuacji dojścia do władzy nowej elity – stara elita nie ustępuje z politycznej sceny całkowicie, gdyż jej część dołącza do nowej. Przyczyn tego zjawiska należy doszukiwać się np. w braku doświadczenia nowo wybranych w sprawowaniu władzy lub obecności w starej elicie przedstawicieli godzących się zmienić środowisko dla uzyskania władzy. Drugi sposób występuje w przypadku, gdy nowa elita przejmuje część wartości lub wzorców zachowań starej elity.

Klasyfikację alternacji proponują K. Hoff, S. Horowitz i B. Milanovic. Po przeanalizowaniu przykładu krajów postkomunistycznych wyróżnili 2 typy alternacji: alternację przywództwa (ang. *leadership alternation*) i alternację ideologiczną (ang. *ideological alternation*). Alternacja przywództwa charakteryzuje się wymianą przedstawicieli organów władzy przez reprezentantów z tej samej opcji politycznej – zmieniają się liderzy, lecz wywodzą się oni z tej samej elity bądź są z nią powiązani, np. kandydatura W. Putina była popierana przez B. Jelcyna, z kolei D. Miedwiediew otrzymał poparcie Putina. Alternacja ideologiczna przewiduje zastąpienie elity rządzącej przedstawicielami reprezentującymi odmienną ideologię. Na poziomie współczesnych państw możemy interpretować tę koncepcję jako alternację programów prezentowanych przez władzę, czyli powinna dokonywać się zmiana realizacji polityki. Zupełnie inną klasyfikację, opierającą się na kryterium stopnia zagwarantowania alternacji, zaproponował

P. Mair, który wyróżnił 3 wzory dokonywania się alternacji władzy, są to alternacje:

- całkowita, gdy elitę rządzących zastępuje nowa siła polityczna (np. Wielka Brytania);
- częściowa, kiedy to przynajmniej jedna partia na skutek wyborów pozostaje w rządzie (np. Niemcy, Holandia);
- niealternacyjna, w sytuacji, gdy partii rządzącej przez długi czas udaje się utrzymywać monopol władzy (Japonia 1955–1993, Indie 1952–1977, Szwecja 1936–1976, Francja 1958–1981).

Do powyższej koncepcji rozgraniczenia wzorów dokonywania się alternacji władzy nawiązuje typologia K. Lundella wskazującego 2 możliwości operacjonalizacji kategorii alternacji i nazywającego je alternacją kategoryczną (ang. *categorical*) i alternacją ciągłą (ang. *continuous*). Pierwsza z nich następuje wtedy, gdy w różnych typach demokracji są widoczne przejawy alternacji. Alternację możemy również uznać za proces ciągły, gdyż w wyniku wyborów dochodzi do ciągłej zmiany elit władzy. Podejście Lundella przedstawia podział na alternację pełną – z zachowaniem tradycji wymiany elity rządzącej – i częściową – wymiana polega na fragmentarycznym zastosowaniu zasady alternacji władzy w państwie.

Alternację władzy można klasyfikować na podstawie propozycji Maira (pełna, częściowa i brak alternacji) oraz Lundella (kategoryczna i ciągła), dokonując podziału na alternację skonsolidowaną, nieskonsolidowaną oraz brak alternacji. Przez alternację skonsolidowaną należy rozumieć całkowitą wymianę elity rządzącej, w sytuacji prawno-ustrojowego uregulowania procesu wyborczego oraz jego cyklicznego charakteru, a także ukształtowanej tradycji wymiany elity rządzącej w państwie. Natomiast w przypadku alternacji nieskonsolidowanej któryś z wymienionych wyżej wymogów występuje w formie niepełnej, dochodzi do częściowej wymiany władzy lub ustawodawstwo nie wpływa na zagwarantowanie procesu alternacji oraz w państwie nie wykrystalizowała się tradycja wymiany elity rządzącej, albo może dochodzić do zmian personalnych, co nie wiąże się ze zmianami polityki rządzących. Za brak alternacji możemy uznać notoryczne wygrane partii rządzącej, co powoduje ukształtowanie jej monopolu władzy.

Maryana Prokop

M. Bratton, *The „Alternation Effect" in Africa*, „Journal of Democracy" 2004, vol. 15, no. 4; K. Hoff, S. Horowitz, B. Milanovic, *Political Alternation, Regardless of Ideology, Diminishes Influence Buying: Lessons from Transitions in Former Communist States*, „Carnegie Endowment for International Peace Policy Outlook" 2005; *Leksykon prawa wyborczego i systemów wyborczych*, B. Michalak, A. Sokala (red.), Wolters Kluwer Polska, Warszawa 2010; J.J. Linz, *Totalitarian and Authoritarian Regimes*, Lynne Rienner Publishers, Boulder 2000; K. Lundell, *Accountability and Patterns of Alternation of Pluralism, Majoritarian and Consensus Democracies*, „Government and Opposition" 2011, vol. 46, no. 2; P. Mair, *Party System Change: Approaches and Interpretations*, Oxford University Press, Oxford 1997; V. Pareto, *Uczucia i działania. Fragmenty socjologiczne*, tłum. M. Dobrowolska, M. Rozpędowska, A. Zinserling, Wydawnictwo Naukowe PWN, Warszawa 1994; M. Prokop, *Aplikacyjność kategorii alternacji władzy w badaniach nad reżimami hybrydalnymi*, „Warmińsko-Mazurski Kwartalnik Naukowy. Nauki Społeczne" 2015, nr 3 (15); M. Prokop, I. Galewska, *The Amendment of the Ukrainian Electoral Law and the Principle of Alternation in Power (Parliamentary Election in 2012)*, „Athenaeum. Polskie Studia Politologiczne" 2013, nr 40; S. Szelenyi, I. Szelenyi, I. Kovach, *Sfragmentaryzowane elity węgierskie: krążenie w polityce, reprodukcja w gospodarce*, [w:] *Elity w Polsce, Rosji i na Węgrzech. Wymiana czy reprodukcja?*, I. Szelenyi, D. Treiman, E. Wnuk-Lipiński (red.), Instytut Studiów Politycznych PAN, Warszawa 1995; G. Ulicka, *Demokracje zachodnie*, Wydawnictwo Naukowe PWN, Warszawa 1992; T. Wieciech, *Alternacja władzy*, [w:] *Encyklopedia politologii. Instytucje i systemy polityczne*, t. II, B. Dziemidok-Olszewska, W. Sokół (red.), Wolters Kluwer Polska Warszawa 2012; tenże, *Zasady alternacji władzy w demokratycznym systemie politycznym*,

[w:] *Adaptacja – reforma – stabilizacja. Przestrzeń publiczna we współczesnych systemach politycznych*, T. Kozielło, P. Maj, W. Paruch (red.), Wydawnictwo Uniwersytetu Rzeszowskiego, Rzeszów 2010; W. Wojtasik, *Funkcje wyborów w III Rzeczypospolitej. Teoria i praktyka*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2012; J. Wójnicki, *Alternacja władzy w państwach Europy Środkowo-Wschodniej po 1990 r.*, „Studia Politicae Universitatis Silesiensis" 2011, t. 7; Ю. Мацієвський, *Еліти в Україні до і після „помаранчевої революції"*, „Політичний менеджмент" 2010, nr 2.

AMBASADA DANYCH (*data embassy*) – forma zabezpieczenia danych istotnych dla danego państwa (dane krytyczne) przez przechowywanie ich kopii zapasowych (tzw. *backup*) poza granicami tego państwa. Dane znajdujące się w ambasadzie danych są odpowiednio zabezpieczone (najwyższy poziom → b e z p i e c z e ń s t w a [t. 1]), podlegają bieżącym aktualizacjom i stałemu monitoringowi. W razie awarii bądź → z a g r o ż e n i a [t. 4] dla danych macierzystych ambasada danych umożliwia kontynuację działania wybranych usług publicznych, a w skrajnym wypadku może umożliwić odbudowę państwowej infrastruktury cyfrowej. Z tego względu ambasadę danych należy uznać za jedno z rozwiązań zabezpieczających cyfrową ciągłość funkcjonowania państwa.

Koncepcja ambasad danych jest rozwijana w związku z coraz większym zagrożeniem → c y b e r a t a k a m i [t. 1] (np. bombardowaniem → a t a k a m i DDoS), fizycznymi aktami sabotażu, ale także → i n w a z j a m i [t. 2] militarnymi, grożącymi czasową lub trwałą utratą dostępu do danych bądź ich bezpowrotną stratą. Ambasady danych mogą również chronić dane przed wypadkami losowymi – awariami systemów IT, → k a t a s t r o f a m i n a t u r a l n y m i [t. 2] czy budowlanymi. W skrajnych sytuacjach ambasada danych mogłaby umożliwić kontynuowanie działalności państwowej także po utracie kontroli rządu nad własnym terytorium, co przewiduje m.in. strategia → c y b e r b e z p i e c z e ń s t w a [t. 1] Estonii.

Ambasady danych opierają się na tworzeniu kopii zapasowych wybranych danych na serwerach znajdujących się fizycznie w innym kraju lub innych krajach. Dywersyfikacja lokalizacji (korzystanie z więcej niż jednego kraju) służy jako dodatkowy element zabezpieczenia. Kraj właściciel danych ma zdalny dostęp do → informacji [t. 2] oraz do mocy obliczeniowej zagranicznych serwerów, co może mieć dodatkowe znaczenie w sytuacji awarii lub zmasowanego ataku. Podstawowa koncepcja ambasady danych, z istotnymi modyfikacjami obejmującymi zakres danych, ich wrażliwość oraz poziom zabezpieczeń, opiera się na wykorzystaniu idei przechowywania materiałów w chmurze.

Transfer i przechowywanie danych powinny być ściśle uregulowane umową bilateralną z państwem gospodarzem, szczególnie w odniesieniu do częściowej lub całkowitej eksterytorialności lokalizacji przechowywania danych na wzór klasycznych placówek dyplomatycznych, których funkcjonowanie, co do zasady, reguluje Konwencja wiedeńska o stosunkach dyplomatycznych, sporządzona w Wiedniu dnia 18 kwietnia 1961 r. (VCDR). Wzorem dla tego typu rozwiązań jest utworzona w 2017 r. estońska

ambasada danych (nazywana umownie Centrum Danych) zlokalizowana w Luksemburgu. Na mocy porozumienia dwustronnego przyznano jej prawa zbliżone do tych przyznawanych ambasadzie fizycznej, w tym immunitet.

W przyszłości kluczowe będzie nakreślenie jasnych zasad tworzenia eksterytorialnych ambasad danych oraz zakresu obowiązywania VCDR. Przykład Estonii pokazał, że na tym etapie rozwoju interpretacyjnego VCDR niezbędne było dodatkowe zabezpieczenie w postaci umowy dwustronnej, a samo porozumienie z Luksemburgiem stanowi istotny precedens, który może wyznaczyć kierunki rozwoju regulacyjnego ambasad danych w przestrzeni prawa międzynarodowego.

Estonia jest słusznie uznawana za jeden z modelowych przykładów wdrażania bezpiecznej infrastruktury cyfrowej umożliwiającej świadczenie usług publicznych. Jednym z kluczowych projektów rozwijanych od 2001 r. jest platforma X-Road. Ambasada danych zlokalizowana w Luksemburgu jest uzupełnieniem i dodatkową gwarancją bezpieczeństwa dla całego zaawansowanego ekosystemu e-państwa i może być rozumiana jako jedna z odpowiedzi na wzrost liczby → c y b e r z a g r o ż e ń [t. 1], w tym zmasowany atak na estońską infrastrukturę z 2007 r. Estońska ambasada danych pozwala na przechowywanie kopii danych krytycznych oraz umożliwia zdalne nimi zarządzanie. Projekt spotkał się z bardzo dobrym przyjęciem, a Estonia pracuje nad stworzeniem kolejnych lokalizacji dla serwerów obsługujących ambasady danych. Obecnie kopie zapasowe w ambasadzie danych Estonii tworzone są dla 10 strategicznych systemów państwowych: sądowego, informacji skarbowej, rejestru gruntów i katastralnego rejestru gruntów, rejestru podatników, rejestru działalności gospodarczej, rejestru ludności, dziennika urzędowego, rejestru dokumentów tożsamości, rejestru ubezpieczeń państwowych.

Wzrost liczby zagrożeń cybernetycznych istotnie zwiększa zapotrzebowanie na tworzenie kopii zapasowych danych krytycznych. Należy odnotować, że koncepcja ambasady danych ma szczególne znaczenie dla krajów narażonych w większym stopniu na cyberataki lub kataklizmy naturalne bądź też niedysponujących odpowiednią krajową infrastrukturą do ochrony danych i bezpiecznego przechowywania ich kopii zapasowych. Jednocześnie kluczowym czynnikiem dla wykorzystywania ambasad danych jest istotny stopień digitalizacji państwowych usług, pozwalający na regularną migrację danych. Jak słusznie zauważyli eksperci (Nick Robinson, Laura Kask, Robert Krimmer), sama ambasada danych powinna być uznawana za element „całościowej polityki, w której należy określić zasady przechowywania informacji dla danych […] o krytycznym znaczeniu dla funkcjonowania państwa", nie może być zatem traktowana jako uniwersalna i jedyna forma zabezpieczenia. Omawiany przykład Estonii pokazuje, że zabezpieczenie kopii zapasowych danych jest realizowane na kilku poziomach – zarówno przez rządowe chmury, kopie fizyczne danych przechowywane w tradycyjnych placówkach dyplomatycznych, jak i ambasadę danych zlokalizowaną w Luksemburgu.

Należy założyć, że ambasady danych będą coraz popularniejszą formą zabezpieczania danych, co może skutkować tworzeniem więcej niż jednej placówki w celu zapewnienia dodatkowej ochrony kopii zapasowych. W Polsce prace nad pilotażowym projektem ambasady danych są prowadzone w ramach zainicjowanego w 2019 r. programu Wspólna Infrastruktura Informatyczna Państwa. Obejmuje on także działania na rzecz Publicznych Chmur Obliczeniowych, Rządowej Chmury Obliczeniowej czy Rządowego Klastra Bezpieczeństwa. W przyjętej 14 kwietnia 2022 r. rekomendacji Rady ds. Cyfryzacji w sprawie stworzenia cyfrowej ambasady RP wskazano na konieczność zapewnienia suwerenności cyfrowej i → b e z p i e c z e ń s t w a i n f o r m a c y j n e g o [t. 1] państwa oraz jego cyfrowych zasobów. Ma to szczególne znaczenie w obliczu → a g r e s j i [t. 1] Federacji Rosyjskiej na Ukrainę. Wśród rekomendacji wymieniono podjęcie współpracy z podmiotami prywatnymi, a także krajami europejskimi (wymieniono tu Luksemburg, Szwajcarię, Norwegię, Wielką Brytanię), stworzenie ram w celu posiadania kopii kluczowych rejestrów państwowych i zdolności do odtworzenia kluczowych zasobów informacyjnych,systemów i usług cyfrowych na wypadek ich uszkodzenia lub całkowitej utraty. Wszystko to powinno skutkować stworzeniem cyfrowej ambasady, będącej w tym wypadku rozszerzeniem polskiej chmury rządowej. W rekomendacji zaznaczono, że lokalizacja cyfrowej ambasady powinna obejmować wiarygodny, stabilny, demokratyczny i bezpieczny kraj europejski, a ośrodek i dane powinny podlegać jurysdykcji Polski (objęcie takimi samymi gwarancjami prawnymi jak dane i serwery w Polsce, co może sugerować wykorzystanie VCDR i dodatkowe zabezpieczenie prawne w postaci umów bilateralnych).

Z punktu widzenia administracji publicznej ambasady danych mogą mieć znaczenie nie tylko dla ochrony danych krytycznych. Wskazuje się, że w przyszłości mogłyby służyć ochronie dziedzictwa kulturowego przez przechowywanie materiałów dokumentacyjnych umożliwiających ewentualną rekonstrukcję zabytków. Tego typu działania będą miały jednak charakter subsydiarny i to od państw decydujących się na otwarcie ambasad danych zależeć będzie, jaka zawartość będzie w nich gromadzona.

Mateusz Łabuz

Agreement between the Republic of Estonia and the Grand Duchy of Luxembourg on the hosting of data and information systems, Luxembourg, 20 June 2017, Journal Officiel du Grand-Duché de Luxembourg, Mémorial A, No. 253; Case study: *The world's first data embassy– Estonia*, [w:] *Embracing Innovation in Government. Global Trends 2018*, OECD 2018; e-Estonia, *Data Embassy – The Digital Continuity of a State*, 9.12.2019, https://e-estonia.com/data-embassy-the-digital-continuity-ofa-state (dostęp 9.04.2023); *Implementation of the Virtual Data Embassy Solution*, Summary Report of the Research Project on Public Cloud Usage for Government, Conducted by Estonian Ministry of Economic Affairs and Communications and Microsoft Corporation, 2015; *Jak współtworzyć nowoczesne państwo na miarę XXI wieku?*, I. Kalita (red.), Krajowa Szkoła Administracji Publicznej, Warszawa 2020; Konwencja wiedeńska o stosunkach dyplomatycznych, sporządzona w Wiedniu dnia 18 kwietnia 1961 r., Dz.U. 1965, nr 37, poz. 232; Ministerstwo Cyfryzacji, *Wspólna Infrastruktura Informatyczna*

Państwa, https://www.gov.pl/web/govtech/ wspolna-infrastruktura-informatyczna-panstwa (dostęp 9.04.2023); A. Piechota, *V Ogólnopolska Konferencja Studencko-Doktorancka „Rozpoznać przeszłość w teraźniejszości. Ochrona dziedzictwa w XXI wieku"*, „Nowa Biblioteka" 2019, nr 4; *Rekomendacja Rady ds. Cyfryzacji stworzenia „cyfrowej ambasady RP" w celu zapewnienia suwerenności cyfrowej i bezpieczeństwa informacyjnego państwa oraz jego cyfrowych zasobów* z 14 kwietnia 2022 r.; N. Robinson, L. Kask, R. Krimmer, *The Estonian Data Embassy and the Applicability of the Vienna Convention: An Exploratory Analysis*, „ICEGOV'19: Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance" 2019; N. Robinson, K. Martin, *Distributed Denial-of-Government: The Estonian Data Embassy Initiative*, „Network Security" 2017, no. 9; B. Sierzputowski, *The Data Embassy under Public International Law*, „International & Comparative Law Quarterly" 2019, vol. 68, no. 1; J.R. Thompson, *E-Government-In-Exile: Non-Territorial State Continuity Using Data Embassies*, Master Thesis, Tallinn University of Technology 2019.

AMERYKAŃSKIE CENTRUM BADAŃ NAD WOJNĄ NOWEJ GENERACJI (Center for the Study of New Generation Warfare, NGW Centre) – ma na celu edukowanie zachodnich elit politycznych i wojskowych, przywództw państw demokratycznych w zakresie przeciwdziałania aktywnemu użyciu przez Federację Rosyjską → w o j n y n o w e j g e n e r a c j i [t. 4]; pomoc społeczeństwom Zachodu w przygotowaniu się do obrony swoich liberalnych demokracji. Podstawą tych wysiłków są ciągłe badania nad rozwijającymi się technikami rosyjskiej → w o j n y [t. 4] nowej generacji. Centrum korzysta z szerokiej gamy narzędzi edukacyjnych – od briefingów i przemówień, przez publikację artykułów i książek, aż po stosowanie różnych form symulacji i komputerowych gier wojennych w celu rozpowszechniania faktów o rosyjskiej → a g r e s j i militarno-politycznej.

Centrum zostało utworzone na podstawie działalności Potomac Foundation w styczniu 2018 r. w obliczu oczywistego → k r y z y s u [t. 2] → b e z p i e c z e ń s t w a m i ę d z y n a r o d o w e g o, który pojawił się w momencie rozpoczęcia wojny rosyjsko-ukraińskiej w 2014 r. Centrum funkcjonuje w ramach prawnych The Petersen Group LLC zarejestrowanej w Commonwealth of Virginia oraz w Departamencie Skarbu USA w 2009 r.

Prezesem Centrum Badań nad Wojną Nowej Generacji jest dr P. Petersen, amerykański ekspert ds. obronności, który od października 1991 r. do grudnia 2017 r. pełnił szereg funkcji w The Potomac Foundation; a dyrektorem operacyjnym G. Melcher, który jest także powiązany z Virginia Tech Applied Research Corporation oraz Alion Science and Technology.

NGW Centre realizuje 3 ogólne kierunki działań:

- UE i państwa członkowskie → NAT O [t. 3] powinny mieć pełne i wspólne zrozumienie wojny, jaką obecnie toczy przeciwko nim państwo rosyjskie;
- liberalne demokracje powinny zrozumieć, że polityka jest sztuką kompromisu;
- dzięki narzędziom edukacyjnym opartym na doświadczeniu placówki UE i państwa członkowskie NATO mogą zharmonizować obronę zbiorową, którą należy

mierzyć nie procentami wydanego PKB, ale → o d s t r a s z a n i e m [t. 3] i skutecznością w obronie ich wartości cywilizacyjnych.

Zgodnie z informacjami na stronie internetowej organizacji w swojej pracy zespół centrum wykorzystuje gry symulacyjne, m.in. CONFLICT – analityczną grę wojenną, której celem jest nauczenie graczy → s t r a t e g i i [t. 4] w sposób heurystyczny, prowadzenie analiz na poziomie teatru działań operacyjnych i pomaganie uczestnikom w zrozumieniu strategii i taktyki przeciwnika w rzeczywistości. Na podstawie otwartych i jawnych danych dla poziomów analizy taktycznej, operacyjnej i strategicznej CONFLICT umożliwia uczestnikom pracę nad różnorodnymi zestawami scenariuszy, testowanie starych założeń i opracowywanie nowych koncepcji operacji. Grę można wykorzystać do pogłębionej analizy elementów takich jak skład głównej struktury sił, ogólna strategia lub potrzeba wcześniejszego rozmieszczenia albo szybkiej → mobilizacji [t. 3] sił. Jeśli zachodzi potrzeba przeprowadzenia bardziej szczegółowych badań na poziomie inżynieryjnym, NGW Centre może wykonać dodatkowe analizy w laboratorium w celu wyjaśnienia pytań i problemów, a następnie kontynuować prace w Parsons Universal Modeling Laboratory (PUMA). Oba narzędzia są zaprojektowane do działania na jawnym poziomie tajności z uczestnikami wielostronnymi.

Jednostki w grze CONFLICT podzielone są na brygady lub bataliony, eskadry lub skrzydła i morskie grupy zadaniowe liczące od 4 do 6 okrętów, w zależności od wielkości i czasu trwania analizowanego scenariusza. Symulacja obejmuje jednostki powietrzne, morskie i lądowe. Jednostki są zróżnicowane wg typu, występują brygady zmotoryzowane, pancerne czy powietrzne. Ten sam typ jednostki jest dodatkowo odróżniony od swoich odpowiedników na podstawie danych dotyczących używanych przez jednostkę technologii i poziomu wyszkolenia.

Mechanika gry umożliwia odzwierciedlenie dyplomacji za pomocą ustalenia rozgrywki między narodami lub organizacjami. Gracze mogą swobodnie wchodzić w interakcje w dowolny sposób, który uznają za odpowiedni, i mogą prowadzić politykę w ramach swoich celów. W ten sposób dany kraj może zdecydować się na wyjście z sojuszu lub przystąpienie do innego, zezwolić na wykorzystanie swoich baz itd. CONFLICT może pomóc w analizowaniu złożonych scenariuszy, które wykorzystują niekinetyczne techniki nowej generacji lub → w o j n ę h y b r y d o w ą [t. 4], a także ułatwić wybór działań, jakie mogą podjąć państwa przed konfliktem zbrojnym.

Gracze otrzymują zestaw celów, które można modyfikować, zwykle koncentrują się na ochronie → s u w e r e n n o ś c i [t. 4] narodowej, kontrolowaniu terytorium itp. Zarządzanie czasem w grze zależy od rodzaju prowadzonej gry. Walka kończy się, gdy jedna lub druga strona poniosła straty większe niż te, które jest gotowa ponieść, aby wykonać misję ofensywną bądź defensywną, zgodnie z rozkazem gracza. Atakujący albo przerwie atak, albo obrońcy opuszczą pozycje obronne, umożliwiając napastnikowi wykorzystanie okazji dokonania przełomu.

Jak podaje organizacja, zespół NGW Centre przeprowadził już symulacje/gry wojenne na wysokim szczeblu w USA, Szwecji, Estonii, Łotwie, Polsce, Wielkiej Brytanii i Rumunii; podczas każdego z tych wydarzeń napotykał pewien opór przed badaniem sposobu działania wroga, który objawiał się jako albo analizowanie najbardziej prawdopodobnego działania wroga, albo najniebezpieczniejszej rzeczy, którą wróg mógłby zrobić. Centrum na swojej stronie internetowej przytacza w tym kontekście termin „rozmyślna ignorancja" J.G. Hinesa, który miałby opisywać ową determinację, by usuwać z pola widzenia możliwe nieprzyjemności. Podejście NGW Centre do symulacji i gier wojennych nie pozwala graczom uniknąć winy za brak działania, tak samo jak za błędne działanie związane z nieuchwyceniem zależności między strategią a np. ukształtowaniem terenu.

Olga Wasiuta

NGWCentre.com (dostęp 15.02.2020).

ANALIZA STRATEGICZNA – termin naukowy i działalność praktyczna odnosząca się do procesu wykorzystywanego w → n a u k a c h o b e z p i e c z e ń s t w i e [t. 3] do badania, przeciwdziałania i zapobiegania → z a g r o ż e n i o m [t. 4] oraz w celach diagnostycznych i prognostycznych. Zgodnie z ujęciem operacyjnym autorstwa Andrzeja Dawidczyka to zespół czynności podejmowanych w zakresie → b e z p i e c z e ń s t w a [t. 1] przez organy kierownicze państwa (za pośrednictwem norm, instytucji, instrumentów polityki bezpieczeństwa, konkretnych metod i narzędzi), a służących identyfikacji procesów i zdarzeń o dużej i bardzo dużej sile oddziaływania oraz procesów i zdarzeń nowych (słabo rozpoznanych i dotychczas niewystępujących), mogących w przyszłości determinować warunki przetrwania oraz rozwoju państwa. Natomiast w ujęciu narzędziowym analiza strategiczna w dziedzinie bezpieczeństwa to zbiór metod, technik i narzędzi pozwalających na zbudowanie zasobu informacyjnego na użytek procesu planowania strategicznego (którego analiza strategiczna jest częścią), a także – strategicznego zarządzania w dziedzinie bezpieczeństwa, a więc zarówno → o b r o n n o ś c i, jak i wojskowości. Pierwsze ze wskazanych ujęć teoretycznych kładzie nacisk na możliwość budowy planu strategicznego, czyli na opracowanie, wybór i realizację najbardziej realnej i efektywnej strategii. Celami drugiego okazują się dookreślenie aktualnych szans, wyzwań i zagrożeń oraz diagnoza zdolności państwa do odpowiedniej reakcji na pojawiające się lub potencjalne nowe szanse, wyzwania i zagrożenia. Tego typu ujęcia kładą ogromny nacisk na komplementarność metod → a n a l i z y s t r a t e g i c z n e j z ich praksеologicznym zastosowaniem w procesie zarządzania bezpieczeństwem.

Analizy strategicznej nie można separować od szeroko pojętej działalności strategicznej, ponieważ bez udziału analizy w procesach z tego zakresu nie można w ogóle mówić o strategicznym podejściu do zarządzania bezpieczeństwem państwa. Dosyć

zgodnie uznaje się w środowisku naukowym, że analiza strategiczna, jako dyscyplina zarysowująca swoje granice badawcze, pojawiła się na przełomie lat 50. i 60. XX w. w związku z sukcesami amerykańskich firm konsultingowych, przy czym jej „ekspansję" kojarzono głównie z naukami z pogranicza ekonomii i zarządzania organizacją (przedsiębiorczości). Złożoność, turbulencyjność, nieprzewidywalność i niejednoznaczność procesów związanych z rozwojem sektora przedsiębiorczości komercyjnej spowodowały żywiołowe wzniecenie zainteresowania kwestiami analizy strategicznej, planowania strategicznego i zarządzania strategicznego. Początkowo na potrzeby analizy strategicznej stosunkowo pobieżnie traktowano kwestię reagowania na zmiany oraz dostosowywania się do nowych tendencji w otoczeniu podmiotu. Ewolucja płaszczyzn, na których prowadzono analizę strategiczną, spowodowała stopniową adaptację ustaleń z zakresu nauk o zarządzaniu na grunt sił zbrojnych i poszczególnych państw.

Głównym cele analizy strategicznej to określenie czynników decydujących o przyszłości państwa oraz sformułowanie odpowiednich strategii działania. Grażyna Gierszewska i Maria Romanowska zwracają uwagę, że analiza strategiczna w obszarze bezpieczeństwa powinna umożliwićrealizację 4 zasadniczych celów:

- poznania otoczenia,
- prognozowania zmian w otoczeniu,
- oceny danego podmiotu,
- prognozy zmian zachodzących wewnątrz podmiotu (państwa). Fundamentalnym założeniem, od którego należy wyjść, jest uznanie podejścia analitycznego za istotne dla rozpatrywania systemu bezpieczeństwa państwa jako całości oraz w rozbiciu na poszczególne jego podsystemy i instytucje odpowiedzialne za kwestie preparacyjne i operacyjne. Istotą analizy strategicznej jest wszakże dekompozycja badanego systemu oraz skupienie się na cechach i relacjach, powstałych w wyniku dekompozycji, elementów, a także jednoczesne zajmowanie się otoczeniem państwa (podmiotu bezpieczeństwa) analizowanym interdyscyplinarnie z wykorzystaniem szeregu metod ilościowych i jakościowych, charakterystycznych dla nauk o bezpieczeństwie, zarządzaniu, polityce, ekonomii, psychologii czy statystyki itp. Zdaniem Joanny Kałkowskiej do katalogu szczegółowych celów analizy strategicznej zaliczyć można m.in.:
- ocenę zdolności i możliwości państwa do realizacji poszczególnych strategii szczegółowych (specjalizacja, dywersyfikacja),
- określenie oczekiwań interesariuszy w →ś r o d o w i s k u b e z p i e c z e ń s t w a [t. 4],
- analizę otoczenia wewnętrznego i zewnętrznego podmiotu bezpieczeństwa oraz zmian w nim zachodzących,
- ocenę konkurencyjności zasobów będących do dyspozycji instytucji państwa,
- określenie zasobów i umiejętności pozwalających na zbudowanie przewagi konkurencyjnej w sferze bezpieczeństwa w przyszłości.

Obecnie przyjmuje się wiele definicji analizy strategicznej, odnoszących się do jej poszczególnych cech, zalet, problemów strategicznych, procedur planowania strategicznego, formułowania i realizacji strategii bezpieczeństwa czy elementów myślenia strategicznego. Przykładowo: Józef Penc w swojej definicji analizy strategicznej podkreśla istotę działań diagnostycznych danego podmiotu oraz jego otoczenia na rzecz budowy planu strategicznego oraz jego realizacji. Zdaniem tego autora analiza strategiczna jest zbiorem metod i działań diagnozujących przedsiębiorstwo (organizacja zarządzania) lub inny podmiot wraz z jego otoczeniem w celu zbadania obecnych i przyszłych okoliczności mogących mieć wpływ na formułowanie wariantów strategii (np. bezpieczeństwa). Trzeba też podkreślić, że współcześnie analizę strategiczną można rozumieć nie tylko przez pryzmat etapowości postępowania, lecz także przez sposób działania właściwy wszystkim podmiotom, które myślą strategicznie. To właśnie poziomy myślenia kategoriami strategicznymi jest podstawą do wyodrębnienia różnych rodzajów analizy strategicznej.

Jeżeli chodzi o rodzaje analizy strategicznej i przyporządkowane im poziomy myślenia strategicznego, to Piotr Daniluk wymienia następujące ich typy:

- analiza ogólna – myślenie ogólne ukierunkowane na zewnątrz pozwala na szerokie spojrzenie na to, co rozgrywać się będzie nawet w stosunkowo odległej przyszłości. Ten typ analizy opiera się na analizie trendów. Wiedza potrzebna do jej przeprowadzenia pochodzi od specjalistów umiejących kojarzyć zjawiska zachodzące na wielu płaszczyznach funkcjonowania państwa oraz rozpatrywane przez pryzmat jednej konkretnej dyscypliny (polityki, ekonomii, technologii itd.);
- analiza celowa – myślenie obiektowe (celowe) ukierunkowane na zewnątrz pozwala skupić się na wybranych podmiotach i przypisanych im obszarów bliskiego otoczenia. Ważne są tu: znajomość uwarunkowań danego sektora bezpieczeństwa oraz podmiotów w nim występujących z ich historią, kulturą organizacyjną i zasadami funkcjonowania;
- analiza podmiotu – myślenie ukierunkowane do wewnątrz pozwala wieloaspektowe przyjrzenie się podmiotowi bezpieczeństwa skutkujące określeniem mocnych i słabych jego stron. Wiedza specjalistyczna dotyczy w tym przypadku funkcji (naukowej, technicznej czy logistycznej), zasobów (informacyjnych czy psychospołecznych) albo podsystemów bezpieczeństwa (podsystem kierowania, podsystem operacyjny);
- analiza integrująca – myślenie integrujące spojrzenie na zewnątrz i do wewnątrz jest ukierunkowane na budowanie wniosków końcowych potrzebnych do konstruowania wstępnych koncepcji strategii. Myślenie tego typu powinno integrować wiedzę osób mających doświadczenie w zakresie planowania strategicznego, budowania strategii oraz oraz analizy otoczenia i podmiotu.

Pomimo – podkreślanej przez specjalistów z zakresu bezpieczeństwa państwa – niekonsekwencji przy prowadzonych w Polsce (w sposób doraźny) przeglądach strategicznych (świadczących o wysokiej kulturze organizacyjnej w wymiarze

strategicznym) analiza strategiczna jest procesem zachodzącym na różnych płaszczyznach bezpieczeństwa, obronności czy zarządzania kryzysowego. To podstawa do budowy → Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, czyli rządowej inicjatywy (akceptowanej na szczeblu prezydenckim) zawierającej zestaw interesów narodowych, celów strategicznych, uwarunkowań środowiska bezpieczeństwa, narzędzi i sposobów zapewniania bezpieczeństwa w perspektywie długofalowej oraz priorytety państwa polskiego w sferze → bezpieczeństwa narodowego [t. 1]. Analiza strategiczna powinna być realizowana interdyscyplinarnie, a zatem powinna uwzględniać wiele faktów i perspektyw z obszaru → bezpieczeństwa politycznego [t. 1], społecznego, militarnego, ekonomicznego i technologicznego. W ujęciu najogólniejszym: analiza strategiczna powinna dostarczyć odpowiedzi na pytania: Co musi zostać zrealizowane? W jakich warunkach ma to nastąpić? Przy jakich ograniczeniach?

Podstawową metodą analizy strategicznej jest zintegrowana analiza SWOT (S – *Strenghts*, W – *Weaknesses*, O – *Opportunities*, T – *Threats*), obejmująca analizę środowiska zewnętrznego podmiotu bezpieczeństwa (szanse i zagrożenia) oraz analizę środowiska wewnętrznego (silne i słabe strony). Chodzi w niej o wskazywanie silnych stron i możliwości wykorzystywania szans przy jednoczesnym eliminowaniu słabości i unikaniu zagrożeń. Inną ważną metodą analizy strategicznej jest metoda PEST (P – *Political*, E – *Economic*, S – *Social*, T – *Technological*), służąca badaniu makrootoczenia podmiotu bezpieczeństwa i określająca kluczowe sfery otoczenia wpływające na funkcjonowanie państwa (polityczne, ekonomiczne, społeczno-kulturowe, technologiczne). Delficka metoda badawcza jest z kolei jedną z metod heurystycznych, bazującą na wiedzy, doświadczeniu i opinii ekspertów. Jej cechami są: niezależność i anonimowość ekspertów oraz ich opinii, różnorodność dobieranych ekspertów pod względem wykształcenia i praktyki zawodowej, wieloetapowość procesu analityczno-badawczego, kolektywny charakter wyników badania, użyteczność metody delfickiej do prognozowania zjawisk i procesów przyrodniczo-technicznych oraz społeczno-politycznych, a także stosowalność metody w analizie teraźniejszości i przyszłości. Metody scenariuszowe są jednym z rodzajów metod analizy strategicznej wykorzystywanych w zarządzaniu strategicznym i należą do kategorii metod analizy otoczenia. Te metody są stosowane w celu prognozowania zjawisk, zdarzeń i procesów, które mogą nastąpić we wciąż zmieniającym się otoczeniu oraz przewidywania ich potencjalnego wpływu na państwo. Metoda scenariuszowa bywa pomocna podczas przeprowadzanej analizy makrootoczenia, formułowania prognoz rozwoju sytuacji, określania misji i celów strategicznych oraz ustalania opcji strategicznych. Z uwagi na wymienione już wcześniej typy analizy strategicznej można przyjąć za użyteczne dla potrzeb bezpieczeństwa m.in. następujące zestawy metod:

- w analizie makrootoczenia – analiza PEST, scenariusze otoczenia, analiza synergiczna, analiza luki strategicznej;

- w analizie szczegółowej – analiza Stakeholders, analiza sił w otoczeniu, struktura domeny/sektora, Analiza Grup Strategicznych, charakterystyka domeny, benchmarking, profil i atrakcyjność sektora;
- w analizie podmiotu – podsystemy, zasoby, funkcje, procesy, metody portfelowe;
- w analizie podsumowującej – analiza SWOT, analiza TOWS, analiza SPACE.

Paweł Łubiński

A.J. Chodubski, *Wstęp do badań politologicznych*, Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2008; P. Daniluk, *Analiza strategiczna bezpieczeństwa. Proces – metody – decyzje*, Bogucki Wydawnictwo Naukowe, Wrocław 2018; tenże, *Bezpieczeństwo i zarządzanie. Analiza strategiczna*, Difin, Warszawa 2015; W. Danielak, E. Frankowska, A. Kułakowska, *Zarządzanie organizacją w aspekcie finansowym i strategicznym. Ujęcie teoretyczne i praktyczne*, Wydawnictwo Exante, Wrocław 2017; A. Dawidczyk, *Analiza strategiczna w dziedzinie bezpieczeństwa państwa. Wybrane metody*, Difin, Warszawa 2020; G. Gierszewska, M. Romanowska, *Analiza strategiczna przedsiębiorstwa*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2014; J. Gryz, *Zarys teorii bezpieczeństwa*, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2011; M. Kozub, A. Mitręga, *Podstawy strategii bezpieczeństwa – wybrane aspekty*, Wydawnictwo Uniwersytetu Jana Kochanowskiego, Kielce 2018; M. Kozub, A. Mitręga, A. Zagórska, *Studia strategiczne w kreowaniu bezpieczeństwa do końca pierwszej połowy XXI wieku*, Wydawnictwo UniwersytetuJana Kochanowskiego, Kielce 2019; M.Z. Kulisz, *Zarządzanie strategiczne bezpieczeństwem Rzeczypospolitej Polskiej*, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2011; M. Marchesnay, *Zarządzanie strategiczne. Geneza i rozwój*, tłum. M. Egeman, Wydawnictwo Poltext, Warszawa 1999; J. Penc, *Strategie zarządzania. Perspektywiczne myślenie i systemowe działanie*, Wydawnictwo Placet, Warszawa 1994; Z. Polcikiewicz, *Teoretyczne i praktyczne aspekty strategii bezpieczeństwa*, Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika, Toruń 2020; Z. Sabak, *Strategia. Słownik terminów*, Wydawnictwo Akademii Narodowej, Warszawa 2014; A. Stabryła, *Zarządzanie strategiczne w teorii i praktyce firmy*, Wydawnictwo Naukowe PWN, Warszawa–Kraków 2002.

ANARCHIZM W POLSCE – już na kilkanaście lat przed odzyskaniem przez Polskę niepodległości w 1918 r. wielu polskich inteligentów inspirował anarchizm. Po pewnym czasie rewidowali oni jednak swoje poglądy, tak jak np. J. Zieliński, który w młodości propagował anarchosyndykalizm, a w niepodległej Polsce piastował urząd radcy w Ministerstwie Opieki Społecznej, czy też L. Kulczycki, który po młodzieńczym opowiadaniu się za anarchizmem w 1920 r. należał już do Narodowej Partii Robotniczej. W młodości dość krótko anarchizm fascynował także A. Niemojewskiego, późniejszego socjalistę, który po wybuchu rewolucji 1905 r. zbliżył się do → n a c j o n a l i z m u [t. 3]. Polityczna droga Niemojewskiego była całkowitym przeciwieństwem zmian światopoglądu społeczno-politycznego J.W. Machajskiego, który w młodości należał do jeszcze wtedy wiernej narodowcom organizacji młodzieżowej „Zet", aby w 1909 r. utworzyć organizację anarchistyczną o nazwie Zmowa Robotnicza, której zwolennicy stosowali terror ekonomiczny wobec władz carskich, kapitalistów i burżuazji. Uważa się, że Machajski na początku XX w. na ziemiach polskich wchodzących w skład Imperium Rosyjskiego rozwinął anarchistyczny ruch robotniczy określany jako machajewszczyzna, który występował przeciwko państwu,

a także inteligencji. Propagatorami idei anarchistycznych na ziemiach polskich na przełomie XIX i XX w. byli również E. Abramowski i A. Wróblewski. Chociaż Abramowski nigdy nie nazywał swoich poglądów anarchistycznymi, to odnoszenie się do tej ideologii nietrudno znaleźć w jego licznych publikacjach. W wydanej w 1904 r. książce *Socjalizm a państwo. Przyczynek do krytyki współczesnego socjalizmu* autor stwierdził, że państwo powinno być zastąpione dobrowolnymi i kooperującymi ze sobą zrzeszeniami. Myśliciel ten na długo przed triumfem bolszewików wypowiadał się negatywnie na temat → k o m u n i z m u [t. 2], w którym widział ograniczenia dla ludzkiej i obywatelskiej wolności. Abramowski jest autorem znanej *Zmowy powszechnej przeciw rządowi*, której słowa na początku XX w. skierowane zostały przeciwko władzy carskiej:

Nie będziemy odtąd korzystać z żadnych jego praw, ani z sądów, ani ze szkół, ani z policji; nie będziemy odtąd przyjmować żadnej służby rządowej, ani pomagać przy dostawach dla wojska, ani kupować rządowych papierów i wódki. Żadnej łączności z najeźdźcami, żadnego zbliżenia się!

Do słów Abramowskiego radykalne środowiska antykomunistycznej opozycji politycznej w Polsce odwoływały się jeszcze w 1989 r.

Przed 1918 r. oraz w niepodległej międzywojennej Polsce ruch anarchistyczny nigdy nie zyskał szerokiej sympatii, można nawet stwierdzić, że miał marginalne znaczenie. Złożyło się na to kilka przyczyn. Najważniejszym powodem było to, że anarchizm w ogóle nie uwzględniał aspiracji odbudowania wolnej Polski. To sprawiało, że traktowany był z dużą rezerwą przez wielu otwarcie i lewicowo nastawionych polskich inteligentów, robotników i chłopów. W powszechnej świadomości społecznej, o ile w ogóle wiedziano, czym jest anarchizm, nie wiązano go z koncepcjami Machajskiego i Abramowskiego, ale z jakąś nową emanacją komunizmu. W rewolucyjnych latach 1905–1907 utożsamiający się z anarchizmem rzemieślnicy w Białymstoku, Warszawie i Łodzi w zdecydowanej większości reprezentowali narodowość żydowską. Około 500 żydowskich białostockich anarchistów-komunistów skupionych w grupie Czarnego Sztandaru zaczęło podążać za słowami J. Grossmana z Odessy, który twierdził, że każdy wyzyskiwacz powinien stać się obiektem ataku, jeśli nie ma nawet bezpośredniego powodu, aby go zamordować. W 1905 r. wśród żydowskich anarchistów z Łodzi i Warszawy działała także organizacja Internacjonał, która dość szybko została rozbita przez rosyjską Ochranę. W latach 1910–1913 w Królestwie Polskim działała również siejąca terror, nieraz wyłącznie przypadkowy bandytyzm, Grupa Rewolucjonistów Mścicieli, której założycielami byli E. Dłużniewski i J. Piątek, wcześniej związani z Polską Partią Socjalistyczną Organizacją Bojową (PPS-OB), potem PPS Frakcją Rewolucyjną.

W Polsce w latach 1926–1939 działała konspiracyjna Anarchistyczna Federacja Polski (AFP). Federacja liczyła w różnych latach od kilkudziesięciu do kilkuset działaczy i sympatyków. W AFP największą liczbę anarchistów stanowiły osoby narodowości żydowskiej, jak J. Rogalski, właśc. J. Szlamowicz, P.L. Marek, S. Filmus,

S.H. Weindling, a także B. Wolman. Ograniczało to skuteczne i większe oddziaływanie AFP na polskie społeczeństwo, w którym wielu anarchistów mylono z komunistami. Anarchiści wszelkimi sposobami przekonywali więc, że są wrogami komunistów, zwłaszcza tych rezydujących na Kremlu. W listopadzie 1928 r. na jednej z warszawskich ulic AFP wywiesiła wielki transparent z napisem: „Niech żyje anarchizm. Precz z międzynarodówką sowiecką, która sprzedała lud rosyjski. Niech żyje międzynarodówka czikagowska". W Baranowiczach w styczniu 1929 r. działacze AFP rozrzucili ulotki i rozlepili odezwy napisane w języku rosyjskim, w których występowali przeciwko ustrojowi politycznemu w ZSRR i kapitalistycznemu w Polsce. Wzrost aktywności AFP w latach 1928–1929 nie uszedł uwadze władzom sanacyjnym II RP. W Tarnowie na początku marca 1929 r. miał miejsce pierwszy w II RP „proces o anarchizm", w którym jeden z członków AFP otrzymał karę 5 lat więzienia. W Warszawie, również w marcu 1929 r., zostało aresztowanych 143 anarchistów. Cios zadany wiosną 1929 r. anarchistom był bardzo poważny. Pod koniec 1929 r. pion polityczny polskiej → p o l i c j i [t. 3] państwowej informował, że polscy anarchiści liczą się z tym, że w Polsce niewykluczony jest nawet całkowity zanik głoszonych przez nich idei.

Przed 1939 r. grupa zwolenników anarchosyndykalizmu działała również w Związku Związków Zawodowych (ZZZ), którego jednym z liderów był komunista T. Pilarski. W 1940 r. anarchizujący działacze ZZZ powołali do życia Syndykalistyczną Organizację „Wolność" (SOW), która stworzyła kilka oddziałów partyzanckich. SOW dysponowała również własną drukarnią wojskową, wydawała m.in. podziemne czasopisma, takie jak „Walka Ludu" czy poradnik wojskowy „Towarzysz Pancerny". W maju 1943 r. anarchosyndykaliści podporządkowali się zbrojnie i operacyjnie Armii Krajowej (AK). W latach 1943–1944 powróciły też dobre relacje z powstałym w 1941 r. Związkiem Syndykalistów Polskich (ZSP), w którego szeregach działała największa liczba konspiratorów wywodzących się z przedwojennego ZZZ. ZSP w przeciwieństwie do anarchizującej SOW był organizacją propaństwową. Zbliżenie polityczne ZSP i SOW było zgodne z intencją AK i wolą władz Polskiego Państwa Podziemnego (PPP). W powstaniu warszawskim syndykaliści walczyli w 104 Kompanii AK.

Po zakończeniu II wojny światowej w Polsce podporządkowanej komunistom odbudowanie legalnie funkcjonującego ruchu anarchistycznego było niemożliwe. W latach 1945–1950 działała natomiast podziemna Federacja Polskich Anarchosyndykalistów (FPAS), której próby uzyskania wpływu w środowiskach robotniczych były całkowicie nieudane. Sympatycy idei anarchistycznych wciąż jednak w Polsce istnieli, pojawiając się na spotkaniach dyskusyjnych warszawskiego Klubu Krzywego Koła (w latach 1955–1962) czy też w latach 1976–1977 na spotkaniach Komitetu Obrony Robotników (KOR). Idee anarchistyczne, w tym wskazówki dotyczące kooperatyzmu proponowanego przez Abramowskiego, odżyły w Polsce wraz z narodzinami NSZZ „Solidarność". W 1980 r. takie poglądy propagował m.in. Z. Szpakowski, współtwórca

solidarnościowego programu „Samorządnej Rzeczypospolitej". O koncepcjach Szpakowskiego, byłego → ż o ł n i e r z a [t. 4] AK i Narodowych Sił Zbrojnych (NSZ) napisała również w 1982 r. zachodnioniemiecka gazeta anarchistyczna „Schwarzer Faden", a także zainteresowała się nimi polska Służba Bezpieczeństwa (SB) (sprawa operacyjnego sprawdzenia „Amelot"). Podczas tej samej operacji SB rozpracowywała inną grupę warszawskich anarchistów, tzw. Sigmę, która istniała w latach 1980–1981. W kolejnych latach nastąpił pewien wzrost zainteresowania anarchizmem, zwłaszcza wśród młodzieży mieszkającej w największych polskich miastach. W Gdańsku w czerwcu 1983 r. rozpoczął działalność Ruch Społeczeństwa Alternatywnego (RSA). Założycielami ruchu byli J. Waluszko, C. Waluszko, K. Skiba i W. „Jacob" Jankowski. O RSA zrobiło się głośno w kręgach dotychczas funkcjonującej opozycji politycznej, ale także SB i milicji po wydarzeniach w Gdańsku 1 maja 1985 r. Tego dnia RSA skutecznie przeciwstawił się pacyfikacji niezależnej solidarnościowej manifestacji przez zmotoryzowane Odwody Milicji Obywatelskiej (ZOMO). ZOMO zostało zaskoczone oporem i podjęciem zaciętej walki przez demonstrantów, wśród których wyróżniali się trójmiejscy anarchiści. Miesiąc wcześniej, tj. w kwietniu 1985 r., powstał ruch Wolność i Pokój (WiP), w którym również znaleźli się zwolennicy anarchizmu tacy jak np. M. Kurzyniec w Krakowie. W maju 1988 r. dzięki staraniom wspomnianego J. Waluszki i K. Galińskiego powstała Międzymiastówka Anarchistyczna, która w listopadzie 1989 r. została przekształcona w Federację Anarchistyczną (FA). W latach 1988–1991 idee anarchistyczne zaczęły cieszyć się zainteresowaniem znacznej grupy młodzieży akademickiej oraz uczniów szkół średnich, zyskały poparcie wśród części Federacji Młodzieży Walczącej, a także przyciągały do siebie osoby związane z kontrkulturą punkową. Popularność RSA, WiP, MA/FA wynikała z następujących przyczyn:

- radykalnego antymilitaryzmu – jako przykłady należy wspomnieć postulat wprowadzenia zastępczej służby wojskowej, bojkot studium wojskowego na polskich uczelniach (jesień 1988 r.), publiczne palenie książeczek poborowych Ludowego Wojska Polskiego (LWP) (wiosna 1989 r.), okupację studium wojskowego na polskich uczelniach (jesień 1989 r.), żądanie wycofania wojsk sowieckich z Polski (burzliwe demonstracje w Krakowie w maju 1989 r.);
- odrzucenia jakiegokolwiek porozumienia z komunistami (tj. Okrągłego Stołu), sprzeciwu wobec nie w pełni demokratycznych wyborów w czerwcu 1989 r.;
- otwartości na kontrkulturę, feminizm, zwrócenia uwagi na problemy ekologiczne (zablokowanie budowy elektrowni jądrowej w Żarnowcu – 1989 r., blokowanie budowy zapory w Czorsztynie 1990 i 1991 r.).

Po wzmożonej działalności na przełomie lat 80. i 90. XX w. aktywność ruchu anarchistycznego w Polsce wyraźnie spadła i podobnie jak w międzywojniu anarchiści mieli politycznie dość marginalne znaczenie. W latach 90. wiele inicjatyw anarchiści przeprowadzali wspólnie z innymi środowiskami politycznymi. W 1992 r. gdańscy anarchiści nawiązali współpracę z Wolnymi Związkami Zawodowymi (WZZ) A. Gwiazdy,

występując przeciwko podwyżkom energii, w obronie kupców gdańskich, a także próbując obalić miejscową radę miasta. W 1994 r. krakowska FA i osoby związane z Klubem im. Józefa Mackiewicza powołały Akademickie Stowarzyszenie na rzecz Wolnej Czeczeni, które organizowało serię pikiet i demonstracji pod hasłem „Wolność dla Czeczeni" oraz konwoje z pomocą dla tego kraju, zaatakowanego i okupowanego przez Federację Rosyjską we wrześniu i październiku 1995 r. oraz w styczniu i lutym 1996 r. Krakowscy anarchiści w 1994 r. zainicjowali również powstanie Komitetu Wolny Kaukaz (KWK). W latach 1993–2001 krakowska FA organizowała też uliczne protesty przeciwko balowi charytatywnemu, który na początku każdego roku odbywał się w miejscowym magistracie. W opinii krakowskiej FA coroczne wydarzenie nie służyło potrzebom ludności, ale było okazją do scalania szemranych interesów miejscowej władzy i biznesu. W 1999 r. anarchiści jednoznacznie występowali przeciwko wejściu Polski do → N A T O [t. 3]. Po wydarzeniach z 11 września 2001 r. trójmiejscy i poznańscy anarchiści w kolportowanych ulotkach pisali, że Amerykanie w ramach podjęcia walki z tzw. światowym → t e r r o r y z m e m [t. 4] winni ją rozpocząć od samych siebie. Wskazywali, że USA w latach 80. XX w. były odpowiedzialne za rozwój muzułmańskich fundamentalistów (→ f u n d a m e n t a l i z m r e l i g i j n y [t. 2]) w Afganistanie. Anarchiści w swoich pismach nie mieli złudzeń, że z ataku na WTC w niedalekiej przyszłości skorzystają takie kraje jak Rosja, Izrael i Turcja, które pod pretekstem walki z terroryzmem rozprawią się z Czeczenami, Palestyńczykami i Kurdami. W XXI w. najliczniejsze protesty, które organizowali lub współorganizowali polscy anarchiści, miały miejsce w marcu 2003 r. po amerykańskim ataku na Irak, zgromadziły one kilkuset demonstrantów w Warszawie, Krakowie, Poznaniu i Wrocławiu. 30 kwietnia 2004 r. w Warszawie przeciwko obradom Światowego Forum Ekonomicznego protestowało kilka tysięcy manifestujących z Polski i całego świata. Anarchiści przewodzili również protestom przeciwko instalacji antyrakietowej. Na demonstracji pod hasłem „Nie chcemy być tarczą USA", do której doszło w Słupsku 29 kwietnia 2008 r., zjawiło się 800 osób. Na czele pochodu maszerowali demonstranci przebrani w maski G.W. Busha, który na łańcuchu trzymał L. Kaczyńskiego i D. Tuska. Anarchiści współorganizowali także protesty uliczne 19–20 lutego 2009 r. w Krakowie, gdzie obradowali ministrowie obrony krajów należących do Paktu Północnoatlantyckiego. Na demonstracji anarchiści zjawili się z wielkim transparentem „NATO legalny terrorysta". W XXI w. wciąż pamiętano o „sprawie czeczeńskiej". W styczniu 2005 KWK zorganizował również protesty przeciwko wizycie prezydenta Putina w 60. rocznicę wyzwolenia obozu w Oświęcimiu. W latach 2009–2019 polscy anarchiści skupiali się też na wielu mniej medialnych zagadnieniach takich jak czynna obrona eksmitowanych lokatorów z kamienic, dokarmianie bezdomnych na ulicach, pomoc emigrantom i ich wspieranie.

Remigiusz Kasprzycki

R. Antonów, *Pod czarnym sztandarem. Anarchizm w Polsce po 1980 roku*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2004; tenże, *Za wolnością – przeciwko państwu. Poglądy współczesnych polskich anarchistów*, Wydawnictwo Adam Marszałek, Toruń 2012; R. Kasprzycki, *Polski ruch anarchistyczny wobec współczesnych konfliktów zbrojnych*, [w:] *Bezpieczeństwo współczesnego świata. Historia, wyzwania, konflikty zbrojne*, J. Karwat (red.), Wydawnictwo Wyższej Szkoły Handlu i Usług, Poznań 2014; A. Kruczkiewicz, *Ruch anarchistyczny w Polsce. Program i działalność 1983–1987*, Inny Świat, Mielec 1997.

ANARCHIZM W PRAKTYCE – anarchiści nie ograniczali swojej działalności wyłącznie do rozważań teoretycznych. Wielu z nich zawiązywało stowarzyszenia, bractwa, federacje, związki, ruchy, a także osobiście brało udział w buntach, rewolucjach, powstaniach i → w o j n a c h [t. 4]. W XIX w. licznie uczestniczyli w rewoltach Wiosny Ludów, Komunie Paryskiej. Najbardziej anarchistyczną rewoltą było jednak trwające w latach 1865–1869 powstanie chłopów-anarchistów w Meksyku. W drugiej fazie powstania w Meksyku jednym z przywódców był J. Lopez Chavez. W XIX-wiecznej Europie Zachodniej wyjątkową aktywność wykazywał

M. Bakunin, który w maju 1849 r. walczył na drezdeńskiej barykadzie, w 1870 r. w powstaniu w Lyonie, a w 1874 r. w Bolonii. W 1863 r. został przywódcą międzynarodowej wyprawy, która szykowała się do militarnego wsparcia polskiego powstania styczniowego. Bakunin w 1864 r. założył tajną organizację spiskową, tzw. Bractwo Międzynarodowe, którego celem miało być przygotowanie wybuchu rewolucji, a w 1868 r. Międzynarodowy Alians Demokracji Socjalistycznej, który przyłączył się do I Międzynarodówki. Od 1870 r. większość anarchistów wchodzących w skład I Międzynarodówki była zrzeszona w tzw. Federacji Jurajskiej, której zdecydowaną większość tworzyli szwajcarscy zegarmistrze z obszaru Jury Szwajcarskiej. Po kilku latach doszło do poważnego sporu politycznego między Bakuninem a Marksem. W 1872 r. Bakunin i pozostali anarchiści zostali usunięci z I Międzynarodówki, czego relegowani nigdy nie zaakceptowali i od 1877 r. zwoływali własne międzynarodówki. Pod koniec XIX w. ruch anarchistyczny najliczniejszych zwolenników miał we Francji, Szwajcarii, Włoszech, Hiszpanii, a także w Rosji.

Na przełomie XIX i XX w. doszło do wydarzeń, które sprawiły, że w niektórych kręgach społeczeństw europejskich i amerykańskich anarchiści utracili sympatię. Powodem były zamachy, które w ramach tzw. terroru indywidualnego przeprowadzali „samotni" anarchiści lub częściej poszczególne anarchistyczne siatki terrorystyczne. W marcu 1881 r. Polak I. Hryniewiecki związany z narodnikami, których inspirował również anarchizm, dokonał udanego zamachu na cara Mikołaja II. W czerwcu 1894 r. włoski anarchista S.G. Caserio zasztyletował prezydenta Francji M.-F. Sadiego Carnota, w październiku 1901 r. L. Czolgosz, wywodzący się z polskiej rodziny imigranckiej, postrzelił amerykańskiego prezydenta W. McKinleya, który w tydzień po zamachu zmarł w szpitalu. W 1882 r. po kongresie anarchistycznym w Sewilli od Federacji Robotników Regionu Hiszpańskiego odłączyła się grupa Los Desheredados

(Wydziedziczeni), która przystąpiła do skrytobójczych mordów i terroru ekonomicznego. Jednym z celów zamachów stali się policyjni tajniacy. Skalę problemu zamachów terrorystycznych przełomu XIX i XX w. ukazują dane z 1891 r. W Europie Zachodniej doszło do 1120 zamachów terrorystycznych, a w USA do 522, w których 20 osób straciło życie. Większość tych zamachów słusznie lub niesłusznie powiązano ze środowiskiem anarchistycznym. Po latach okazało się, że wiele terrorystycznych akcji było wyłącznie policyjnymi prowokacjami, których celem było rozbicie lub osłabienie ruchu anarchistycznego. W Hiszpanii w latach 1883–1884 → s ł u ż b y s p e c j a l n e [t. 4] wykreowały fikcyjną organizację anarchistyczną La Mano Negra (Czarna Ręka), która – jak głoszono – chciała w Andaluzji wymordować wszystkich obszarników i zarządców ziemskich. Rozprawienie się z Czarną Ręką posłużyło hiszpańskiej władzy do rozbicia Wydziedziczonych i rozpętania represji wobec wszystkich anarchistów. Metodą prowokacji posłużyła się prawdopodobnie amerykańska → p o l i c j a [t. 3]. Podczas robotniczego mityngu 4 maja 1886 r. wybuchła bomba, zabijając 20 osób, w tym 7 policjantów. Po tym wydarzeniu rozpoczęto represje wobec amerykańskich anarchistów. W latach 1905–1907 najchętniej z podobnych prowokacji korzystała carska Ochrana, nie tylko wobec anarchistów, ale wszystkich zagrażających władzy Imperium Rosyjskiego rewolucjonistów.

W XX w. niejednolity politycznie ruch anarchistyczny nigdy nie wypracował wspólnego stanowiska wobec stosowania → p r z e m o c y [t. 3], zezwolenia na działania o charakterze terrorystycznym, często określane jako tzw. → p r o p a g a n d a [t. 3] czynem, a także popierania lub dezaprobaty wobec wojen czy też rozwijania własnych sił zbrojnych wzorowanych na armiach innych państw. We Francji na początku XX w. powstała anarchizująca Liga Antymilitarystyczna, w Wielkiej Brytanii pacyfistyczne komuny tołstojowskie, które próbowały zawiązywać się nawet w carskiej Rosji, z kolei w Amsterdamie w czerwcu 1904 r. rewolucyjni syndykaliści organizowali Kongres Antymilitarystyczny. W 1914 r. w większości środowisk anarchistycznych konsternację wywołała decyzja cieszącego się sporym autorytetem P. Kropotkina, który wezwał do czynnego udziału w I wojnie światowej i opowiedział się po stronie ententy. W Rosji w lipcu 1917 r. anarchiści wraz z bolszewikami przeprowadzili nieudany przewrót. W czasie rewolucji październikowej anarchiści mieli najliczniejszych zwolenników wśród marynarzy, w listopadzie 1917 r. 200-osobowy oddział anarchisty I. Żuka szturmował carską szkołę junkrów, a anarchista A. Żeleznikow na czele wolnego oddziału kronsztadzkich marynarzy aresztował członków rządu tymczasowego. Drogi anarchistów i bolszewików zaczęły się coraz bardziej rozchodzić. Poważnym osłabieniem dla rosyjskich anarchistów było niezrealizowanie powszechnego uzbrojenia narodu, a także niedopuszczenie przez bolszewików do utworzenia tzw. Czarnej Gwardii, anarchistycznych sił zbrojnych. Obawy bolszewików nie były bezpodstawne. W latach 1918–1921 na terenie południowo-wschodniej Ukrainy rozgorzało anarchistyczne powstanie, na którego czele stał N. Machno. Wierne mu oddziały walczyły z białymi Petlury,

ale także z bolszewikami. Kluczowe dla Machno było poparcie go przez utworzoną w Charkowie w 1918 r. Konfederację Grup Anarchistycznych Ukrainy, zwaną Nabat. Ostatni raz anarchiści przeciwstawili się zbrojnie bolszewikom w 1921 r. w czasie powstania w Kronsztadzie. Od połowy 1922 r. anarchiści w Rosji bolszewickiej byli coraz mocniej prześladowani. Przyjmuje się, że w ZSRR w latach 20. i 30. represjonowano od 80 do nawet 120 tys. anarchistów lub ich zwolenników. W 1932 r. w ZSRR zlikwidowano również ostatnią pacyfistyczną tołstojowską komunę.

W międzywojennej Europie najsilniejszy ruch anarchistyczny funkcjonował w Hiszpanii, gdzie w 1927 r. założono Iberyjską Federację Anarchistyczną (Federación Anarquista Ibérica, FAI). Szacuje się, że już w trakcie → w o j n y d o m o w e j [t. 4] w Hiszpanii, tj. w 1937 r., liczba osób należących do Krajowej Konfederacji Pracy (Confederación Nacional del Trabajo, CNT), hiszpańskiej anarchosyndykalistycznej centrali związków zawodowych, sięgnęła 1,5 mln członków. Mimo konfliktu, jaki we wcześniejszych latach występował między FAI i CNT, po przewrocie gen. Franco wszystkie siły anarchistyczne w Hiszpanii zdecydowanie opowiedziały się po stronie Republiki, wśród nich znaleźli się nawet oficerowie o przekonaniach anarchistycznych. Przykładowo mjr C. Mera dowodził IV Korpusem republikańskiej armii. W większości jednak anarchiści tworzyli własne milicje robotnicze, które opanowały całą Katalonię i znaczną część Aragonii. Mimo → z a g r o ż e n i a [t. 4] przez wojska gen. Franco hiszpańscy komuniści, głównie na polecenie Moskwy, skupili się przede wszystkim na atakowaniu anarchistycznych oddziałów, które latem 1937 r. zostały całkiem rozbite. W Hiszpanii już nigdy ruch anarchistyczny nie odzyskał dawnego znaczenia.

Podobna zapaść i stagnacja w ruchu anarchistycznym nastąpiły po II wojnie światowej na całym świecie. W USA było to już widoczne w międzywojniu. Także w Europie Zachodniej ruch anarchistyczny dotknął wyraźny → k r y z y s [t. 2], zmniejszyła się liczba osób bezpośrednio zaangażowanych w omawianą ideologię i utożsamiających się z nią. Taką tendencję potwierdziły kongresy Międzynarodowej Federacji Anarchistycznej, które odbyły się w 1949 r. w Paryżu i w 1958 r. w Londynie. Niezbyt wielkie znaczenie miało np. założenie w 1950 r. przez brytyjskich anarchosyndykalistów tzw. Solidarity Federation, znanej pod skrótowcem SolFed. W Szwecji Centralna Organizacja Szwedzkich Robotników (Sveriges Arbetares Centralorganisation, SAC) w 1957 r. praktycznie zerwała z syndykalistycznym anarchizmem. Po II wojnie światowej nie inaczej było w Europie Środkowo-Wschodniej, gdzie próby odradzania się i tak słabego międzywojennego anarchizmu z uwagi na komunistyczny zamordyzm, a także całkowitą kontrolę polityczną społeczeństwa, nie miały żadnych szans powodzenia.

W Europie Zachodniej i USA wzrost aktywności anarchistów związany był ściśle z czasem studenckiej rewolty 1968 r. Niestety, wiele młodzieżowych organizacji tak jak anarchiści z przełomu XIX i XX w. ponownie wybrało drogę terrorystyczną. W Wielkiej Brytanii w 1968 r. powstała anarchistyczna Angry Brigade (Brygada

Gniewu), której członkowie do 1970 r. ostrzelali amerykańską ambasadę w Londynie, podłożyli bombę w jednym z londyńskich komisariatów policji, ładunki wybuchowe w Ministerstwie Pracy, dokonali ataków bombowych na biura koncernu Ford Motor Company i samochód stacji telewizyjnej BBC. W lipcu 1970 r. policja aresztowała ścisłe dowództwo Brygady Gniewu, a organizacja została rozbita. Podobnie jak kilka dekad wcześniej, tak w 2 poł. XX w. służby specjalne w celu zniechęcenia społeczeństwa do anarchistów zaczęły stosować dobrze sprawdzone metody prowokacji. W latach 1969–2004 we Włoszech przeprowadzono kilkanaście takich „działań operacyjnych". Pierwszą była tzw. sprawa Piazza Fontana, kiedy w grudniu 1969 r. od wybuchu bomb zginęło 17 osób. O zamachy oskarżono anarchistów, ale po 25 latach przyznano, że bomby przygotowały i zdetonowały włoskie służby specjalne w ramach tzw. → s t r a t e g i i [t. 4] napięcia polegającej na zastraszaniu społeczeństwa i wzmocnieniu władzy państwowej. Od 1996 do 2004 r. prowadzono natomiast tzw. sprawę Mariniego, od nazwiska włoskiego prokuratora A. Mariniego, na polecenie którego pod zarzutem działalności terrorystycznej zatrzymywano, aresztowano i represjonowano kilkuset włoskich anarchistów. Ostatecznie w kwietniu 2004 r. odbył się proces 55 oskarżonych anarchistów, z czego 44 osoby zostały uniewinnione. Na początku XXI w. na całym świecie zatrzymano, aresztowano i uwięziono kilkuset anarchistów. W 2004 r. w więzieniach przebywało 20 aktywistów Earth Liberation Front (ELF), obok Earth First! i Animal Liberation Front najbardziej radykalnej anarchizującej ekologicznej organizacji na świecie. W USA dożywotnie wyroki więzienia odsiadywali m.in. związani z ELF i skazani za → t e r r o r y z m [t. 4] T. Kaczynski i F. Thompson. Różnego rodzaju wsparcia więzionym anarchistom stara się udzielać reaktywowany w 1967 r. Anarchistyczny Czarny Krzyż (ACK), którego działalność w latach 30. XX w. całkowicie zamarła. Poza pomocą więzionym anarchistom ACK sporządza także raporty o prześladowanych na całym świecie anarchistach. W latach 2008–2009 do największej liczby aktów terrorystycznych doszło w Grecji. Anarchizujące grupy takie jak Konspiracyjne Komórki Ognia, Frakcja Nihilistów, Walka Rewolucyjna czy Gangi Sumienia głównie w Atenach i Salonikach przeprowadziły falę ataków przeciwko bankom, salonom samochodowym, towarzystwom ubezpieczeniowym, komisariatom policyjnym i budynkom rządowym. Akty terroryzmu w Grecji zbiegły się w czasie z polityczno-ekonomiczno-społecznym kryzysem. W Atenach doszło także do licznych i burzliwych demonstracji ulicznych, w których zawsze brała udział znaczna liczba anarchistów, tak jak 1 maja w latach 80. i 90. w niemieckich miastach, zwłaszcza w berlińskiej dzielnicy Kreuzberg (udział tzw. Rewolucyjnego Bloku), czy w latach 1999–2001 w antyglobalistycznych protestach w Seattle, Pradze i Genui. Podczas protestów w amerykańskim Seattle tamtejsza policja po raz pierwszy została zaskoczona taktyką stosowaną przez zamaskowanych anarchistów z Black Blocu (BB), którzy zastosowali taktykę tzw. wędrujących blokad ulicznych. Działanie to polegało na stałym przemieszczaniu się małych grup demonstrantów

w różne części Seattle, co powodowało paraliż miasta i chaos koordynacji jednostek policyjnych.

Od jesieni 2018 r. anarchiści z BB są obecni w czasie francuskich protestów organizowanych przez tzw. Ruch Żółtych Kamizelek.

Na kilka lat przed rozpadem ZSRR anarchizm zaczął się odradzać w Rosji, Ukrainie, Estonii, Łotwie i Litwie. Mimo pierestrojki Gorbaczowa większa część komunistów z obawą patrzyła na nawet niewielki wzrost popularności anarchizmu w pewnych kręgach sowieckiego społeczeństwa. W maju 1990 r. KGB zamordowało P. Siudę, anarchosyndykalistę, jednocześnie świadka i dokumentalistę masakry robotników w czerwcu 1962 r. w Nowoczerkasku. Mimo wielu przeciwności, konfliktów i różnorodności w Moskwie w sierpniu 1995 r. założono rosyjską Konfederację Rewolucyjnych Anarchosyndykalistów. Antymilitarystyczne hasła, poparcie dla Czeczenii, a także potępienie → a n e k s j i Krymu przez rosyjskich anarchistów nie mogły być tolerowane. Od 2000 r. notowano coraz więcej przypadków zaginięcia i mordowania rosyjskich anarchistów, często bardzo młodych aktywistów. Było to o tyle zaskakujące, że w pierwszej dekadzie XXI w. liczebność ruchu anarchistycznego w Federacji Rosyjskiej wyraźnie zmalała. Szacuje się, że w FR w 2010 r. funkcjonowało jedynie od 800 do 1 tys. czynnych anarchistów. Prawdopodobnie na polecenie Federacyjnej Służby Bezpieczeństwa (FSB) FR w Moskwie w styczniu 2009 r. zastrzelono 26-letnią dziennikarkę i anarchistkę A. Barburową. Wobec rosyjskich anarchistów i antyfaszystów represje zwiększyły się w ostatnich 5–6 latach. W Symferopolu w maju 2014 r. agenci FSB zatrzymali anarchistę O. Kołczenkę, którego pod pretekstem działalności terrorystycznej wywieziono do Moskwy, następnie do Rostowa n. Donem, w którym sąd skazał go na 10 lat łagru. We wrześniu 2019 r. Kołczenko został zwolniony. Największy atak na anarchistów FSB przeprowadziło na terenie całej Rosji na początku stycznia 2018 r. Miało to związek z marcowymi wyborami, było też swoistym pokazem siły rosyjskiej władzy wobec opozycji. Według raportu ACK rosyjskie FSB wymyśliło anarchistyczno-terrorystyczną organizację „Sieć", którą w mieście Penza miał założyć

D. Pczelincew. Działania wobec nieistniejącej „Sieci" posłużyły FSB do intensyfikacji represji wobec rosyjskiego anarchizmu. Prześladowani i zdeterminowani rosyjscy anarchiści, niczym XIX-wieczni narodnicy w carskim imperium, odpowiedzieli indywidualnym terrorem. Pod koniec października 2018 r. 17-letni anarchista M. Złobicki zdetonował bombę w rejonowej siedzibie FSB w Archangielsku. Sprawca zamachu zginął i zranił 4 funkcjonariuszy FSB.

Remigiusz Kasprzycki

Anarchizm: nowe perspektywy?, K. Warmuz, K. Pfeifer (red.), Fundacja „dzień dobry! kolektyw kultury", Siemianowice Śląskie 2017; D. Grinberg, *Ruch anarchistyczny w Europie Zachodniej 1870–1914*, Wydawnictwo Naukowe PWN, Warszawa 1994; P. Laskowski, *Szkice z dziejów anarchizmu*, Muza, Warszawa 2007; L. Kołakowski, *Główne nurty marksizmu. Powstanie – rozwój – rozkład*, Aneks, Londyn 1988; E. Posłuszna, *Terroryzm anarchistyczny*

– *istota, taktyka, organizacja*, „Bezpieczeństwo Narodowe" 2013, nr IV (28); „Inny Świat", pismo anarchistyczne (Mielec) nr 1–45, 1993–2016; „a-tak", pismo anarchistyczne (Kraków), nr 5–8, 2002–2004.

ANARCHIZM W TEORII – nazwa doktryny politycznej i ruchu społecznego, etymologicznie oznaczająca „bezrząd" (od stgr. ἄναρχος, anarchos, bez władcy). Różne oblicza polityczne anarchizmu, często wzajemnie sprzeczne, w pełni uformowały się w XIX w. Od tego stulecia do dnia dzisiejszego dla anarchistów głównym wrogiem pozostaje państwo, chronione przez m.in. wojsko, → p o l i c j ę [t. 3] i sądownictwo. Według anarchistów monarchie i → d y k t a t u r y [t. 2] wspierane moralnie przez religię oraz laickie demokracje z aparatem → p r o p a g a n d y [t. 3] i manipulacji są jednakowo złe, ponieważ opierają się na zniewoleniu jednostek czy też całych grup społecznych. P.-J. Proudhon, jeden z najważniejszych myślicieli anarchistycznych, w XIX w. zdefiniował państwo jako zracjonalizowany system dominacji i kontroli. W przekonaniu anarchistów państwo podporządkowuje ludzi w imię korzyści rządzących, interesu obcego kapitału, a także z powodu uległości i służalczości wobec innego kraju, nazywanego sojusznikiem.

Anarchiści zawsze byli przeciwnikami władzy absolutnej i monarchii, zdecydowanie popierali większość rewolucji. Co ciekawe, wielu z nich szybko rozczarowywały rewolucje, a oni sami stawali się ich ofiarami. Nie inaczej było z Wielką Rewolucją Francuską. M. Bakunin, równie słynny co Proudhon XIX-wieczny anarchista i rewolucjonista, stwierdził, że Wielka Rewolucja Francuska mimo pozytywnych konsekwencji takich jak unicestwienie monarchii, a także ogłoszenie → p r a w c z ł o w i e k a [t. 3] przyniosła niebywałe umocnienie scentralizowanego państwa. M. Stirner, ojciec europejskiego anarchoindywidualizmu, ocenił zaś, że po 1789 r. liczne państwa europejskie stały się „bogiem doczesnym", a jednostki zostały w nich podporządkowane ogółowi. W XIX-wiecznej Europie Zachodniej i USA nie miał dla większości anarchistów znaczenia ustrój państwa. Anarchiści wrogo odnosili się zarówno do monarchistyczno-feudalnych reliktów minionych wieków, jak i do demokracji, która w ich opinii tylko pozornie głosi idee wolności i równości. L. Spooner, jeden z współtwórców amerykańskiego anarchoindywidualizmu, szczególnie krytycznie występował przeciwko zasadzie tajności wyborów, twierdząc, że zasada ta zdejmuje z wyborców odpowiedzialność za czyny osób, które będą ich reprezentować. Anarchiści wzywali więc do „aktywnej absencji wyborczej", niektórzy szli dalej, sugerując, aby dopisywać na listach wyborczych osoby nieżyjące albo wrzucać do urn wyborczych kawałki fosforu, które miały niszczyć oddane już karty. Wielu anarchistów do chwili obecnej zaleca bojkot wyborów, powtarzając swoje credo, wg którego „gdyby wybory rzeczywiście coś zmieniały, to już dawno byłyby zabronione".

Dla XIX-wiecznych anarchistów kluczowe stało się rozwiązanie problemu codziennego ludzkiego bytu. Wspomniany wcześniej Proudhon czynił to w książkach

Co to jest własność?, *Myśl ogólna rewolucji w XIX wieku* i *System sprzeczności ekonomicznych, czyli filozofia nędzy.* W pierwszej z wymienionych autor uznaje, że każda nieuczciwie zdobyta i niewypracowana własność jest kradzieżą, w drugiej sprowadza każdą formę rządu do oficjalnego lub nieoficjalnego terroru państwa, począwszy od osobistego, przez polityczny, na fiskalnym skończywszy. Jego słynne słowa „być rządzonym", które wyliczają wszelkie formy pogardy i represji panującej władzy wobec obywatela, w XXI w. wciąż chętnie cytują artyści i muzycy (zob. utwór zespołu Dezerter *Być rządzonym*). W *Systemie sprzeczności ekonomicznych, czyli filozofii nędzy* Proudhon nie ufa wizji doskonałego społeczeństwa żyjącego w perfekcyjnym państwie, które założyli w swoich dziełach Hegel i Marks. Zamiast funkcjonowania instytucji państwa francuski myśliciel proponuje koncepcję społeczeństwa zbudowanego jako sieć wzajemnych, dobrowolnych zobowiązań, którą nazywa mutualizmem. Proudhon i niektórzy anarchiści w XIX i początkach XX w. trafnie przewidywali, że budowane państwo komunistyczne zostanie właścicielem dóbr, a co gorsza, przejmie władzę nad osobami i ich wolą. Z uwagi na silne przywiązanie do własności prywatnej, woli utrzymania kary śmierci, patriarchalizmu i poszanowania wartości, jaką jest rodzina, koncepcje Proudhona są znacznie bliższe współczesnym konserwatystom niż wielu anarchistom.

Poważny wkład w XIX-wieczną myśl anarchistyczną miał także wymieniony wcześniej Stirner. Ten niemiecki myśliciel w słynnej publikacji *Jedyny i jego własność* znacznie rozbudował zapoczątkowaną jeszcze pod koniec XVIII w. przez W. Godwina teorię anarchizmu indywidualnego. W założeniach Stirnera najważniejsze pozostaje własne „ja", czyli realizacja osobistych potrzeb. Wrogo traktowane są natomiast wszelkie ograniczenia, które starają się zawładnąć i kierować człowiekiem. Niemiecki filozof uważa za zupełnie obce i niemające znaczenia wszelkie płynące z zewnątrz zobowiązania. Postulatem Stirnera jest realizacja własnych, osobistych pragnień. Stirner nie wzywa więc do rewolucji, obalenia państwa, ale do buntu, zapanowania nad samym sobą, uważa, że człowiek zbuntowany nie musi walczyć z państwem, ponieważ staje mu się ono całkowicie obojętne. Skupiony na własnych potrzebach buntownik nie interesuje się losem państwa. W opinii A. Camusa poglądy Stirnera usprawiedliwiają dokonywanie zbrodni i stanowią podwalinę dla wszystkich form → t e r r o r y z m u [t. 4] anarchistycznego, który miał miejsce w XIX i XX w.

Dla przyszłych kształtów ruchu anarchistycznego okazało się istotne zaangażowanie wymienionych już wcześniej Rosjan: Bakunina, a także

P. Kropotkina, którzy znaczną część swojego życia spędzili w Europie Zachodniej. Bakunina, wielkiego przyjaciela Polaków walczących o niepodległość, czego nie można powiedzieć o Proudhonie, uznaje się za jednego z twórców tzw. anarchizmu kolektywistycznego, tj. prądu, który w przyszłości miał znacznie większy wpływ na ruch anarchistyczny niż wcześniej opisany mutualizm Proudhona. Bakunin głosił pełną wolność jednostki, człowieka żyjącego w ścisłym związku ze społeczeństwem, na

które jednocześnie powinien mieć jak największy wpływ. Anarchizm kolektywistyczny zakładał zlikwidowanie własności prywatnej i oddanie jej do dyspozycji swobodnie tworzonych kolektywów, tj. specjalnie tworzonych wspólnot produkcyjnych zarówno w miastach, jak i na wsi. Kropotkin, ze względu na swoje arystokratyczne pochodzenie określany jako „anarchistyczny książę", znany jest z 2 dzieł*: Nauka współczesna i anarchizm* oraz *Pomoc wzajemna jako czynnik rozwoju,* w którym przeciwstawił się pojęciu marksistowskiej „walki o byt", w zamian zaś zaproponował „prawo pomocy wzajemnej"; dowodził, że współpraca zwierząt i ludzi ma dla rozwoju gatunku większe znaczenie niż rywalizacja. Autor twierdził, że aparat państwa celowo tłumi altruistyczne postawy między ludźmi. Stworzył on podstawy tzw. anarchokomunizmu, które na przełomie XIX i XX w. rozwinęli Włoch E. Malatesta, a także Francuzi S. Faure, J. Grave i É. Reclus.

Pod koniec XIX w. na bazie anarchokomunizmu i wolnościowego socjalizmu wyłonił się anarchosyndykalizm, nurt, który zyskał znaczną popularność dopiero po 1920 r. Duży wkład w powstanie anarchosyndykalizmu mieli Francuzi F. Pelloutier i G.E. Sorel, choć dystansowali się od anarchizmu, zwłaszcza drugi z wymienionych myślicieli. Anarchosyndykaliści uważają, że podstawowe funkcjonowanie państwa sprowadza się do wspierania własności prywatnej, a także przywilejów gospodarczych, społecznych i politycznych tej grupy społecznej. W związku z tym anarchosyndykaliści kładą nacisk na wzajemną solidarność robotników (anarchosyndykalizm był i częściowo dalej pozostaje krytyczny wobec inteligencji) i tzw. akcji bezpośredniej (bez interwencji stron trzecich, czyli różnego szczebla przedstawicieli władzy, sędziów, negocjatorów itp.). Anarchosyndykalizm postuluje samorządność robotniczą. Anarchosyndykaliści ufają, że robotnicy są w stanie przejmować miejsca pracy i samodzielnie nimi zarządzać. Na początku XX w. Sorel i jego zwolennicy przeszli na stronę skrajnie prawicową, łącząc poglądy syndykalistyczne z silnie manifestowanym patriotyzmem. Sorel jest więc również uznawany za teoretyka narodowego syndykalizmu, do którego odwoływali się włoscy faszyści, a także polski Obóz Narodowo-Radykalny.

Bakunina, Kropotkina, Stirnera i Proudhona wiele dzieliło, ale łączyło jedno – zdecydowana wrogość wobec religii, religijności człowieka oraz moralności opartej na wskazówkach Biblii. Zupełnie inaczej niż w przypadku L. Tołstoja, przez wielu uznawanego za prekursora chrześcijańskiego anarchizmu, choć pisarz z Jasnej Polany niekoniecznie uznawał się za anarchistę. Tołstoj, który w świecie zyskał sławę dzięki zasadzie „niesprzeciwiania się złu siłą", swoje krytyczne uwagi wobec cywilizacji, zafałszowania Cerkwi, sądów, kapitalistów, a także instytucji państwa i wojska zawarł w dziełach literackich oraz rozprawach moralno-filozoficznych takich jak *Spowiedź* czy też *Droga życia*. W tej ostatniej Tołstoj stwierdza, że funkcjonowanie państwa opiera się na → p r z e m o c y [t. 3], a „armia jest niczym innym niż zgromadzeniem zdyscyplinowanych zabójców". Myśl Tołstoja miała istotny wpływ na rozwój XX-wiecznego antymilitaryzmu i pacyfizmu. Do przekonań Tołstoja odwoływali się

w swoich publikacjach m.in. R. Rolland i Mahatma Gandhi. Do idei chrześcijańskiego anarchizmu w 1. poł. XX w. nawiązał także N. Bierdiajew. Świadectwem tego są jego książki: *Królestwo Ducha i Królestwo cezara*, *Głoszę wolność*, a przede wszystkim *Autobiografia filozoficzna*. Bierdiajew uważał, że każda władza ziemska sprzeczna z duchem chrześcijaństwa jest z natury zła, a jedyne, co pozwala jej funkcjonować, to propaganda i manipulowanie społecznymi masami. W 2. poł. XX w. idee chrześcijańskiego anarchizmu rozwijali francuski filozof J. Ellul i Amerykanin V.M. Eller. W połowie XX w. pojawiły się nowe prądy, teorie i doktryny anarchistyczne, a niektóre już wcześniej funkcjonujące znacznie zyskały na popularności. W 1957 r. powstał sytuacjonizm (niektóre źródła nazywają go także neoanarchizmem), którego kulminacyjny moment przypada na studencką rewoltę 1968 r. W opinii sytuacjonistów, którzy skupiali zawsze wyjątkowo liczną grupę artystów i literatów, wolność zostanie zrealizowana tylko wtedy, kiedy jednostka wyzwoli się od materialnych zachcianek, codziennej walki o byt. Neoanarchiści sugerują więc, że przebudowa stosunków społecznych, w tym obalenie państwa, może nastąpić za pomocą nowych ekologicznych technologii, a także spontanicznej rewolucji, która obali państwo, własność prywatną, pracę najemną i wynikającą z niej bezmyślną konsumpcję. Dla zrealizowania tego celu potrzebne jest wcześniejsze przeobrażenie ludzkiej świadomości, która zerwie z panującą moralnością, prawem, modą i konwenansami. Za najważniejszych teoretyków tego nurtu anarchizmu uznaje się m.in. P. Goodmana, R. Veneigeu,

G. Deborda i zmarłego w 2006 r. M. Bookchina, głównego teoretyka tzw. ekologii społecznej, autora wydanej również w Polsce książki *Przebudowa społeczeństwa.* Od lat 60. XX w. następuje intensyfikacja feminizmu anarchistycznego, propagowanego znacznie wcześniej przez takie działaczki jak E. Goldman i V. de Cleyre. Zainicjowano tzw. zielony anarchizm, w którego obrębie pojawiły się 2 nurty: wspomniany już nurt ekologii społecznej, dość umiarkowany, proponujący harmonijne współistnienie świata ludzi i przyrody, związany z Bookchinem, a także prymitywizm anarchistyczny, który całkowicie odrzuca zdobycze nauki i cywilizacji. Propagatorem radykalnego skrzydła ekologicznego anarchizmu jest J. Zerzan. Pod koniec lat 60. XX w. pojawił się również libertarianizm zwany anarchizmem wolnościowym, anarchizmem rynkowym lub anarchistycznym kapitalizmem. Anarchizm wolnorynkowy zapoczątkowany został w USA przez M. Rothbarda i K. Hessa. Zwolennicy anarchizmu wolnościowego zakładali pełną wolność w kwestiach ekonomicznych, panowanie nieskrępowanego wolnego rynku. Ten prąd anarchistyczny zakłada zniesienie wszelkiego rodzaju instytucji państwowych i społecznych, które mają zostać zastąpione przez prywatną inicjatywę i dobrowolne stowarzyszenia. W kwestiach etyczno-społecznych libertarianie wskazują, że każdy człowiek powinien mieć całkowitą swobodę dysponowania swoją osobą i tym wszystkim, co posiadł, pod warunkiem, że swoimi działaniami nie ogranicza wolności innych jednostek.

W dwóch pierwszych dekadach XXI w. nie jest łatwo określić, który nurt anarchizmu jest wiodący. Nie jest również łatwo powiedzieć, czy większe znaczenie ma fakt, że dziś omawianą ideologię wspierają swoją publicystyką i publicznymi wystąpieniami niemłodzi już intelektualiści – tacy jak N. Chomsky, który nie ukrywa swoich sympatii dla anarchosyndykalizmu, co potwierdzają jego liczne publikacje, np. *Polityka, anarchizm, lingwistyka*, lub Hakim Bey, właśc. P.L. Wilson, autor słynnej teorii i zarazem książki *Tymczasowa Strefa Autonomiczna* – czy też może większe znaczenie, przynajmniej w docieraniu do młodzieży, ma anarchistyczny hip-hop, muzyka takich zespołów jak szwedzki Looptroop, amerykański Public Enemy lub francuska raperka Keny Arkana.

Remigiusz Kasprzycki

Anarchizm: nowe perspektywy?, K. Warmuz, K. Pfeifer (red.), Fundacja „dzień dobry! kolektyw kultury", Siemianowice Śląskie 2017; D. Grinberg, *Ruch anarchistyczny w Europie Zachodniej 1870–1914*, Wydawnictwo Naukowe PWN, Warszawa 1994; P. Laskowski, *Szkice z dziejów anarchizmu*, Muza, Warszawa 2007; „Inny Świat", pismo anarchistyczne (Mielec), nr 1–45, 1993–2016.

ANEKSJA (od łac. *annexio*, przyłączenie, okupacja) – działanie administracyjne i koncepcja w prawie międzynarodowym odnosząca się do przymusowego przyłączenia lub zagarnięcia przez jedno państwo całości albo części terytorium innego państwa, najczęściej przy użyciu siły, poprzez wojskową okupację podbitego terytorium bądź w wyniku wygranej → w o j n y [t. 4]; przeprowadzona wbrew prawu międzynarodowemu. W odróżnieniu od → s e c e s j i [t. 4], gdy terytorium jest przekazywane lub sprzedawane na mocy traktatu, aneksja jest aktem jednostronnym – terytorium jednego państwa zostaje zajęte przez inne państwo. Aneksja stała się głównym sposobem powiększania terytorium jednego państwa kosztem drugiego. W niektórych przypadkach aneksja jest uważana za rodzaj kolonialnego zajęcia, a jednym z jej rodzajów jest tworzenie państw z marionetkowymi → r e ż i m a m i [t. 3] (np. terytorium Abchazji i Osetii Południowej, gdzie rozmieszczone zostały siły zbrojne Federacji Rosyjskiej, Naddniestrze). Aneksja może wystąpić jako przyłączenie całego terytorium (np. aneksja terytorium Chanatu Krymskiego w 1783 r. przez Imperium Rosyjskie, aneksja Austrii przez Rzeszę Niemiecką w 1938 r.) lub części terytorium pewnego państwa (np. aneksja historycznych regionów Bośni i Hercegowiny w 1908 r. przez Austro-Węgry). Aneksja zakłada realne zajęcie danego terytorium i wyraźny zamiar jego trwałego wykorzystania.

Aneksję należy odróżniać od okupacji, która sama w sobie nie prowadzi do zmiany statusu prawnego tego terytorium. Na przykład Bośnia i Hercegowina, która była pod okupacją (czyli *de facto* pod kontrolą) Austro-Węgier w 1878 r., została przyłączona do nich w 1908 r., a wcześniej uważana była formalnie za terytorium Imperium Osmańskiego. Zazwyczaj w wyniku aneksji miejscowa ludność przyłączonego terytorium w państwie anektującym tworzy etniczną mniejszość narodową.

W Imperium Rosyjskim w historii i polityce zamiast terminu prawnego „aneksja", który był używany w Europie, stosowano określenia takie jak „zbieranie ziem" lub „poszerzanie" i „przyłączanie ziemi". Natomiast w stosunku do analogicznych działań innych imperiów wykorzystywano pojęcie „zagarnięcia". Ekspansja rosyjska w XIX w. dotyczyła także aneksji części terytorium należącego do Chin.

Przykładem aneksji jest np. zagarnięcie przez Niemcy w wojnie z Francją w 1871 r. Alzacji i Lotaryngii, aneksja przez Niemcy zachodnich terenów Polski w październiku 1939 r. czy aneksja przez ZSRR w październiku 1939 r. wschodnich województw II Rzeczypospolitej, a w czerwcu 1940 r. Litwy, Łotwy, Estonii i rumuńskiej Besarabii. Aneksja przez ZSRR części Polski w 1939 r. została uznana przez Anglię i USA dopiero na konferencji poczdamskiej w 1945 r., a reakcja na aneksję Łotwy, Litwy i Estonii była wówczas jedynie milczącą zgodą.

Aneksję często poprzedza podbój i okupacja wojskowa podbitego terytorium. Czasami, jak w przypadku niemieckiej aneksji Austrii w 1938 r., podboju można dokonać poprzez groźbę użycia siły bez czynnych działań wojennych i bez aktywnej wrogości. Okupacja wojskowa nie stanowi ani nie musi prowadzić do aneksji. Gdy okupacja wojskowa doprowadza do aneksji, państwo anektujące terytorium innego państwa ogłasza ustanowienie swojej władzy. Izrael złożył taką deklarację, anektując Wzgórza Golan w 1981 r., podobnie jak Rosja po aneksji ukraińskiej Autonomicznej Republiki Krymu w 2014 r.

Mogą istnieć warunki, które eliminują konieczność podboju przed aneksją. Na przykład w 1910 r. Japonia wkroczyła do Korei, a cesarz ogłosił, że gubernia zostanie formalnie włączona do Cesarstwa Wielkiej Japonii. Korea została anektowana przez proklamację.

Podbój wojskowy nie jest jedyną drogą do aneksji. Aneksja Hawajów przez USA pod koniec XIX w. była procesem pokojowym, opartym na dobrowolnej akceptacji przez hawajski rząd amerykańskiej władzy. USA powstały jako połączenie 13 kolonii, ale stały się narodem 50 stanów. Teksas np. był początkowo niezależną republiką, która zdecydowała o przyłączeniu się do USA.

Formalne procedury w przypadku aneksji nie są określone w prawie międzynarodowym (np. włoską aneksję Etiopii w 1936 r. formalizował dekret wydany przez króla Włoch). → M i ę d z y n a r o d o w e p r a w o h u m a n i t a r n e [t. 3] definiuje aneksję jako bezprawne, przymusowe przyłączenie przez jedno państwo całości lub części terytorium innego państwa, albo jakiejkolwiek przestrzeni, która znajduje się pod jego kontrolą bądź we wspólnym władaniu społeczności międzynarodowej. Aneksja została wyraźnie zabroniona dopiero w XX w., przy czym aneksje przedwojenne nie były uważane za sprzeczne z prawem międzynarodowym aż do 1945 r.

W klasycznym prawie międzynarodowym aneksja była legalną metodą nabywania terytorium i do początku XX w. zwycięzca konfliktu zbrojnego mógł całkowicie lub częściowo zajmować i anektować obszary należące do swojego przeciwnika. Zasada

uti possidetis (od łac. wyrażenia *uti possidetis, ita possideatis*, co posiadasz, będziesz posiadał) jest zasadą prawa międzynarodowego, która miała ogromne znaczenie dla wyznaczania granic. Umożliwia ona stronie walczącej roszczenie do terytorium, które zdobyła w drodze wojny. Według tej zasady strony prowadzące konflikt zbrojny lub wojnę godzą się na ich zakończenie z zachowaniem aktualnego w danym momencie stanu posiadania, a więc na usankcjonowanie wszystkich zdobyczy (terytoriów i innych dóbr), które miały w posiadaniu w chwili zawarcia pokoju; chyba że traktat stanowi inaczej; jeżeli taki traktat nie zawiera warunków dotyczących posiadania mienia i terytorium wziętego podczas wojny, wówczas obowiązuje zasada *uti possidetis*.

Międzynarodowe prawo dotyczące użycia siły przez państwa znacznie ewoluowało w XX w. Artykuł 10 Statutu Ligi Narodów z 1919 r. zabraniał członkom anektowania innych terytoriów. Najważniejsze porozumienia w tym zakresie to konwencje haskie z 1907 r., konwencje Ligi Narodów z 1920 r. i pakt Brianda–Kellogga z 1928 r., międzynarodowy traktat ustanawiający wyrzeczenie się wojny jako instrumentu polityki narodowej, którego punktem kulminacyjnym jest obecnie obowiązujący art. 2 ust. 4 I rozdziału Karty Narodów Zjednoczonych z 26 czerwca 1945 r. w brzmieniu: „Wszyscy członkowie powstrzymają się w swych stosunkach międzynarodowych od groźby użycia siły lub użycia jej przeciwko całości terytorialnej lub niepodległości któregokolwiek państwa". Wynika z niego międzynarodowy zakaz okupacji i aneksji.

Zgodnie ze współczesnym prawem międzynarodowym aneksja jest jednym z rodzajów → a g r e s j i i pociąga za sobą międzynarodową odpowiedzialność prawną. Współcześnie zakazana jest przez prawo międzynarodowe, użycie siły przeciwko integralności terytorialnej lub niezależności politycznej jest nielegalne.

Po II wojnie światowej próbami formalnej aneksji były m.in. włączenie okupowanych syryjskich Wzgórz Golan oraz części terytoriów Palestyny do Izraela (uznawane przez USA), przyłączenie Timoru Wschodniego w 1975 r. przez Indonezję, włączenie Kuwejtu do Iraku w 1990 r., które było przyczyną wojny w Zatoce Perskiej. Karta ONZ i Akt końcowy KBWE uznały aneksję za nielegalną, jako konsekwencję zakazu agresji oraz respektowania zasady → s u w e r e n n o ś c i p a ń s t w a [t. 4] i jego integralności terytorialnej.

W marcu 2014 r. Rosja dokonała nielegalnej aneksji Półwyspu Krymskiego, a dokładniej Autonomicznej Republiki Krymu, będącej wówczas częścią Ukrainy, co stało się najbardziej rażącym zawłaszczaniem ziemi w Europie od czasu II wojny światowej. Po aneksji wprowadzono rosyjskie prawo, zawierające m.in. surowe regulacje w sprawie prowadzenia pokojowych protestów, określające konieczność rejestracji organizacji pozarządowych, ustawodawstwo dyskryminujące prawa osób LGBT oraz przepisy znacząco ograniczające wolność słowa i zgromadzeń. Pomimo polityki władz Krymu i Rosji *de iure* Krym nadal należy do Ukrainy.

Zgodnie z przepisami ukraińskiej Ustawy o zapewnieniu praw i wolności obywateli na czasowo okupowanym terytorium Ukrainy z dnia 15 kwietnia 2015 r. terytorium Autonomicznej Republiki Krymu oraz Sewastopol są integralną częścią terytorium Ukrainy, na którym obowiązuje ustawodawstwo ukraińskie; uznanie tych obszarów za czasowo okupowane wynika z okupacji rosyjskiej. Zdaniem ówczesnego Naczelnego Dowódcy Sił Sojuszniczych w Europie gen. P. Breedlove'a Rosja wykorzystuje okupację do utworzenia strefy → k o n f l i k t u z a m r o ż o n e g o [t. 2], aby zapobiec zbliżeniu się tego czy innego państwa na wschodzie Europy do Zachodu.

Gwałtowna aneksja Krymu, podobnie jak pseudoreferendum oraz wszystkie wynikające z niego akty prawne (a co za tym idzie i sama aneksja), nie została uznana przez władze Ukrainy i społeczność międzynarodową z kilkoma wyjątkami (Syria, Korea Północna, Serbia, Armenia, Afganistan). Aneksja nie jest uznawana przez Zgromadzenie Ogólne ONZ, Zgromadzenie Parlamentarne Rady Europy, Zgromadzenie Parlamentarne OBWE i jest sprzeczna z decyzją Komisji Weneckiej. ONZ w związku z aneksją Krymu oświadczyła, że w aneksji tej użyto nielegalnej siły wojskowej, co spowodowało, że większość państw demokratycznych nałożyło surowe → s a n k c j e [t. 4] na Rosję. Rosja odrzuca pogląd, że była to aneksja, i traktuje ją jako przystąpienie do Federacji Rosyjskiej państwa, które właśnie ogłosiło niezależność od Ukrainy w wyniku referendum.

Terminem często używanym w Rosji do opisu tych wydarzeń jest „ponowne zjednoczenie" (воссоединение), „powrót Krymu do Rosji", aby podkreślić fakt, że Krym kiedyś był częścią Imperium Rosyjskiego.

Olga Wasiuta

A. Dolya, *The Annexation of Crimea: Lessons for European Security*, Fondation Robert Schuman, „European Issues" 2016, no. 382; T. German, *Abkhazia and South Ossetia: Collison of Georgian and Russian Interests*, „Russie.Nei.Visions" 2006, vol. 11; Karta Narodów Zjednoczonych, Statut Międzynarodowego Trybunału Sprawiedliwości i Porozumienie ustanawiające Komisję Przygotowawczą Narodów Zjednoczonych, Dz. U. 1947, nr 23, poz. 90; A. Paul, *Crimea One Year After Russian Annexation*, „European Policy Centre" 2015; S. Pavlović, *Balkan Anschluss: The Annexation of Montenegro and the Creation of the Common South Slavic State*, Purdue University Press, West Lafayette 2008; O. Wasiuta, *Aneksja*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; O. Wasiuta, S. Wasiuta, *Wojna hybrydowa Rosji przeciwko Ukrainie*, Wydawnictwo Arcana, Kraków 2017; О. Задорожній, *Анексія Криму – міжнародний злочин*, Видавництво К.І.С., Київ 2015.

ANTYDOSTĘPOWE ZDOLNOŚCI (ang. *Anti-Access*/*Area Denial*) – zdolności w zakresie izolowania pola walki, w światowym piśmiennictwie najczęściej określane akronimem A2/AD. Pierwszy człon źródłowej nazwy (*Anti-Access*) wskazuje na uniemożliwienie przeciwnikowi wejścia na teatr działań wojennych lub neutralizację sił przeciwnika (baz, okrętów) już zlokalizowanych w obrębie danego obszaru. Działania te mają wymiar strategiczno-operacyjny i realizowane są za pomocą ofensywnych

środków dalekiego zasięgu (np. przeznaczonych do niszczenia celów lądowych pocisków rakietowych, manewrujących przeciwokrętowych pocisków rakietowych czy też – jak w przypadku Chin – balistycznych). Drugi człon (*Area Denial*) – podkreśla wymiar operacyjno-taktyczny, który opiera się przede wszystkim na pozbawieniu przeciwnika swobody działania na danym obszarze. Kluczową rolę odgrywają więc środki defensywne, zwłaszcza systemy obrony przeciwlotniczej i przeciwrakietowej, a także środki → w a l k i r a d i o e l e k t r o n i c z n e j [t. 4].

Termin zyskał rozgłos w kontekście rozbudowy chińskich możliwości militarnych w rejonie Morza Południowochińskiego. Pojęcie A2/AD pojawiło się w niezależnym raporcie obronnym w USA w 1997 r. Kilka lat później zostało opisane w *Quadrennial Defense Review* – cyklicznie ukazującym się dokumencie Pentagonu, przedstawiającym amerykańską doktrynę wojskową oraz → z a g r o ż e n i a m i l i t a r n e [t. 4] USA. Amerykańscy analitycy uznali, że dzięki pozyskaniu nowoczesnych, precyzyjnych systemów rozpoznawczych i uderzeniowych operujących z dogodnie zlokalizowanych baz, a także poprzez budowę zintegrowanego systemu obrony powietrznej Chiny są w stanie podważyć swobodę działania sił amerykańskich w rejonie Azji Południowo-Wschodniej.

W pierwszej dekadzie XXI w. zainteresowanie zdolnościami izolowania pola walki zanikło na rzecz koncepcji zwalczania → t e r r o r y z m u [t. 4]. Pojawiło się po raz kolejny w *Quadrennial Defense Review* z 2010 r., w którym napisano, iż siły powietrzne i → m a r y n a r k a w o j e n n a [t. 3] USA wspólnie pracują nad połączoną koncepcją → w o j n y [t. 4] powietrzno-morskiej w celu pokonania przeciwnika dysponującego zaawansowanymi zdolnościami A2/AD. Spośród polskich badaczy zdolności A2/AD należy wspomnieć J. Bartosiaka, który w książce *Pacyfik i Eurazja. O wojnie* skupił się m.in. na chińskich zdolnościach antydostępowych na Zachodnim Indo-Pacyfiku takich jak okręty podwodne, pociski balistyczne DF-21F czy broń antysatelitarna.

Termin A2/AD pojawia się również w kontekście Rosji, która konsekwentnie rozmieszcza środki izolowania pola walki w kolejnych regionach. Są to tzw. bańki (ang. *bubbles*) antydostępowe. Chodzi przede wszystkim o region Morza Bałtyckiego z obwodem kaliningradzkim oraz region Morza Czarnego z Krymem, co w założeniu ma uniemożliwić siłom → N A T O [t. 3] działanie w regionach o dużym znaczeniu strategicznym. Zakłada się, że blokada znacznej części Morza Bałtyckiego może udaremnić wysiłki NATO w celu przyjścia z pomocą państwom bałtyckim w razie wybuchu konfliktu zbrojnego z Rosją. Termin A2/AD w odniesieniu do Rosji zastosowali m.in. autorzy dokumentu *AirSea Battle. A Point-of-Departure Operational Concept* oraz K. Weinberger w publikacji *Russian Anti-Access and Area Denial.* Pozostałe rosyjskie bastiony antydostępowe – będące rejonami koncentracji militarnych sił i środków w obszarach o dużym znaczeniu strategicznym i politycznym, często sąsiadującymi z rejonami wzmożonej aktywności militarnej potencjalnego

przeciwnika – to Półwysep Kolski, Kamczatka, rejon Władywostoku i Nachodki, Noworosyjsk oraz rosyjskie instalacje wojskowe w Syrii, skupione przede wszystkim wokół bazy Humajmim (ros. *Awiabaza Chmiejmim*). W przypadku Chin strefy A2/AD koncentrują się wzdłuż całego pasa wybrzeży, szczególne znaczenie ma wyspa Hajnan, pozwalająca kontrolować Morze Południowochińskie wraz ze spornymi wyspami Spratly i Wyspami Paracelskimi (gdzie również budowane są chińskie instalacje wojskowe), rejon Cieśniny Tajwańskiej, wybrzeże Morza Wschodniochińskiego w rejonie Szanghaju, rejon Zatoki Pohaj z wysuniętym półwyspem Szantung w pobliżu stołecznego Pekinu.

Podkreślić należy, że podejście antydostępowe nie jest nowością i występuje w sztuce wojennej bez mała od początku wojen. Przykładem może być m.in. wojna grecko-perska i → b i t w a pod Termopilami (480 r. p.n.e.), podczas której mniej liczebne wojsko spartańskie wykorzystało ukształtowanie terenu (przesmyk termopilski) uniemożliwiające pełne zastosowanie przewagi liczebnej Persów. Innym przykładem może być bitwa o Anglię i brytyjska sieć radarów utrudniająca Luftwaffe dostęp do terytorium brytyjskiego. Przez stulecia wyrazem podejścia antydostępowego była także budowa różnego rodzaju fortyfikacji.

Rozwój → t e c h n i k i w o j s k o w e j [t. 4] umożliwił objęcie bańkami antydostępowymi znacznych obszarów, w tym też nieznajdujących się pod bezpośrednią kontrolą strony budującej tego rodzaju zdolności. Poszczególne rodzaje broni objęte kategorią zdolności antydostępowych również nie są nowością, gdyż rakietowe systemy przeciwlotnicze czy przeciwokrętowe stanowią nieodłączny element nowoczesnych armii od kilkudziesięciu lat. Należy przy tym podkreślić, że kontrola danego obszaru w dużej mierze ma charakter potencjalny. Pierwszym ograniczeniem są bariery fizyczne, np. horyzont radiolokacyjny, powodujący, że strefa rażenia systemów przeciwlotniczych cechuje się rosnącym pułapem bezpiecznym (poniżej którego niszczenie celów nie jest możliwe) wraz ze wzrostem zasięgu rażenia. Drugim, oczywistym wręcz ograniczeniem, są dążenia przeciwnika do przełamania zdolności antydostępowych, np. przez wykorzystanie samolotów o utrudnionej wykrywalności dla radarów (tzw. → s t e a l t h t e c h n i k i [t. 4]) czy też środków rażenia odpalanych spoza zasięgu systemów przeciwlotniczych (tzw. broń *stand-off*).

Rafał Kopeć, Tomasz Wójtowicz

J. Bartosiak, *Pacyfik i Eurazja. O wojnie*, Wydawnictwo Jacek Bartosiak, Warszawa 2016; S. Frühling, G. Lasconjarias, *NATO, A2/AD and the Kaliningrad Challenge*, „Survival. Global Politics and Strategy" 2016, vol. 58, iss. 2; J. Johnson, *Washington's Perception and Misperceptions of Beijing's Anti-Access Area-Denial (A2-AD) 'Strategy': Implications for Military Escalation Control and Strategic Stability*, „The Pacific Review" 2017, vol. 30, iss. 3; R. Kopeć, *Antydostępowe zdolności*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; A. Lanoszka, M.A. Hunzeker, *Confronting the Anti-Access/ Area Denial and Precision Strike Challenge in the Baltic Region*, „The RUSI Journal" 2016, vol. 161, iss. 5; *Nowa oś globalnej konfrontacji. Amerykańsko-chińska rywalizacja*

militarna, „Wojny i Konflikty. Przeszłość – Teraźniejszość – Przyszłość" 2016, nr 1 (1); J. van Tol, M. Gunzinger, A. Krepinevich, J. Thomas, *AirSea Battle. A Point-of-Departure Operational Concept*, Center for Strategic and Budgetary Assessments, Washington 2010; K. Weinberger, *Russian Anti-Access and Area Denial*, Institute for the Study of War, Washington 2016.

ANTYRAKIETOWE SYSTEMY – systemy obrony przed pociskami rakietowymi, zasadniczo mające na celu niszczenie ich w trakcie lotu. Termin odnosi się generalnie do obrony przed rakietowymi pociskami balistycznymi, dlatego bardziej adekwatnym określeniem jest „obrona przeciwbalistyczna". Rakietowy pocisk balistyczny to pocisk rakietowy, na który podczas lotu, po zakończeniu pracy silnika, nie działają żadne siły oprócz oporu powietrza, przyciągania ziemskiego i bezwładności. Pocisk ten więc przebywa pewien odcinek drogi po torze balistycznym, tj. po torze podobnym do toru lotu kamienia wyrzuconego z katapulty, procy (określenie „balistyczny" pochodzi od stgr. βάλλειν – *ballein*, rzucać) lub pocisku wystrzelonego z broni palnej. Systemy antyrakietowe *de facto* odpowiadają więc na → z a g r o ż e n i e [t. 4] ze strony jednego typu rakiet – dominującego jednak z punktu widzenia przenoszenia → b r o n i n u k l e a r n e j , czy też szerzej → b r o n i m a s o w e g o r a ż e n i a , czyli rakiet balistycznych. Rakiety balistyczne stanowią bardzo trudny cel przede wszystkim ze względu na znaczne prędkości, jakie osiągają, stromą trajektorię lotu oraz duży pułap. Drugi typ rakiet, rakiety manewrujące (ang. *cruise missile*) wykorzystujące aerodynamiczną siłę nośną do utrzymania się w powietrzu, wykazuje właściwości lotne podobne do samolotów, więc do ich zwalczania stosuje się systemy przeciwlotnicze.

Precyzyjne rozgraniczenie pomiędzy systemami przeciwlotniczymi i przeciwrakietowymi nie zawsze jest możliwe. Wybrane systemy przeciwlotnicze mają pewne, chociaż ograniczone, możliwości zwalczania pocisków balistycznych, z kolei systemy przeznaczone do obrony przeciwrakietowej w obrębie atmosfery ziemskiej są również w stanie zwalczać cele aerodynamiczne. Przykładem jest system Patriot wykorzystujący pociski przeciwlotnicze PAC-2 z ograniczonymi zdolnościami antybalistycznymi oraz pociski przeciwrakietowe PAC-3, zdolne także do niszczenia samolotów. Egzoatmosferyczne systemy antyrakietowe, przeznaczone do niszczenia celów poza atmosferą ziemską, cechują się również zdolnością do niszczenia satelitów, które ze względu na przewidywalną trajektorię lotu są celami znacznie łatwiejszymi do neutralizacji niż rakiety balistyczne. Ograniczeniem w tym przypadku jest z kolei wysokość orbity, po której porusza się satelita – zasadniczo systemy te są zdolne do niszczenia obiektów na niskich orbitach okołoziemskich. Przykładem wykorzystania systemu antyrakietowego do niszczenia satelity jest operacja Burnt Frost z 20 lutego 2008 r., w ramach której Amerykanie zestrzelili własnego satelitę rozpoznawczego, nad którym utracono kontrolę, przy użyciu odpalanego z pokładu okrętu pocisku antybalistycznego SM-3.

Prace nad systemami antybalistycznymi rozpoczęto w latach 40. XX w., niedługo po wejściu do służby operacyjnej pierwszych rakiet balistycznych. W czasie

→ z i m n e j w o j n y [t. 4] systemy te dynamicznie rozwijano w USA i ZSRR. Potrzeba ich pozyskania związana była z zagrożeniem ze strony rakietowych pocisków balistycznych, które zastąpiły samoloty w roli podstawowego nośnika głowic nuklearnych, a tym samym stały się zasadniczym elementem strategicznego uderzenia na terytorium przeciwnika. Początkowo zakładano budowę systemów zdolnych do obrony głównych miast i miejsc bazowania własnych rakiet balistycznych przed strategicznym atakiem przeciwnika. Ostatecznie, w ograniczonym zakresie wdrożono do służby systemy obrony punktowej – Safeguard w USA oraz A-35 i A-135 w ZSRR. Na przeszkodzie wdrożeniu systemów na większą skalę stanęły ogromne koszty, problemy techniczne (ze względu na ograniczoną precyzję naprowadzania systemy wykorzystywały głowice nuklearne), a także kalkulacja, która skłoniła supermocarstwa do zahamowania prac nad systemami mogącymi naruszyć kruchą równowagę strategiczną. Zgodnie z paradoksem ofensywy–defensywy broń ofensywna (rakiety balistyczne z głowicami nuklearnymi) stała się w sensie strategicznym narzędziem obrony, a broń defensywna (systemy antyrakietowe) spełniała funkcję ofensywną – miała umożliwić atak rakietowy bez obawy o uderzenie odwetowe przeciwnika. Konsekwencją niepokoju związanego z niekontrolowanym wyścigiem zbrojeń w tym zakresie było podpisanie przez USA i ZSRR układu o obronie przeciwrakietowej ABM (Anti-Ballistic Missile Treaty) w 1972 r. (układ został wypowiedziany przez USA 14 grudnia 2001 r. i pół roku później stracił moc obowiązującą).

Po zakończeniu zimnej wojny punkt ciężkości przeniósł się na systemy działające w skali operacyjnej, mające chronić przed ograniczonym atakiem rakietowym, np. ze strony państw określanych przez USA jako zbójeckie (ang. *rogue states* – np. Iran, Korea Północna). Katalizatorem działań w tym zakresie było wykorzystanie systemów Patriot do zwalczania irackich pocisków balistycznych podczas operacji Pustynna Burza w 1991 r. Obecnie systemy antyrakietowe różnych warstw (najwyższa obejmuje systemy zdolne do niszczenia rakiet międzykontynentalnych w środkowej fazie lotu – przykładem jest amerykański system Ground Based Interceptor) są rozwijane przez wszystkie czołowe potęgi militarne, przede wszystkim przez USA, Rosję, Izrael, a także przez Chiny i Indie.

Zwalczanie pocisków rakietowych możliwe jest we wszystkich fazach lotu (przede wszystkim dotyczy to pocisków balistycznych, w których wypadku w sposób wyraźny wyodrębnia się poszczególne fazy), a wymagania z tym związane prowadzą do budowy wyspecjalizowanych systemów. Jest to najlepiej widoczne na przykładzie amerykańskiego wielowarstwowego Systemu Obrony Przeciwrakietowej BMD (Ballistic Missile Defense). Do zwalczania rakiet w fazie lotu silnikowego (ang. *boost phase*) projektowano laserowy system Airborne Laser oraz rakietowy Kinetic Energy Interceptor, nie weszły one jednak do użycia operacyjnego. Obecnie rozważa się zastosowanie w tym celu pocisków przeciwlotniczych AIM-120 AMRAAM wystrzeliwanych z samolotów F-35, ew. systemów (laserowych lub rakietowych) montowanych na

bezzałogowych statkach latających o dużej długotrwałości lotu. Do zwalczania rakiet w środkowej fazie lotu (ang. *midcourse phase*) przeznaczone są pociski Ground Base Interceptor (GBI) rozmieszczone w bazach w Kalifornii i na Alasce oraz pociski SM-3 o nieco mniejszych możliwościach przestrzennych wystrzeliwane z pokładów okrętów wyposażonych w systemy Aegis oraz rozlokowanych na lądzie instalacji Aegis Ashore (amerykańskie instalacje w Rumunii i Polsce – ta druga w budowie, dwie planowane instalacje japońskie). Za zwalczanie rakiet w fazie terminalnej (ang. *terminal phase*) odpowiadają systemy Terminal High Altitude Area Defense (THAAD – wyższa warstwa) oraz PAC-3 (niższa warstwa).

Rafał Kopeć

D. Jankowski, *Amerykański system obrony przeciwrakietowej*, Wydawnictwo Adam Marszałek, Toruń 2011; R. Kopeć, *Antyrakietowe systemy*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; tenże, *Powrót „gwiezdnych wojen". Trendy rozwojowe amerykańskiej obrony przeciwrakietowej*, „Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate" 2019, nr 9 (4); tenże, *Militarne metody zapobiegania proliferacji broni masowego rażenia*, Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2015; tenże, *Systemy antyrakietowe zimnej wojny – uwarunkowania strategiczne*, „Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate et Educatione Civili" 2013, nr 3; P. Turczyński, *Amerykańskie koncepcje tarczy antyrakietowej w Europie*, Poltext, Warszawa 2012; D.A. Wilkening, *Does Missile Defence in Europe Threaten Russia?*, „Survival. Global Politics and Strategy" 2012, vol. 54, iss. 1; *Wpływ tarczy antyrakietowej na pozycję międzynarodową Polski. Konsekwencje umieszczenia elementów systemu obrony przeciwrakietowej Stanów Zjednoczonych na terytorium Rzeczypospolitej Polskiej*, M. Chorośnicki, A. Gruszczak (red.), Koło Studentów Stosunków Międzynarodowych UJ, Instytut Nauk Politycznych i Stosunków Międzynarodowych UJ, Kraków 2008.

ANTYTERRORYSTYCZNA OPERACJA (ang. *anti-terrorist operation*) – zestaw skoordynowanych środków ukierunkowanych na ostrzeganie przed czynami przestępczymi o charakterze terrorystycznym, zapobieganie im i ich zwalczanie; uwalnianie zakładników (zob. → w z i ę c i e z a k ł a d n i k a [t. 4]), neutralizacja terrorystów; minimalizacja skutków ataku terrorystycznego lub innego przestępstwa o charakterze terrorystycznym.

Wiele państw podejmuje działania na rzecz międzynarodowego pokoju i → b e z p i e c z e ń s t w a w ramach operacji militarnych poza granicami kraju. Obecnie mają one przede wszystkim charakter działań antyterrorystycznych, co przekłada się na prowadzenie czynności prewencyjnych, obronę przed atakami terrorystycznymi, udział w czynnym zwalczaniu → t e r r o r y z m u [t. 4] oraz uczestnictwo w likwidacji skutków zamachów terrorystycznych. Należy mieć na uwadze, że operacje antyterrorystyczne z wykorzystaniem instrumentu militarnego mogą być prowadzone również w sferze wewnętrznej, czego przykłady odnajdujemy współcześnie w Ukrainie.

Zgodnie z *Joint Doctrine for Military Operation Other Than War* operacje inne niż wojenne obejmują użycie sił zbrojnych w szerokim zakresie operacji

prowadzonych na mniejszą skalę niż → w o j n a [t. 4]. Zgodnie z doktryną przyjętą przez → N A T O [t. 3] operacje tego typu obejmują m.in.:

- kontrolę proliferacji → b r o n i m a s o w e g o r a ż e n i a i zbrojeń konwencjonalnych;
- zwalczanie → za g r o ż e ń [t. 4] o charakterze terrorystycznym;
- zwalczanie międzynarodowego handlu narkotykami;
- zapewnienie bezpieczeństwa i swobody transportu;
- wymuszanie egzekwowania → s a n k c j i [t. 4] nałożonych przez organizacje międzynarodowe;
- akcje o charakterze humanitarnym;
- wspieranie władz cywilnych;
- ewakuowanie → l u d n o ś c i c y w i l n e j [t. 3];
- operacje o charakterze pokojowym;
- ochronę żeglugi morskiej i szlaków morskich;
- obecność sił zbrojnych w rejonie operacji;
- działania o charakterze wymuszającym;
- wspieranie bądź zwalczanie ruchów narodowowyzwoleńczych i separatystycznych (zob. → s e p a r a t y z m [t. 4]);
- odzyskiwanie ciał, szczątków poległych → ż o ł n i e r z y [t. 4] lub cywili;
- uderzenia i rajdy.

Operacje antyterrorystyczne związane są z praktyką, taktyką wojskową, technikami i → s t r a t e g i ą [t. 4] stosowaną przez rząd, wojsko, organy ścigania, biznes i agencje wywiadowcze do zwalczania terroryzmu lub zapobiegania mu. Strategie walki z terroryzmem obejmują także próby przeciwdziałania finansowaniu terroryzmu. Siły Zbrojne USA używają terminu zagranicznej obrony wewnętrznej w programach wspierających inne państwa w próbach tłumienia powstań, bezprawia lub działalności wywrotowej albo w celu ograniczenia warunków, w których → z a g r o ż e n i a b e z p i e c z e ń s t w a [t. 4] mogą się rozwijać.

Pierwszą jednostkę antyterrorystyczną w historii utworzył brytyjski minister spraw wewnętrznych W. Harcourt w odpowiedzi na nasilającą się w Wielkiej Brytanii w latach 80. XIX w. kampanię terroru przeprowadzoną przez wojujących fenianów (tajne irlandzkie stowarzyszenie niepodległościowe założone ok. 1858 r.). Specjalny Oddział Irlandzki (Special Irish Branch) został początkowo utworzony jako sekcja Wydziału Śledczego (Criminal Investigation Department) Londyńskiej Policji Metropolitalnej (London Metropolitan Police) w 1883 r. w celu zwalczania irlandzkiego terroryzmu republikańskiego poprzez infiltrację i działalność wywrotową. Harcourt stworzył stałą jednostkę zajmującą się zapobieganiem → p r z e m o c y [t. 3] o podłożu politycznym za pomocą nowoczesnych technik. Z czasem nazwa jednostki została zmieniona na Oddział Specjalny (Special Branch), ponieważ zakres jej kompetencji stopniowo rozszerzał się, aby skutecznie odgrywać rolę w zwalczaniu terroryzmu, obcej działalności

i infiltracji → p r z e s t ę p c z o ś c i z o r g a n i z o w a n e j [t. 3]. Organy ścigania w Wielkiej Brytanii i innych krajach ustanowiły podobne jednostki.

Siły antyterrorystyczne rozszerzyły się wraz z rosnącym zagrożeniem terroryzmem pod koniec XX w. W szczególności po atakach z 11 września 2001 r. zachodnie rządy uczyniły wysiłki przeciwdziałania terroryzmowi priorytetem, intensyfikując współpracę zagraniczną, uwzględniając zmianę taktyki i zastosowanie środków prewencyjnych.

Większość strategii antyterrorystycznych wiąże się z przechwytywaniem komunikacji i śledzeniem osób, które zagrażają bezpieczeństwu państwa. Nowa technologia rozszerzyła jednak zakres działań wojskowych i organów ścigania. Taka działalność jest często skierowana do pewnych grup, określonych na podstawie pochodzenia lub religii, co jest źródłem rozmaitych kontrowersji politycznych. Masowy nadzór całej ludności budzi zastrzeżenia ze względu na swobody obywatelskie. Terroryści, szczególnie samotne wilki, są często trudniejsi do wykrycia z powodu ich obywatelstwa lub statusu prawnego.

Aby wybrać skuteczne działanie, gdy terroryzm wydaje się bardziej odosobnionym przypadkiem, odpowiednie organizacje rządowe muszą zrozumieć źródło, motywacje, metody przygotowania i taktykę grup terrorystycznych. Dobra organizacja działań antyterrorystycznych jest podstawą takich przygotowań, a także politycznego i społecznego zrozumienia wszelkich problemów, które mogą zostać rozwiązane.

Jeśli chodzi o aspekty prawne, to np. w Wielkiej Brytanii przepisy antyterrorystyczne obowiązują od ponad 30 lat. Ustawa o zapobieganiu przemocy z 1939 r. została przyjęta w odpowiedzi na kampanię przemocy Irlandzkiej Armii Republikańskiej (IRA) realizowaną przez organizację w ramach planu S (S-Plan, Sabotage Campaign). W 1973 r. akt ten został uchylony, by zastąpić go ustawą o zapobieganiu terroryzmowi, powstałą w odpowiedzi na problemy w Irlandii Północnej. W latach 1974–1989 przepisy przejściowe ustawy były corocznie odnawiane. W 2000 r. ustawa została zastąpiona bardziej trwałą Ustawą o zwalczaniu terroryzmu, przestępczości i bezpieczeństwie z 2000 r., a potem Ustawą o zapobieganiu terroryzmowi z 2006 r., którą opracowano w następstwie zamachów bombowych z 7 lipca 2005 r. w Londynie.

W USA rozwiązania prawne związane z omawianą kwestią obejmują orzeczenia dotyczące krajowego stosowania środków śmiercionośnych przez organy ścigania. USA uchwaliły USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001) po atakach z 11 września 2001 r., a także szereg innych przepisów i zarządzeń wykonawczych odnoszących się do → b e z p i e c z e ń s t w a n a r o d o w e g o . Departament Bezpieczeństwa Wewnętrznego dostał uprawnienia w celu koordynowania działań antyterrorystycznych, a także krajowych reakcji na poważne klęski żywiołowe i wypadki. W lutym 2017 r. administracja Trumpa postanowiła przebudować amerykański program rządowy i zmienić jego nazwę na Przeciwdziałanie brutalnemu

ekstremizmowi (Countering Violent Extremism Task Force, CVE), aby skupić się wyłącznie na ekstremistach islamistycznych.

Jedną z głównych trudności we wdrażaniu skutecznych środków antyterrorystycznych jest ograniczanie swobód obywatelskich i prawa do prywatności, zarówno w odniesieniu do obywateli, jak i osób zatrzymanych przez państwa próbujące walczyć z terrorem. Czasami działania zmierzające do zaostrzenia bezpieczeństwa były postrzegane jako nadużycia władzy, a nawet naruszenia → p r a w c z ł o w i e k a [t. 3]. Przykładami takich problemów są:

- przedłużające się przetrzymywanie w odosobnieniu bez wyroku sądowego lub długie okresy prewencyjnego zatrzymania;
- ryzyko poddania torturom podczas transferu, zwrotu i ekstradycji osób między krajami lub w obrębie krajów;
- przyjęcie środków bezpieczeństwa, które ograniczają prawa lub wolności obywateli i naruszają zasady niedyskryminacji.

Wyżej wymienione kwestie odzwierciedliły się w sposobie traktowania więźniów torturowanych w amerykańskim więzieniu Abu Ghurajb w Iraku i innych miejscach, co skłania do międzynarodowej kontroli operacji amerykańskich w wojnie z terroryzmem; setki cudzoziemców zatrzymywano w więzieniu Guantanamo, bezterminowo oraz bez aktu oskarżenia i wyroku sądowego, mimo że wg międzynarodowych i amerykańskich standardów konstytucyjnych takie praktyki są zakazane. Setki osób podejrzewanych o związki z talibami lub Al-Kaidą pozostają w długoterminowym areszcie w Pakistanie lub w kontrolowanych przez USA ośrodkach w Afganistanie. Chiny wykorzystały „wojnę z terroryzmem", aby uzasadnić swoją politykę w przeważnie muzułmańskim Regionie Autonomicznym Sinciang-Ujgur, by zdusić tożsamość Ujgurów. W Maroku, Arabii Saudyjskiej, Tunezji, Jemenie i innych krajach wiele osób zostało aresztowanych i arbitralnie zatrzymanych w związku z podejrzeniem o akty terrorystyczne lub powiązania z opozycyjnymi grupami zbrojnymi. Niektóre kraje postrzegają ataki wyprzedzające jako legalną strategię.

Obejmują one przechwytywanie, zabijanie lub neutralizowanie podejrzanych terrorystów, zanim będą mogli przeprowadzić atak. Izrael, Wielka Brytania, USA i Rosja przyjęły takie podejście, podczas gdy państwa Europy Zachodniej raczej tego nie robią. Inną ważną metodą neutralizacji prewencyjnej jest przesłuchanie znanych lub podejrzewanych terrorystów w celu uzyskania → i n f o r m a c j i [t. 2] o konkretnych działaniach, celach, tożsamości innych terrorystów, niezależnie od tego, czy osoby przesłuchiwane są winne. Czasami stosuje się ekstremalne metody przesłuchań polegające np. na pozbawianiu snu lub odurzaniu narkotykami i innymi środkami chemicznymi.

Terroryzm był często wykorzystywany do usprawiedliwiania interwencji wojskowych w krajach takich jak Pakistan czy Rosja (np. druga rosyjska → i n w a z j a [t. 2] na Czeczenię). Było to również główne uzasadnienie amerykańskiej inwazji na Afganistan.

Obecnie wiele krajów posiada specjalne jednostki wyznaczone do radzenia sobie z zagrożeniami terrorystycznymi. Oprócz różnych agencji bezpieczeństwa istnieją elitarne jednostki taktyczne, znane też jako jednostki misji specjalnych, których rolą jest bezpośrednia inwigilacja terrorystów i zapobieganie atakom terrorystycznym. Takie jednostki wykonują działania prewencyjne, podejmują się ratowania zakładników, jak również działają w ramach akcji bezpośrednich i reakcji na ataki.

Praktycznie w każdym państwie funkcjonują dobrze wyszkolone zespoły antyterrorystyczne. Taktyka, techniki i procedury są stale rozwijane, większość tych środków dotyczy ataków terrorystycznych, które mają wpływ na dany obszar lub zagrażają działaniom tych zespołów. O wiele trudniej poradzić sobie z zabójstwem, a nawet represjami wobec pojedynczych osób, ze względu na krótki (jeśli w ogóle) czas ostrzegania i szybką eksfiltrację zabójców. Większość działań antyterrorystycznych na poziomie taktycznym jest prowadzona przez państwowe, federalne i krajowe organy ścigania lub agencje wywiadowcze. W niektórych krajach wojsko może zostać wezwane w ostateczności. Oczywiście, w krajach, w których wojsko zezwala na prowadzenie operacji policyjnych, nie stanowi to problemu, a operacje antyterrorystyczne prowadzone są przez wojsko.

Zakres systemów antyterrorystycznych jest bardzo duży pod względem fizycznym (długie granice, rozległe obszary, duży ruch w zatłoczonych miastach itp.), a także w innych wymiarach, takich jak rodzaj i stopień zagrożenia terroryzmem, konsekwencje polityczne i dyplomatyczne oraz kwestie prawne. W tym środowisku rozwój trwałego systemu ochrony przed terroryzmem jest trudnym zadaniem. Taki system powinien łączyć różnorodne, najnowocześniejsze technologie, aby umożliwić stałe misje wywiadowcze, obserwacyjne i rozpoznawcze oraz zagwarantować możliwość potencjalnej odpowiedzi na zagrożenie.

Właściwie wszystkie państwa świata mają swoje agencje antyterrorystyczne. W Polsce za antyterrorystyczne operacje odpowiada Centrum Antyterrorystyczne (CAT) →Agencji Bezpieczeństwa Wewnętrznego, na wzór sztabów istniejących we wszystkich militarnych mocarstwach, takich jak Rosja, USA czy Wielka Brytania. Powstała instytucja integruje i koordynuje działania i wysiłki wszystkich służb i agend rządowych odpowiedzialnych za bezpieczeństwo. Jest to jednostka koordynacyjno-analityczna w zakresie przeciwdziałania terroryzmowi i jego zwalczania. Służbę w nim pełnią, oprócz funkcjonariuszy ABW, oddelegowani funkcjonariusze, żołnierze i pracownicy m.in. → Policji [t. 3], Straży Granicznej, → Służby Ochrony Państwa [t. 4], →Agencji Wywiadu, →Służby Wywiadu Wojskowego [t. 4], →Służby Kontrwywiadu Wojskowego [t. 4], GROM-u (Grupa Reagowania Operacyjno-Manewrowego) oraz Służby Celnej. Realizują oni zadania w ramach kompetencji instytucji, którą reprezentują. Ponadto z Centrum Antyterrorystycznym aktywnie współpracują inne podmioty uczestniczące w systemie ochrony antyterrorystycznej RP, takie jak → Rządowe Centrum Bezpieczeństwa [t. 3], Ministerstwo Spraw Zagranicznych,

→ Państwowa Straż Pożarna [t. 3], Generalny Inspektor Informacji Finansowej, Sztab Generalny Wojska Polskiego, Żandarmeria Wojskowa itp. Istotą systemu funkcjonowania CAT ABW jest koordynacja procesu wymiany informacji między uczestnikami systemu ochrony antyterrorystycznej, umożliwiająca wdrażanie wspólnych procedur reagowania w przypadku zaistnienia jednej z czterech kategorii zdefiniowanego zagrożenia:

- zdarzenia terrorystycznego zaistniałego poza granicami Polski mającego wpływ na bezpieczeństwo RP i jej obywateli;
- zdarzenia terrorystycznego zaistniałego na terenie Polski mającego wpływ na bezpieczeństwo RP i jej obywateli;
- uzyskania informacji o potencjalnych zagrożeniach mogących wystąpić na terenie Polski i poza granicami RP;
- uzyskania informacji dotyczących prania pieniędzy lub transferów środków finansowych mogących świadczyć o finansowaniu działalności terrorystycznej.

Biorąc pod uwagę charakter operacyjnych działań antyterrorystycznych, krajowe organizacje wojskowe zazwyczaj nie mają jednostek, których wyłącznym obowiązkiem jest realizacja tych zadań. W niektórych przypadkach ramy prawne, w których działają, zabraniają jednostkom wojskowym prowadzenia działalności na arenie krajowej. Na przykład polityka Departamentu Obrony USA, oparta na ustawie Posse Comitatus, zabrania krajowych operacji antyterrorystycznych prowadzonych przez wojsko USA. Jednostki przydzielone do niektórych operacyjnych zadań antyterrorystycznych są często jednostkami specjalnymi.

W Ukrainie Antyterrorystyczne Centrum przy Służbie Bezpieczeństwa Ukrainy zostało utworzone 11 grudnia 1998 r., zgodnie z dekretem prezydenta, w celu organizowania i prowadzenia operacji antyterrorystycznych i koordynacji działań wszystkich, którzy walczą z terroryzmem lub biorą udział w operacjach antyterrorystycznych. Operacja antyterrorystyczna (ATO) na wschodzie Ukrainy, która trwała od 14 kwietnia 2014 r. do 30 kwietnia 2018 r., była kompleksem wojskowych i specjalnych kroków organizacyjnych i prawnych ukraińskich sił bezpieczeństwa mających na celu zwalczanie nielegalnych działań rosyjskich i prorosyjskich sił zbrojnych w czasie wojny we wschodniej Ukrainie.

13 kwietnia 2014 r. Ukraina ogłosiła rozpoczęcie operacji antyterrorystycznej bez wprowadzenia stanu wojennego z udziałem Sił Zbrojnych Ukrainy. Strefą operacji antyterrorystycznej były objęte 2 regiony: doniecki i ługański (14 kwietnia 2014 r.) oraz okręg iziumski i miasto Izium w obwodzie charkowskim (od 14 kwietnia do 7 września 2014 r.). Dekret w sprawie ATO został podpisany przez p.o. prezydenta Ukrainy O. Turczynowa 13 kwietnia 2014 r. Następnego dnia zatwierdzono dekret o natychmiastowych środkach w celu zwalczania zagrożenia terrorystycznego i zachowania integralności terytorialnej Ukrainy, który wyznaczał oficjalny start operacji antyterrorystycznej.

Według oświadczeń władz ukraińskich reżim prawny operacji antyterrorystycznej w celu przeciwdziałania działalności nielegalnych rosyjskich i prorosyjskich sił zbrojnych podczas → a g r e s j i wiosną 2014 r. został wybrany ze względu na pilną potrzebę przeprowadzenia wyborów prezydenckich i parlamentarnych. Wybory nie byłyby możliwe w warunkach wprowadzenia stanu wojennego.

13 czerwca 2017 r. sekretarz Rady Bezpieczeństwa Ukrainy Turczynow złożył oświadczenie, że Ukraina musi zakończyć operację antyterrorystyczną i przejść do nowego formatu bezpieczeństwa określającego zasady polityki państwa w sprawie uwolnienia okupowanych terytoriów.

30 kwietnia 2018 r. status działań zbrojnych na wschodzie Ukrainy został zmieniony z ATO na Operację Sił Połączonych (Operacja Objednanych Sil, OOS). Zmiana ta wynikała z zapisów ustawy o polityce państwa w celu zabezpieczenia → s u w e r e n n o ś c i [t. 4] Ukrainy na tymczasowo okupowanych terytoriach obwodów donieckiego i ługańskiego (tzw. ustawa o reintegracji Donbasu). Rada Najwyższa Ukrainy przyjęła tę ustawę 18 stycznia, dokument przewidywał zakończenie operacji antyterrorystycznej i wprowadzenie stanu wojennego lub stanu wyjątkowego oraz przekazanie przez Służbę Bezpieczeństwa zarządzania operacją Połączonemu Sztabowi Operacyjnemu Sił Zbrojnych Ukrainy. Podkreślono ściśle militarny charakter rosyjskiej inwazji. 16 marca 2018 r. podczas wizyty w Donbasie ówczesny prezydent Ukrainy P. Poroszenko ogłosił prawne zakończenie operacji antyterrorystycznej i przedstawił nowego dowódcę OOS, zaznaczając:

> Rozpoczynamy operację wojskową pod kierownictwem Sił Zbrojnych Ukrainy w celu obrony jedności terytorialnej, suwerenności i niepodległości naszego państwa. Choć ATO się zakończyła, to sprzeciw wobec rosyjskiego agresora zakończy się dopiero wtedy, gdy wyzwolona zostanie ostatnia piędź ukraińskiej ziemi – zarówno w obwodach donieckim i ługańskim, jak i na terytorium okupowanego Krymu.

Po 4 latach trwania ATO wojna w Donbasie otrzymała status operacji wojskowej *par excellence*. W ciągu 4 lat, dzięki ogólnoukraińskiej solidarności, odwadze i patriotyzmowi całego narodu ukraińskiego, zadania operacji antyterrorystycznej zostały zrealizowane. Format ATO pozwolił w swoim czasie zniweczyć plany Kremla, który narzucał całemu światu tezę o przewrocie państwowym w Ukrainie. Umożliwiono także przeprowadzenie demokratycznych wyborów, które odbyły się w warunkach agresji Federacji Rosyjskiej. Zmiany stanowiły reakcję na swoistą dwuwładzę: do tej pory obrona kraju, prowadzona przez wojsko, dowodzona była przez Służbę Bezpieczeństwa Ukrainy. Zarządzanie działalnością sił bezpieczeństwa powierzono Siłom Zbrojnym Ukrainy. OOS obejmuje obwody ługański i doniecki oraz wybrzeże Morza Azowskiego.

Operacja Połączonych Sił systematyzowała użycie Sił Zbrojnych Ukrainy do realizacji zadań, stworzyła dokładną strukturę systemu dowodzenia, podporządkowała siły i zasoby kierownictwu wojskowemu, stworzyła sztab operacyjny jako główny organ

dowodzenia operacją we wskazanych obszarach. W ramach strefy objętej działaniami OOS obowiązuje → s t a n n a d z w y c z a j n y [t. 4], mogą być wyznaczane także strefy ograniczonego dostępu lub zamknięte. Dostęp do nich zależy od decyzji osób wyznaczonych do dowodzenia na poszczególnych szczeblach operacji. Został również ustanowiony reżim określający strefy:

- zieloną – przebywanie i przemieszczanie osób ma miejsce bez ograniczeń, z wyjątkiem stref ograniczonego dostępu;
- żółtą – przebywanie i przemieszczanie osób odbywa się na podstawie dokumentów tożsamości, z uwzględnieniem przeszukań osób, pojazdów i rzeczy, realizowany na granicach stref zamkniętych i w strefach zamkniętych;
- czerwoną – przebywanie osób w tych obszarach jest zabronione, a dostęp możliwy jedynie dzięki pozwoleniu wydanemu przez dowództwo OOS. Ten reżim dostępu ustanawiany jest w obszarze działań bojowych i w rejonach zamkniętych.

Olga Wasiuta

I. Arreguín-Toft, *How to Lose a War on Terror: A Comparative Analysis of a Counterinsurgency Success and Failure*, [w:] *Understanding Victory and Defeat in Contemporary War*, J. Ångström, I. Duyvesteyn (eds.), Routledge, London 2007; tenże, *Tunnel at the End of the Light: A Critique of U.S. Counter-Terrorist Grand Strategy*, „Cambridge Review of International Affairs" 2002, vol. 15, no. 3; E. Bakker, T. Veldhuis, *A Fear Management Approach to Counter-Terrorism*, „The International Centre for Counter-Terrorism – The Hague 3" 2012, no. 1; *Bezpieczeństwo narodowe Polski w XXI w. Wyzwania i strategie*, R. Jakubczak, J. Flis (red.), Bellona, Warszawa 2006; *Counter-Terrorism, Human Rights and the Rule of Law: Crossing Legal Boundaries in Defence of the State*, A. Masferrer, C. Walker (eds.), Edward Elgar Publishing, Cheltenham 2013; M. Deflem, *Social Control and the Policing of Terrorism Foundations for a Sociology of Counterterrorism*, „American Sociologist" 2004, vol. 35; tenże, *The Policing of Terrorism: Organizational and Global Perspectives*, Routledge, New York 2010; J. Dorsey, Ch. Paulussen, *The Boundaries of the Battlefield: A Critical Look at the Legal Paradigms and Rules in Countering Terrorism*, „The International Centre for Counter-Terrorism – The Hague 4" 2013, no. 3; N. Lee, *Counterterrorism and Cybersecurity: Total Information Awareness*, Springer, Cham 2015; A. Merari, *Terrorism as a Strategy in Insurgency*, „Terrorism and Political Violence" 1993, vol. 5, iss. 4; J. Mitchell, *Identifying Potential Terrorist Targets: A Study in the Use of Convergence*, G2 Whitepaper on Terrorism, Counterterrorism Conference, Washington 2006; PAP, Defence24, *Ukraina: operacja wojskowa, zamiast antyterrorystycznej*, 1.05.2018, Defence24.pl (dostęp 1.01.2020); *Terror in the Holy Land: Inside the Anguish of the Israeli-Palestinian Conflict*, J. Kuriansky (ed.), Greenwood Publishing Group, London 2006; O. Wasiuta, S. Wasiuta, *Wojna hybrydowa Rosji przeciwko Ukrainie*, Wydawnictwo Arcana, Krakow 2017; *АТО завершилася, почалася ООС: що зміниться на Донбасі із введенням „особливого порядку"*, 1.05.2018, TSN.ua (dostęp 1.01.2020); Ю.В. Нікітін, *Антитерористична операція як необхідна форма протидії злочинності та забезпечення безпеки суспільства*, „Держава та регіони" 2014, № 2 (44); М.Л. Погребицький, *Антитерористична операція і міжнародний тероризм*, „Південноукраїнський Правничий Часопис" 2015, № 2.

ANTYTERRORYZM – metody, → t a k t y k i, → s t r a t e g i a i całokształt działań o charakterze ochronnym realizowanych przez specjalne agencje rządowe (policja, służby wywiadowcze, organy ścigania, jednostki wojskowe itp.), przeznaczone

do zwalczania lub zapobiegania → t e r r o r y z m o w i [t. 4]. Obejmuje monitorowanie działalności, gromadzenie i analizę danych wywiadowczych, a także działania wojskowe w celu stłumienia działalności terrorystycznej, zmniejszenie prawdopodobieństwa zaistnienia zamachu terrorystycznego oraz minimalizację jego skutków. Mieści w swoim zakresie ochronę osób i obiektów, przygotowanie planów działania w sytuacjach kryzysowych, zarządzanie siłami i środkami reagowania kryzysowego oraz działania analityczne w celu określania, oceny i prognozowania możliwych → z a g r o ż e ń [t. 4]. Strategia zwalczania terroryzmu to plan rządu dotyczący wykorzystania instrumentów władzy krajowej do neutralizacji terrorystów, ich organizacji i ich siatek, aby uniemożliwić im użycie → p r z e m o c y [t. 3] w celu zaszczepienia strachu i zmuszenia rządu lub jego obywateli do reagowania zgodnie z celem terrorystów. Strategia obejmuje również zapobieganie i powstrzymywanie wszelkich prób finansowania terroryzmu z wykorzystaniem broni, sprzętu lub innych środków finansowania.

Mimo ciągle powstających nowych zagrożeń i wyzwań terroryzm nadal jest uważany za największe zagrożenie dla krajów i należy do najbardziej niebezpiecznych przestępstw przeciwko podstawom ustroju konstytucyjnego i → b e z p i e c z e ń s t w a n a r o d o w e g o [t. 1] państw. Dlatego podstawowe zadania polityki wewnętrznej państw w zakresie bezpieczeństwa narodowego i obrony to zapobieganie zdarzeniom o charakterze terrorystycznym, przygotowanie do przejmowania nad nimi kontroli, reagowanie w razie wystąpienia takich zdarzeń oraz usuwanie ich skutków, w tym odtwarzanie zasobów przeznaczonych do reagowania na nie.

Pomimo podwyższonego poziomu zagrożenia zamachami terrorystycznymi na świecie i zaangażowania Polski w działania w ramach międzynarodowych koalicji antyterrorystycznych zagrożenie terrorystyczne w Polsce ze strony osób lub organizacji pochodzących z tzw. krajów podwyższonego ryzyka utrzymuje się na stosunkowo niskim poziomie, a terytorium państwa polskiego traktowane jest jedynie jako cel rezerwowy ewentualnych ataków. Istnieje jednak, o czym świadczą ataki terrorystyczne w innych krajach, realne zagrożenie ze strony pojedynczych osób, niezwiązanych bezpośrednio z organizacjami terrorystycznymi. Możliwe jest także podejmowanie prób wykorzystania terytorium RP do budowy zaplecza logistycznego w celu prowadzenia zamachów w innych krajach europejskich.

Przyjęta w grudniu 2005 r. przez UE strategia zwalczania terroryzmu definiuje 4 filary, które umożliwiają skuteczną walkę z terroryzmem. W ramach pierwszego filaru – zapobiegania – dąży się do walki z radykalizacją postaw i z werbowaniem terrorystów przez identyfikowanie metod, środków → p r o p a g a n d y [t. 3] i wykorzystywanych narzędzi z uwzględnieniem nowych zjawisk, takich jak terroryści działający w pojedynkę, zagraniczni bojownicy oraz posługiwanie się przez terrorystów mediami społecznościowymi. Drugim filarem jest ochrona obywateli i infrastruktury oraz ograniczenie podatności na atak m.in. poprzez poprawę →

b e z p i e c z e ń s t w a [t. 1] granic, systemów transportu i kluczowej infrastruktury. Kolejnym priorytetem jest ściganie, które polega na śledzeniu (i ściganiu) terrorystów na terytorium kraju i w skali światowej, na utrudnianiu im planowania, podróżowania i łączności, na niszczeniu sieci wsparcia, na odcinaniu od źródeł finansowania i dostępu do środków ataku, a także na stawianiu terrorystów przed wymiarem sprawiedliwości. Czwarty filar to reagowanie, polegające na przygotowywaniu się do zarządzania skutkami ataków terrorystycznych i minimalizacji tych skutków, a także na poprawianiu zdolności do likwidacji następstw, do skoordynowanej reakcji i do pomocy dla ofiar zamachów.

Obecnie kilka krajów dysponuje jednostką sił specjalnych przeznaczoną do reagowania antyterrorystycznego z elitarnymi jednostkami taktycznymi, mającą działać w razie ataku terrorystycznego lub mu zapobiec. Te siły mogą należeć do sektora wojskowego (wojsko, lotnictwo, → m a r y n a r k a w o j e n n a [t. 3]) oraz cywilnego (głównie w zakresie → b e z p i e c z e ń s t w a p u b l i c z n e g o [t. 1]). Takie jednostki są specjalnie wyszkolone w złożonej taktyce zwanej *Close Quarters Battle*, kładącej nacisk na ukrywanie się i rozwój misji przy minimalnych stratach. Zazwyczaj te siły dzielą się na: jednostki zdobywcze i kontrolne (zespoły szturmowe), snajperów, jednostki antybombowe, personel pomocniczy (np. piloci śmigłowców) oraz oficerów → w y w i a d u [t. 4]. Przykładowe jednostki to: Special Air Service z Wielkiej Brytanii i Special Air Service Regiment z Australii; YAMAM z izraelskiej straży granicznej i Sayeret Matkal z armii Izraela; oddział GSG 9 niemieckiej straży granicznej i KSK armii niemieckiej; jednostki amerykańskiej policji metropolitalnej zwanej SWAT, US Navy Seals – DEVGRU; COT policji federalnej Brazylii, siły specjalne armii brazylijskiej i DAE marynarki portugalskiej.

Polska prowadzi działania antyterrorystyczne poprzez system antytetorystyczny, rozumiany jako zbiór służb i instytucji powołanych do rozpoznawania zagrożeń, do przeciwdziałania im i ich zwalczania, mających odpowiednie uprawnienia i kompetencje, wyposażonych w środki przymusu, połączonych zintegrowanym systemem łączności, wymiany → i n f o r m a c j i [t. 2] i realizujących działania bezpośrednie pod tym samym dowództwem przy jednoczesnym informowaniu społeczeństwa o realnych lub potencjalnych zagrożeniach i odpowiednich postawach z tym związanych.

Podstawowym aktem prawnym polskiego systemu antyterrorystycznego, kompleksowo regulującym problematykę przeciwdziałania, zwalczania i reagowania na zagrożenia o charakterze terrorystycznym oraz usuwania ich skutków jest ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych. Umożliwia ona konsolidację poszczególnych podmiotów systemu antyterrorystycznego, z podziałem na sfery odpowiedzialności w określonych fazach działania. Pozwala to na pełne wykorzystanie potencjału służb, które realizują swoje zadania, a do tego wykorzystują podstawy prawne wynikające z innych ustaw, a także z przepisów wewnętrznego kierowania. Przepisy wewnętrzne powoływały również w niektórych służbach specjalne

komórki organizacyjne do walki z potencjalnymi zagrożeniami terrorystycznymi. W Polsce system antyterrorystyczny stanowią organy administracji publicznej, instytucje, służby, a także organy pomocnicze i opiniodawczo-doradcze, które działają na 3 poziomach – strategicznym, operacyjnym oraz taktycznym.

Na poziomie strategicznym Prezes Rady Ministrów i Rada Ministrów podejmują kluczowe działania o charakterze systemowym w zakresie ochrony antyterrorystycznej kraju. Minister Spraw Wewnętrznych i Administracji, który realizuje funkcję koordynacyjną, zarówno bezpośrednio, jak i poprzez działanie nadzorowanych służb (tj. Policji, Straży Granicznej, Służby Ochrony Państwa oraz → Państwowej Straży Pożarnej [t. 3]), odpowiada za przygotowanie do przejmowania kontroli nad zdarzeniami o charakterze terrorystycznym w drodze zaplanowanych przedsięwzięć, reagowanie w przypadku wystąpienia takich zdarzeń oraz odtwarzanie zasobów przeznaczonych do reagowania na te zdarzenia. Z perspektywy funkcji koordynacyjnej Ministra Spraw Wewnętrznych i Administracji w systemie przeciwdziałania i zwalczania terroryzmu, szczególnie istotne jest przewodniczenie Międzyresortowemu Zespołowi do Spraw Zagrożeń Terrorystycznych, który wraz z Kolegium ds. Służb Specjalnych i Rządowy Zespół Zarządzania Kryzysowego jest organem doradczym. Kolejnym ważnym podmiotem jest Szef → Agencji Bezpieczeństwa Wewnętrznego [t. 1], odpowiadający za zapobieganie zagrożeniom o charakterze terrorystycznym.

Na poziomie operacyjnym za koordynację zadań odpowiada Centrum Antyterrorystyczne Agencji Bezpieczeństwa Wewnętrznego oraz w odniesieniu do kwestii związanych z zarządzaniem kryzysowym – → Rządowe Centrum Bezpieczeństwa [t. 3]. Agencja Bezpieczeństwa Wewnętrznego jest ustawowo zobowiązana do rozpoznawania zagrożeń terrorystycznych i zapobiegania aktom terroru. Pozyskiwanie i analizowanie informacji pozwala na ocenę źródeł i skali zjawiska, wytypowanie grup potencjalnych zamachowców, rozpoznanie ich planów i zaplecza logistycznego. Ponadto do zadań Agencji Bezpieczeństwa Wewnętrznego należy także rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo, istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych wchodzących w skład → infrastruktury krytycznej [t. 2], a także systemów teleinformatycznych właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej. W ramach współdziałania Szef ABW informuje Dyrektora RCB o uzyskaniu informacji o możliwości wystąpienia sytuacji kryzysowej będącej skutkiem zdarzenia o charakterze terrorystycznym, zagrażającego infrastrukturze krytycznej, życiu lub zdrowiu ludzi, mieniu w znacznych rozmiarach, dziedzictwu narodowemu lub środowisku. Na poziomie taktycznym za realizację zadań ustawowych są odpowiedzialne poszczególne służby i instytucje, w których zakresie właściwości pozostaje antyterrorystyczna ochrona państwa (ABW, AW, Policja, SG, SKW, SWW,

ŻW, SOP, RCB, PSP, MON, Służba Celno-Skarbowa, MSZ, Prokuratura Krajowa, BBN, organy samorządowe).

Działania antyterrorystyczne są realizowane w 4 fazach. Pierwszą jest zapobieganie, koncentrujące się na rozpoznawaniu zagrożeń, ochronie granicy państwowej, działaniach wywiadowczych i kontrwywiadowczych, ochronie obywateli i placówek RP poza granicami państwa, monitorowaniu środków masowego przekazu, wymianie informacji, przeciwdziałaniu finansowaniu terroryzmu, ochronie → cyberprzestrzeni [t. 1], zapobieganiu radykalizacji i rekrutacji do organizacji terrorystycznych, a także na polityce migracyjnej, azylowej, informacyjnej oraz edukacyjnej. Druga faza to przygotowanie, obejmujące opracowywanie planów i zwiększanie zasobów, ocenę zabezpieczenia potencjalnych celów ataku, ochronę infrastruktury krytycznej, systemów transportowych i skupisk ludzkich, jak również współpracę z sektorem prywatnym. Trzecia faza zawiera w sobie działania na miejscu zdarzenia, w tym działania kontrterrorystyczne, czynności operacyjno-rozpoznawcze i dochodzeniowo-śledcze, → współpracę cywilnowojskową, komunikację ze społeczeństwem oraz pomoc ofiarom. Ostatnia faza – odbudowy – odpowiada za odtwarzanie sił i środków.

Zadania z zakresu zarządzania kryzysowego, w tym – w odniesieniu do zapobiegania, przeciwdziałania i usuwania skutków zdarzeń o charakterze terrorystycznym, są realizowane także na poziomie lokalnym. Kluczowa rola w tym zakresie przypada wojewodom, organom właściwym w zakresie zarządzania kryzysowego na terenie województwa, odpowiedzialnym za zapewnienie współdziałania wszystkich organów administracji rządowej i samorządowej działających w województwie i kierowanie ich działalnością w zakresie zapobiegania zagrożeniu życia, zdrowia lub mienia oraz zagrożeniom środowiska, bezpieczeństwa państwa i utrzymania porządku publicznego, ochrony praw obywatelskich, a także zapobiegania →klęskom żywiołowym i innym nadzwyczajnym zagrożeniom oraz zwalczania i usuwania ich skutków. Do zadań wojewody należy również prowadzenie czynności logistycznych zapewniających warunki sprawnego i efektywnego wykorzystania dostępnych zasobów osobowych, rzeczowych i finansowych na miejscu zdarzenia o charakterze terrorystycznym. Natomiast powiat wykonuje określone ustawami zadania publiczne o charakterze ponadgminnym, w tym – w zakresie porządku publicznego i bezpieczeństwa obywateli. Ponadto w ramach zagospodarowania przestrzennego są uwzględniane przez samorząd terytorialny potrzeby bezpieczeństwa państwa mające na celu m.in. zapewnienie warunków do reagowania na zagrożenia o charakterze terrorystycznym.

W razie zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym albo w razie wystąpienia takiego zdarzenia może zostać wprowadzony jeden z czterech stopni alarmowych:

I stopień alarmowy (stopień ALFA) – wprowadzany w razie otrzymania informacji o możliwości wystąpienia zdarzenia o charakterze terrorystycznym lub sabotażowym, którego rodzaj i obszar są trudne do określenia;

II stopień alarmowy (stopień BRAWO) – wprowadzany po uzyskaniu informacji o możliwości wystąpienia zdarzenia o charakterze terrorystycznym lub sabotażowym, gdy konkretny cel nie został rozpoznany, jednak pojawiło się większe ryzyko zagrożenia działalnością o podłożu terrorystycznym;

III stopień alarmowy (stopień CHARLIE) – ogłaszany, gdy zaistniało konkretne zdarzenie świadczące o celu potencjalnego ataku terrorystycznego, a także w razie uzyskania informacji o osobie bądź grupie ludzi przygotowujących działania terrorystyczne lub sabotażowe;

IV stopień alarmowy (stopień DELTA) – ogłaszany w przypadku wystąpienia zdarzenia terrorystycznego lub sabotażowego albo gdy prawdopodobieństwo ich wystąpienia jest wysokie. Stopnie alarmowe wprowadza, zmienia i odwołuje w drodze zarządzenia – w zależności od rodzaju zagrożenia zdarzeniem terrorystycznym – Prezes Rady Ministrów, po zasięgnięciu opinii ministra właściwego do spraw wewnętrznych i Szefa ABW, a w przypadkach niecierpiących zwłoki – minister właściwy do spraw wewnętrznych, po zasięgnięciu opinii Szefa ABW, o czym niezwłocznie informuje Prezesa Rady Ministrów.

W celu wzmocnienia przygotowania państwa na możliwość wystąpienia zdarzeń o charakterze terrorystycznym niezbędne okazuje się intensyfikowanie działań integrujących przedsięwzięcia realizowane przez wszystkich uczestników wielopodmiotowego systemu antyterrorystycznego RP.

Z myślą o skutecznym przeciwdziałaniu i reagowaniu na zagrożenia terrorystyczne niezbędna staje się wszechstronna współpraca wszystkich służb i instytucji zaangażowanych w szeroko rozumiane działania antyterrorystyczne. Ważnym aspektem jest także zapewnienie efektywnej współpracy cywilno-wojskowej, zwłaszcza poprzez usprawnienie procedur umożliwiających użycie → S i ł Z b r o j n y c h R P [t. 4] do wsparcia innych służb realizujących zadania w zakresie zwalczania terroryzmu lub usuwania skutków ewentualnych zamachów terrorystycznych. Jedynie koordynacja oraz wielopłaszczyznowe podejście zarówno do zagrożeń o charakterze terrorystycznym, jak i do prowadzonych działań antyterrorystycznych zapewnią efektywność systemu antyterrorystycznego RP, a tym samym – zwiększenie bezpieczeństwa wszystkich obywateli RP.

Anna Netreba

R. Borkowski, *Kontrterroryzm i antyterroryzm (aspekty teoretyczne i praktyczne)*, „Bezpieczeństwo. Teoria i praktyka" 2016, nr 3; M. Górka, *Polityka antyterrorystyczna jako dylemat demokracji liberalnej*, „Świat Idei i Polityki" 2017, nr 16;*Strategia UE w dziedzinie walki z terroryzmem*, Rada Unii Europejskiej, Bruksela2005; *System antyterrorystyczny RP*, https://www.gov.pl/web/mswia/system-antyterrorystyczny-rp (dostęp 20.11.2021); Uchwała nr 292 Rady Ministrów z dnia 9 grudnia 2014 r. w sprawie „Narodowego Programu Antyterrorystycznego na lata 2015–2019", Dz.U. 2014, poz. 1649; Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych, Dz.U. 2016, poz. 904.

ARCHITEKTURA *ZERO TRUST* (architektura „zero zaufania") – model zabezpieczenia zasobów sieciowych organizacji, polegający na nieustannym weryfikowaniu i uwierzytelnianiu użytkowników w celu sprawdzenia uprawnień dostępowych i ograniczenia skali szkód w razie ataku. Ze względu na całościowość rozwiązań można ją również określić jako plan cyberbezpieczeństwa podmiotu, jego rezultatem powinno być stworzenie spójnego systemu cyberbezpieczeństwa i konsekwentne egzekwowanie zasady zerowego zaufania.

Architektura *zero trust* (*zero trust architecture*, ZTA) jest stosunkowo nowym rozwiązaniem z zakresu → c y b e r b e z p i e c z e ń s t w a [t. 1], dlatego bywa określana mianem „nowego paradygmatu" lub „nowego modelu". Stanowi odpowiedź na rosnącą liczbę → c y b e r z a g r o ż e ń [t. 1], szczególnie ataków → r a n s o m w a r e, co wymaga nieustannego podnoszenia poziomu zabezpieczeń i skoncentrowania się na zapewnianiu wewnętrznej ochrony różnych systemów równocześnie, a nie – co było dominującą → s t r a t e g i ą [t. 5] – ochrony granic systemów czy punktów końcowych, podatnych chociażby na ataki typu *phishing*.

Historię powstania ZTA należy łączyć z powszechnymi procesami przechodzenia do pracy w środowisku sieciowym, szczególnie z wykorzystaniem rozwiązań opartych na → c h m u r z e o b l i c z e n i o w e j [t. 5], choć pierwsze koncepcje bazujące na zasadzie ograniczonego zaufania (wówczas – deperymetryzacji) pojawiły się już w 2004 r. W kolejnym piętnastoleciu liczne organizacje wdrażały elementy zerowego zaufania w różnych formach. W 2018 r. amerykański Narodowy Instytut Standardów i Technologii (National Institute of Standards and Technology, NIST) opublikował materiał rekomendujący wprowadzanie całościowego modelu architektury *zero trust*.

W kolejnych latach katalizatorami zmian były pandemia → C O V I D - 1 9 [t. 5] i spopularyzowanie pracy zdalnej, a także przybierające na sile – częściowo wiążące się z nowymi formami pracy – cyberzagrożenia. Wytyczne NIST stały się podstawą rozwiązań przyjmowanych przez organizacje oraz prac prowadzonych przez narodowe instytucje odpowiedzialne za cyberbezpieczeństwo. W Polsce na opracowaniu NIST opiera się wprost publikacja wchodząca w skład zbioru rekomendacji standaryzujących (Narodowe Standardy Cyberbezpieczeństwa), przygotowana w 2021 r. przez pełnomocnika rządu ds. cyberbezpieczeństwa i zatytułowana *Architektura bezpieczeństwa systemów informatycznych w modelu „Zero zaufania"*.

Wskazane wyżej dokumenty powielają 7 zasad ZTA, wypracowanych początkowo przez Narodowy Instytut Standardów i Technologii. Stały się one fundamentami modelu:

1) Wszystkie źródła danych i usługi obliczeniowe są uznawane za zasoby.
2) Cała komunikacja jest zabezpieczona niezależnie od lokalizacji w sieci.
3) Dostęp do poszczególnych zasobów podmiotu jest przyznawanyna zasadzie sesji.

4) Dostęp do zasobów jest określany przez dynamiczną zasadę – w tym obserwowalny stan tożsamości klienta, aplikacji lub usługi oraz żądającego zasobu – i może obejmować inne atrybuty behawioralne i środowiskowe.
5) Podmiot monitoruje i mierzy integralność i → b e z p i e c z e ń s t w o [t. 1] wszystkich posiadanych i powiązanych zasobów.
6) Wszelkie uwierzytelnianie i autoryzacja zasobów są dynamiczne i ściśle egzekwowane przed uzyskaniem dostępu.
7) Podmiot gromadzi jak najwięcej → i n f o r m a c j i [t. 2] o aktualnym stanie aktywów, infrastruktury sieciowej i komunikacji oraz wykorzystuje je do poprawy swojego poziomu bezpieczeństwa.

Architektura *zero trust* opiera się na założeniu, że żadnemu użytkownikowi i wykorzystywanemu przez niego urządzeniu próbującemu uzyskać dostęp do zasobów sieciowych nie można ufać („zero zaufania"). Tworzenie całego ekosystemu zabezpieczeń zaczyna się od konstatacji, że sieć nie jest bezpieczna, może zostać naruszona, a napastnik znajduje się wewnątrz niej – to oznacza, że każdy użytkownik i każde urządzenie mogą być napastnikiem i tak powinny być traktowane. Stąd też każde udane uwierzytelnienie traktowane jest jako teoretyczne przełamanie zabezpieczeń. Podejście to bazuje na słusznej obserwacji, że znaczna część ataków jest przeprowadzana z użyciem skradzionych danych dostępowych. Można to zobrazować odwróceniem klasycznej maksymy prawniczej o domniemaniu niewinności – w ZTA zakłada się, że każdorazowo należy domniemywać „winę" użytkownika (jego złe intencje), dopóki ten nie dokona uwierzytelnienia na konkretnym poziomie, a i poprawne uwierzytelnienie powinno podlegać ścisłemu monitoringowi. Stąd wszystkie procesy muszą być traktowane jako potencjalne zagrożenie.

Innowacyjność paradygmatu ZTA obejmuje zakwestionowanie przyjmowanej dotychczas reguły, że wstępne uwierzytelnienie użytkownika lub urządzenia i ich obecność w sieci wewnętrznej powinny być traktowane z zaufaniem. Wejście do sieci jest bowiem początkiem procesu. Architektura *zero trust* wymaga ciągłego potwierdzania tożsamości i uprawnień w zależności od żądań dostępu, co powinno pociągać za sobą dynamiczne wielokrotne uwierzytelnianie i autoryzację, szczególnie za pomocą weryfikacji dwuskładnikowej (2FA) lub wieloskładnikowej (MFA). Model ZTA bazuje zatem na przekonaniu, że „napastnik" znajduje się już w środowisku wewnętrznym organizacji, a jego kolejne ruchy można ograniczyć przez nadawanie użytkownikom najmniej uprzywilejowanych poziomów dostępu (zasada najmniejszych uprawnień bądź też specyficznie rozumiana zasada *need-to-know*). W ramach ZTA, ze względu na segmentację granic i ograniczenie dostępów, samo wejście do sieci nie oznacza jej całkowitej penetracji przez napastnika, co pozwala na znaczne ograniczenie szkód.

Architektura *zero trust* opiera się także na nieustannym monitorowaniu ruchu sieciowego – zarówno zewnętrznego (próby wejścia do sieci), jak i wewnętrznego (ruch już uwierzytelnionych użytkowników) – oraz poziomu zagrożenia. Analiza ta powinna

mieć stały charakter, odbywać się w czasie rzeczywistym z wykorzystaniem potencjału sztucznej inteligencji i obejmować wszystkie komponenty sieciowe i elementy infrastruktury IT.

Niezbędne wydaje się ustanowienie tzw. ciągłej diagnostyki i ograniczania zagrożeń (z ang. *continuous diagnostics and mitigation*, CDM). Podmioty wdrażające ZTA powinny opracować szczegółowe procedury na wypadek stwierdzenia naruszenia bezpieczeństwa któregokolwiek z poziomów dostępu, adekwatne do stopnia naruszenia. Zalecane jest dysponowanie systemem zarządzania informacjami i zdarzeniami (*security informationand event management system*).

Architektura *zero trust* powinna istotnie wpłynąć na poziom zabezpieczeń nowoczesnych organizacji, podnosząc jednocześnie poziom zaufania. Obejmuje to nie tylko zabezpieczenia przed atakami z zewnątrz, lecz także znaczną redukcję → r y z y k a ze strony użytkowników posiadających odpowiednie uprawnienia dostępowe. Należy założyć, że ZTA będzie zyskiwać na znaczeniu, szczególnie w dobie pracy zdalnej oraz migrowania danych organizacji do chmury, a wobec pozytywnych rekomendacji ze strony kluczowych podmiotów państwowych i międzynarodowych i coraz bardziej zaawansowanych prac nad wdrażaniem tego modelu może w przyszłości stać się jednym ze standardów. Należy odnotować, że znaczna część podmiotów dysponuje obecnie przynajmniej częścią rozwiązań wchodzących w skład ZTA, co znacznie ułatwi implementację niewdrożonych dotychczas zasad. Niewykluczone, że model ZTA będzie rozszerzany o klasyczne podejście koncentrujące się na ochronie obwodowej, tyle że z dostosowaniem poziomu zabezpieczeń środowiska wewnętrznego.

Opublikowane w styczniu 2022 r. memorandum gabinetu prezydenta Stanów Zjednoczonych obliguje agencje rządowe do spełnienia określonych standardów w zakresie cyberbezpieczeństwa do końca roku podatkowego 2024, w tym do wdrożenia zasad architektury *zero trust*. Uzupełnieniem dla wytycznych NIST mogą być rekomendacje Agencji ds. Cyberbezpieczeństwa i Bezpieczeństwa Infrastruktury (Cybersecurity and Infrastructure Security Agency, CISA), która opracowała Zero Trust Maturity Model, oparty na 5 filarach bezpieczeństwa: tożsamości użytkownika (ciągłe uwierzytelnianie), urządzeniu (ciągłe poświadczenia zgodności, analiza ryzyka), sieci (segmentacja, całkowite szyfrowanie wymiany), obciążeniu aplikacji (dostęp tylko po uwierzytelnianiu, monitoring ruchu) i danych (szyfrowanie wszystkich danych). Prace prowadzone w USA i Polsce należy traktować jako przykłady prób implementacji modelu, potwierdzające jednocześnie jego skuteczność weryfikowaną dotychczas głównie na bazie doświadczeń podmiotów prywatnych.

Mateusz Łabuz

L. Alevizos, V.-T. Ta, M.H. Eiza, *Augmenting Zero Trust Architecture to EndpointsUsing Blockchain: A State-of-The-Art Review*, „Security and Privacy" 2021, vol. 5; *Architektura bezpieczeństwa systemów informatycznych w modelu „Zero zaufania"*, NSC 800-207, wer. 1.0,

Warszawa 2021; Business Insider Polska, *Czym jest architektura Zero Trust? Model, zasady i bezpieczeństwo*, 20.05.2022, https://businessinsider. com.pl/technologie/nowe-technologie/architektura-zero-trust-model-zasady-i-bezpieczenstwo/m0vv212 (dostęp 10.04.2023); CISCO, *Foundations of a Zero Trust Implementation. A framework for Application Developers, Site Reliability Engineers, and Network Engineers*, 2022; Cybersecurity and Infrastructure Security Agency, *Zero Trust Maturity Model*, 2021; N. Howe i in., *Seven Elements of Highly Successful Zero Trust Architecture*, Zscaler 2022; A. Kerman i in., *Implementing a Zero Trust Architecture*, Project Description, National Institute of Standards and Technology, 2020; PwC, *Zero Trust Architecture: A Paradigm Shift in Cybersecurity and Privacy*, 2020; *Rekomendacje dla modelu „zero zaufania"*, https://www.gov.pl/ web/baza-wiedzy/rekomendacje-zero-zaufania (dostęp 10.04.2023); S. Rose i in., *Zero Trust Architecture*, National Institute of Standards and Technology, Special Publication 800-207, 2020; S.D. Young, *Memorandum for the Heads of Executive Departments and Agencies on Moving the U.S. Government toward Zero Trust Cybersecurity Principles*, M-22-09, Executive Office of the President, Washington D.C., 26 January 2022; *Zero Trust Reference Architecture. Version 2.0*, R. Freter (ed.), Department of Defense, 2022.

ARMIA HYBRYDOWA – armia Federacji Rosyjskiej/rosyjski korpus okupacyjny, znana również jako połączone rosyjsko-separatystyczne siły (wg terminologii USA: United Russian Separatist Forces), jest strukturą wojskową podlegającą Południowemu Okręgowi Wojskowemu Sił Zbrojnych FR, podczas → w o j n y [t. 4] na wschodzie Ukrainy okupuje część jej terytorium. Armia została utworzona przez Rosję pod koniec 2014 r. i na początku 2015 r. na bazie regularnych rosyjskich oddziałów inwazyjnych i zbrojnych kolaboracjonistycznych oddziałów tzw. Armii Noworosji działającej na okupowanych terytoriach obwodu donieckiego i ługańskiego Ukrainy.

Armią zarządza dowództwo w obwodzie rostowskim: w latach 2014– 2015 nazywano ją 12. Dowództwem Rezerwy, a od sierpnia 2015 r. Centrum Wojsk Terytorialnych Południowego Okręgu Wojskowego (FR) stacjonującego w Nowoczerkasku, podlega bezpośrednio Sztabowi Generalnemu w Moskwie.

Według danych Głównego Zarządu Wywiadu Ministerstwa Obrony Ukrainy formowanie 2 korpusów armii opierało się na batalionowo-taktycznych grupach inwazyjnych rosyjskich sił zbrojnych działających w Ukrainie w sierpniu i wrześniu 2014 r., a także na nielegalnych formacjach zbrojnych kierowanych przez oficerów Sztabu Generalnego GRU i FSB.

W lipcu 2015 r. major rosyjskich sił zbrojnych, który został schwytany przez siły ukraińskie, przedstawił szczegółowe dowody dotyczące struktury i działań 12. Dowództwa Rezerwy. Latem 2015 r. siły terrorystyczne utworzone przez lokalnych i rosyjskich terrorystów zostały zastąpione przez ustrukturyzowane jednostki wojskowe regularnej armii FR. W sierpniu 2015 „Inform Napalm" opublikowało badanie, zgodnie z którym 12. Dowództwo Rezerwy jest przykrywką dla sił okupacyjnych w Donbasie – wojskowych wysłanych do służby wojskowej do Nowoczerkaska faktycznie kierowano do Donbasu.

Ranga operacyjna i bojowa armii hybrydowej/wojsk okupacyjnych przeprowadzana jest zgodnie ze standardami i statutami wojskowymi Sił Zbrojnych FR. Oddziały zostały połączone w 2 korpusy, liczące ponad 33 tys. → ż o ł n i e r z y [t. 4] i oficerów:

- na 1. Korpus Armii składało się 5 brygad, 3 pułki, oddzielne bataliony i jednostki zabezpieczenia;
- na 2. Korpus Armii składały się 4 brygady, 2 pułki, oddzielne bataliony i jednostki zabezpieczenia.

W sierpniu 2015 r. ówczesny przewodniczący Rady Bezpieczeństwa Narodowego i Obrony Ukrainy A. Turczynow powiedział, że formowanie i działanie korpusów świadczą o tworzeniu rosyjskich wojsk okupacyjnych/ armii hybrydowej wg niemieckiego modelu Waffen-SS (zbrojne oddziały niemieckiej nazistowskiej formacji paramilitarnej) podczas II wojny światowej, kiedy jednostki te były tworzone z zagranicznych ochotników oraz cudzoziemców i obcokrajowców, a na ich czele stali oficerowie SS. Zagraniczni ochotnicy z okupowanych terytoriów wykorzystywani byli jako „mięso armatnie" w szeregach jednostek Waffen-SS.

Wiosną 2016 r. Siły Zbrojne FR rozpoczęły tworzenie 3. korpusu armii na terytorium Rosji w pobliżu granicy z Ukrainą. Utworzono również Centrum Informacyjnej Konfrontacji w celu poprawy skuteczności prowadzenia wojny informacyjnej przeciwko Ukrainie. Centrum jest częścią Obrony Sił Terytorialnych, na jego czele stoi płk Sił Zbrojnych FR K.L. Karpow.

Do zadań centrum należy:

- zdyskredytowanie przywódców politycznych i dowództwa Sił Zbrojnych Ukrainy wywołujące brak zaufania do nich;
- formułowanie poglądów na temat rozprzestrzeniania się rasizmu i nietolerancji etnicznej w Ukrainie;
- przekonanie społeczności międzynarodowej do tezy o systematycznym łamaniu przez władzę ukraińską reżimu zawieszenia broni oraz ukrytym nagromadzeniu przez Siły Zbrojne Ukrainy sił i środków wzdłuż linii demarkacyjnej w celu wznowienia aktywnych działań wojennych;
- tworzenie negatywnego wizerunku Sił Zbrojnych Ukrainy poprzez oskarżanie ukraińskich żołnierzy o popełnienie zbrodni i bezprawne działania, w szczególności wobec → l u d n o ś c i c y w i l n e j [t. 3];
- demoralizacja ukraińskich żołnierzy;
- kształtowanie nastrojów antyukraińskich wśród ludności czasowo okupowanego terytorium Ukrainy.

Strukturę Centrum Informacyjnej Konfrontacji tworzą:

- Departament izolacji informacyjnej obszaru działań bojowych (zapewnia całkowitą dominację rosyjskich środków masowego przekazu w → p r z e s t r z e n i i n f o r m a c y j n e j [t. 3] czasowo okupowanego terytorium Ukrainy);

- Departament dezinformacji i kontrpropagandy (dyskredytuje przywództwo polityczne i dowództwo Sił Zbrojnych Ukrainy);
- Departament współpracy wojskowo-cywilnej (tworzy negatywny obraz Sił Zbrojnych Ukrainy, oskarżając ukraiński personel wojskowy o popełnienie zbrodni i bezprawne działania wobec ludności cywilnej).

Według Głównego Zarządu Wywiadu Ministerstwa Obrony Ukrainy w kwietniu 2016 r. prawie 70% osobowego personelu korpusu stanowili obywatele rosyjscy (w tym 45% rosyjskiego personelu wojskowego i 25% rosyjskich najemników), pozostałe 30% tworzyli obywatele ukraińscy z terytoriów okupowanych obwodów donieckiego i ługańskiego. Według Ministerstwa Spaw Wewnętrznych Ukrainy w 2018 r. armia hybrydowa FR liczyła 35 tys. osób. W jej arsenale znajdowało się 478 czołgów, 848 pojazdów opancerzonych, 750 systemów artyleryjskich i moździerzy, 208 systemów wyrzutni rakiet, 363 sztuki broni przeciwpancernej, 419 zestawów obrony przeciwpowietrznej.

Rosyjska armia hybrydowa prowadzi → w o j n ę h y b r y d o w ą [t. 4] na terytorium Ukrainy, która obejmuje działania → p o l i c j i [t. 3], polityków, sędziów, prawników (i wielu innych) oraz wreszcie samą armię, tworzoną przez żołnierzy, którzy nie przyznają się, że są z FR.

Do armii hybrydowej zaliczamy:

- personel wojskowy, czyli regularną armię;
- żołnierzy z poboru, którzy podpisali kontrakty, tj. najemników rosyjskich;
- tzw. rosyjskich „kazaków", których Kreml często wykorzystuje do wykonywania zadań poza granicami państwa;
- czeczeńskich najemników (wszyscy są związani z R. Kadyrowem);
- innych najemników (np. serbscy żołnierze czy liczni przedstawiciele narodów azjatyckich);
- byłych przedstawicieli Berkutu (specjalnych oddziałów milicji podległych MSW Ukrainy, które zostały rozwiązane w lutym 2014 r.);
- etnicznych Rosjan mieszkających w Ukrainie;
- → p i ą t ą k o l u m n ę [t. 3] (miejscowi, którzy działają jako obcy agenci);
- rosyjskich „turystów" (nacjonaliści, szowiniści, którzy udają Ukraińców);
- ukraińskich żołnierzy i oficerów, którzy zdezerterowali z armii ukraińskiej albo którzy w niej działali jako zdrajcy lub szpiedzy;
- lokalnych przestępców przeszkolonych w obozach szkoleniowych i mających broń;
- miejscowych bojówkarzy, którzy dobrowolnie walczą przeciwko Ukraińcom;
- zwerbowanych miejscowych mieszkańców, którzy są poddawani poważnej presji ze strony rosyjskich służb specjalnych (najczęściej stoją na punktach kontrolnych i udzielają wywiadów zachodnim mediom);
- mieszkańców, którzy zostali zmuszeni do walki (głównie młodzi lub bardzo młodzi ludzie potrzebujący pieniędzy);

- rosyjskich przestępców bądź więźniów, którzy zostali objęci amnestią w zamian za działalność wojskową w Ukrainie;
- rosyjskie siły specjalne (rzadko widoczne w mediach, wykorzystywane są w walce do tworzenia przewagi Rosji na polu walki);
- oficerów rosyjskiego → w y w i a d u [t. 4] wojskowego (Główny Zarząd Wywiadowczy Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej, GRU GSzt SZ FR);
- rosyjskich oficerów Sił Zbrojnych FR, którzy identyfikują się jako przedstawiciele grupy ustalającej przebieg linii demarkacyjnej;
- grupy wywiadowczo-dywersyjne (DRG) sił rosyjsko-terrorystycznych;
- agentów FSB (sprawdzają i kontrolują wszystkich innych);
- dowódców (dowodzenie tym wojskiem jest skoncentrowane w rękach rosyjskich generałów);
- prawdziwych aktorów i aktorek, których wykorzystuje się do celów propagandowych, celowo poszukujących uwagi zachodnich dziennikarzy z zamiarem odegrania dramatycznej roli i podtrzymywania → p r o p a g a n d y [t. 3] Kremla;
- dziennikarzy pracujących w celu → d e z i n f o r m a c j i i propagandy (oni również odbywają szkolenia wojskowe i walczą przeciwko Ukraińcom).

10 zasad taktycznych armii hybrydowej Federacji Rosyjskiej:

- Dywersyjne grupy wywiadowcze – organizują one ataki punktowe, np. na przejściach między blokadami dróg, które polegają na minowaniu i tworzeniu zasadzek na drogach, nieoczekiwanych atakach na poszczególne pozycje. Być może w 2014 r. zastosowanie takiej taktyki było uzasadnione – część miejscowej ludności sympatyzowała z uzbrojonymi → z i e l o n y m i l u d z i k a m i [t. 4], a Siły Zbrojne Ukrainy nie zawsze orientowały się w sytuacji poza głównymi drogami. Obecnie nie jest ona już skuteczna, ponieważ:
  a) Ukraina stworzyła linię ciągłą frontu, budując na niej wzmocnioną obronę, która pozwala kontrolować całe terytorium linii frontu;
  b) jest to ziemia ukraińska, na której mieszkają Ukraińcy i nawet na okupowanym terytorium pomagają Siłom Zbrojnym Ukrainy, np. informując o podejrzanych osobach z bronią.
- Chowanie się za cywilami – należy do podstaw współczesnej rosyjskiej taktyki, którą Kreml wykorzystywał jeszcze podczas wojny rosyjsko-czeczeńskiej, rozmieszczając swoje pozycje na cmentarzach, podwórkach szkół, w przedszkolach, szpitalach i budynkach mieszkalnych. Kreml miał nadzieję, że armia ukraińska zacznie strzelać w kierunku budynków i dzielnic mieszkalnych, tak jak armia rosyjska robiła to w Czeczenii. Rezultatem miał być uderzający obraz „ludobójstwa ludu Donbasu" (zob. → l u d o b ó j s t w o [t. 3]), który miał być pokazany państwom Zachodu. Takie plany Kremla zawiodły, dlatego Rosjanie musieli wymyślać historie o „ukrzyżowanych dzieciach" i sami ostrzeliwali okupowane przez siebie terytoria.

- Ukrywanie własnej obecności – potrzebne Rosji właśnie po to, by bezkarnie ukrywać się za ludnością cywilną i popełniać inne → z b r o d n i e w o j e n n e [t. 4]. Według Kremla „Naszej armii tam nie ma". Żołnierze armii hybrydowej zasłaniają znaki taktyczne na standardowym wyposażeniu, w tym na samochodach ciężarowych, rosyjskich czołgach, transporterach czy wyrzutniach rakiet; zamiast poświadczeń wojskowych FR wydaje się dokumenty nieuznawanych państw, odcina się z mundurów wojskowych znaki identyfikacyjne, ukrywa okoliczności, a nawet fakty śmierci rosyjskich żołnierzy we wschodniej Ukrainie, którzy zginęli „na urlopach w Donbasie". Żołnierze rosyjscy stracili szacunek do munduru i sztandaru wojskowego – wartości, na których opierały się i opierają siły zbrojne każdego państwa.
- Taktyka wypychania – polega na tym, że po każdej kolejnej podpisanej umowie Moskwa natychmiast zaczyna ją łamać. Wykorzystuje ów moment uścisku dłoni, moment dzielenia się „szczerymi" słowami, aby zrobić kolejny – zwykle niewielki – krok w kierunku realizacji własnych interesów. Może to być np. zajęcie kilku opuszczonych domów w strefie neutralnej w trakcie zawieszenia broni. Taktyka ta jest prymitywna, ale przynosi rezultaty: po zajęciu domów umieszcza się tam obserwatora, potem korektora, później broń palną. Następnie rozpoczyna się regularne ostrzeliwanie pozycji Sił Zbrojnych Ukrainy. Ukraińskie wojsko już zrozumiało tę taktykę i obecnie okupantom coraz trudniej jest wykonywać takie działania.
- Taktyka otoczenia – na wzór taktyki Mongołów, którzy nigdy całkowicie nie otaczali wroga, lecz zawsze pozostawiali mu drogę ucieczki, ponieważ wróg przyparty do ściany zaciekle się broni, a wróg, który ma miejsce do wycofania się, jest mniej uważny i ucieka wąskim przesmykiem, gdzie hordy mogą go dogodnie pokonać. Częste konflikty, zatargi i wojny wyrobiły u Rosjan podejrzliwość, poczucie konieczności stosowania daleko posuniętych środków ostrożności, a zarazem upodobanie do najrozmaitszych podstępów wojennych. Cenę za „uczciwe słowo rosyjskiego oficera" zapłacono w pobliżu Iłowajska, kiedy ostrzelany został „zielony korytarz". Armia atakowała zawsze w kilku kierunkach jednocześnie, utrudniając w ten sposób rozpoznanie i stwierdzenie, który kierunek ataku jest główny, czym wymuszała podzielenie sił przeciwnika. Armia mongolska, również dla zmylenia przeciwnika, starała się zawsze wracać z wyprawy inną drogą niż ta, którą przybyła. Stosowała pozorowane odwroty, które nierzadko miały na celu wywabienie przeciwnika z dobrze ufortyfikowanych pozycji i podprowadzenie go w pobliże ustawionych w zasadzce głównych sił. Mongołowie prowadzili wojny do ostatecznego zwycięstwa, czyli do pełnego podporządkowania lub wybicia danego ludu.
- Zasada koncentracji głównych wysiłków – stosowana jest także przez armię hybrydową. Na przykład w → b i t w i e pod Debalcewem Rosjanie, zasłaniając się właśnie podpisanym w Mińsku zawieszeniem broni, ściągnęli żołnierzy z wszystkich innych części frontu.

- Najeźdźcy stosują również kilka kierunków ataku ofensywnego – przed tym przygotowują się, prowadzą wywiad, próbują wskazać najsłabszy punkt obrony. Dopiero po przygotowaniach usiłują przedrzeć się przez obronę i otoczyć jednostki ukraińskie (jeśli nie fizycznie, to przynajmniej werbalnie, aby w przestrzeni informacyjnej rozpowszechnić dezinformację). Ostatnim razem dowódcy wojskowi Putina próbowali zastosować te techniki pod Marijinką latem 2015 r. Jednak w odpowiedzi na koncentrację sił wroga Siły Zbrojne Ukrainy skupiły ogień artyleryjski w ich obszarze.
- Oprócz doświadczeń czeczeńskich i afgańskich Kreml przyjął także zachodnią praktykę prywatnych formacji wojskowych – tzw. 1. (doniecki) i 2. (ługański) Korpus Armijny w „republikach ludowych" są w rzeczywistości prywatną armią Putina, tworzoną głównie przez zmotoryzowaną piechotę. Są dokładnie takie same jak w rosyjskiej armii, świetnie wyposażone, bardzo dobrze wyszkolone i zorganizowane. Uzupełniają je „ochotnicy" i „separatyści" z FR, a rekrutacja najemników odbywa się za pośrednictwem rosyjskich biur rekrutacyjnych. Jednak armia hybrydowa FR to nie tylko wynajęta piechota, lecz również profesjonalni wojskowi z sił zbrojnych FR, którzy zestrzelili malezyjskiego boeinga 777 i prowadzą uderzenia rakietowe na terytorium Ukrainy.
- W wojnie w Donbasie okupanci wykorzystują 2 szeregi – prywatną armię Putina w pierwszym i część regularnej armii FR w drugim. Ofensywa tej hybrydowej armii zwykle wygląda następująco: prywatna armia „ochotników" jest mięsem armatnim dla pierwszego uderzenia, w dalszych działają jednostki regularnej armii FR. Użycie prywatnej armii jest korzystne, ponieważ ofiarom nie trzeba płacić z budżetu państwa, a ich rodziny również nie otrzymują odpowiednich odszkodowań. Niemożliwe jest obliczenie rzeczywistych strat tej prywatnej armii.
- Propaganda i wojna informacyjna – chociaż mówimy głównie o taktyce wojskowej, nie należy zapominać, że wojna w Donbasie nie byłaby możliwa bez bezprecedensowej w historii ludzkości kampanii medialnej wykorzystującej dezinformację ludności i przemyślany terror psychologiczny wymierzony przeciwko obywatelom po obu stronach frontu.

W sieciach społecznościowych odbywa się wiele dyskusji dotyczących tego, jak nazwać armię, która walczy przeciwko Ukraińcom po stronie tzw. separatystów: rebelianci, separatyści, prorosyjscy separatyści czy armia rosyjska, ponieważ część miejscowych obywateli również walczy po ich stronie (zob. → s e p a r a t y z m [t. 4]). Takie połączenie różnorodnych grup naprawdę niełatwo jednoznacznie określić armią. Mimo wszystko to właśnie Rosja prowadzi wojnę i jest to jej celowa taktyka, polegająca także na kultywowaniu obcego wpływu oraz dyskredytowaniu systemu demokratycznego. Armia rosyjska jest armią hybrydową, która próbuje stać się częścią lokalnego środowiska i dlatego tak trudno ją rozpoznać.

Ponadto rosyjscy wojskowi są wyposażeni tak samo jak bojówkarze „DRL" i „ŁRL". Odznaki wojskowe, insygnia i znaki taktyczne są stosowane bardzo niekonsekwentnie, co dodatkowo komplikuje sytuację.

Rosyjska armia hybrydowa to armia zamalowanych tablic rejestracyjnych i armia zerwanych szewronów. Zwykle żołnierze każdej armii są dumni ze swoich barw i insygniów, ponieważ to ich identyfikuje, jest ich symbolem, z którym idą do walki. Dla każdego żołnierza flaga oznacza przynależność do kraju, a żołnierz rosyjski umiera z hybrydowym czerwono-niebieskim krzyżem, który bardziej kojarzy się z amerykańskimi konfederatami z wojny secesyjnej z lat 1861–1865 niż z Rosją. Podstępna hybrydowa wojna Rosji zabrała rosyjskim żołnierzom nawet ich honor – prawo do śmierci pod swoją rodzimą flagą.

Olga Wasiuta

M. Kennard, *Irregular Army: How the US Military Recruited Neo-Nazis, Gang Members, and Criminals to Fight the War on Terror*, Verso Books, New York 2012; D. Sikkema, *Ruined America: The Rise of the Hybrid Army*, Lulu.com, Washington 2017; S.A. Southworth, S. Tanner, *U.S. Special Forces: A Guide to America's Special Operations Units: The World's Most Elite Fighting Force*, Da Capo Press, Cambridge 2002; D. Waller, *The CIA Secret Army*, 3.02.2003, Time.com (dostęp 15.02.2020); O. Wasiuta, *Armia hybrydowa*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; O. Wasiuta, S. Wasiuta, *Wojna hybrydowa Rosji przeciwko Ukrainie*, Wydawnictwo Arcana, Krakow 2017; E. Tsybulenko, J.A. Francis, *Separatists or Russian Troops and Local Collaborators? Russian Aggression in Ukraine: The Problem of Definitions: Jus Ad Bellum, Jus In Bello, Jus Post Bellum*, [w:] *The Use of Force against Ukraine and International Law*, S. Sayapin, Tsybulenko E. (eds.), T.M.C. Asser Press, Springer, The Hague 2018; *США изменили подход в освещении роли Москвы в кризисе в Украине*, 30.04.2015, Krymr.com (dostęp 15.02.2020); *Гібридна армія РФ під Світлодарськом понесла великі втрати – ГУР*, 30.06.2016, UA-News.liga.net (dostęp 15.02.2020); *Гібридна армія Путіна пішла в атаку на ВСУ під Жолобком, підняваши прапор морської піхоти РФ,* 26.09.2019, Unia.net.ua (dostęp 15.02.2020); *Складові гібридної війни. Аналізуй, вивчай, протидій – перемагай*, Veterano.com.ua (dostęp 15.02.2020); *Розвідка розкрила структуру окупаційних військ РФ в Донбасі*, 27.04.2016, UA-News.liga.net (dostęp 15.02.2020); *бойовиків на Донбасі – громадяни Росії, 25% – кадрові військові та 45% – так звані «добровольці», – воєнна розвідка*, 27.04.2016, UACrisis.org (dostęp 15.02.2020).

ARMIA ZAWODOWA – wojsko lub jego część złożona z → ż o ł n i e r z y [t. 4], dla których bycie w armii jest zawodem, głównym zadaniem, jakim zajmują się zawodowo w życiu, za które są wynagradzani i które stanowi główne źródło ich utrzymania. Ten rodzaj armii najczęściej przeciwstawia się armii poborowej, która składa się z osób wcielonych do wojska bez wyraźnego żądania bądź chęci z ich strony. Nie oznacza to, że w armii poborowej znajdują się wyłącznie żołnierze, którzy nie chcieli się znaleźć w wojsku. Niekiedy w armiach poborowych, zwłaszcza w chwilach → z a g r o ż e n i a [t. 4] niepodległości czy w szczególnej sytuacji politycznej, poborowi mogą wykazywać się szczególnym zaangażowaniem, natomiast nie jest to regułą.

Współcześnie dokonuje się coraz dalej idąca profesjonalizacja armii. Badacze często podkreślają istnienie 3 okresów w rozwoju sił zbrojnych. W latach 1900–1945, we wczesnej nowoczesności, przed okresem → z i m n e j w o j n y [t. 4] charakterystyczne były armie masowe, w okresie zimnej wojny, określanym jako późna nowoczesność, dominowały duże armie zawodowe. Obecnie w okresie pozimnowojennym, zwanym także ponowoczesnością, dokonuje się ich redukcji na rzecz małych armii zawodowych.

Wiele europejskich państw podejmuje obecnie działania reformatorskie, a w szczególności na rzecz profesjonalizacji sił zbrojnych i eliminacji poboru. W Europie tylko kilka państw, takich jak Finlandia, Austria, Cypr, Estonia i Grecja, nadal utrzymuje pobór do wojska, a jedynie 3 z 27 członków → NAT O [t. 3], Grecja, Estonia i Norwegia, nadal utrzymuje pełny pobór, przy czym niektóre z tych krajów rozważają eliminację obowiązkowego poboru. Ten proces profesjonalizacji, choć zgodny z bieżącymi trendami, ma wiele niezamierzonych i nieprzewidzianych konsekwencji. Profesjonalne wojsko jest prawie zawsze mniejsze niż armia poborowa.

Jak zauważono, pozycje sił zbrojnych zostały zredukowane, niejednokrotnie w pośpiechu, co przyspieszyła dodatkowo rezygnacja z poboru. W konsekwencji zawodowa jednostka wojskowa jest najprawdopodobniej bardziej zdolna niż podobna siła poborowa, ale zawodowe organizacje bojowe są na ogół mniejsze od jednostek poborowych i mniej liczne, co prowadzi do zmniejszenia zdolności netto. Pomimo trwającego → k r y z y s u [t. 2] zatrudnienia w Europie niektóre państwa mają problemy ze znalezieniem wystarczającej liczby ochotników. Niemcy, które dość gwałtownie zawiesiły pobór w 2010 r., mają trudności w rekrutacji 60 tys. zawodowych żołnierzy, których potrzebują do obsadzenia wszystkich miejsc w armii. W związku z tym wydaje się, że Niemcy będą musiały zredukować swoje siły zbrojne jeszcze bardziej, niż pierwotnie zakładano. Zawodowi żołnierze są znacznie drożsi w rekrutacji, szkoleniu i utrzymaniu niż żołnierze poborowi, którzy często otrzymują wynagrodzenie tylko na utrzymanie podczas służby. Wysoki koszt personelu wojskowego stanowi większość europejskich wydatków wojskowych, co jest istotnym problemem. Należy wspomnieć także o konieczności wypłacania konkurencyjnych wynagrodzeń dla żołnierzy zawodowych w celu przyciągnięcia ochotników do armii. Ponadto trzeba zagwarantować środki na pokrycie wielu świadczeń takich jak koszty leczenia i emerytura, które dotyczą pracowników otrzymujących wynagrodzenie. Jako pracownicy rządowi żołnierze zawodowi zazwyczaj korzystają z bardzo atrakcyjnych i kosztownych świadczeń.

Profesjonaliści często kosztują więcej, ponieważ ich szkolenie jest bardziej wyrafinowane i dłuższe, co powoduje wzrost kosztów jednostkowych. Podczas gdy wojska z poboru mogą być kosztowne również ze względu na stały wymóg szkolenia nowych żołnierzy, przygotowania te są nierzadko krótsze oraz uproszczone i stosunkowo tańsze. Natomiast profesjonaliści muszą być w stanie obsługiwać i utrzymywać bardzo specjalistyczny sprzęt, co wymaga zaawansowanego i ciągłego szkolenia. Profesjonalizacja

doprowadziła też do wysokiego stopnia specjalizacji, przy czym zakres zadań wysoko wykwalifikowanych profesjonalistów nie jest szeroki. W porównaniu z armiami z czasów zimnej wojny istnieje bardzo niewiele podstawowych jednostek piechoty, które mogą wykonywać zadania o wielopoziomowym stopniu skomplikowania.

Profesjonalizacja europejskich armii ma również istotny wpływ na inne obszary. Ponieważ wielu młodym Europejczykom udało się uniknąć poboru do wojska poprzez służbę zastępczą w dziedzinach takich jak opieka zdrowotna, ratownictwo, a nawet ochrona środowiska, organizacje działające w tych sferach borykają się ze znalezieniem wystarczającej liczby wolontariuszy, np. w Niemczech jest to tylko ok. 1/10 wymaganej liczby wolontariuszy w służbie zdrowia od czasu zlikwidowania poboru w 2010 r. Dotyczy to także służb ratowniczych takich jak Bundesanstalt Technisches Hilfswerk (THW, Federalna Agencja Pomocy Technicznej), która odgrywa ważną rolę w zarządzaniu ratownictwem w czasie katastrof. W wyniku profesjonalizacji wyraźne zmiany zaszły również w obszarze rezerw sił zbrojnych w wielu krajach. Siły rezerwowe są często w dużym stopniu uzależnione od stałego napływu żołnierzy kończących aktywną służbę. Większość z nich ma wtedy zobowiązania rezerwowe, które muszą wypełnić. Profesjonaliści nie mają jednak takich obowiązków. Nie przechodzą oni do rezerw po krótkim pobycie na służbie czynnej.

W związku z tym przepływ wyszkolonych żołnierzy do rezerw w Europie znacznie spadł.

W konsekwencji redukcji aktywnych sił zbrojnych w Europie dostrzegalny jest spadek stanu liczebnego sił zbrojnych. Podczas zimnej wojny wiele narodów szczyciło się bardzo licznymi siłami rezerwowymi, przekraczającymi w niektórych przypadkach 0,5 mln żołnierzy. Według Bilansu Wojskowego 1989–90 Niemcy miały rezerwy przekraczające 700 tys. żołnierzy, Hiszpania ponad 800 tys., a Włochy 520 tys. żołnierzy. Nawet mała Szwajcaria mogła zmobilizować ponad 600 tys. żołnierzy. Obecnie żaden naród europejski z wyjątkiem Finlandii nawet nie zbliża się do standardów zimnowojennych. Członkowie NATO tacy jak Belgia, Włochy i Holandia mają mniej niż 10% sił rezerwowych, którymi dysponowali podczas zimnej wojny. Nawet kraje nienależące do NATO zarządzają dziś znacznie mniejszymi rezerwami: Szwecja i Szwajcaria mają tylko 1/3 sił rezerwowych z tych, które były dostępne w 1990 r. Ponadto wiele z istniejących sił rezerwowych nie znajduje się już w zorganizowanych jednostkach takich jak bataliony piechoty, są to raczej jednostki dostępne do → m o b i l i z a c j i [t. 3] lub nie mają żadnych rzeczywistych zdolności bojowych, jak np. Francuskie Rezerwy Obywatelskie. Brakuje im zatem odpowiedniej struktury do przeprowadzania wszelkiego rodzaju współczesnych misji wojskowych.

Nie tylko jest znacznie mniej sił rezerwowych, ale też ich możliwości są w dużej mierze ograniczone. W czasie zimnej wojny siły rezerwowe wielu państw NATO i państw spoza sojuszu mogły pochwalić się możliwością wystawienia, czasami w bardzo krótkim czasie, dywizji dość dobrze wyszkolonych i wyposażonych żołnierzy ze

sprecyzowanymi zadaniami do wykonania. Natomiast obecnie taki stan rzeczy nie jest już spotykany. Tytułem egzemplifikacji wg Bilansu Wojskowego z 1990 r. armia niemiecka miała ponad 700 tys. rezerwistów, dzięki czemu mogła powołać do działania kilkanaście brygad → o b r o n y n a r o d o w e j [t. 3], 15 pułków obrony narodowej i 150 kompanii obrony narodowej, dla porównania w 2010 r. rezerwy Armii Niemieckiej wynosiły 144 tys. Według dokumentów rządu niemieckiego rocznie finansowanych jest tylko 2,5 tys. rezerwowych przydziałów czasowych. Podobna sytuacja jest we Francji: w 1990 r. po mobilizacji mogła powołać 3 dywizje, 7 brygad obrony terytorialnej i kolejne 20 pułków terytorialnych, 20 lat później Francja miała ok. 100 jednostek wielkości kompanii liczących ok. 100 żołnierzy każda. Tak samo w przypadku Włoch, które w 1990 r. mogły wystawić 240 tys. żołnierzy w 7 brygadach, ale w 2010 r. już tylko 38 tys. rezerwistów wojskowych, nie mając żadnej struktury organizacyjnej rezerwy.

Możliwości obecnych sił rezerwowych w Europie rodzą więc wiele wątpliwości i uwag krytycznych. Ponieważ wymóg obrony ojczyzny zdawał się słabnąć, zmniejszyło się również zapotrzebowanie na formalne organizacje o określonych możliwościach. Tendencja ta wydaje się rozwijać coraz szybciej, ponieważ zmniejsza się ilość rezerw, podobnie jak liczba i rodzaj jednostek rezerwowych.

Specyficzną konkurencją wobec armii zawodowej pozostaje także rozwój tzw. cywilów funkcyjnych, których zadania zarezerwowane były niegdyś wyłącznie dla wojskowych. Na przykład to prywatne firmy ochroniarskie nierzadko przejmują funkcje, które mają zasadniczo wojskowy charakter, takie jak ochrona instalacji wojskowych. Organizacje wojskowe są zawsze odpowiedzialne za własne → b e z p i e c z e ń s t w o, ale w praktyce często nawet działania wokół głównych zadań są zlecane podmiotom cywilnym. Profesjonalizacja wielu europejskich armii przyspiesza ten trend, ponieważ zawodowi żołnierze są zbyt drodzy, by pełnić służbę wartowniczą przy wejściach do baz wojskowych.

Podobnie żołnierze zawodowi są zbyt cenni, aby pełnić wiele prozaicznych funkcji niezbędnych do działania współczesnych sił zbrojnych. Wiele zadań logistycznych, takich jak transport, zaopatrzenie i gastronomia, wykonywanych jest przez cywilów. Może to stwarzać problemy podczas rozlokowania jednostek wojskowych, ponieważ zdolności te mogą występować tylko u cywilnych kontrahentów, którzy je przejęli. Odnosi się to również do wielu funkcji konserwacyjnych. Nowoczesny sprzęt wojskowy jest często tak wyrafinowany, że wymaga specjalnego wsparcia serwisowego ze strony kontrahentów, a wsparcie to musi także towarzyszyć sprzętowi wszędzie tam, gdzie się on znajduje. Oznacza to, że we współczesnych konfliktach można się spotkać z wieloma kontrahentami na polu walki. Wykonawcy okrętów od dawna towarzyszą → m a r y n a r k o m w o j e n n y m [t. 3] przy ich rozmieszczaniu, a w ciągu ostatnich dwóch dekad obserwujemy ogromny wzrost wsparcia ze strony wykonawców na Bałkanach, Bliskim Wschodzie i w Afganistanie. Jak zauważono,

wykonawcy ci świadczą wyjątkowo szeroki zakres usług, w tym w zakresie bezpieczeństwa.

Jednakże wsparcie to często wykracza daleko poza wsparcie logistyczne. Wiadomo, że → l u d n o ś ć c y w i l n a [t. 3] bierze udział w wojskowych operacjach bojowych, mimo że ich umowa zwykle tego zabrania. Nierzadko konieczność wykonywania dodatkowych obowiązków, zwłaszcza w przypadku operacji związanych z bezpieczeństwem osobistym, znajdowała wykonawców walczących na polu → b i t w y . Firmy te były również mocno zaangażowane w realizację zadania wojskowego polegającego na szkoleniu lokalnych rdzennych sił wojskowych i bezpieczeństwa. Cywilni pracownicy ministerstw obrony narodowej i wykonawcy znajdują się obecnie na całym polu walki, w tym w wielu sztabach, gdzie pełnią liczne funkcje kadrowe tradycyjnie sprawowane przez oficerów wojskowych. Nie chodzi jednak tylko o to, że ludność cywilna przejęła zadania wojskowe, także wojsko stało się bardziej cywilne. Wiele operacyjnych sił specjalnych nie nosi mundurów podczas wykonywania swoich misji, lecz raczej codzienne ubrania, które pozwalają żołnierzom wtopić się w lokalną ludność, nawet jeśli oznacza to łamanie dawnych zasad wojny. Ta tendencja do stosowania niestandardowego ubioru rozprzestrzenia się nawet na jednostki konwencjonalne, które niejednokrotnie oprócz mundurów noszą zestaw przedmiotów cywilnych, a także korzystają z rozmaitych cywilnych przedmiotów takich jak noże i plecaki.

Warto podkreślić też, że gdy większość państw w Europie profesjonalizuje swoje siły zbrojne w omawiany sposób, zrywa relację łączącą obywateli z wojskiem powstałą w wyniku służby wojskowej z poboru.

Może to przyczynić się z jednej strony do poprawy reputacji i wizerunku żołnierzy, ponieważ negatywne aspekty służby przymusowej zanikają wraz ze wzrostem statusu zawodowego i postrzegania kompetencji żołnierzy. Z drugiej jednak, jak w przypadku wielu państw, które dokonały profesjonalizacji sił zbrojnych, przepaść między społeczeństwem a siłami zbrojnymi, które je chronią, będzie się powiększać, przyczyniając się do braku zrozumienia i wzajemnej sympatii.

Żołnierze biorący udział w wielu misjach, także w zagranicznych misjach wsparcia pokoju, często zaczynają tracić swoje podstawowe umiejętności bojowe, np. artylerzystom do utrzymania i rozwijania tych umiejętności niezbędne jest regularne operowanie przy przydzielonych im działach, co nie jest łatwe, gdyż są zaangażowani w inne zadania, takie jak patrolowanie miast. Wraz z profesjonalizacją sił zbrojnych problem ten może łatwo stać się bardziej dotkliwy. Wysłanie minimalnie wyszkolonego poborowego żołnierza do zapewnienia wsparcia dużej imprezy sportowej jest czymś zupełnie innym niż wysłanie tam dobrze wyszkolonego i kosztownego profesjonalisty. Wykorzystywanie armii zawodowych do realizacji funkcji niezwiązanych bezpośrednio z celami wojskowymi budzi ogromne wątpliwości. Wielokrotnie jednak armie są proszone o wykonywanie zadań takich jak zbieranie śmieci i gaszenie pożarów, nierzadko ze szkodą dla ich gotowości do pełnienia swojej podstawowej

funkcji. Choć siły wojskowe zaangażowane w cywilne zadania pomocnicze czerpią z tego określone korzyści, jest to związane również z pewnym kosztem. Częstokroć nie da się ich łatwo relokować. Wycofanie się z danego zadania wsparcia cywilnego w celu realizacji innego działania niejednokrotnie wymaga dużo czasu. Współcześni żołnierze zawodowi są niekiedy tak kosztowni, że wykorzystywanie ich do takich zadań jak służba wartownicza czy wywóz śmieci wydaje się niewłaściwą inwestycją.

Jakub Idzik

Z. Barany, *The Soldier and the Changing State: Building Democratic Armies in Africa, Asia, Europe, and the Americas*, Princeton University Press, Princeton–Oxford 2012; Ch. Bellamy, *The Evolution of Modern Land Warfare: Theory and Practice*, Routledge, New York–London 2015; J. Burk, *Military Culture*, [w:] *Encyclopedia of Violence, Peace & Conflict*, L.R. Kurtz (ed.), Elsevier, Oxford 2008; J.L. Clarke, *What Should Armies Do: Armed Forces and Civil Security*, Routledge, London 2014; *Department of Defense Dictionary of Military and Associated Terms*, Joint Chiefs of Staff, Washington 2020; M. Nuciari, *The Study of the Military. Models for the Military Profession*, [w:] *Handbook of the Sociology of the Military*, G. Caforio, M. Nuciari (eds.), Springer, Cham 2018; *The Palgrave Handbook of Security, Risk and Intelligence*, R. Dover, H. Dylan, M. Goodman (eds.), Palgrave Macmillan, London 2017; F.S. Pearson, M.O. Lounsbery, N. Southeastern, J. Sislin, *Arms Trade, Economics of*, [w:] *Encyclopedia of Violence, Peace & Conflict*, L.R. Kurtz (ed.), Elsevier, Oxford 2008; D. Westwood, *Armies: Organization and Tactics*, [w:] *Ground Warfare: An International Encyclopedia*, S. Sandler (ed.), ABC-CLIO, Santa Barbara–Denver–Oxford 2002.

ARTYLERIA – jest jednym z najbardziej efektywnych i najdłużej wykorzystywanych typów broni w historii wojska. Geneza armat i prochu strzelniczego nie jest dobrze znana, jednak armaty zostały po raz pierwszy wymienione w dekrecie miasta Florencji z 1326 r. W ciągu wieków artyleria dowiodła, że w odpowiednich rękach potrafi siać spustoszenie na polu → b i t w y. Przez blisko 3 tys. lat uchodziła za najbrutalniejsze, a zarazem najskuteczniejsze narzędzie → w o j n y [t. 4]. Słowo „artyleria" jest często rozumiane jako „machina służąca do wystrzeliwania pocisków w czasie wojny". Niewątpliwie artyleria zyskała dobrą sławę za sprawą swojej potęgi w zrównywaniu z ziemią obranego celu. Słowo to pochodzi od Anglo-Normanów oraz ze środkowej Francji, gdzie wyewoluowało ze stfr. czasownika *artillier* oznaczającego „zaopatrywać w broń", później stało się terminem określającym różne rodzaje broni. Artyleria zaczęła być kojarzona z balistycznymi machinami wojennymi dopiero kilka dekad po jej wprowadzeniu, odnosiła się do urządzeń takich jak katapulty, trebusze i łuki, których działanie polegało na przemieszczeniu wagi oraz wykorzystaniu siły odrzutu do miotania pocisków. Dopiero w pierwszych dekadach XV w., ponad 100 lat po pierwszym użyciu, termin zaczął określać broń czarnoprochową oraz uzbrojenie o właściwościach wybuchowych.

Artyleria nie była dostatecznie skuteczna aż do końca średniowiecza.

Postęp technologiczny przyczynił się jednak do tego, że broń rycerska, pancerze płytowe oraz inne tradycyjne uzbrojenie stały się przestarzałe, o artylerii zaś zaczęto

myśleć jako o broni opartej na działaniu ładunku wybuchowego. Znaczenie samego słowa podążało tym samym za rozwojem uzbrojenia, od procy, przez katapulty, aż do tureckich bombard i nowocześniejszych dział. Do XVII w. znaczenie pojęcia artylerii poszerzało się: od samych machin wojennych dawniej, przez amunicję wykorzystywaną przez nie, aż po jednostki wojskowe odpowiedzialne za ich rozmieszczenie. Artyleria ze względu na swoje działanie określana bywa mianem dział „grzmotu i pioruna", głównie przez charakterystyczny odgłos powstający w wyniku wystrzału. Na początku machiny wojenne odgrywały rolę artylerii, a więc były środkiem do miotania obiektów zbyt ciężkich, aby mógł tego dokonać pojedynczy człowiek. W ten sposób machiny te nakreśliły podstawowe zasady funkcjonowania artylerii. Historyczne zapisy poświadczają użycie nowatorskich machin przeciwko murom Jerozolimy w VIII w. p.n.e. Były one prawdopodobnie przodkami katapult i balist zasilanych skręconymi sznurami wykonanymi z włosia, sierści czy ścięgien.

Średniowieczną katapultę najczęściej wyposażano w ramię zakończone elementem przypominającym łyżkę, służącym do miotania pocisków. Schemat katapult przyjęty przez Greków oraz starożytnych Rzymian był bardziej dopracowany niż ten z czasów średniowiecza, miały one bowiem skórzany sznur przymocowany do ramienia, co dawało wrażenie i efekt działania procy. Kiedy ramię katapulty zostało wyposażone w procę, jego długość wydłużono dokładnie o długość procy do niego przymontowanej, dodatkowo waga całej katapulty tylko nieznacznie się zwiększyła, bez jakiegokolwiek wpływu na samo jej działanie. Im dłuższe było ramię, tym dłużej przebywało w powietrzu oraz tym dalej wyrzucało pocisk, przy założeniu że waga amunicji była taka sama. Różnica jest dostrzegalna, gdy porównuje się proce krótkie i długie. Dodanie procy do ramienia zwiększało moc machiny nawet o 50%.

Konstrukcja balisty w dużym stopniu przypominała kuszę: horyzontalne ramiona, pomiędzy którymi znajdował się napięty niczym cięciwa sznur. Balista miała możliwość wystrzeliwania zarówno włóczni, jak i kamieni. Podobnie jak współczesne działa polowe balista strzelała płasko, bezpośrednio w cel. Mimo podobieństw do kuszy była w stanie regulować siłę naciągu cięciwy, kusza zaś mogła oddać jedynie strzał z pełnego napięcia. Pocisk był oparty o cięciwę, która z kolei zabezpieczana była przez hak zaczepiony o pętlę na samej cięciwie.

W zestawieniu z poprzednio wymienionymi urządzeniami oblężniczymi Greków czy Rzymian trebusz jest stosunkowo nowym wynalazkiem. Pierwszy trebusz pojawił się we Francji w XII w., podczas gdy katapulta czy balista istniały jeszcze kilka wieków przed erą chrześcijańską. Trebusz zawdzięcza siłę rażenia sile grawitacji oraz ciężarowi obciążników, inaczej niż w przypadku katapult czy balist. Na początku 2. poł. XII w. trebusz w znacznej mierze zastąpił katapultę, ponieważ z łatwością strzelał pociskami o wadze ponad 100 kg, czyli 5–6 razy cięższymi niż w przypadku największych katapult.

Wprawdzie katapulty niszczyły wieże i umocnienia ciągłymi i skoncentrowanymi salwami, ale już jeden 100-kilogramowy kamień wyrzucony z trebusza był w stanie

zatrząść najsilniejszą twierdzą. Głównym przeznaczeniem trebuszy było niszczenie górnych części umocnień oraz murów twierdz, aby były one łatwiejsze do pokonania za pomocą drabin oraz innego sprzętu. Katapulta dzięki dużemu polu rażenia sprawdzała się lepiej w sianiu zamętu wśród ludności wewnątrz oblężonego obiektu. Narodziny wielkich armat i dział znanych w większości z XX i XXI w. datuje się na moment wynalezienia czarnego prochu, który służył do wyrzucania pocisków z lufy takich urządzeń. Pierwsze bitewne użycie przedmiotu przypominającego działo zanotowano 28 stycznia 1132 r., kiedy gen. Han Shizhong z dynastii Song zdobył miasto Fujjin, ostrzeliwując je za pomocą kory z drzewa bambusowego przystosowanej do miotania ołowianych drobin czy też śrutu. Był więc on pierwszą osobą, która wykorzystała działa artyleryjskiego w walce.

Ówczesne działa, mimo że prymitywne, wraz z czarnym prochem zaczęły odgrywać coraz ważniejszą rolę na polach bitew, co w znacznej mierze przyczyniło się do ich zawrotnego rozwoju m.in. w Azji oraz XIII-wiecznej Europie. Konstrukcję bambusową zastąpiono wówczas ołowiem i żeliwem, a za amunicję służyły ładunki śrutowe, żelazne, a także kamienne kule, strzały, czasem nawet zwykłe metalowe resztki. Wynalezienie czarnego prochu uznaje się za jedno z najbardziej znaczących wydarzeń w rozwoju artylerii i historii świata. Wczesna wersja prochu nie miała właściwości wybuchowych, lecz z czasem się to zmieniło.

Właściwa broń zasilana czarnym prochem powstała w XIII w., a w połowie XIV w. nowa broń zaczęła zmieniać oblicze pola bitwy. Chociaż wynalazek pochodził z Chin, to nie wywołał znaczących zmian w Państwie Środka, zupełnie inaczej niż w Europie w późnym średniowieczu. Jak sugeruje sama nazwa, ładunek wybuchowy występował pierwotnie w postaci proszku – pyłu, który palił się powoli i wytwarzał małe ciśnienie. We wczesnych próbach konstrukcji dział wcale nie oznaczało to nic złego, gdyż nie wytrzymałyby większego ciśnienia. Jednakże już w połowie XV w. wytwórcy czarnego prochu zaczęli zbijać i formować proch w większe ziarna, a więc granulat, co skutkowało wzrostem prędkości spalania, zwiększeniem ciśnienia i dawało większą prędkość wylotową pocisku.

W Europie w 2. poł. XV w. odlewnictwo rozwijało się bardzo dynamicznie, co sprawiło, że bombardy nie były jedynymi działami, a z czasem zaczęły być zastępowane przez coraz lepsze, nowocześniejsze i co ważne, lżejsze egzemplarze. XVI w., z punktu widzenia rozwoju artylerii, upłynął głównie na rozwiązywaniu odwiecznego problemu dotyczącego ogromnej wagi dział, unowocześnianiu amunicji oraz zwiększeniu mobilności jednostek artylerii. Dzięki temu cesarz Ferdynand mógł zaatakować Turków w 1556 r. razem z 57 ciężkimi oraz 127 lekkimi jednostkami artylerii.

Na początku XV w. zaczęła pojawiać się amunicja w postaci żelaznych kul. Zwiększona skuteczność nowej amunicji razem z ulepszonym prochem umożliwiały dalszy rozwój w budowaniu mniejszych i silniejszych dział. Przed XVI w. działa oblężnicze były dominującymi urządzeniami na polu bitwy. Później jednak wytwarzano działa

z żelaza, które były stosowane na lądzie, do obrony oraz w marynarce. Jeszcze później równocześnie rozwijano działa odlewane z żelaza i działa wykonane z brązu. Niektóre z nich były nawet ozdabiane renesansowymi rycinami.

Następnym krokiem w ewolucji dział było odlewanie kołków wystających z obu bocznych stron działa. Sprawiło to, że zmiana kąta nachylenia działa nie była już uciążliwa, a także ułatwiło transport. Potem zaczęto rozwijać platformy, na których montowano działa, początkowo mało ergonomiczne z czasem ustępowały kołowym, solidnym powozom artyleryjskim. Wraz z wynalezieniem przez Francuzów przodka – pojazdu dwukołowego, do którego mocowano działo w celu przetransportowania go – ok. 1550 r. nastąpił kolejny krok w standaryzacji kalibru dział artyleryjskich.

W międzyczasie pierwsza armata przypłynęła na pokładzie okrętu Kolumba poszukującego Nowego Świata. Gdy obserwator Pinty zauważył ląd wczesnym rankiem 12 października 1492 r., odgłos wystrzału lombard dał znać załodze Świętej Marii, że poszukiwania zostały zakończone (ląd odkryty wtedy przez hiszpańską flotę dzisiaj nazywany jest Bahamami). W ciągu następnego stulecia nie tylko galeony, ale także liczne fortyfikacje w hiszpańskiej flocie były uzbrojone w armaty, odstraszające rozbójników chcących zaskarbić sobie prawo do hiszpańskich znalezisk. Od czasu do czasu podróżnicy zatrzymywali dla siebie armaty jako zdobycz, jak np. Drake w 1586 r., który zabrał ze sobą 14 średnich armat wykonanych z brązu, pochodzących z drewnianego fortu St. Augustine.

W angielskich koloniach w okresie XVI i XVII w. powszechniejsze były lżejsze działa, jednak w znanych nam opisach historycznych nie ma wzmianki o armatach, które w tamtych czasach były oddzielną klasą dział. Częściej można znaleźć informacje o kolubrynach i półkolubrynach, ale przede wszystkim o falkonetach, falkonach, minionach czy sakerach.

W XVI w. pojawiła się nowa dziedzina naukowa, która zajmowała się balistyką. W 1537 r. N. Tartaglia opublikował pierwszą rozprawę naukową o artylerii. Wypróbowywano różne konstrukcje, z których z czasem rezygnowano, by w późniejszych stuleciach znaleźć dla nich lepsze zastosowanie, np. w już istniejących działach z systemami zamkowymi. Początkowo takie działa nie cieszyły się uznaniem, głównie z powodu braku dokładnie domykanego zamka skutkującego wydobywaniem się gazów prochowych. Poza tym jego prymitywna konstrukcja powodowała nierzadko zacięcia poprzez zaklinowanie się zamka i lufy, co z kolei poważnie uszkadzało go w wyniku wstrząsu spowodowanego wystrzałem, uniemożliwiając ponowne użycie działa.

J. Žižka zapoczątkował wykorzystanie mobilnej artylerii w wojnach husyckich w latach 1419–1424. Używano wówczas lekkich dział ciągniętych przez najlepsze konie, a nie woły, jak wcześniej. Francuzi ulepszyli ten system, zwiększając mobilność swoich dział, co sprawdzało się w rozpraszaniu skupionych grup pikinierów w bitwach z Włochami na początku XVI w. Sława Francuzów nie trwała jednak długo, Niemcy pod panowaniem Maksymiliana I zostali pionierami w dziedzinie artylerii i posługiwali

się działami zdolnymi do rażenia celów odległych o niemal 1,5 km. Niemieckie drużyny artyleryjskie utrzymywały reputację najlepszych operatorów dział w Europie. Od 1525 r. Hiszpanie zaczęli tworzyć formacje ciężkozbrojnych → ż o ł n i e r z y [t. 4] piechoty, w których skład wchodzili pikinierzy oraz arkebuzerzy i muszkieterzy (żołnierze uzbrojeni w muszkiety). Takie rozwiązanie pozwoliło im zdominować pole bitwy. Po pojawieniu się muszkietu rozwój artylerii zatrzymał się. Mimo że artyleria była dobrze rozwinięta pod względem mobilności, powozy, na których ją montowano, nadal zdawały się obszerne i ciężkie. Aby przemieścić angielską ciężką armatę w dogodne miejsce, zaprzęgano 23 konie, a do przemieszczenia kolubryny potrzebowano 9 olbrzymich zwierząt.

Jako amunicję wykorzystywano wówczas żelazne, odlewane kule, bomby (żelazne kule wypełnione czarnym prochem), kanistry (pojemniki wypełnione małymi śrucinami) oraz kartacze (pociski odłamkowe). Do transportu amunicji początkowo używano taczek i wózków, a czasami sami żołnierze przenosili ją na plecach. Szybkość, z jaką przemieszczano armatę, zależała od artylerzysty kanoniera idącego pieszo obok działa, którym operował. Był to zatem trudny okres historyczny dla drużyny artyleryjskiej. Dowódcą artylerii zazwyczaj był żołnierz, sam transport zaś wynajmowano.

Cztery wieki technologicznego rozwoju doprowadziły do daleko idących zmian. Od małych wazopodobnych narzędzi cenionych za donośny dźwięk, przez działa o największym kalibrze, jakie kiedykolwiek wyprodukowano, po bombardy i coraz mniejsze, ale potężniejsze armaty. Działa z XVII w. strzelały tak daleko, jak te z XIX w. Były potężne, ale ich słabą stroną były mobilność, organizacja i taktyka. Z powodu małego postępu w tych dziedzinach w bitwach dominowały wciąż piki i muszkiety.

Dopiero pod okiem szwedzkiego króla Gustawa II Adolfa artyleria zaczęła zajmować swoje prawowite miejsce na polu bitwy. Preferował on mobilność swoich wojsk, a popularna broń skórzana (ang. *leather canon*) jego autorstwa była już na tyle mobilna, że jej obsługa oraz transport nie wymagały więcej niż 2 ludzi. Jednakże król zrezygnował z tego projektu na rzecz żelaznych półkolubryn produkcji dowódcy i inżyniera wojskowego

L. Torstenssona. Same działa ważyły ok. 230 kg i transportowano je, wykorzystując 2 konie. Ich konstrukcja pozwalała na skuteczne użytkowanie z grupą zaledwie 3 operatorów. Scalenie ze sobą ładunku prochowego i pocisku w jeden nabój zastąpiło stare metody rozdzielnego ładowania, a także zwiększyło szybkostrzelność. Dawny standard jednego działa na 1 tys. żołnierzy Gustaw Adolf zwiększył do 6 dział oraz dodatkowo wyposażył każdy pułk w parę lekkich działek. Zdawał sobie sprawę również ze znaczenia skoncentrowanego ognia, więc często zbierał działa w silne baterie, a swoją → s t r a t e g i ę [t. 4] opierał na bombardowaniu wrogich formacji piechoty za pomocą ostrzału artyleryjskiego, podczas gdy kawaleria neutralizowała ociężałe i niemobilne działa wroga. Strategia ta sprawdziła się – w 1631 r. Gustaw rozniósł w pył hiszpańskie czworoboki w Breitenfeld.

Podążając za szwedzkim przykładem, reszta narodów zaczęła modyfikować swoją artylerię, a prowadzenie objęli Niemcy, Francuzi oraz Austriacy. Z czasem sekrety artylerii stopniowo zanikały, operatorzy stawali się profesjonalnymi żołnierzami, a brąz stał się ulubionym materiałem do wyrobu broni.

Na początku XVIII w. działa były używane do ochrony punktów rozlokowania wojsk oraz do osłabiania nadchodzących formacji wroga. Przeważała tendencja używania ciężkich baterii osłanianych przez stałe fortyfikacje, były to standardowe działania artylerii. Z drugiej strony sam fakt posiadania takich sił nie zawsze gwarantował wygraną w bitwie, ale z odpowiednim dowodzeniem, szkoleniem załogi oraz dyscypliną artyleria była w stanie w dużej mierze kierować przebiegiem starcia.

W Ameryce Północnej działa miały zbyt duże rozmiary, aby można było ich skutecznie używać w walce z Indianami. Z uwagi na duże odległości w Ameryce transport ograniczał się zwykle do wykorzystania dróg wodnych, przeszkodą dla transportu lądowego były gęste lasy. W czasie wybuchu wojny o niepodległość amerykańskie wojska artyleryjskie składały się ze zbieraniny dział, moździerzy i haubic każdego typu o nawet 13 różnych kalibrach. Od kiedy import nie był możliwy, mało rozwinięty przemysł odlewniczy w koloniach rozpoczął produkcję dział, przed 1775 r. odlewnie w Filadelfii wytwarzały działa z brązu i żelaza.

W tym czasie w Europie król Prus Fryderyk II Wielki użył dział podczas kampanii wojny siedmioletniej (1756–1763). Aby móc dotrzymać kroku kawalerii, Fryderyk umieścił działa na transporcie konnym, zachowując mobilność kawalerii. Jego oddziały artyleryjskie składały się głównie z lekkich dział i haubic, co pozwalało na formowanie małych baterii w ważnych punktach strategicznych, rozpoczynania ofensywy, a także osłaniania rozstawienia kolumn. Co ważne, mógł on w każdej chwili zmieniać ustawienie baterii w zależności od rozwoju sytuacji.

Francuska artyleria J.-B. de Gribeauvala dawała się we znaki za sprawą dynamicznego tempa i przytłaczającej siły ognia baterii, które po prostu miażdżyły siły przeciwnika. Gribeauval unowocześnił przyrządy celownicze i wyposażenie całej artylerii; zmniejszył długość i ograniczył wagę dział bez ograniczenia zasięgu ich strzału, a także znormalizował kalibry dział i amunicji. Stworzył powozy, których części mogły być wymieniane z innymi tak, aby były uniwersalne, oraz szkolił zawodowych żołnierzy kierowców. Dla obrony wybrzeża zastosował obrotowe platformy mające koła z tyłu konstrukcji, poruszające się po szynach, co znacząco upraszczało celowanie do ruchomych celów przy ułatwionym skręcie działa w lewo czy w prawo. Tego typu wyposażenie wprowadzone przez Gribeauvala zapoczątkowało powstanie wielu nowych taktyk, które wprowadzał sam Napoleon.

Napoleon Bonaparte wiele zyskał dzięki nowym wynalazkom, udało mu się za ich pomocą doprowadzić skuteczność ówczesnej artylerii do perfekcji. Pod jego dowództwem zadaniem piechoty było przejmowanie terenu zaraz po tym, jak artyleria rozprawiła się z siłami wroga. Napoleon wysyłał swoich artylerzystów do przodu, aby jak

najszybciej zmniejszyli dystans i otworzyli ogień przeciwko wrogim formacjom z zastosowaniem kartaczy. Tym zagraniem artyleria Napoleona efektywnie unicestwiała szyki oponentów. Artyleria odgrywała tak ofensywną rolę, że piechota i kawaleria docierały do luk w obronie wroga właściwie bez zadawania strat.

Po okresie napoleońskim historia artylerii przeważnie utożsamiana jest z zapisem jej skuteczności technicznej razem z ulepszeniami czy zmianami w już i tak dobrze zakorzenionych zasadach jej stosowania. Najdawniejsze działa i koncepcje wykorzystania artylerii odbierać można dziś jako proste i prymitywne, jeśli zestawić je ze współczesnymi zdobyczami techniki znamionującymi jej rozwój i coraz to nowsze możliwości. Kamieniem milowym w rozwoju artylerii było ujawnienie w 1897 r. przez armię francuską nowej broni, działa 75 mm mle 97, które z biegiem czasu otrzymało wdzięczną nazwę „sławnej siedemdziesiątki piątki Francuzów". Omawiany wytwór inżynierii artyleryjskiej wprowadził koncepcję szybkostrzelnego działa z szybko działającym mechanizmem zamkowym. Posługiwało się ono amunicją scaloną oraz tarczą. Jedną z rewolucyjnych właściwości francuskiego działa był system kontroli odrzutu, w którym wykorzystano zasadę pneumatyki płynów oraz gazów do wprowadzenia lufy działa z powrotem na pozycję gotowości do strzału, to z kolei dawało znacznie zwiększoną szybkostrzelność i stałą celność – system gwarantował, że lufa po wystrzale wracała na swoją poprzednią pozycję, co wykluczało potrzebę wtórnego obierania celu.

Amunicja scalona razem z nowoczesnym systemem zamkowym zapewniała szybkie ładowanie działa jednym ruchem. Koncepcja amunicji scalonej polegała na zastosowaniu metalowego cylindrycznego pojemnika ze spłonką u podstawy wypełnionej bezdymnym prochem, szczelnie domkniętej przez pocisk. System kontroli odrzutu powodował, że działo nie przesuwało się do tyłu po oddawaniu strzału, co pozwalało operatorom na przebywanie zaraz przy urządzeniu, za tarczą chroniącą przed potencjalnie wrogim ostrzałem, a to z kolei umożliwiało lepsze zaopatrzenie w amunicję oraz dodatkowo ułatwiało ładowanie. Przeciętna obsługa takiego działa była w stanie utrzymać szybkostrzelność działa na poziomie 20 strzałów na minutę. Taki stan rzeczy był prawdziwym fenomenem w rozwoju artylerii.

Z dnia na dzień francuski wynalazek uczynił przestarzałą każdą inną jednostkę artylerii na świecie. Znamienne pozostaje to, że Francuzi osiągnęli podobny efekt w przypadku broni małokalibrowej, wprowadzając do użycia karabin Lebel mle 1886, który zdecydowanie przewyższał swymi osiągami uzbrojenie przeciwników w tamtym okresie. Twórcy dumni ze swoich osiągnięć kurczowo się ich trzymali, nawet do tego stopnia, że pozwoliło to innym państwom na wytworzenie o wiele lepszych konstrukcji. Natomiast w 1900 r. wszystkie państwa na świecie mające artylerię zaczęły wymagać od swoich wytwórców broni produkcji szybkostrzelnych dział. Przed 1914 r. wszystkie wojownicze armie miały już taki sprzęt, traktowany jako pierwszoliniowa artyleria, lecz rezerwy wciąż korzystały z prowizorycznych modyfikacji przestarzałych już dział. Zmasowana produkcja wojenna wkrótce zapewniła ogromną ilość

nowoczesnego wyposażenia, a w wyniku wojny zostało także wprowadzone uzbrojenie, które znajdowało się dopiero w fazie rozwoju jeszcze na początku XX w.

Należy jednak podkreślić, że w ostatecznym rozrachunku, wraz z upływem czasu, najważniejszym czynnikiem w konstruowaniu uzbrojenia była waga, która musiała zostać zoptymalizowana na tyle, aby zespół 6–8 koni był w stanie przetransportować broń w ciągu dnia marszu. Średnie działa (oblężnicze) mogły ważyć więcej, ale musiały być przewożone partiami, aby zmieścić się w wyznaczonym limicie. XX w. wiązał się także z pojawieniem się ciągnika na silnik zasilany benzyną. Kilka armii przeprowadzało testy tego urządzenia. Mimo niewątpliwego postępu niejednokrotnie okazywało się, że zawodność silnika prowadziła do wniosku, że lepiej wykorzystywać w dalszym ciągu konie. Powodowało to, że koncepcja użycia silnika została w większości państw odsunięta na dalszy plan.

Artyleria wykorzystywana w okresie II wojny światowej nie była znacząco lepsza od tej z czasów I wojny światowej. Jedyne różnice dostrzegalne były w zastosowaniu ciągników mechanicznych do wielkich dział, wykorzystywano także pneumatyczne ogumienie, rozkładane powozy, skuteczniejszą amunicję oraz zaawansowaną metalurgię produkowanych dział.

Podczas II wojny światowej nastąpił kolejny przełom w artylerii – wynalezienie dział samobieżnych. Wojny wymagały znacznych nakładów ekonomicznych, więc rozwój nowej kategorii artylerii został początkowo wstrzymany, ale zauważono zwiększające się zapotrzebowanie na tego rodzaju broń, spowodowane szybko rozwijającymi się formacjami pancernymi – rozwój artylerii powtórnie stał się priorytetem. Należy także wspomnieć, że kolejnym wytworem artyleryjskiej inżynierii w trakcie II wojny światowej stał się pocisk kierowany, a także udoskonalone rakiety stanowiące niezależną broń balistyczną.

Późne lata 40. XX w. były okresem zamętu w wojskowości, spowodowanego odkryciem energii atomowej oraz pocisku kierowanego. Artyleria nadbrzeżna została zdemontowana w wielu państwach, nie było już na nią zapotrzebowania, zwłaszcza gdy pocisk balistyczny mógł po prostu przelecieć nad linią obrony. Nagle wszystkie zasoby i środki zostały skupione na rozwijaniu kierowanych pocisków z głowicami atomowymi i rakiet do obrony powietrznej, a także statków powietrznych i ich uzbrojenia. Kiedy inżynierowie i naukowcy dostatecznie wykorzystali możliwości rozwoju uzbrojenia z użyciem energii nuklearnej, skupili się na artylerii.

Nie oznacza to jednak, że jej zasady działania zostały diametralnie zmienione, wręcz przeciwnie, nadal były to długie rury wystrzeliwujące pociski w wyniku spalania ładunku miotającego. Do gotowej już mieszanki dodano jedynie stosowną dozę rozwiązań pochodzących ze współczesności, do obliczeń balistycznych służyły już komputery, a nie człowiek z kartką papieru i ołówkiem. Oznaczało to, że obliczenia były nie tylko szybsze, ale stawały się bardziej złożone, co przekładało się na znaczy wzrost precyzji prowadzonego ostrzału wraz ze zwiększoną szybokstrzelnością.

Amunicja została wzbogacona o układy scalone w charakterze nowych zapalników czasowych, które były przystępniejsze niż bezpośrednie metody. Zaczęto używać kombinacji kompasów żyroskopowych, podczerwieni, laserów oraz radarów razem z satelitami, aby perfekcyjnie oddawać kolejne strzały. Samoloty bezzałogowe wyposażane w kamery z podczerwienią oraz inne wyszukane cuda technologii prowadziły nadzór daleko w głąb terytorium wroga w czasie rzeczywistym bez potencjalnych strat w ludziach. Tak dalece zaawansowane urządzenia mogły dostarczać → i n f o r m a c j i [t. 2] dla artylerii na ziemi tak, jak dawni zwiadowcy i obserwatorzy z lornetkami w dłoni mogliby tylko zamarzyć. Wszystkie te wynalazki dostarczały o wiele więcej informacji dla artylerzysty niż kiedykolwiek w historii, zapewniając zwiększoną celność i zmniejszenie czasu reakcji.

Oznaczało to, że artyleria samobieżna nabrała nowego znaczenia.

Dotychczasowe holowane działa zyskały możliwość samodzielnego poruszania się, co pozwalało na dynamiczną zmianę lokalizacji zaraz po oddaniu strzału i uniknięcie w ten sposób kontrostrzału wroga. Do tego czasu artyleria zaadaptowała do swojego uzbrojenia rakiety, a we wczesnych latach 60. XX w. ciężka artyleria przeciwlotnicza została niemal całkowicie zastąpiona rakietami. Sprawiło to, że olbrzymie armaty odchodziły bezpowrotnie do przeszłości. Ich miejsce zajęły tzw. ICBM-y (od ang. *intrecontinental balistic missile*, międzykontynentalny pocisk balistyczny), zdolne do lotu z jednego końca globu na drugi, oraz taktyczne pociski balistyczne o zasięgu kilkuset kilometrów.

W środowisku współczesnego pola bitwy artyleria odgrywa dominującą rolę, zapewniając siłę ognia w starciu z udziałem mieszanego uzbrojenia. Należy jednak zaznaczyć, że w przeciwieństwie do dawnych trendów obecnie liczą się precyzyjne uderzenia o charakterze przeciwwagowym na arenie w strukturze sieciowej, inaczej niż w przypadku wykorzystania → b r o n i n u k l e a r n e j . Pole działań zostaje scharakteryzowane przez przejrzystość pola bitwy wymagającego wysokiego poziomu nieliniowości do zapewnienia jednoczesnego prowadzenia działań na poziomach taktycznym, operacyjnym i strategicznym. Artyleria zajmuje się nadzorem, wyznaczaniem celów, ostrzałem wybranych celów oraz szacowaniem wyrządzonych szkód, kształtuje pole bitwy tak, aby zapewnić przejrzystość teatru działań. Współczesne możliwości działania artylerii daleko wykraczają poza skalę, w jakiej wyobrażać sobie można było jej działania kilka wieków temu. Tylko od zamożności społeczeństw i państw, budżetów przeznaczonych na uzbrojenie oraz odpowiedzialności polityków zależy to, jakie środki zostaną przeznaczone na produkcję i zakup broni. Dotyczy to w znaczącym stopniu także artylerii.

Rozwój artylerii jest obecnie pochodną najnowocześniejszych technologii ery komputeryzacji i informatyzacji, które zrewolucjonizowały rozwój uzbrojenia i wiele innych elementów pola walki. W ciągu stuleci artyleria przebyła drogę od armat czarnoprochowych, dział, których ogniem kierował człowiek na koniu z lornetką polową,

określający kierunek wiatru za pomocą poślinionego palca, do dział ostrzeliwujących i trafiających cele bez bezpośredniego kontaktu wzrokowego amunicją samonaprowadzaną; od zabawnych petard do pocisków balistycznych zdolnych przelecieć 8 tys. km i rozdzielić się na oddzielne głowice bojowe lecące w kierunku wielu różnych wybranych celów; od dział przeciw balonom do automatycznych działek Gatlinga wyrzucających z siebie do 6 tys. sztuk 20-mm pocisków na minutę. Właściwym podsumowaniem przedstawionych innowacji w zakresie rozwoju artylerii mogą być słowa I. Hogga:

> „Co jeszcze wymyślą?" nie jest odpowiednim pytaniem, tylko „Co jeszcze mogą wymyślić?". Wydaje się, że ludzkość dotarła do momentu, w którym trudno wyobrazić sobie to, co już nie zostało wynalezione, a XXI wiek dopiero co się zaczął.
>
> *Jakub Idzik*

P.E. Chevedden, L. Eigenbrod, V. Foley, W. Soedel, *Trebuchet*, „Scientific American" 1995, Special Online Issue no. 1; *Field Artillery Cannon Weapons Systems and Ammunition Handbook*, Defense Technical Information Center, Oklahoma 1981; Ch.F. Foss, *Artillery of the World*, Ian Allan, London 1974; B.I. Gudmundsson, *On Artillery*, Praeger, Westport 1993; J. Idzik, *Broń elektromagnetyczna jako znaczący krok w rozwoju artylerii*, „Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate" 2019, nr 9 (2); tenże, *Ołowiany grad: rozwój i główne uwarunkowania działania artylerii w XX wieku*, „Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate" 2019, nr 9 (1); tenże, *Ołowiany grad: zarys historii rozwoju artylerii do czasów przednapoleońskich*, „Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate" 2018, nr 8; J. Kinard, *Artillery: An Illustrated History of Its Impact*, ABC-CLIO, Santa Barbara–Denver–Oxford 2007; A. Manucy, *Artillery Through the Ages: A Short Illustrated History of Cannon, Emphasizing Types Used in America*, National Park Service, Washington 1949; J.E. McKenney, *The Organizational History of Field Artillery 1775–2003*, Centre of Military History, United States Army, Washington 2007; K. Morton, *Artillery through the Ages: An Etymology*, „Lingua Frankly" 2014, vol. 2; R. Payne-Gallwey, *The Projectile Throwing Engines of the Ancients*, Longmans, Green & Co, London–New York–Bombay–Calcutta 1907; P.H. Stevens, *Artillery Through the Ages*, Franklin Watts, New York 1967; D. Stevenson, *The Field Artillery Revolution and the European Military Balance, 1890–1914*, „The International History Review" 2018, vol. 41 (6); D. Westwood, *Artillery*, [w:] *Ground Warfare: An International Encyclopedia*, S. Sandler (ed.), ABC-CLIO, Santa Barbara–Denver–Oxford 2002.

ASYMILACJA (z łac. *assimilatio*, upodobanie, zrównanie, od *similis*, podobny) – pojęcie to pojawiło się pierwszy raz w XVI w. w pracach biologicznych. W tym czasie oznaczało czynności związane z przyjmowaniem – wchłanianiem i przyswajaniem treści pokarmowych przez organizmy żywe. Dopiero wiek później terminu zaczęto używać jako oznaczenia „upodabniania", „czynienia podobnym". Dla socjologów pojęcie asymilacji w znaczeniu procesu społecznego upowszechniło się dopiero w 2. poł. XIX w. i związane jest od samego początku z pojęciem rasy oraz powiązań między mniejszością a większością. W Polsce przyjmuje się, że pierwszy raz termin ten został

użyty w 1818 r. przez W. Krasińskiego w wydanej przez niego broszurze antysemickiej zatytułowanej *Aperçu sur les Juifs de Pologne par un officier general polonois*. Jednak musiało upłynąć kolejne pół wieku, by termin ten trafił do użytku publicznego. W latach 20. XX w. pojęcie to w USA stosowano na określenie dołączania przybyłych imigrantów do społeczeństwa amerykańskiego. Asymilacja ma wiele definicji, które różnią się w zależności od dziedziny. W literaturze przedmiotu funkcjonuje wiele ujęć i typologii asymilacji.

Wyróżnia się 4 stopnie wstępowania imigrantów do społeczeństwa przyjmującego. W kolejności są to: separacja, adaptacja, integracja oraz asymilacja. Termin asymilacji oznacza złożony proces, który charakteryzuje częściowe lub całkowite scalanie elementów dwóch bądź większej liczby grup kulturowych, a także przyswojenie cech właściwych danej zbiorowości. Asymilację oznaczamy jako przyjmowanie przez inną narodowość języka i dominujących cech kulturowych, które charakteryzują określoną demograficznie i kulturowo zbiorowość. W konsekwencji doprowadza do utożsamiania się danej narodowości z ludnością, która tworzy dane państwo. Słownik języka polskiego wskazuje znaczenie asymilacji jako „przystosowanie się do życia w obcej grupie przez przejęcie jej kultury i przyswojenie sobie cech właściwych tej grupie; też: wchłonięcie obcej grupy". O asymilacji mowa jest najczęściej, kiedy imigranci dostosowują się do zasad współżycia społecznego w państwie, w którym zamieszkali, albo w kontekście przystosowania członków mniejszości narodowych do zasad, którym kieruje się dane społeczeństwo, naród, stanowiące większość w danym kraju lub regionie. Asymilację obrazowo definiuje G. Babiński, określając ją jako „zmniejszanie się zróżnicowania".

Kolejną definicję przedstawia T. Paleczny – socjolog kultury, narodu i stosunków etnicznych. Jest on zdania, że:

> asymilacja polega na integracji różnorodnych społecznie i kulturowo, odmiennych rasowo i religijnie, odrębnych etnicznie i narodowo grup kulturowych, ich mieszaniu się, tworzeniu uniwersalnych, wspólnych dla wszystkich uczestników kodów komunikacyjnych, symboli i norm. Asymilacja obejmuje różnorodne zjawiska, w tym unifikacji i uniwersalizacji językowej, synkretyzacji religijnej i hybrydyzacji rasowej, etnicznej, prowadząc do wyłaniania i utrwalania nowych, transkulturowych rodzajów tożsamości.

Dalej Paleczny pojęciem tym określa proces „zachodzący w następstwie impaktu kulturowego i dyfuzji dwóch lub większej liczby grup o różnych kulturach i pochodzeniu etnicznym".

Natomiast Hieronim Kubiak, socjolog, definiuje asymilację jako:

> syndrom procesów zachodzących w kraju imigracyjnym, w wyniku którego jednostki i grupy pochodzące z odmiennych narodów oraz państw zostają przetworzone i wchłonięte przez ten kraj.

Asymilację określa dalej jako sytuację społeczną. Powiązana jest ona wg niego z procesem reakcji następujących w wyniku zderzenia się na jednym terytorium 2 lub więcej zbiorowości społecznych. Szczególnie zmiany te można zauważyć w dziedzinie społecznej, kulturalnej i osobowości. Kubiak podkreśla, że proces asymilacyjny dotyczy imigrantów zarówno pochodzących z ukształtowanych narodów, jak i tych, którzy wywodzą się z narodów dopiero się kształtujących lub też imigrantów powiązanych z grupami etnicznymi. Wszystkie asymilowane osoby przechodzą charakterystyczne dla tego procesu fazy. Według Kubiaka początkowo związane są one z umacnianiem bądź kształtowaniem przynależności do grupy narodowej lub etnicznej, z której pochodzą. Jego zdaniem dopiero w późniejszym czasie następuje identyfikowanie się z państwem, w którym się osiedliły.

W 1994 r. E. Morawska wyróżniła 3 etapy procesu asymilacji:

- nawiązanie relacji społecznych z osobami należącymi do grupy dominującej;
- zanik grupowej identyfikacji etnicznej;
- zanik indywidualnej lub subiektywnej identyfikacji etnicznej.

Negatywny wpływ na występowanie tych etapów wywrzeć mogą bariery językowe, zakazy religijne, uprzedzenia. Inne czynniki to wysoka liczba nowo przybyłych imigrantów i pielęgnowanie ich dotychczasowej kultury w różnego rodzaju organizacjach. Wskazuje się, że największe trudności z asymilacją przedstawiają najczęściej pierwsze pokolenia imigrantów, które muszą stawić czoła zupełnie innej niż do tej pory rzeczywistości. Przyjmuje się, że im większa jest odległość geograficzna i dystans kulturowy, tym asymilacja kulturowa może być dłuższym i trudniejszym procesem.

Wskazuje się, że asymilacja przebiega na 2 obszarach – społecznym i psychicznym. Oznacza to, że dostosowanie osoby zasymilowanej jest pełne i zawiera w sobie także zmianę sposobu myślenia i wartościowania. Asymilacja związana jest z asymetrią między członkami asymilowanej mniejszości a asymilującą większością. Zachodzi tutaj zjawisko pełnego identyfikowania się z kulturą dominującą. Następuje też porzucenie dotychczasowych, starych wzorców kulturowych i przyjęcie wartości, norm przedstawianych przez nowo przyjętą kulturę i społeczeństwo zamieszkujące dany region.

Kubiak dzieli asymilację na państwową oraz narodową. Pierwszą z nich upatruje w więzi obywatelstwa, natomiast asymilację narodową określa jako proces o wiele dłuższy, ale i trudniejszy niż asymilacja państwowa. Asymilacja narodowa wiąże się z zaadaptowaniem i identyfikowaniem jednostki lub grupy mniejszości z obcą dla siebie wspólnotą narodową.

Kolejną kwestią związaną z opisywanym zagadnieniem jest teoria asymilacji. Przyjęte przez Kubiaka założenia, że każda grupa imigrująca ma swoje poglądy, ale też każde państwo przyjmujące cechuje zbiór przestrzeganych zasad, prowadzą do wyodrębnienia 3 rodzajów ideologii asymilacyjnych. Pierwsza z nich – ideologia asymilujących państw czy narodów – sprowadza się do twierdzenia, iż państwo jest

najodpowiedniejszą instytucją do kierowania procesem asymilacyjnym. Jej głównym celem jest włączenie imigrantów w sposób umożliwiający pozostanie przy obecnie obowiązujących strukturach polityczno-kulturowych, bez wprowadzania większych zmian. Kolejna teoria to ideologia typowa dla asymilujących społeczeństw politycznych. Wiąże się z państwami przyjmującymi, które nie mają całkowicie uformowanej kultury odznaczającej dany naród. W konsekwencji wspomniane kraje nie mogą żądać od imigrantów lojalności implikowanej w pierwszej teorii, a jedynie oczekują znajomości języka i poszanowania państwa, do którego przybyli. Trzecia i ostatnia ideologia związana jest z nadziejami, dążeniami i niepokojami asymilowanych.

Proces asymilacji może zostać przeprowadzony dobrowolnie, niezależnie lub też pod przymusem, zgodnie z prowadzoną przez państwo polityką. Nacisk w tym wypadku oznacza narzucenie wartości, kultury i norm ludności dominującej. Należy pamiętać, że asymilacja dokonywana pod przymusem (w wyniku podboju, → a n e k s j i , dominacji kolonialnej) skutkuje w dużej części przypadków separacją i uwidaczniającą się odrębnością kulturową. Proces asymilacji nie zawsze toczy się pokojowo, niejednokrotnie zdarzają się antagonizmy oraz natrafia się na problemy o zabarwieniu ekonomicznym, ideologicznym, kulturowym, politycznym. Kubiak wyróżnił 5 głównych rodzajów asymilacji:

- przymusową,
- dobrowolną,
- kierowaną,
- narodową,
- państwową.

Paleczny podkreśla za M. Gordonem, amerykańskim socjologiem:

> w klasycznym ujęciu asymilacja jest złożonym, wielopoziomowym i wielowymiarowym, długim, międzypokoleniowym procesem łączenia, spajania i wyłaniania nowego transkulturowego, złożonego, wielokulturowego społeczeństwa obywatelskiego.

Asymilację jako proces wielokierunkowy podobnie definiuje M. Kula – polski historyk zajmujący się historią społeczną. Przekonuje on, że:

> proces asymilacji jest klasycznym procesem wieloczynnikowym i jako taki należy go analizować – nawet jeśli do celów poznawczych wyodrębnia się poszczególne czynniki i bada się kolejno oddziaływanie każdego z nich.

W. Warner i L. Srole w 1945 r. stworzyli koncepcję asymilacji linearnej. Według niej na upodobnienie imigrantów do ludności przyjmującej duży wpływ ma wydłużający się okres zamieszkiwania wśród danej społeczności. Proces asymilacji wzmacniany jest z pokolenia na pokolenie, kultura kraju pochodzenia z biegiem czasu zaczyna mieć coraz mniejsze znaczenie. Imigranci upodabniają swoje zachowania i zaczynają przestrzegać podobnych norm jak ludność przyjmująca.

Gordon do wskazanej problematyki podszedł bardziej wielowymiarowo. W 1964 r. wyznaczył 7 etapów asymilacji, mianowicie:

- kulturowy (akulturację),
- strukturalny,
- amalgamacyjny,
- identyfikacyjny,
- osobowościowy,
- behawioralny,
- obywatelski.

Podkreślił, że najważniejszą rolę odgrywa asymilacja kulturowa i strukturalna. Pierwsza z nich łączy się z wyzbyciem elementów własnej kultury oraz przyjęciem wzorców społeczności przyjmującej. Natomiast asymilacja strukturalna związana jest z uczestnictwem imigrantów w poszczególnych elementach charakteryzujących społeczeństwo przyjmujące (np. kluby towarzyskie). Asymilacja wg Gordona rozpoczyna się od wymiaru kulturowego i może zostać zaprzestana na tym etapie, jeśli jednak osiągnie poziom strukturalny, to w odpowiednim czasie uwidocznią się także pozostałe formy asymilacji.

Asymilację związaną z przystosowywaniem się do nowej wspólnoty można podzielić na 3 strefy: strukturalną, kulturową oraz osobowościową. Najczęściej odbywają się one z biegiem lat – obejmują kilka pokoleń. Autorem tego podziału jest Kubiak, a opracowując go, opierał się na założeniach Gordona. Tego typu podział występuje zawsze – bez względu na przyczyny, przebieg, ilość, różnorodność grup i ludzi.

Pierwsza z nich – asymilacja strukturalna – wiąże się z przenikaniem członków grupy asymilowanej do kręgów społecznych, politycznych, gospodarczych itp. wspólnoty dominującej. Znacząca w tym względzie jest adaptacja do panującego prawa oraz zajęcie miejsca w odpowiedniej klasie i warstwie społecznej.

Drugi etap stanowi asymilacja kulturowa lub akulturacja – inaczej określane jako nabywanie przez jednostkę bądź grupę, która stanowi mniejszość, reguł zachowań grupy dominującej. Asymilacja kulturowa związana jest z amalgamacją, czyli mieszaniem się grup rasowych, etnicznych bądź wyznaniowych (np. poprzez zawieranie małżeństw). Łączy się także z przyjęciem wartości, języka i religii dominujących. Akulturacja występuje w pełni, kiedy językiem macierzystym dla imigranta staje się język społeczeństwa przyjmującego. Wielokrotnie można spotkać się w tym przypadku z dwujęzycznością czy też dwukulturowością, jednak z podkreśleniem większego znaczenia nowo nabytej tożsamości. Akulturacja następuje zazwyczaj w drugim pokoleniu migrantów.

Trzeci etap to asymilacja osobowościowa – związana z tożsamością jednostek. Migrant umacnia poczucie przynależności do obecnej grupy dominującej i wyzbywa się poczucia członkostwa w poprzedniej wspólnocie. Z tym etapem łączy się również asymilacja behawioralna (związana z dopasowywaniem wzorców zachowań

występujących w społeczeństwie przyjmującym), symboliczna i identyfikacyjna. Taki stan otrzymywany może być dopiero w 3. pokoleniu imigrantów bądź później.

Na etap pośredni między asymilacja kulturową a strukturalną wskazywał już w 1985 r. D. Massey. Określił ją mianem asymilacji przestrzennej, która powiązana została z miejscem zamieszkania. Zauważył, że zasymilowane osoby, które przybyły do Ameryki i ugruntowały swoją pozycję na rynku pracy, nierzadko podejmowały się zmian miejsca zamieszkania. Opuszczały one dzielnice, w których sąsiadowały z członkami swojej dotychczasowej grupy, osiedlały się najczęściej wśród ludności rasy białej należącej do klasy średniej. Sprawiało to, że imigranci poprzez uczestnictwo w różnego rodzaju strukturach w coraz większym stopniu asymilowali się ze społeczeństwem amerykańskim. Przykład ten pokazuje również, że w ówczesnych czasach w Ameryce za grupę dominującą uważano jedynie ludność rasy białej należącą do klasy średniej.

Asymilacja skutkuje ciągłymi zmianami rozkładu grup biorących udział w oddziaływaniach kulturowych, czego efektem jest powstawanie nowych konfiguracji wartości i harmonii. Inaczej mówiąc, proces asymilacji doprowadza do pojawienia się nowego systemu społecznego i kulturalnego.

W Polsce i Europie największa skala asymilacji związana była z integracją mniejszości narodowych i etnicznych z rdzennymi mieszkańcami. Wywołana była przede wszystkim przez zmiany terytorialne, ustrojowe, konflikty etniczne, akceptację międzynarodowych reguł prawa dotyczącego mniejszości narodowych oraz wzrastające wsłuchiwanie się w potrzeby mniejszości narodowych przez państwa.

Paulina Rus

Asymilacja, Sjp.pwn.pl (dostęp 8.12.2019); *Asymilacja*, MFiles.pl (dostęp 15.01.2020); *Asymilacja*, Wsjp.pl (dostęp 8.12.2019); M. Budyta-Budzyńska, *Adaptacja, integracja, asymilacja – próba ujęcia teoretycznego*, [w:] *Integracja czy asymilacja? Polscy imigranci na Islandii*, M. Budyta-Budzyńska (red.), Wydawnictwo Naukowe Scholar, Warszawa 2011; D. Grzybek, *Współczesne rozumienie asymilacji imigrantów w społeczeństwie amerykańskim*, „Zeszyty Naukowe Towarzystwa Doktorantów UJ. Nauki Społeczne" 2013, nr 6 (1); H. Kubiak, *Asymilacja etniczna w płaszczyźnie struktury społecznej*, [w:] *Założenia teorii asymilacji*, H. Kubiak, A.K. Paluch (red.), Zakład Narodowy im. Ossolińskich, Wrocław 1980; M. Kula, *Kilka uwag o asymilacji w świetle doświadczeń latynoamerykańskich*, [w:] *Założenia teorii asymilacji*, H. Kubiak, A.K. Paluch (red.), Zakład Narodowy im. Ossolińskich, Wrocław 1980; T. Paleczny, *Charakterystyka mniejszości etnicznych a procesy integracji narodowej w krajach Ameryki Łacińskiej*, „Przegląd Polonijny" 1997, z. 4 (86); tenże, *Procesy asymilacji, transkulturacji i uniwersalizacji kulturowej: przegląd problematyki*, „Krakowskie Studia Międzynarodowe" 2017, nr 3 (XIV); A. Popielarczyk-Pałęga, *Tożsamość narodowa, tożsamość etniczna, identyfikacja narodowa jednostki – rozważania metodologiczne na przykładzie środowisk polonijnych*, „Łódzkie Studia Teologiczne" 2018, t. 27, nr 3.

ATAK DDOS (*Distributed Denial of Service*, „rozproszona odmowa dostępu do usługi") – jedna z najczęściej stosowanych form ataku hakerskiego o charakterze wolumetrycznym, skierowana przeciwko przepustowości i stabilności systemów

komputerowych lub usług realizowanych za pośrednictwem sieci. Jej celem jest zakłócenie, spowolnienie lub zablokowanie funkcjonowania usługi przez jednoczesne wysłanie zapytań z wielu jednostek, generujące nienormatywny ruch sieciowy (tzw. zalewanie, z ang. *flooding*). Nadmierna liczba jednoczesnych zapytań może skutkować przeciążeniem zasobów sieciowych, w tym zużyciem dostępnych zasobów obliczeniowych, a w konsekwencji ich sparaliżowaniem i odmową dostępu dla uprawnionych użytkowników. Pożądanym skutkiem ataku typu DDoS jest przerwanie ciągłości działania celu ataku, a przez to jego czasowa niedostępność. Jak wskazuje Igor Protasowicki, „ataki tego typu wykorzystują słabość architektury TCP / IP oraz serwerów DNS umożliwiającą przeciążenie zasobów systemowych sztucznie wygenerowanym ruchem sieciowym". Jedną z form ataku DDoS jest technika SYNFlooding, w ramach której systemy napastnika wysyłają znaczną liczbę pakietów z zapytaniem, jednocześnie ignorując odpowiedź serwera. Według statystyk prezentowanych przez Microsoft ataki wymierzone w protokoły TCP / IP stanowiły zdecydowaną większość (63%) przeprowadzonych w 2022 r. ataków typu DDoS, które były wymierzone w infrastrukturę tej firmy.

Atak w formie odmowy dostępu do usługi (DoS) jest kwalifikowany jako atak „rozproszony", gdy ruch skutkujący przeciążeniem zasobów sieciowych jest generowany z więcej niż jednego źródła (współdziałanie wielu urządzeń). Rozproszenie ataku zapewnia większą anonimowość napastnikowi, co utrudnia lub uniemożliwia późniejszą atrybucję. Podstawowym założeniem z punktu widzenia atakującego jest doprowadzenie do sytuacji, w której przepustowość urządzeń zostaje przekroczona. Wówczas każde kolejne połączenie zostanie odrzucone lub zakończy się niepowodzeniem. Zwiększanie liczby urządzeń wysyłających jednoczesne zapytania zwiększa tym samym efektywność ataku, a jednocześnie utrudnia skuteczne przeciwdziałanie.

Przeprowadzenie ataku typu DDoS wymaga zatem masowości zapytań i ich odpowiedniego skoordynowania. Do tego typu działań często wykorzystywane są → b o t n e t y [t. 1] (grupy zainfekowanych urządzeń z dostępem do internetu), które pozwalają na wysłanie setek tysięcy jednoczesnych zapytań do atakowanego łącza, systemu, serwera, sieci lub usługi, co powoduje czasowe lub trwałe przeciążenie zasobów sieciowych. Ataki z użyciem sieci komputerów pozwalają ominąć ograniczenia w postaci braku odpowiedniej liczby urządzeń zdolnych do wysłania jednoczesnego zapytania znajdujących się w fizycznym posiadaniu atakującego. Wykorzystanie botnetu jest zazwyczaj poprzedzone zainfekowaniem tysięcy urządzeń (tzw. urządzenia zombie, nad którymi przejęto zdalną kontrolę), które następnie zostają podporządkowane osobie bądź grupie odpowiadającej za atak. Wraz z upowszechnieniem urządzeń IoT (Internet of Things), bardziej podatnych na zainfekowanie, tworzenie botnetu stało się łatwiejsze, a wykrywanie przejęcia kontroli nad urządzeniami – trudniejsze.

Niektórzy autorzy podnoszą, że ataki DDoS są jednymi z najprostszych do wykonania, co jednak nie w pełni oddaje przebieg całości procesu od zainfekowania

urządzeń, stworzenia botnetu, jednoczesnego wykorzystania urządzeń, do zablokowania zasobów sieciowych. Prymitywnym atakom przeciążeniowym towarzyszą także bardziej skomplikowane ataki wielowektorowe, które odznaczają się większą wszechstronnością i bazują na wykorzystywaniu luk w konfiguracji serwerów i usług. Należy także podkreślić, że wraz z wyspecjalizowaniem się grup hakerskich (np. prorosyjskiej grupy Killnet, odpowiedzialnej głównie za ataki typu DDoS), dostępnością już stworzonych botnetów oraz powszechnością szkodliwego oprogramowania zdolnego do wygenerowania masowej liczby zapytań (tego typu narzędzia są dostępne w internecie za niewielką opłatą i pozwalają na daleko idące działania ofensywne) ataki DDoS mają potencjał do dalszego zwiększania zasięgu oddziaływania i stanowią jedno z największych wyzwań w dziedzinie → c y b e r b e z p i e c z e ń s t w a [t. 1].

Oprócz osiągnięcia głównego celu w postaci (częściowej) odmowy dostępu do usługi ataki typu DDoS mogą skutkować naruszeniem integralności i poufności danych, a w niektórych wypadkach generować → r y z y k o utraty danych. Mogą mieć także wymiar ekonomiczny, gdy służą szantażowi i wyłudzeniom. Wówczas cyberprzestępcy przeprowadzają atak typu DDoS w skali pełnej lub ograniczonej, by pokazać swoje możliwości i uwiarygodnić zagrożenie. Następnie żądają okupu, który jest warunkiem koniecznym do odblokowania przepustowości. Pod tym względem ataki typu DDoS mogą przypominać ataki z wykorzystaniem → r a n s o m w a r e bądź też łączyć się z innymi formami szkodliwej działalności w → c y b e r p r z e s t r z e n i [t. 1]. Ataki typu DDoS są także z powodzeniem wykorzystywane jako zasłona dymna. Zaangażowanie zasobów ludzkich i technologicznych do odparcia ataku oraz towarzyszący temu chaos mogą bowiem skutecznie odwracać uwagę od innych celów osiąganych równolegle przez atakującego.

Przebieg ataków typu DDoS różni się w zależności od formy, celu i czasu ataku. Obecnie zdecydowana większość ataków typu DDoS trwa krócej niż godzinę, a często na atak składa się seria pomniejszych kilkudziesięciosekundowych uderzeń, umożliwiających redukcję wykorzystywanych zasobów oraz rozłożenie konsekwencji ataku w czasie. Warto jednak podkreślić – co ma związek z intensywnością działań, motywacją atakującego oraz możliwościami defensywnymi zaatakowanego podmiotu – że niektóre ataki typu DDoS mogą trwać nawet kilkanaście dni i doprowadzić do długotrwałego paraliżu usług.

Do pierwszych ataków typu DDoS – choć w formie innej niż znane współcześnie – doszło w połowie lat 90. XX w. Były wówczas wykorzystywane jako forma społecznego strajku, sieciowej manifestacji niezadowolenia. W 1995 r. jedną z pierwszych tego typu prób podjęła grupa włoskich aktywistów, którzy przez zaangażowanie użytkowników liczyli na wygenerowanie nienormatywnego ruchu na francuskich stronach rządowych. Podobną → s t r a t e g i ę [t. 5] wykorzystywali meksykańscy zapatyści. W kolejnych latach ataki typu DDoS były coraz lepiej koordynowane i opierały się na wykorzystaniu nie masowego zaangażowania społecznego, a odpowiedniego

oprogramowania generującego ruch przeciążający. W 2010 r. grupa Anonymous dokonała udanych ataków na systemy PayPal, Visa i MasterCard w odpowiedzi na odmowę przyjmowania wpłat na rzecz szefa WikiLeaks. Motywacja ataków typu DDoS ewoluowała od działań społecznych (forma protestu) w kierunku działań o charakterze *stricte* przestępczym lub politycznym.

Według statystyk prowadzonych przez odpowiedzialne za cyberbezpieczeństwo agencje międzyrządowe i narodowe liczba ataków typu DDoS wzrastała w ostatniej dekadzie nawet o kilkaset procent rocznie, choć okresowo notowane są także spadki, które należy łączyć ze zmianami strategii działania cyberprzestępców i aktywnością agencji przeciwdziałających → c y b e r p r z e s t ę p c z o ś c i [t. 1]. W latach 2021–2022 FBI i → E u r o p o l [t. 2] rozbiły znaczną liczbę botnetów, co pozwoliło na zamknięcie części usług *DDoS-to-hire* (płatnego „wynajęcia" botnetu do przeprowadzania ataków).

Wobec coraz częstszego wykorzystywania ataków typu DDoS do wywierania presji politycznej zyskują one nowy wymiar. Wiąże się to z aktywnością aktorów państwowych lub finansowanych przez państwa (*state sponsored actors*) oraz tzw. haktywistów, którzy przez ataki hakerskie komunikują swój sprzeciw i poglądy polityczne. Rosyjska → a g r e s j a [t. 1] przeciwko Ukrainie przyczyniła się do wzmożenia motywowanych politycznie działań grup przestępczych w cyberprzestrzeni. Systemy teleinformatyczne Ukrainy i wspierających ją krajów (np. Polski, krajów bałtyckich, nordyckich, częściowo także Niemiec) stały się jednym z głównychcelów ataków prorosyjskich grup hakerskich. W związku z rosnącym zagrożeniem → c y b e r a t a k a m i [t. 1] Rzeczpospolita Polska wprowadziła stopień alarmowy CHARLIE-CRP, aktywność zwiększyły także zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT). Celem ataków, które zostały częściowo przeprowadzone z terytorium Federacji Rosyjskiej, stały się m.in. strony internetowe Senatu RP.

Wśród przeprowadzonych w ostatnich latach ataków typu DDoS motywowanych politycznie wskazać należy uderzenie w tajwańskie strony internetowe w związku z wizytą spikerki Izby Reprezentantów Stanów Zjednoczonych Nancy Pelosi w sierpniu 2022 r. W ich wyniku wyłączone zostały m.in. serwisy tajwańskiego Ministerstwa Obrony i Ministerstwa Spraw Zagranicznych. W 2023 r. zanotowano serię ataków typu DDoS na strony internetowe niemieckich lotnisk, co powszechnie wiązano z aktywnością prorosyjskich grup hakerskich. Celem ataku stały się podmioty wchodzące w skład → i n f r a s t r u k t u r y k r y t y c z n e j [t. 2] w Polsce, Estonii, Finlandii czy Stanach Zjednoczonych. Ataki typu DDoS wymierzono również w infrastrukturę firm prywatnych: w 2022 r. potężny atak przypuszczono na Google Cloud, celem → h a k e r ó w [t. 2] stały się choćby polskie oddziały Orange.

Ataki typu DDoS mają charakter wysoce szkodliwy. Współcześnie są jednym z największych zagrożeń dla spójności i stabilności funkcjonowania systemów komputerowych i usług sieciowych, a przez to jednym z najczęściej wykorzystywanych przez

hakerów rozwiązań. Szczególne niebezpieczeństwa wiążą się z atakami typu DDoS na elementy infrastruktury krytycznej oraz systemy teleinformatyczne, od których zależy stabilność funkcjonowania państwa i społeczeństwa. Wśród nich wymienić należy systemy: bankowe, służby zdrowia, administracji publicznej, zawiadujące logistyką.

Czasowe uniemożliwienie korzystania z systemów sieci i usług może prowadzić do sparaliżowania działania określonych podmiotów publicznych i niepublicznych. Skutkami wyłączenia niektórych usług mogą być: 1) wywołanie chaosu i niepokojów społecznych w związku z uniemożliwieniem działania istotnych z punktu widzenia gospodarki bądź relacji społecznych systemów teleinformatycznych; 2) narażenie zaatakowanych podmiotów na znaczne straty finansowe związane z niedostępnością ich usług; 3) straty wizerunkowe związane z niedostępnością usług dla odbiorców, a co za tym idzie – osłabienie pozycji rynkowej podmiotów prowadzących działalność biznesową; 4) obnażenie słabości cyberzabezpieczeń i spadek zaufania do zdolności zapewniania stabilności i integralności zaatakowanych systemów, sieci lub usług; 5) strach społeczeństwa i niechęć do korzystania z systemów i usług narażonych na cyberataki; 6) zastraszanie społeczeństwa, klasy politycznej, dostawców usług, skutkujące naciskami i decyzjami w sferze politycznej; 7) skutki prawne na gruncie prawa karnego i cywilnego, jak również w przestrzeni międzynarodowej, szczególnie w wypadku zaangażowania aktorów państwowych lub quasi-państwowych.

Bezpieczeństwo systemów teleinformatycznych oraz ciągłość dostępu do danych i usług są współcześnie jednymi z kluczowych kryteriów efektywnego funkcjonowania podmiotów państwowych i niepaństwowych. Wśród technik zapobiegania atakom typu DDoS wskazuje się m.in. zwiększanie przepustowości sieci; chronienie usług w chmurze przez wykorzystywanie zasobów zewnętrznych; segmentację sieci; równoważenie obciążeń; wykrywanie i odróżnianie anomalii; klasyfikowanie ruchu przychodzącego; odrzucanie złośliwego ruchu, w tym blokowanie określonych adresów IP. Podmioty powinny dysponować odpowiednimi strategiami na wypadek ataku oraz odpowiednim poziomem koordynacji z wyspecjalizowanymi jednostkami przeciwdziałającymi cyberprzestępczości.

Mateusz Łabuz

Azure Network Security Team, *2022 in Review: DDoS Attack Trends and Insights*, 21.02.2023, https://www.microsoft.com/en-us/security/blog/2023/02/21/2022-inreview-ddos-attack-trends-and-insights/ (dostęp 27.03.2023); C. Douligeris i in., *Rozproszona odmowa usługi. Krajobraz zagrożeń wg Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA)*, ENISA, 2020; G. Coleman, *Anonymous in Context: The Politics and Power behind the Mask*, „Internet Governance Papers" 2013, no. 3; Cybersecurity and Infrastructure Security Agency, *Understanding and Responding to Distributed Denial-of-Service Attacks*, MS-ISAC, 2022; *Dobre praktyki w zakresie przeciwdziałania atakom DDoS*, KNF CSIRT, Warszawa 2022; F.J. Ennemoser, P. Sattler, J. Zirngibl, *State of the Art of DDoS Mitigation Techniques*, Seminar IITM WS 21/22, Network Architectures and Services, 2022; B.B. Gupta, A. Dahiya, *Distributed Denial of Service (DDoS) Attacks. Classification, Attacks, Challenges and Countermeasures*, CRC Press, Boca Raton FL 2021; Health-ISAC, *Distributed Denial of Service (DDoS) Attacks*, 2021; J.-P. Jung,

Anpassungsfähig und komplex – DDoS-Angriffe und ihre Metamorphose, 21.03.2023, Tagesspiegel Background Cybersecurity, https://background.tagesspiegel.de/cybersecurity/ anpassungsfaehig-und-komplex-ddos-]angriffe-und-ihre-metamorphose (dostęp 26.03.2023); R. Lemos, *How DDoS Attacks Techniques Have Evolved Over Past 20 Years*, 17.03.2018, https://www.eweek.com/security/how-ddos-attacks-techniques-have-evolved-over-past-20-years (dostęp 27.03.2023); J. Ohlig, *Denial of Service – ein Dauerbrenner unter den Cyberangriffen*, 14.04.2022, Tagesspiegel Background Cybersecurity, https://background.tagesspiegel.de/cybersecurity/denial-of-service-ein-dauerbrenner-unter-den-cyberangriffen (dostęp 26.03.2023); A.E. Patkowski, *Cyber Defence – rozproszona obrona przed atakami DDoS*, „Biuletyn Instytutu Automatyki i Robotyki" 2011, nr 31; N. Pohlmann, *Cyber-Sicherheit.Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung*, Springer Vieweg, Wiesbaden 2019; I. Protasowicki, *Wpływ zagrożenia atakami DOS/DDOS na bezpieczeństwo teleinformatycznej infrastruktury krytycznej*, „Modern Management Review" 2018, t. 23, nr 25(1).

ATAK INFORMACYJNY – (ang. *information attack*) aktywne działanie będące elementem → w a l k i i n f o r m a c y j n e j [t. 4]; ofensywne działanie informacyjne. W dokumencie *Podstawy wojny informacyjnej* (oryg. *Cornerstones of Information Warfare*) opracowanym przez Siły Powietrzne USA (United States Air Force), atak informacyjny definiowany jest wąsko jako bezpośrednie uszkodzenie (naruszenie) → i n f o r m a c j i [t. 2], bez widocznych zmian w fizycznym nośniku danej informacji. W samej idei ataku informacyjnego informacja traktowana jest zarówno jako odrębna broń, jak i możliwy do obrania cel ataku. Wszelkie narzędzia, technologie i metody informacyjne wykorzystywane podczas ataku informacyjnego, a szerzej podczas → w o j n y i n f o r m a c y j n e j [t. 4], nazywane są bronią informacyjną. Wynikiem ataku informacyjnego jest zakłócenie → p r o c e s ó w i n f o r m a c y j n y c h [t. 3] (takich jak m.in. generowanie, gromadzenie, przechowywanie, transmisja, transformacja, udostępnianie, interpretacja i wykorzystywanie informacji).

Sam termin ataku informacyjnego jest wykorzystywany w literaturze przedmiotu stosunkowo rzadko i odnoszony jest zazwyczaj do ogólnych → z a g r o ż e ń [t. 4] dla → b e z p i e c z e ń s t w a i n f o r m a c y j n e g o (np. państwa). Zdecydowanie częściej teoretycy i praktycy stosują nazwy konkretnych ataków, które mogą być zebrane pod wspólną nazwą ataków informacyjnych. Należy go zatem ujmować jako szeroki znaczeniowo termin, wykorzystywany do określenia celowych działań naruszających bezpieczeństwo informacyjne. Właśnie ta celowość działań wyodrębnia atak informacyjny z grupy wszystkich zagrożeń dla bezpieczeństwa informacyjnego, które mogą obejmować również działania przypadkowe/ nieświadome, np. związane z brakiem wiedzy osób pracujących z systemem informacji, awarie oprogramowania i sprzętu oraz → k a t a s t r o f y n a t u r a l n e [t. 2]. Działania w ramach ataku informacyjnego można zebrać w 2 głównych grupach działań:

- działania mające na celu „ukrycie" prawdziwej informacji lub uniemożliwienie do niej dostępu;
- działania wprowadzające nieprawdziwą informację.

W literaturze przedmiotu można także zidentyfikować koncepcje utożsamiające atak informacyjny z walką informacyjną lub traktujące atak informacyjny jako jeden z obszarów walki informacyjnej. W ujęciach, wg których atak informacyjny jest jednym z obszarów walki informacyjnej, walka ta dzielona jest zazwyczaj na → walkę elektroniczną [t. 4] (ang. *electronic warfare*), → operacje psychologiczne [t. 3] (ang. *psychological operations*), → oszustwa wojskowe [t. 3] (ang. *military deception*), środki → bezpieczeństwa (ang. *security measures*), ataki fizyczne na procesy informacyjne (ang. *physical attack on information processes*), ataki informacyjne na procesy informacyjne (ang. *information attack on information processes*) rozumiane wąsko, czyli jako niszczenie/naruszanie informacji bez uszkadzania fizycznego nośnika informacji, np. poprzez wykorzystywanie → złośliwego oprogramowania komputerowego [t. 4], do którego zaliczamy m.in. wirusy, bomby logiczne, oprogramowanie szpiegujące.

W szerokim znaczeniu, praktycznie utożsamiającym atak informacyjny z walką informacyjną, atak ten może przyjąć formę ataku informatycznego, ataku elektronicznego (walki elektronicznej), ataku ogniowego (niszczenia fizycznego), działań psychologicznych lub działań dezinformacyjnych. Atak informatyczny obejmuje działania w sferze przetwarzania danych cyfrowych w celu uszkodzenia lub zmodyfikowania zasobów konkretnego systemu komputerowego albo sieci komputerowej. Atak informatyczny może spowodować m.in. uniemożliwienie użycia systemu komputerowego lub generowanie fałszywych danych. Atak elektroniczny uwzględnia natomiast atak laserowy bądź atak elektromagnetyczny i powoduje zakłócenie działania lub uszkodzenie systemów radioelektronicznych. W ataku ogniowym wykorzystuje się broń fizycznie niszczącą system informacyjny (np. poprzez uszkodzenie stacji przekaźnikowej albo linii komunikacyjnej). Atak psychologiczny polega na przekazywaniu informacji, która ma wywrzeć określony wpływ na percepcję, przetwarzanie informacji i procesy decyzyjne odbiorców. Oddziaływanie informacyjne może być realizowane za pomocą materiałów drukowanych (np. ulotek i prasy), radia, telewizji i internetu. Działania dezinformacyjne dotyczą natomiast wprowadzania przeciwników w błąd co do zamierzeń, planów i działań poprzez rozpowszechnianie fałszywych informacji. Fałszywe informacje mogą być przekazywane ustnie lub pisemnie, rozpowszechniane poprzez fałszywe dokumenty bądź przygotowanie działań pozorujących.

W praktycznym ujęciu atak informacyjny może obejmować m.in. manipulowanie informacją, naruszenia bezpieczeństwa informacji (związane z naruszeniem poufności, dostępności i integralności danych i informacji, np. nieautoryzowany dostęp do informacji, niszczenie lub modyfikowanie informacji, wprowadzanie fałszywych informacji, wyciek informacji, blokowanie dostępu do informacji osobom uprawnionym), niszczenie oprogramowania, zablokowanie przepływów informacji. Sposoby ataków

informacyjnych mogą zostać również podzielone wg celu ataku (tab. 1) – celem ataku mogą być kanały komunikacji oraz dane, informacje i wiedza, które za pomocą kanałów komunikacji są przekazywane i przetwarzane (dane przetwarzane w informację, a informacje w wiedzę).

Tab. 1. Przykłady sposobów ataków informacyjnych wg piramidy dane – informacje – wiedza

Cel ataku informacyjnego		Sposoby ataku informacyjnego	
Kanały komunikacji	Dane (surowe dane)	Zmiana, zniszczenie, zablokowanie dostępu	Zakłócenia w kanałach komunikacji
	Informacje (dane przetworzone, w odpowiednim kontekście)	Ograniczenie/modyfikacja procesów informacyjnych	
	Wiedza (informacje przetworzone i wykorzystywane przez człowieka)	Zmiany w postrzeganiu informacji, zmiana kontekstu	

Źródło: oprac. własne na podstawie W. Hutchinson, *Information Warfare and Deception*, „Informing Science" 2006, vol. 9.

Na skutek ataku informacyjnego może dojść m.in. do uszkodzenia → infrastruktury krytycznej [t. 2] państwa, a także zaburzenia funkcjonowania sił zbrojnych, → policji [t. 3] i służb specjalnych. Celem ataków informacyjnych mogą być systemy informacyjne (np. bazy danych), m.in. instytucji państwowych i organów władzy, instytucji wojskowych, finansowych, podmiotów realizujących zadania publiczne i mediów publicznych. Atak informacyjny skutkuje naruszeniami/zakłóceniami procesów informacyjnych i samej informacji, które wpływają na procesy decyzyjne i świadomość sytuacji u ludzi. Takie generowane zakłócenia mają wpływ na procesy poznawcze człowieka (m.in. przetwarzanie informacji, ustalanie priorytetów i skupienie uwagi, zaufanie do informacji oraz jej interpretację). Wśród zakłóceń można wymienić m.in. nadmiar informacji, zbyt szybki przepływ informacji, niezorganizowaną zawartość informacyjną, niespójność informacji pochodzących z różnych źródeł, opóźnienie w przekazywaniu informacji, niską jakość lub wiarygodność informacji (np. brak pewności w zakresie pochodzenia albo źródła informacji). W tab. 2 zaprezentowano, jaki efekt (techniczny, funkcjonalny i operacyjny) mogą mieć ataki informacyjne. Efekty techniczne dotyczą działania systemów komputerowych, efekty funkcjonalne obejmują wymierne, konkretne efekty związane z zawartością informacyjną i ilością informacji, natomiast efekty operacyjne odnoszą się do procesów przetwarzania informacji przez człowieka.

Tab. 2. Przykłady efektów ataku informacyjnego

Typ ataku	Cel ataku	Efekt techniczny	Efekt funkcjonalny	Efekt operacyjny
Zakłócenie komunikacji	System informacyjny	Blokada sygnału	Utrata informacji	Opóźniona lub błędna decyzja
Ingerencja w proces komunikacji	Zarządzanie informacją	–	Błędne przekazywanie informacji, przeciążenie generowane przez system (np. powtarzanie komunikatów diagnostycznych)	Opóźnienie, dezorientacja
Ingerencja w proces komunikacji	Proces podejmowania decyzji	–	Wpływ znikomy	Opóźnienie, dezorientacja, podejmowanie złych decyzji
Wirus komputerowy	System informacyjny	Awaria systemu	Utrata danych	Opóźniona lub błędna decyzja
Robak w sieci	Zarządzanie informacją	–	Opóźnienie lub przeciążenie, utrata funkcji sieci	Opóźniona decyzja
Atak psychologiczny, wiadomości propagandowe	Proces decyzyjny	–	–	Wpływ na podejmowane decyzje
Oszustwa (wprowadzanie w błąd)	Proces decyzyjny	–	–	Manipulacja percepcją

Źródło: oprac. na podstawie L.S. Johnson, *Toward a Functional Model of Information Warfare*, Central Intelligence Agency Washington DC Center For The Study Of Intelligence, Fort Belvoir 1997.

W dokumencie *Global Trends. Paradox of Progress* opracowanym przez Narodową Radę Wywiadu USA (National Intelligence Council), uwzględniającym prognozę zmian w formie prowadzenia działań wojennych do 2035 r., ataki informacyjne (wraz ze zdalnymi atakami z wykorzystaniem broni precyzyjnego rażenia i systemami zautomatyzowanymi) zostały uznane za ataki, które w dużej mierze zastąpią bezpośrednie starcia zbrojne.

Paulina Motylińska

M.R. Endsley, D.G. Jones, *Disruptions, Interruptions and Information Attack: Impact on Situation Awareness and Decision Making*, „Human Factors and Ergonomics Society Annual Meeting Proceedings" 2001, vol. 45 (2); B. Hutchinson, M. Warren, *Information Warfare: Corporate Attack and Defence in a Digital World*, Butterworth Heinemann, Oxford 2001; W. Hutchinson, *Information Warfare and Deception*, „Informing Science" 2006, vol. 9; L.S. Johnson, *Toward a Functional Model of Information Warfare*, Central Intelligence Agency Washington DC Center For The Study Of Intelligence, Fort Belvoir 1997; Z. Modrzejewski, *Operacje informacyjne*, AON, Warszawa 2015; P. Motylińska, *Atak informacyjny*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo,

Wydawnictwo Libron, Kraków 2019; R. Szpyra, *Militarne operacje wojskowe*, AON, Warszawa 2003; R.W. Taylor, E.J. Fritsch, J. Liederbach, *Digital Crime and Digital Terrorism*, Pearson, Prentice Hall, Upper Saddle River 2006; United States Air Force, *Cornerstones of Information Warfare*, 1995; A. Żebrowski, *Determinanty walki informacyjnej*, [w:] *Walka informacyjna. Uwarunkowania – incydenty – wyzwania*, H. Batorowska (red.), Uniwersytet Pedagogiczny im. KEN w Krakowie, Kraków 2017.

ATAK SYMULTANICZNY – polega na przeprowadzeniu w tym samym czasie lub krótkich odstępach czasu uderzeń na cele miękkie z wykorzystaniem materiałów wybuchowych bądź broni palnej (albo obu równocześnie) w różnych punktach miasta (lub w tym samym miejscu, ale w krótkich odstępach czasu). Tak przeprowadzony atak cechują:

- duża liczba poszkodowanych, zabitych i rannych z różnymi rodzajami obrażeń, które stanowią wyzwanie dla systemu opieki przedszpitalnej oraz szpitalnej, problem z wdrożeniem prawidłowego systemu segregacji poszkodowanych na etapie opieki przedszpitalnej (Madryt 2004), konieczność uruchomienia zapasów środków opatrunkowych (Madryt 2004, Londyn 2005);
- chaos organizacyjny i komunikacyjny – ataki symultaniczne powodują bardzo dużą liczbę zgłoszeń do → c e n t r ó w p o w i a d a m i a n i a r a t u n k o w e g o od świadków zdarzenia, rodzin osób rannych, często przekazujących sprzeczne → i n f o r m a c j e [t. 2] co do rodzaju, miejsca i czasu zdarzenia (np. Madryt 2004);
- konieczność stworzenia/uruchomienia specjalnych punktów i numerów informacyjnych dla rodzin osób rannych, zaginionych lub zmarłych wraz z rozbudowaną siecią pomocy psychologicznej dla potrzebujących;
- medialność oraz masowość – tego typu zdarzenia stanowią *breaking news* (wiadomości z ostatniej chwili) dla telewizji i programów informacyjnych na całym świecie, dzięki czemu stają się tematem nr 1, osiągnięcie wysokiej medialności i szerokiego spektrum odbiorców jest jednym z celów działań terrorystów;
- poczucie bezsilności i bezradności wśród społeczeństwa – uczucie bezsilności, pytanie, czy atakowi dałoby się zapobiec, pretensje do służb o brak odpowiedniej reakcji; bardzo często zapomina się o tym, że służby zapobiegają różnym atakom już w fazie przygotowania, ale informacje o tym nie są przekazywane → o p i n i i p u b l i c z n e j [t. 3];
- w przyszłości spadek wartości turystycznej miejsc, w których przeprowadzone zostały ataki terrorystyczne, a więc konsekwencje ekonomiczne dla lokalnej społeczności oraz władz.

W następstwie ataków dochodzi do zmian procedur postępowania państw, władz miejskich na wypadek → s y t u a c j i k r y z y s o w e j [t. 4] o charakterze masowym. W miejscach doświadczonych atakami symultanicznymi wprowadzono specjalne plany reagowania kryzysowego na wypadek zamachu terrorystycznego (np. Platercam – Madryt, White Plan – Paryż).

Sięgając do historii najkrwawszych zamachów symultanicznych, należy wspomnieć:

- Madryt 2004 r. – 194 zabitych, 1858 rannych;
- Londyn 2005 r. – 52 zabitych, 700 rannych;
- Bombaj 2008 r. – 175 zabitych, 293 rannych;
- Paryż 2015 r. – ok. 130 zabitych, ok. 300 rannych;
- Bruksela 2016 r. – 32 zabitych, 316 rannych.

Andrzej Ziarko

P. Guła, *Medyczne skutki terroryzmu*, PZWL Wydawnictwo Lekarskie, Warszawa 2017; tenże, *Terroryzm a medycyna*, Zdrowie i Zarządzanie, Kraków 2009; *Surgery During Natural Disasters, Combat, Terrorist Attacks, and Crisis Situations*, R.B. Lim (ed.), Springer, Cham 2016; A. Ziarko, *Atak symultaniczny*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; tenże, *Zabezpieczenie medyczne miejsc zamachów terrorystycznych na przykładzie wydarzeń z 11 marca 2004 roku w Madrycie*, [w:] *Współczesne problemy bezpieczeństwa państwa*, O. Wasiuta, P. Mazur (red.), Katolicki Uniwersytet Lubelski Jana Pawła II w Lublinie, Stalowa Wola 2017.

ATTACHÉ OBRONY – szef jednostki organizacyjnej funkcjonującej w ramach przedstawicielstwa dyplomatycznego – ataszatu obrony. Aktualnie w polskim prawie attaché obrony to oficer zawodowy Wojska Polskiego wyznaczony do pełnienia służby w przedstawicielstwie dyplomatycznym RP, wykonujący zadania ministra obrony narodowej oraz reprezentujący → S i ł y Z b r o j n e R P [t. 4] w państwie przyjmującym, samodzielnie lub przy pomocy ataszatu obrony, posiadający stopień dyplomatyczny. Attaché obrony mianowany jest przez ministra spraw zagranicznych na wniosek ministra obrony narodowej i podlega szefowi przedstawicielstwa dyplomatycznego (ambasadorowi). Działa jednak wg poleceń i instrukcji otrzymywanych bezpośrednio z ministerstwa obrony, gdzie też składa sprawozdania. Attaché obrony w przeciwieństwie do szefa misji dyplomatycznej, który reprezentuje całe państwo wysyłające, jest reprezentantem jedynie sił zbrojnych państwa wysyłającego w państwie przyjmującym. Jest ponadto akredytowany w sposób stały w państwie przyjmującym (choć fizycznie nie musi w nim przebywać).

Historycznie działalność ataszatów związana była ze szpiegostwem wojskowym, którego tradycja sięga czasów starożytnych. Pierwsze jego ślady można odnaleźć już w starożytnym Rzymie. Również w czasach średniowiecznych istniała funkcja attaché, ale rzadkością było włączanie specjalnych obserwatorów wojskowych do misji dyplomatycznych, ponieważ → w o j n y [t. 4] były zbyt mało złożone i pozbawione podziału zadań wojskowych oraz planowania, by wymagać specjalnych przedsięwzięć wywiadowczych. W czasach nowożytnych, odkąd w XVI i XVII w. rozpowszechniły się misje dyplomatyczne, stojący na ich czele dyplomaci przesyłali do swoich krajów raporty dotyczące sytuacji politycznej, gospodarczej i militarnej w państwie swojej służby. Jako że kwestie → b e z p i e c z e ń s t w a uznawano za bardzo ważne również

w tamtym czasie, istotnym elementem raportów były → i n f o r m a c j e [t. 2] na temat sił zbrojnych państwa przyjmującego. W związku z tym, że cywilni dyplomaci nie mieli specjalistycznej wojskowej wiedzy, ich raporty cechowały się sporą niedokładnością, władcy zaczęli wysyłać oficerów w charakterze ambasadorów lub łączników i doradców wojskowych przy sojuszniczych armiach.

Rzeczywisty rozwój instytucji oficjalnego przedstawicielstwa pod postacią obserwatora wojskowego w składzie poselstwa wiąże się z okresem wojen koalicyjnych w Europie na przełomie XVII i XVIII w. Jako oficer łącznikowy emisariusz wojskowy był przydzielany do armii sprzymierzonej w celu uzgadniania jej ruchów w sposób bardziej kompetentny, niż mogli to czynić ambasadorowie. Udzielał on informacji dowódcy armii sprzymierzonej, składał sprawozdania z wykorzystania przez odbiorcę subsydiów pieniężnych i reprezentował ambasadora w sytuacji, gdy ten nie mógł opuścić stolicy. Znacząca pozycja emisariuszy wysyłanych przez ministerstwa wojny powodowała obawy ministerstw spraw zagranicznych o ich dominację w polityce zagranicznej. Inną formą relacji wojskowych praktykowanych przez władców była wymiana adiutantów. Stosowano ją po to, aby podkreślić szczególne zaufanie do drugiego monarchy. Adiutant rezydował stale przy dworze monarchy, zapewniając bezpośrednie kontakty między władcami. Nie był to zatem attaché wojskowy w pełnym tego słowa znaczeniu, gdyż działał poza strukturami przedstawicielstwa dyplomatycznego. Poza nimi działali także obserwatorzy wojskowi okazjonalnie wysyłani przez państwa do śledzenia działań zbrojnych lub manewrów w innym państwie. W odróżnieniu do attaché wojskowych obserwatorzy nie rezydowali na stałe w danym państwie, ale doraźnie, w razie potrzeby. W XIX w. stosowana była też – szczególnie między państwami niemieckimi a Rosją – praktyka nadawania władcy drugiego państwa honorowego tytułu szefa pułku. Praktykowano również przyjmowanie obcych władców za patronów lub szefów sztabu własnych jednostek wojskowych.

Rozwój myśli wojskowej i rywalizacja militarna państw w XIX w., szczególnie w okresie wojen napoleońskich, wywarły duży wpływ na określenie roli i zadań eksperta wojskowego. Nasilone współzawodnictwo wojskowe zrodziło zapotrzebowanie na fachowe wiadomości wojskowe o obcych armiach. Państwa zaczęły wysyłać oficerów jako członków misji dyplomatycznych także na krótkotrwałe okresy pracy w poselstwach.

Autorem idei ustanowienia funkcji attaché wojskowego był pruski oficer płk von Massenbach, który w 1795 r. przedstawił projekt utworzenia takich stanowisk przy pruskich przedstawicielstwach dyplomatycznych za granicą. Za pierwszego w historii dyplomatę wojskowego uważa się hrabiego

J. Lagrange'a – sekretarza poselstwa francuskiego w Wiedniu w 1809 r. Dwa lata później podobne stanowisko przy sztabie cesarza Napoleona I objął płk A. Czernyszew – adiutant cara Aleksandra I. Zasadnicze cechy funkcji attaché wojskowego ujawniły się w 1860 r., kiedy to po wojnie krymskiej upowszechniła się praktyka ustanawiania

przez wielkie mocarstwa takich stanowisk przy przedstawicielstwach dyplomatycznych. Tytuł attaché, dotychczas zarezerwowany tylko dla dyplomatów cywilnych, od połowy XIX w. we Francji został przyznany również członkom korpusu sztabu generalnego (oficerom). Przyjęto też zasadę, że funkcję tę mogli pełnić oficerowie w stopniu majora, którą stosowano później w większości państw. Termin „attaché wojskowy" po raz pierwszy pojawił się w 1867 r. w spisach personelu dyplomatycznego brytyjskiego Ministerstwa Spraw Zagranicznych i dotyczył początkowo wyłącznie oficera akredytowanego przy ambasadzie w Paryżu. Od czasu powołania stanowiska attaché wojskowego sprawozdania dyplomatyczne o charakterze wojskowym nabrały bardziej fachowego charakteru, ponieważ zawierały specjalistyczne informacje o innych armiach.

Powołanie informatorów wojskowych w 1. poł. XIX w. we Francji i Prusach doprowadziło do powstania pierwszej w historii *Instrukcji dla oficera sztabu generalnego przydzielonego do przedstawicielstwa zagranicznego*, wydanej w Austrii w 1810 r. Nakazywano w niej oficerowi uzyskiwanie dokładnych i szczegółowych danych o sprawach wojskowych w kraju rezydowania, zdawanie ambasadorowi dokładnych sprawozdań ze wszystkich swych czynności. Mimo że nie występowało wówczas jeszcze oficjalne określenie „attaché wojskowy", była to pierwsza instrukcja dla oficerów pełniących tę funkcję.

W kolejnych latach XIX w. i z początkiem XX w. instytucja attaché wojskowego była już rozpowszechniona w praktyce europejskiej oraz światowej i objęła takie kraje jak Rosja, Austria, Wielka Brytania, Kanada czy USA. Attaché jako eksperci wojskowi zyskali sobie wysoką pozycję w środowisku dyplomatów, odnoszono się do nich jednak z nieufnością, traktując ich często jak szpiegów. Podczas I wojny światowej attaché wojskowi państw uczestniczących w niej wspierali w sposób legalny i nielegalny wysiłki wojenne swoich krajów. Niektórzy z nich angażowani byli przez swoje kraje do działań na rzecz ustanowienia pokoju lub zawieszenia broni. W latach międzywojennych ekspertów wojskowych wykorzystywano do negocjacji, kontroli i nadzoru porozumień rozbrojeniowych oraz do prowadzenia dochodzeń w przypadku sytuacji konfliktowych i incydentów wojskowych. Wraz z początkiem XX w. krąg dyplomatów wojskowych powiększył się, co wynikało z pojawienia się nowych rodzajów sił zbrojnych. Tradycyjne → w o j s k a l ą d o w e [t. 4] zostały uzupełnione o siły morskie i powietrzne. Dlatego obok attaché wojskowego pojawili się attaché morscy i lotniczy jako przedstawiciele tych rodzajów sił zbrojnych. Również w Polsce, zaraz po odzyskaniu niepodległości w 1918 r., przystąpiono do budowy służby dyplomacji wojskowej. Pierwsza taka placówka powstała 3 listopada 1918 r. w Wiedniu. Zasadniczym problemem w działalności polskich ataszatów wojskowych w latach międzywojennych były ograniczenia finansowe, co powodowało, że nie były tak skuteczne jak struktury z innych państw. Podstawowym zadaniem ataszatów w tamtym czasie było zbieranie informacji o potencjale militarnym innych państw, organizowanie ważnych wizyt na

terenie państwa przyjmującego, negocjowanie projektu konwencji wojskowej polsko-angielskiej (1939 r.) oraz współpraca z kręgami wojskowymi państw przyjmujących.

W okresie II wojny światowej polski rząd na uchodźstwie posługiwał się instytucją ataszatów na zasadach wypracowanych przed wojną. Po wojnie współzawodnictwo militarne Wschodu i Zachodu oraz → z i m n a w o j n a [t. 4] uczyniły pracę rozpoznawczą attaché wojskowych szczególnie ważną i trudną. Wówczas zadania dyplomatów wojskowych powszechnie rozumiano jako współpracę obronną. W rzeczywistości stanowiły one jednak przykrywkę dla zadań wywiadowczych. Dopiero w 1945 r., na mocy Karty Narodów Zjednoczonych, wprowadzony został prawny zakaz użycia siły lub groźby jej użycia w stosunkach międzynarodowych. Zadania dyplomacji zostały skierowane na rzecz współpracy, działań pokojowych i prewencyjnych, związanych z zapobieganiem konfliktom albo ograniczaniem ich skutków. Zmiany te znalazły odzwierciedlenie także w nazewnictwie, termin attaché wojskowego został zastąpiony pojęciem attaché obrony.

Na przełomie wieków ewoluowały również funkcje attaché obrony (wojskowych). Ich zasadniczą rolą w XIX i XX w., aż do zakończenia zimnej wojny, była funkcja informacyjna. Attaché wojskowych jednoznacznie kojarzono z → a g e n t a m i w y w i a d u , natomiast ataszaty z oddziałami wywiadowczymi działającymi pod przykrywką dyplomacji. Interesowanie się rozwojem sił zbrojnych obcego państwa, stopniem ich przygotowania do prowadzenia wojny i ogólnym potencjałem wojennym należało – w początkach rozwoju dyplomacji – do obowiązków ambasadorów i innych dyplomatów. Właśnie ta dziedzina ich działalności powodowała nadanie im miana „szpiegów" lub „honorowych szpiegów".

Radykalna zmiana postrzegania zadań attaché wojskowych nastąpiła po 1989 r., kiedy to wskutek zmian w środowisku → b e z p i e c z e ń s t w a m i ę d z y n a r o d o w e g o usytuowano attaché wojskowego jako tego, który odgrywa kluczową rolę w narodowej → d y p l o m a c j i o b r o n n e j [t. 2]. Obok tradycyjnych zadań pojawiły się nowe, bardziej specjalistyczne, związane z np. reformami sektora obronnego i → b e z p i e c z e ń s t w a w państwach przechodzących transformację ustrojową, popieraniem działań na rzecz wspierania pokoju i udziałem w cywilnych operacjach → z a r z ą d z a n i a k r y z y s o w e g o [t. 4] czy też ze zwalczaniem → t e r r o r y z m u [t. 4].

W prawie dyplomatycznym przyjmuje się, że attaché obrony wypełnia kilkanaście zasadniczych funkcji. Jest to zbieranie informacji wojskowych, reprezentowanie swojej armii i jej dowództwa w państwie przyjmującym oraz służenie pomocą i radą szefowi misji dyplomatycznej w rozwiązywaniu zagadnień wojskowych. W ramach funkcji informacyjnej attaché zbierają informacje o różnych przejawach aktywności wojskowej państwa przyjmującego. Muszą to jednak czynić z zachowaniem wszelkich zasad legalności, zachowując przepisy państwa przyjmującego i szanując własny status dyplomatyczny. Sprowadza się to do stosowania jedynie → b i a ł e g o w y w i a d u ,

czyli pozyskania informacji tylko z legalnych źródeł. Za nielegalne uważa się szpiegostwo, przekupstwo obywateli i namawianie ich do dostarczania tajnych informacji.

Funkcja reprezentacyjna polega na reprezentowaniu własnego ministerstwa obrony lub rodzaju sił zbrojnych wobec odpowiednika w państwie przyjmującym. Wiąże się to z wyrażaniem interesów własnego kraju w sferze obronności i bezpieczeństwa oraz przygotowywaniem wizyt wysokich rangą przedstawicieli państwa przyjmującego w państwie wysyłającym. W ramach funkcji negocjacyjnej attaché podejmują działania w zakresie zacieśniania współpracy w sprawach obrony i bezpieczeństwa. Funkcja kontrolno-zarządcza polega na kontroli realizacji programów współpracy wojskowej i w zakresie bezpieczeństwa oraz zarządzaniu nimi. Funkcja budowy środków zaufania stawia attaché obrony w roli jednej z gwarancji, że nawet w sytuacji pogorszenia wzajemnych stosunków politycznych między państwami relacje militarne i w zakresie bezpieczeństwa między nimi nie ulegną radykalnemu pogorszeniu. Rolą attaché obrony jest więc podejmowanie działań na rzecz budowy i rozwoju przyjaznych stosunków oraz współpracy między państwami, udział w procesie przygotowywania i zawierania umów i porozumień wojskowych z siłami zbrojnymi gospodarzy oraz dotyczących wymiany licencji, technologii i produkcji zbrojeniowej.

W ramach funkcji promocyjnej rola attaché obrony wyraża się w promowaniu własnego państwa w państwie przyjmującym np. poprzez promowanie tradycji militarnych oraz własnego przemysłu zbrojeniowego. Ma to szczególne znaczenie dla pozyskiwania nowych rynków zbytu dla rodzimego uzbrojenia i wnosi do działalności ataszatu obrony także wymiar ekonomiczny. W ramach rozpoznawania potencjału militarnego, założeń doktryny, zadań strategiczno-operacyjnych oraz polityki wojskowej państwa przyjmującego rolą attaché obrony jest poznawanie sił zbrojnych państwa gospodarza, ich tradycji, poziomu wyszkolenia bojowego, osiągnięć w dziedzinie techniki, organizacji i użycia wojsk oraz założeń strategiczno-operacyjnych. Do jego zadań należy ponadto rozpoznawanie kierunków polityki zagranicznej państwa przyjmującego, zakresu udziału w sojuszach wojskowych i powiązań gospodarczych dotyczących obronności. Śledzenie zmian personalnych i funkcyjnych na wyższych stanowiskach wojskowych, politycznych i administracyjnych oraz ogólna znajomość życiorysów i charakterystyk wyższych dowódców wojskowych, a także kierownictwa cywilnego państwa przyjmującego to również zadanie attaché obrony. Warto wspomnieć też o funkcji doradczej, jaką pełnią attaché obrony wobec szefa misji dyplomatycznej (ambasadora, posła) oraz personelu placówki dyplomatycznej w sprawach militarnych i związanych z bezpieczeństwem. Funkcja administracyjna natomiast polega na wykonywaniu zadań administracji wojskowej, a funkcja ochronna obejmuje ochronę interesów własnego państwa w sferze obronności oraz opiece nad jego obywatelami. Istotną funkcję pełni attaché obrony w zakresie zarządzania kryzysowego. Uaktywnia się ona w sytuacji nadzwyczajnej w państwie przyjmującym i może polegać np. na nadzorze nad ewakuacją, dostarczaniu przez siły zbrojne państwa wysyłającego pomocy humanitarnej.

Zadaniem attaché obrony jest także obserwowanie współpracy militarnej państwa przyjmującego z innymi krajami, jak również udzielanie władzom wojskowym państwa przyjmującego oficjalnych informacji o siłach zbrojnych własnego kraju, pośredniczenie w kontaktach pomiędzy władzami wojskowymi obu krajów, udział w imprezach wojskowych (ćwiczenia, pokazy, uroczystości, wizyty w jednostkach, wystawy, konferencje).

W ramach współpracy z władzami wojskowymi państwa przyjmującego zadaniem attaché obrony jest prowadzenie wstępnych uzgodnień umów o współpracy wojskowej, zakupu i sprzedaży broni oraz sprzętu wojskowego itp. Zadaniem dodatkowym jest czuwanie attaché obrony nad poszanowaniem przez państwo przyjmujące umów i porozumień ograniczających zbrojenia lub dotyczących rozbrojenia. W ramach funkcji popularyzatorsko-informacyjnej historii i tradycji attaché obrony podejmuje współpracę z organizacjami kombatanckimi w kraju urzędowania, współdziała ze służbą konsularną w zakresie opieki nad miejscami pamięci narodowej i pomnikami chwały oręża w kraju przyjmującym, inspiruje wyjazdy i wizyty zagraniczne → o k r ę t ó w w o j e n n y c h [t. 3], pododdziałów wojskowych, wojskowych zespołów artystycznych, orkiestr wojskowych itp. Inne zadania attaché obrony obejmują terminowe przesyłanie meldunków i sprawozdań dotyczących realizacji zadań oficjalno-reprezentacyjnych, udzielanie, w razie potrzeby, pomocy → ż o ł n i e r z o m [t. 4] oraz członkom ich rodzin przebywającym na terenie państwa przyjmującego i otaczanie ich opieką. W czasie wojny lub konfliktu zbrojnego attaché obrony utrzymuje łączność z dowództwem państwa koalicyjnego bądź też podejmuje się obserwacji w państwie neutralnym przestrzegania przez nie zasad neutralności. Rola attaché obrony sprowadza się więc do prowadzenia działalności mającej na celu zacieśnienie przyjaznych stosunków oraz umacniania współpracy między siłami zbrojnymi obu krajów, a także obserwowania sytuacji wojskowo-politycznej kraju przyjmującego i rozpoznawania sił zbrojnych.

Sabina Olszyk

J. Barcik, *Dyplomacja w systemie bezpieczeństwa narodowego*, Wyższa Szkoła Oficerska Wojsk Lądowych im. gen. Tadeusza Kościuszki, Wrocław 2014; *Defence Attachés*, „Geneva Centre for the Democratic Control of Armed Forces Backgrounder" 2007, no. 7; L. Drab, *Dyplomacja obronna w procesie kształtowania bezpieczeństwa RP*, Wydawnictwo Difin, Warszawa 2018; L. Drab, A. Sochan, *Attaché obrony: status i funkcjonowanie: wybór dokumentów*, Wojskowe Centrum Edukacji Obywatelskiej im. płk. dypl. Mariana Porwita, Warszawa 2016; J. Gryz, *Współczesny kształt dyplomacji wojskowej*, [w:] *Nowe oblicza dyplomacji*, B. Surmacz (red.), Wydawnictwo UMCS, Lublin 2013; R. Kupiecki, *Attaché obrony i jego środowisko pracy*, „Dyplomacja Obronna" 2016, t. 1; S. Olszyk, *Attaché obrony – rola i zadania w działaniach na rzecz bezpieczeństwa*, [w:] *Współczesna polityka bezpieczeństwa: aspekty polityczne, gospodarcze i militarne*, t. 2, M. Delong, M. Malczyńska-Biały (red.), Wydawnictwo Uniwersytetu Rzeszowskiego, Rzeszów 2018; Ustawa z dnia 27 lipca 2001 r. o służbie zagranicznej, Dz. U. 2001, nr 128, poz. 1403; A. Vagts, W.T.R. Fox, *Defence and Diplomacy. The Soldier and the Conduct of Foreign Relations*, King's Crown Press, New York 1958; Zarządzenie Ministrów Spraw Zagranicznych i Obrony Narodowej w sprawie szczególnych zasad wykonywania obowiązków

służbowych przez żołnierzy zawodowych pełniących służbę w placówkach zagranicznych oraz organizacji i funkcjonowania w placówkach zagranicznych ataszatów obrony z 27 maja 2004 r., Dz. Urz. MSZ 2004 nr 3, poz. 28 z późn. zm., Dz. Urz. MON 2004, nr 6, poz. 57 z późn. zm.

ATASZAT OBRONY (WOJSKOWY) – samodzielna jednostka organizacyjna resortu → o b r o n y n a r o d o w e j [t. 3], która funkcjonuje w ramach służby zagranicznej reprezentującej państwo na arenie międzynarodowej, obok stałej misji dyplomatycznej (ambasady) i urzędów konsularnych. Stanowi wsparcie dla służby zagranicznej pracującej na rzecz → b e z p i e c z e ń s t w a [t. 1] i działa przy przedstawicielstwach dyplomatycznych RP na całym świecie. Te przedstawicielstwa są komórkami łącznikowymi między narodami a sojuszniczymi władzami wojskowymi.

Na czele ataszatu stoi → *a t t a c h é* o b r o n y [t. 1], którym zawsze jest oficer w służbie czynnej, najczęściej w stopniu od majora do generała. Ta funkcja stanowi wynik historycznej ewolucji rozwiązań formalnych, zabezpieczających potrzeby właściwej reprezentacji swoich interesów wojskowych przez państwo, realizowanych wobec innych uczestników stosunków międzynarodowych. *Attaché* obrony jest delegowany za granicę przez własne państwo i od ponad dwustu lat pozostaje kluczowym składnikiem ochrony i realizacji interesów narodowych w przestrzeni międzynarodowej. *Attaché* obrony stoi niejako na pierwszej linii frontu – reprezentuje swój kraj za granicą i odpowiada za współpracę międzypaństwową. Jest bezpośrednim przełożonym personelu ataszatu obrony i odpowiada za przestrzeganie przepisów o służbie wojskowej żołnierzy zawodowych i przepisów prawa pracy, a także organizuje pracę ataszatu obrony. W skład ataszatu obrony wchodzą – obok *attaché* obrony oraz jego zastępcy lub zastępców z określonych rodzajów wojsk (np. *attaché* wojskowy, morski, lotniczy) – kierownik ataszatu oraz pracownik lub pracownicy personelu technicznego. *Attaché* obrony jest przedstawicielem Ministra Obrony Narodowej (MON) w państwie przyjmującym lub w większej liczbie państw, również za ich zgodą. Okres jego pobytu na placówce trwa przeważnie 3–4 lata i zależy od indywidualnych wyników pracy oraz potrzeb służbowych MON.

Zasady wykonywania obowiązków służbowych, a także organizacjai funkcjonowanie ataszatów wojskowych w placówkach zagranicznych leżą w gestii Ministra Spraw Zagranicznych i Ministra Obrony Narodowej. W strukturze ambasady ataszat obrony nie stanowi odrębnej jednostki organizacyjnej, ale funkcjonuje w ramach placówki dyplomatycznej państwa wysyłającego jako jej wyodrębniona część i podlega ambasadorowi pod względem politycznym i protokolarno-dyplomatycznym. *Attaché* obrony jest zatem częścią personelu dyplomatycznego i ma stopień dyplomatyczny. Jego przełożonym jest jednak minister obrony narodowej, który scedował kierowanie tymi placówkami na dyrektora Departamentu Wojskowych Spraw Zagranicznych MON. Taka sytuacja powoduje, że *attaché* obrony jest podwójnie podporządkowany: jednocześnie podlega szefowi misji dyplomatycznej, w ramach której funkcjonuje (a tym samym

– Ministerstwu Spraw Zagranicznych) oraz Ministerstwu Obrony Narodowej, którego zadania wykonuje i któremu składa sprawozdania.

Funkcje ataszatu obrony ewoluowały na przełomie wieków. Współcześnie taka jednostka realizuje zadania Ministra Obrony Narodowej oraz reprezentuje → S i ł y Z b r o j n e R P [t. 4] w państwie przyjmującym. Zadania wiążą się zatem z bezpośrednią aktywnością *attaché* obrony i dotyczą zagadnień obejmujących polityczno-wojskową działalność w stosunkach między państwami i ich siłami zbrojnymi, mogących wpływać na kształt bezpieczeństwa państwa. Należą do nich:

- zadania reprezentacyjne – reprezentowanie własnej armii i jej dowództwa w państwie przyjmującym oraz doradztwo szefowi misji w zakresie zagadnień wojskowych, utrzymywanie oficjalnych kontaktów z władzami wojskowymi państwa przyjmującego, w tym zapewnienie i ułatwienie kontaktów dwustronnych wynikających z międzynarodowej współpracy wojskowej oraz podejmowanie działań na rzecz zacieśnienia współpracy w ramach → d y p l o m a c j i p r e w e n c y j n e j [t. 2] i budowy środków zaufania, przygotowywania wizyt, rozmów w sprawie zawarcia porozumienia w określonych dziedzinach;
- zadania informacyjne – obowiązek zbierania informacji dotyczących aktywności wojskowej kraju przyjmującego, a zwłaszcza polityki bezpieczeństwa i jego możliwości militarnych, kierunków jego polityki zagranicznej, zakresu udziału w sojuszach wojskowych i powiązań gospodarczych dotyczących → o b r o n n o ś c i , struktur wojskowych oraz ich sposobów zorganizowania, jak również planów budżetowych kraju przyjmującego na kolejny rok i potencjalnych zmian, ponadto znajomość decydentów, którzy w armii państwa przyjmującego pełnią najwyższe funkcje w poszczególnych rodzajach wojsk, i utrzymywanie z nimi kontaktu, obserwacja współpracy militarnej z innymi krajami państwa – gospodarza itd. *Attaché* obrony ma obowiązek przekazywać pozyskane → i n f o r m a c j e [t. 2] własnemu ministrowi obrony. Zadania informacyjne muszą być jednak realizowane z zachowaniem wszelkich zasad legalności oraz prawa państwa przyjmującego w poszanowaniu własnego statusu dyplomatycznego. W praktyce sprowadza się to do stosowania jedynie tzw. → b i a ł e g o w y w i a d u [t. 1], czyli dopozyskiwania informacji z legalnych źródeł;
- zadania promocyjne – promowanie własnego państwa w państwie przyjmującym w zakresie tradycji militarnych oraz promowanie własnego przemysłu zbrojeniowego. Ma to szczególne znaczenie dla pozyskiwania nowych rynków zbytu dla rodzimego uzbrojenia i wnosi do działalności ataszatu obrony także wymiar ekonomiczny;
- zadania szkoleniowe – organizacja przedsięwzięć mających na celu doskonalenie warsztatu działania oficerów dyplomatów i usprawniających realizację zadań dyplomatycznych oraz szkoleń dla nowych członków wojskowego korpusu dyplomatycznego w zakresie spraw protokolarno-dyplomatycznych i merytorycznych realizowanych na danej placówce dyplomatycznej lub misji wojskowej;

- zadania kontrolno-zarządcze – kontrola realizacji i zarządzaniu programami współpracy wojskowej i w zakresie bezpieczeństwa, wspieranie polskich kontyngentów wojskowych w sferze dyplomatyczno-organizacyjnej oraz informacyjnej;
- zadania organizacyjno-administracyjne – np. udzielanie zgody na przeloty samolotów wojskowych nad danymi krajami oraz na przejazdy kolumn wojskowych na ćwiczenia, organizowanie uroczystości związanym ze świętem własnych sił zbrojnych oraz uczestnictwo w tych uroczystościach, pośredniczenie w przesyłaniu korespondencji – korespondencja ministrów obrony państwa przyjmującego i wysyłającego odbywa się bezpośrednio tylko przez ataszat obrony itp.;
- zadania popularyzatorsko-informacyjne – utrzymywanie więzi z kombatantami i środowiskami kombatanckimi w kraju urzędowania, współdziałanie ze służbą konsularną w zakresie opieki nad miejscami pamięci narodowej i pomnikami chwały oręża polskiego w kraju przyjmującym;
- inne zadania – np. udzielanie, w razie potrzeby, pomocy i opieki żołnierzom oraz członkom ich rodzin przebywającym na terenie państwa przyjmującego, w czasie → w o j n y [t. 4] lub → k o n f l i k t u z b r o j n e g o utrzymywanie stałej łączności z dowództwem państwa przyjmującego itp.

Attaché obrony, w przeciwieństwie do szefa misji dyplomatycznej, który reprezentuje całe państwo wysyłające, jest reprezentantem jedynie sił zbrojnych państwa wysyłającego w państwie przyjmującym. Jest ponadto akredytowany w sposób stały w państwie przyjmującym (choć fizycznie nie musi w nim przebywać). W zakresie protokołu dyplomatycznego *attaché* obrony przysługuje miejsce w kolejności pierwszeństwa wśród członków personelu dyplomatyczno-konsularnego, po radcy – ministrze. W czasie nieobecności *attaché* obrony ataszatem obrony kieruje – wyznaczony przez niego lub przez Szefa Biura Ataszatów Wojskowych – → ż o ł n i e r z [t. 4] zawodowy, o czym informuje się kierownika placówki. Zgodnie z prawem oraz praktyką dyplomatyczną, *attaché* obrony wchodzi w skład personelu dyplomatycznego ambasady i jego status prawny nie różni się od pozostałych dyplomatów. Korzysta on z przywilejów i immunitetów dyplomatycznych, do których należą m.in.:

- nietykalność osobista – dyplomata wojskowy nie podlega aresztowaniu czy też zatrzymaniu w jakiejkolwiek formie Władze państwa przyjmującego są zobowiązane do traktowania *attaché* obrony z należytym szacunkiem i zabezpieczać przed zamachami na jego osobę, wolność lub godność;
- immunitet jurysdykcyjny – dyplomata wojskowy nie podlega sądom państwa przyjmującego w sprawach karnych, cywilnych i administracyjnych. Dotyczy to zarówno działalności służbowej jak i prywatnej oraz członków jego rodziny, jeśli nie są oni obywatelami państwa przyjmującego,
- immunitet egzekucyjny – wyłączenie jego osoby i mienia z wykonania wyroku sądowego lub decyzji organu administracyjnego.

W Polsce nabór kandydatów na stanowiska w ataszatach obrony jest otwarty dla wszystkich żołnierzy zawodowych. Wymaga się od nich wiedzy na temat zagadnień związanych z bezpieczeństwem oraz z regionem świata, do którego mieliby zostać skierowani. Sprawdzana jest również znajomość języka angielskiego, umożliwiająca płynną komunikację oraz gwarantująca twórcze i bezkolizyjne funkcjonowanie w nowym miejscu. Możliwe jest także wymaganie znajomości innych języków urzędowych, zwłaszcza w razie wyjazdu do ataszatu w państwie europejskim. Kandydaci przechodzą ponadto rozmowy kwalifikacyjne oraz testy psychologiczne, badanie wariografem, są też sprawdzani przez odpowiednie służby.

Wydatki na utrzymanie ataszatu obrony są pokrywane z budżetu Ministerstwa Spraw Zagranicznych na ogólnych zasadach dotyczących jednostek budżetowych w ramach planowanych i przyznawanych środków finansowych placówki zagranicznej. *Attaché* obrony korzysta z funduszu dyspozycyjnego kierownika placówki zagranicznej w granicach limitu ustalonego między Dyrektorem Sekretariatu Ministra Spraw Zagranicznych a Szefem Biura Ataszatów Wojskowych, przy uwzględnieniu specyficznej pozycji *attaché* obrony, w tym – konieczności organizowania imprez dyplomatycznych.

Zadania ataszatu obrony wobec kierownika placówki zagranicznej obejmują:

- informowanie o sytuacji wojskowej państwa przyjmującego;
- informowanie o politycznych aspektach kontaktów własnych i członków personelu ataszatu obrony z przedstawicielami państwa przyjmującego oraz pracownikami placówek zagranicznych innych państw;
- informowanie o wytycznych, otrzymywanych z Ministerstwa Obrony Narodowej, w odniesieniu do polityczno-wojskowych aspektów działalności ataszatu obrony;
- informowanie o sytuacji w polskich kontyngentach wojskowych znajdujących się na terytorium państwa przyjmującego;
- informowanie o wszelkich naruszeniach przez państwo przyjmujące przywilejów i immunitetów przysługujących mu oraz członkom personelu ataszatu obrony z racji zajmowanych stanowisk;
- informowanie o programach obchodów Święta Wojska Polskiego, wzajemnych wizytach delegacji ministerstw obrony i sił zbrojnych, wizytach okrętów wojennych, eskadr lotniczych, komisji mieszanych ministerstw obrony i sił zbrojnych oraz wojskowych misji specjalnych, a także imprezach i uroczystościach wynikających z członkostwa Rzeczypospolitej Polskiej w sojuszach i organizacjach międzynarodowych.

Jeżeli w wystąpieniach *attaché* obrony i członków personelu ataszatu obrony są zawarte aspekty polityczne, treść wystąpienia należy uzgodnić z kierownikiem placówki zagranicznej. Udostępnia on wówczas *attaché* obrony informacje o politycznych aspektach działalności prowadzonej przez siebie i przez członków personelu misji dyplomatycznej, a w razie potrzeby zapewnia udział *attaché* obrony lub osoby przez niego wyznaczonej w pracach zespołów problemowych.

Do początku lat 90. XX w. ataszaty wojskowe podlegały MON poprzez Oddział Ataszatów Wojskowych Sztabu Generalnego Wojska Polskiego,który był usytuowany w strukturze Zarządu II Sztabu Generalnego WP. Po rozwiązaniu Układu Warszawskiego w 1991 r. przystąpiono do dostosowywania struktur organizacyjnych WP do standardów → N A T O [t. 3]. Na bazie Zarządu II Sztabu Generalnego i → k o n t r - w y w i a d u [t. 2] Wojskowej Służby Wewnętrznej utworzono Wojskowe Służby Informacyjne (WSI) bezpośrednio podległe Ministrowi Obrony Narodowej, a z Oddziału Ataszatów Wojskowych, utworzono podległe WSI – Biuro Ataszatów Wojskowych (BAW). Odpowiadało ono za organizację i prowadzenie przygotowań kandydatów do służby w ataszatach obrony, utrzymywanie stałych kontaktów z korpusem *attachés* wojskowych. Do zadań BAW należało także organizowanie i zabezpieczanie spotkań z kierownictwem Ministerstwa Obrony Narodowej oraz wizyt i podróży informacyjnych. Kolejna reorganizacja w 2006 r. przyniosła rozwiązanie WSI, a następnie – likwidację BAW. Obecnie w MON funkcjonują 2 departamenty zajmujące się → d y - p l o m a c j a w o j s k o w ą [t. 2]:

1. Departament Wojskowych Spraw Zagranicznych (DWSZ) – odpowiedzialny za współpracę międzynarodową resortu obrony. Realizuje zadania związane z udziałem przedstawicielstw resortu w misjach organizacji międzynarodowych oraz udziela wsparcia protokolarnego. Zajmuje się weryfikacją umów międzynarodowych dotyczących kontroli zbrojeń. Departament zajmuje się przygotowywaniem wizyt i spotkań ministrów i wiceministrów obrony narodowej z partnerami zagranicznymi. W ramach departamentu istnieje Oddział Ataszatów Wojskowych, który podlega bezpośrednio dyrektorowi DWSZ, natomiast bezpośrednim przełożonym attachés obrony jest podsekretarz stanu MON właściwy do spraw polityki obronnej i współpracy międzynarodowej poprzez dyrektora DWSZ i szefa Oddziału Ataszatów Wojskowych. Oddział jest odpowiedzialny za: organizowanie i kierowanie działalnością ataszatów obrony przy przedstawicielstwach dyplomatycznych; przygotowanie kandydatów do pracy w ataszatach obrony; przygotowywanie udziału i monitorowanie działalności polskich obserwatorów; reprezentowanie resortu wobec Wojskowego Korpusu Dyplomatycznego akredytowanego w RP oraz organizowanie dla niego spotkań informacyjnych i wizyt w jednostkach wojskowych Sił Zbrojnych RP.
2. Departament Polityki Bezpieczeństwa Międzynarodowego (DPBM) – opracowuje założenia, cele i zadania polskiej polityki obronnej i bezpieczeństwa w aspekcie międzynarodowym. Zajmuje się określaniem wytycznych, analiz, prognoz oraz planów. Uczestniczy w procesach planowania obronnego NATO i UE.

Do utworzenia lub likwidacja ataszatu obrony, podobnie jak do utworzenia lub likwidacji stanowiska przeznaczonego dla żołnierza zawodowego w przedstawicielstwie, dochodzi po porozumieniu – odpowiednio – Szefa WSI i Podsekretarza Stanu w Ministerstwie Obrony Narodowej ds. Polityki Obronnej z Dyrektorem Generalnym

Służby Zagranicznej. Przygotowanie kandydatów do służby w ataszatach obrony prowadzi i organizuje Biuro Ataszatów Wojskowych Inspektoratu Wojskowych Służb Informacyjnych. Zakres szkolenia jest ustalany na drodze uzgodnień między właściwymi komórkami organizacyjnymi MSZ a BAW. Kandydatów do służby w przedstawicielstwach przygotowują komórki organizacyjne MON. Zakres szkolenia uzgadniają one z właściwymi komórkami MSZ. To ministerstwo umożliwi kandydatom do objęcia stanowisk w ataszatach obrony oraz w przedstawicielstwach odbycie w nich krótkoterminowych staży i praktyk. Koszty związane z delegowaniem żołnierzy zawodowych w takim przypadku poniesie MON. Z kolei MSZ udzieli, w miarę możliwości, pomocy w zakwaterowaniu żołnierzy zawodowych na zasadach dotyczących członków służby zagranicznej. Liczba placówek dyplomatycznych świadczy o randze państwa i jego udziale w polityce globalnej.

Regulacje prawne dotyczące powoływania i działalności ataszatów obrony zawarto w przepisach wewnętrznych danego państwa. W Polsce jest to przede wszystkim Ustawa z dnia 27 lipca 2001 r. o służbie zagranicznej i wydane na jej podstawie Zarządzenie ministrów spraw zagranicznych i obrony narodowej z dnia 27 maja 2004 r. w sprawie szczególnych zasad wykonywania obowiązków służbowych przez żołnierzy zawodowych pełniących służbę w placówkach zagranicznych oraz organizacji i funkcjonowania w placówkach zagranicznych ataszatów obrony.

Wpływ na likwidację bądź rozszerzenie ataszatów obrony ma intensywność współpracy polityczno-obronnej między państwami, potrzeby bezpieczeństwa, jak również interesy przemysłu obronnego. Z tego względu sieć ataszatów ulega ciągłym zmianom, w zależności od zmiennych uwarunkowań bezpieczeństwa i interesów narodowych. Aktualnie Polska ma 57 takich przedstawicielstw, a polscy *attachés* są akredytowani w 104 państwach (stan na 31 lipca 2021). W Polsce jest akredytowanych 51 *attachés* obrony z innych państw (stan na 31.07.2021). W ostatnich latach nowe polskie ataszaty powstały w Etiopii, w Azerbejdżanie i w Armenii. Współcześnie można dostrzec wyraźny trend tworzenia ataszatów regionalnych, które odpowiadają za kilka państw, oraz powstają w miejscach, gdzie jest ważne monitorowanie sytuacji bezpieczeństwa, a także nawiązanie lepszej współpracy obronnej. Główną tego przyczyną jest zainteresowanie sytuacją w regionie, natomiast stosunki wojskowe z poszczególnymi państwami są ograniczone. Nie bez znaczenia są także oszczędności finansowe. Regionalne zadania powierzono m.in. polskiemu ataszatowi w Brazylii (2010 r.). Placówka składa się z 3 osób, a odpowiada za kontakty z całą Ameryką Południową. Ataszat regionalny powstał także w Arabii Saudyjskiej (2013 r.) i obejmuje także Zjednoczone Emiraty Arabskie i Katar. Jest to region szczególnie ważny ze względu na sytuację na Półwyspie Arabskim, w Iraku czy w Syrii. Praktyka pokazała, że powstanie ataszatu w Arabii Saudyjskiej znacznie ożywiło współpracę wojskową między państwami, a promowanie rodzimego przemysłu obronnego staje się opłacalne zwłaszcza wtedy, gdy państwa położone w rejonie sporo inwestują w obronność. W 2008 r. reaktywowano

także polski ataszat w Finlandii. Zdecydowała o tym m.in. współpraca polskich zakładów zbrojeniowych z fińską Patrią przy produkcji transporterów opancerzonych „Rosomak", budowanych w Polsce na fińskiej licencji. W 2015 r. powołano ponadto przedstawicielstwo wojskowe w Etiopii. Zdecydowały o tym udział naszego kraju w misjach UE oraz obecność wojskowa w Czadzie i w Republice Środkowoafrykańskiej. Szczególnym ataszatem jest ten na Ukrainie. Jego obecne zadania polegają nie tylko na monitorowaniu sytuacji w tym kraju, lecz także na poszukiwaniu możliwości udzielenia pomocy Ukraińcom m.in. w tworzeniu służby zdrowia. Obserwuje się także łączenie ataszatów i powierzanie placówce w jednym kraju zadań obejmujących także sąsiednie państwa.

Gdy zlikwidowano polską placówkę w Brukseli, powstał ataszat krajówBeneluksu (Belgii, Holandii, Luksemburga) z siedzibą w Hadze. Ponieważ jednym z istotniejszych zadań ataszatów jest wspieranie polskich kontyngentów wojskowych w sferze dyplomatyczno-organizacyjnej oraz informacyjnej, powołano takie placówki w Afganistanie i Pakistanie – z uwagi na fakt, że Polska brała udział w operacji ISAF. Podobna sytuacja miała miejsce podczas interwencji w Iraku – ataszat w tym kraju wzmocniono o stanowisko zastępcy, ponieważ uznano, że po wycofaniu polskich wojsk rozwinie się współpraca między resortami obrony.

Szczególnie ważną rolę w ramach służby zagranicznej pracującej na rzecz bezpieczeństwa odgrywa Stałe Przedstawicielstwo RP przy NATO, na bieżąco uczestniczące w procesach decyzyjnych Sojuszu Północnoatlantyckiego. Ważne zadania na rzecz bezpieczeństwa realizuje także Stałe Przedstawicielstwo RP przy Unii Europejskiej.

Sabina Olszyk

L. Drab, *Dyplomacja obronna w procesie kształtowania bezpieczeństwa RP*, Difin, Warszawa 2018; R. Kupiecki, *Attaché obrony i jego środowisko pracy*, „Dyplomacja Obronna" 2016, t. 1; K. Mularczyk, *Znaczenie ataszatów wojskowych we współczesnej polityce zagranicznej Rzeczypospolitej Polskiej*, „Rocznik Bezpieczeństwa Międzynarodowego" 2017, vol. 11, nr 1; S. Olszyk, *Attaché obrony – rola i zadania w działaniach na rzecz bezpieczeństwa*, [w:] *Współczesna polityka bezpieczeństwa. Aspekty polityczne, gospodarcze i militarne*, t. 2, M. Delong, M. Malczyńska-Biały (red.), Wydawnictwo Uniwersytetu Rzeszowskiego, Rzeszów 2018; Ustawa z dnia 27 lipca 2001 r. o służbie zagranicznej, Dz.U. 2001, nr 128, poz. 1403; Zarządzenie ministrów spraw zagranicznych i obrony narodowej z dnia 27 maja 2004 r. w sprawie szczególnych zasad wykonywania obowiązków służbowych przez żołnierzy zawodowych pełniących służbę w placówkach zagranicznych oraz organizacji i funkcjonowania w placówkach zagranicznych ataszatów obrony, Dz.Urz. MSZ 2004, nr 3, poz. 28, oraz Dz.Urz. MON 2004, nr 6, poz. 57.

AUDYT BEZPIECZEŃSTWA INFORMACJI – zaplanowana, celowa, systematyczna i kompleksowa analiza poziomu → b e z p i e c z e ń s t w a → i n f o r m a c j i [t. 2] w organizacji. Podczas audytu bezpieczeństwa informacji analizowane są zarówno rozwiązania techniczne i organizacyjne, jak i procesy i zachowania

informacyjne, które wpływają na bezpieczeństwo informacji. Audyt bezpieczeństwa informacji jest istotnym narzędziem zarządzania bezpieczeństwem informacji (czyli zespołu działań obejmujących planowanie, organizowanie i kontrolowanie → p r o c e s ó w i n f o r m a c y j n y c h [t. 3], obejmujących m.in. generowanie, gromadzenie, przechowywanie, transmisję, transformację, udostępnianie, interpretację i wykorzystywanie informacji).

Celem audytu jest:

- sprawdzenie, czy system zarządzania bezpieczeństwem informacji w organizacji spełnia wymagania bezpieczeństwa ustalone przez daną organizację, jest zgodny z wymogami norm (np. międzynarodowych), wymogami prawa lub wymogami podmiotów trzecich (np. współpracujących firm, partnerów organizacji, dostawców, klientów itd.);
- ustalenie, czy sam system zarządzania bezpieczeństwem informacji jest odpowiednio wdrożony;
- zidentyfikowanie obszarów (technicznych, organizacyjnych) wpływających na poziom bezpieczeństwa, które wymagają udoskonalenia.

Audyt powinien obejmować analizę wszystkich elementów systemu zarządzania bezpieczeństwem informacji, w tym analizę polityki bezpieczeństwa informacji, klasyfikację i kontrolę aktywów, bezpieczeństwa osobowego, fizycznego i środowiskowego w kontekście → b e z p i e c z e ń s t w a i n f o r m a c y j n e g o , zarządzanie systemami informatycznymi i sieciami komputerowymi oraz kontroli dostępu. Podczas badania poszczególnych elementów systemu zarządzania bezpieczeństwem informacji analizie podlega:

- Polityka bezpieczeństwa informacji (PBI) – czyli dokument (lub ew. kilka dokumentów) zawierający zbiór zaleceń, reguł i wytycznych postępowania, których przestrzeganie ma na celu zapewnienie odpowiedniego poziomu bezpieczeństwa informacji w organizacji. Podczas analizy tego elementu systemu sprawdzane jest m.in. to, czy w ogóle taka polityka została opracowana, czy dokument został udostępniony pracownikom oraz czy został przeczytany, czy sposób opracowania dokumentu jest jasny, zwięzły i zrozumiały, czy polityka zawiera podział odpowiedzialności i kompetencje pracowników (szczególnie w zakresie bezpieczeństwa informacji i zarządzania procesami informacyjnymi), czy obejmuje opis mechanizmów i terminarz wdrażania kolejnych etapów zarządzania bezpieczeństwem informacji, czy sam dokument zawiera opis wszystkich niezbędnych elementów infrastruktury bezpieczeństwa, odpowiedzialności, zadań poszczególnych osób, autoryzacji urządzeń do przetwarzania informacji, analizy, czy konieczne jest zatrudnienie kogoś z zewnątrz, współpracy między jednostkami, przeglądu stanu bezpieczeństwa, zabezpieczeń przed dostępem osób z zewnątrz organizacji, wymogów bezpieczeństwa w zawieranych umowach, przetwarzania danych przez firmy zewnętrzne. Ważne jest również sprawdzenie, czy PBI nie zawiera zbyt

szczegółowych informacji o zastosowanych rozwiązaniach technicznych, których ujawnienie mogłoby zwiększyć ryzyko naruszenia bezpieczeństwa informacji.

- Klasyfikacja i kontrola aktywów – podczas przeprowadzania audytu konieczne jest sporządzenie spisu inwentarzowego zawierającego wykaz:
  - aktywów informacyjnych (takich jak: dane, pliki, nośniki, procedury związane z bezpieczeństwem informacji, plan ciągłości działania organizacji w → s y t u a c j a c h k r y z y s o w y c h [t. 4], procedury awaryjne, materiały szkoleniowe, kopie zapasowe itp.),
  - aktywów oprogramowania (m.in. oprogramowanie, za pomocą którego zapisywane i przechowywane są dane, systemy operacyjne, systemy zabezpieczające, oprogramowanie biurowe, oprogramowanie specjalistyczne),
  - aktywów fizycznych (m.in. sprzęt komputerowy, serwery, urządzenia peryferyjne, np. drukarki i skanery, nośniki danych, np. dyski i płyty, ale także pomieszczenia i meble),
  - usług (usługi związane z przekazywaniem danych i informacji, usługi pomocy technicznej, np. klimatyzacja, oświetlenie, system ogrzewania).

  Po sporządzeniu spisu konieczne są nadanie ważności zidentyfikowanym aktywom (czyli określenie, które aktywa są szczególnie istotne dla funkcjonowania organizacji), analiza potrzeb użytkowników aktywów oraz ustalenie poziomu wykorzystania aktywów (czyli kto, w jakim czasie i w jakim celu korzysta z aktywów/informacji; analiza, które aktywa są niezbędne do wykonywania obowiązków służbowych). Badanie wykorzystania aktywów może być szczególnie pomocne w przypadku wykrycia nadużyć lub naruszeń bezpieczeństwa informacji. Dzięki takim zapisom można ustalić m.in. to, kto i kiedy korzystał z zasobów, jaki był cel wykorzystania zasobów lub jakie były uprawnienia osoby korzystającej.
- Bezpieczeństwo osobowe – jednym z najsłabszych elementów systemu bezpieczeństwa informacji jest człowiek i jego działalność, dlatego podczas prowadzenia audytu należy sprawdzić aspekty wpływające na odpowiedni poziom bezpieczeństwa osobowego. W trakcie audytu analizuje się m.in. to, czy umowy o pracę precyzują procedury bezpieczeństwa informacyjnego oraz czy zawierają one klauzule o zachowaniu poufności i tajemnicy firmowej, czy opisy obowiązków służbowych zawierają dane o zakresie dostępu do informacji, czy uprawnienia dostępu do informacji są faktycznie dostosowane do obowiązków danego pracownika, czy dana osoba ma dostęp tylko do tych informacji, które są niezbędne do wykonywania jej obowiązków, czy system rekrutacji pracowników zawiera elementy sprawdzania, czy kandydat jest podatny na celowe lub przypadkowe naruszenia bezpieczeństwa informacji, czy prowadzone są szkolenia dla pracowników z zakresu bezpieczeństwa informacji oraz jaka jest ich tematyka, czy pracownicy są świadomi sankcji za naruszenia bezpieczeństwa informacji, czy pracownicy wiedzą, jak reagować na naruszenia bezpieczeństwa informacji, niewłaściwe funkcjonowanie

oprogramowania lub systemu bezpieczeństwa i gdzie takie naruszenia bądź nieprawidłowe funkcjonowanie zgłaszać, jak wygląda system zgłaszania naruszeń i błędów (i czy w ogóle jest) oraz jak wygląda procedura postępowania dyscyplinarnego w przypadku wykrycia naruszeń spowodowanych przez pracowników.

- Bezpieczeństwo fizyczne i środowiskowe – obejmuje wszelkie zabezpieczenia budynków, pomieszczeń, szaf, w których przechowuje się dokumenty itd. Podczas audytu analizie podlega funkcjonowanie fizycznego obwodu zabezpieczającego, w tym m.in. kart magnetycznych, alarmów, bramek z wykrywaczami metali, wzmocnionych ścian, zabezpieczeń biometrycznych, recepcji ze strażnikiem; należy także sprawdzić, czy strategiczne pomieszczenia, np. serwerownia, zawierają odpowiednie zabezpieczenia (np. kraty w oknach, wzmocnione drzwi, silne zamki lub systemy na karty, zabezpieczenia biometryczne, odpowiednią klimatyzację, szczelny sufit, niepalne wykładziny). Konieczna jest też kontrola osób, które mają dostęp do zasobów firmy, np. czy osoby wchodzące do budynku są weryfikowane i jeśli tak, to w jaki sposób, czy pracownicy korzystają z identyfikatorów, czy w biurach mogą przebywać osoby trzecie, czy są specjalne pomieszczenia do przyjmowania gości. Oprócz tego sprawdza się, czy kontrolowane są urządzenia peryferyjne (takie jak drukarki, faksy i ksero), czy okna i drzwi są zamykane po opuszczeniu pomieszczenia, czy kopie zapasowe są przechowywane w odpowiedni sposób, czy pracownicy wiedzą o istnieniu obszarów bezpiecznych w organizacji, czy lokalizacja sprzętu jest odpowiednia (czy np. nie ma ryzyka zniszczenia), czy sprzęt jest nadzorowany, czy sprzęt jest zabezpieczony przed kradzieżą, pożarem, zalaniem, drganiami, dymem, materiałem wybuchowym, czy pracownicy spożywają posiłki przy sprzęcie, jakie są zabezpieczenia zasilania i okablowania, czy jest zasilanie awaryjne, czy sprzęt jest odpowiednio konserwowany, czyszczony itd., kto zajmuje się konserwacją, jak często, jak wygląda kwestia pracy w domu na sprzęcie służbowym, czy dane z dysków są usuwane przed sprzedażą lub utylizacją używanego sprzętu, czy w organizacji wprowadzono politykę czystego biurka i czystego ekranu, jak wygląda polityka wynoszenia sprzętu poza siedzibę firmy.
- Zarządzanie systemami informatycznymi i sieciami komputerowymi – analiza tych elementów obejmuje analizę obsługi i zarządzania systemami informatycznymi i sieciami w danej organizacji oraz samego funkcjonowania systemów i sieci. Podczas audytu analizowana jest działalność obsługi technicznej, sprawdza się, czy jest prowadzona dokumentacja wszystkich zmian w systemach (np. aktualizacje oprogramowania, wgranie nowych programów lub aplikacji, modyfikacje funkcjonowania systemów) oraz czy dokumentowane są wszelkie błędy systemów, błędy działania aplikacji, awarie itd., czy są opracowane procedury reagowania na naruszenia (np. w przypadku odmowy dostępu do systemu albo naruszenia dostępności, poufności i integralności informacji), czy pojemności dysków są odpowiednie, czy pracownicy są przeszkoleni z użytkowania nowego systemu, jak wygląda ochrona

przed szkodliwym oprogramowaniem (np. czy pracownicy korzystają tylko z legalnego oprogramowania, czy przeprowadzane są niezbędne i regularne aktualizacje, czy na wykorzystywanym sprzęcie jest zainstalowane oprogramowanie antywirusowe, czy są wykonywane przeglądy oprogramowania), czy tworzone są kopie zapasowe danych i dokumentów, kto ma dostęp do sieci oraz jak zarządza się nośnikami danych (np. gdzie przechowuje się płyty CD z danymi, czy i w jaki sposób nośniki są niszczone w przypadku, gdy nie są już wykorzystywane).

- Kontrola dostępu do systemu – dotyczy analizy polityki kontroli dostępu do systemu i bezpośrednio do informacji. Analiza podczas audytu obejmuje sprawdzenie m.in. tego, czy użytkownicy systemów mają odpowiednio określone prawa do informacji, jak wygląda system rejestracji nowych użytkowników w systemach, system budowania haseł dostępu i wylogowywania użytkowników, jak wygląda mechanizm zabierania pracownikom uprawnień do kont (np. w przypadku zwolnienia lub urlopu), jak wygląda system logowania oraz system uwierzytelniania użytkowników podczas pracy zdalnej albo poza siedzibą firmy, czy ograniczono czas trwania sesji logowania, czas trwania połączenia i czy wprowadzono automatyczne zamknięcie systemu po upływie tego czasu lub w przypadku bezczynności użytkownika, jak wygląda procedura pozostawiania sprzętu bez opieki (np. podczas przerw pracowników, nieobecności pracownika przy biurku lub w pomieszczeniu), czy stosuje się podpisy cyfrowe bądź szyfrowanie i jeśli tak, to w jakich sytuacjach, kiedy takie podpisy i mechanizmy szyfrowania są wymagane lub stosowane. Należy także przeanalizować procesy zarządzania ciągłością działania w sytuacji krytycznej (np. w przypadku wystąpienia awarii sprzętu komputerowego czy serwerów, awarii zasilania lub klęski żywiołowej).

Każda zidentyfikowana podczas audytu niezgodność z ustalonymi wcześniej wymaganiami albo odkryte naruszenie bezpieczeństwa muszą zostać odpowiednio udokumentowane i wyjaśnione.

Specyficzną odmianą audytu bezpieczeństwa informacji jest audyt certyfikacyjny (np. obejmujący analizę zgodności systemu zarządzania bezpieczeństwa informacji z normą PN-EN ISO/IEC 27001:2017-06 – wersja polska lub analizę zabezpieczeń informatycznych wg normy PN-ISO/ IEC 15408).

Zalecane jest, aby audyt bezpieczeństwa informacji przeprowadzany był cyklicznie. Zgodnie z Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych podmioty publiczne w Polsce mają obowiązek przeprowadzenia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji nie rzadziej niż raz w roku. Rozporządzenie zezwala także podmiotom publicznym na tworzenie systemu zarządzania bezpieczeństwem informacji na podstawie normy PN-ISO/IEC 27001. Wykaz elementów określonych w rozporządzeniu, które należy uwzględnić w systemie zarządzania bezpieczeństwem informacji

w podmiotach publicznych, może stanowić podstawę do sporządzenia listy elementów podlegających analizie podczas prowadzenia audytu bezpieczeństwa informacji. Według wskazanego dokumentu zarządzanie bezpieczeństwem informacji ma być realizowane poprzez:

- zapewnienie aktualizacji zasad bezpieczeństwa obowiązujących wewnątrz podmiotu,
- przeprowadzanie inwentaryzacji sprzętu i oprogramowania, służących do przetwarzania informacji,
- przeprowadzanie analiz ryzyka utraty atrybutów bezpieczeństwa informacji,
- nadawanie (i w razie potrzeby aktualizowanie) pracownikom odpowiednich uprawnień do przetwarzania informacji,
- organizowanie szkoleń w zakresie bezpieczeństwa informacji (np. dotyczących naruszeń, odpowiedzialności prawnej za naruszenia),
- zapewnienie ochrony informacji przed np. kradzieżą lub nieuprawnionym dostępem oraz zabezpieczenie informacji przed nieuprawnioną ingerencją (np. jej usunięciem albo zniszczeniem),
- ustanowienie zasad pracy z urządzeniami mobilnymi i pracy zdalnej,
- zapewnienie odpowiedniego poziomu bezpieczeństwa systemów teleinformatycznych (np. poprzez aktualizację oprogramowania, odporność na awarie, stosowanie mechanizmów kryptograficznych),
- wprowadzenie systemu raportowania incydentów naruszenia bezpieczeństwa informacji,
- przeprowadzanie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji.

Audyt może być prowadzony przez audytorów z firmy zewnętrznej (audyt zewnętrzny) lub powołanych do tego zadania przedstawicieli danej organizacji (audyt wewnętrzny). Oba rozwiązania charakteryzują się pozytywnymi i negatywnymi cechami, a wybór między nimi musi być ściśle powiązany z potrzebami i specyfiką organizacji. W literaturze przedmiotu podkreśla się, że audyt zewnętrzny łączony jest z większą obiektywnością i niezależnością wyników. Audyt prowadzony jest zazwyczaj w kilku etapach, które obejmują:

- inicjowanie audytu i analizę dokumentacji organizacyjnej i technicznej (czyli ustalenie stanu obowiązującego w zakresie bezpieczeństwa informacji),
- przygotowanie i przeprowadzenie działań audytowych (czyli ustalenie stanu faktycznego),
- udokumentowanie przebiegu i efektów audytu (w tym sporządzenie raportu z audytu),
- zakończenie audytu i działania poaudytowe.

Co istotne, po zakończeniu audytu następuje przeprowadzenie działań poaudytowych, czyli m.in. skorygowanie odnalezionych nieprawidłowości, wdrożenie zaleceń

sformułowanych podczas audytu, przeprowadzenie szkoleń dla pracowników oraz zaplanowanie dalszych działań zwiększających poziom bezpieczeństwa informacyjnego w organizacji. Raport poaudytowy powinien zawierać listę konkretnych zaleceń/wytycznych dotyczących zwiększenia poziomu bezpieczeństwa informacji. W trakcie planowania audytu nie powinno się pomijać etapu przygotowawczego, w którym określane są cele audytu, wykorzystywane narzędzia i techniki zbierania danych, budżet finansowy i budżet czasu, wskazywane są również osoby odpowiedzialne za prowadzenie działań audytowych.

Podczas etapu przygotowawczego konieczne jest także zyskanie przychylności i poparcia wśród pracowników i kierownictwa organizacji.

Wśród metod i technik zbierania informacji w trakcie prowadzenia audytu znajdują się m.in. wywiady, rozmowy i spotkania z pracownikami, badania ankietowe, prowadzenie grup fokusowych, obserwacje działań, warunków i środowiska procesów informacyjnych, analiza dokumentów (np. instrukcji, opisów procedur, licencji, sprawozdań ze spotkań, zapisów pomiarów, polityk), analiza innych informacji (np. informacji zwrotnych od klientów), analiza zawartości posiadanych lub prowadzonych przez organizację baz danych i stron internetowych.

Wyniki audytu mogą zostać wykorzystane do opracowania skutecznej polityki bezpieczeństwa informacji.

Paulina Motylińska

M. Hajder, L. Hajder, *Innowacyjna Gmina: Audyt bezpieczeństwa informacyjnego*, Wyższa Szkoła Informatyki i Zarządzania w Rzeszowie, Rzeszów 2018; J. Janczak, A. Nowak, *Bezpieczeństwo informacyjne: wybrane problemy*, AON, Warszawa 2013; A. Jezierska, A. Koziara, *Audyt wewnętrzny a bezpieczeństwo informacji*, [w:] *Bezpieczeństwo informacyjne w dyskursie naukowym*, H. Batorowska, E. Musiał (red.), Uniwersytet Pedagogiczny im. KEN w Krakowie, Kraków 2017; J. Łuczak, M. Tyburski, *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001*, Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu, Poznań 2010; A. Myśko, E. Młodzik, *Bezpieczeństwo informacji – dylematy związane z realizacją obowiązku prowadzenia audytu wewnętrznego w jednostkach sektora finansów publicznych*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Finanse, Rynki Finansowe, Ubezpieczenia" 2014, nr 833 (72); Norma PN-EN ISO/IEC 27001:2017-06 – wersja polska; Norma PN-ISO/IEC 15408 – wersja polska; A. Nowak, W. Scheffs, *Zarządzanie bezpieczeństwem informacyjnym*, AON, Warszawa 2010; M. Pałęga, M. Knapiński, *Audyt zgodności z normą ISO/IEC 27001: 2013 jako narzędzie diagnozy i doskonalenia systemu zarządzania bezpieczeństwem informacji w przedsiębiorstwie*, [w:] *Innowacje w zarządzaniu i inżynierii produkcji*, t. 2, R. Knosal (red.), Oficyna Wydawnicza PTZP, Opole 2016; T. Polaczek, *Audyt bezpieczeństwa informacji w praktyce*, Wydawnictwo Helion, Gliwice 2006.

AUDYT BEZPIECZEŃSTWA OBIEKTU – zespół obiektywnych działań, których celem jest zweryfikowanie i podniesienie poziomu → b e z p i e c z e ń s t w a [t. 1] w zakresie funkcjonowania danego obiektu. Audyt ma zestawić stan wymagany ze stanem faktycznym kontrolowanego obszaru. Metodę tę stosowano już w czasach starożytnych przez porównywanie zapisów zawartych w księgach rachunkowych ze stanem rzeczywistym,który powinien je odzwierciedlać.

Audyt bezpieczeństwa obiektu to zespół aktywnych procesów polegających na weryfikacji funkcjonowania procedur oraz zabezpieczeń. Działania te obejmują:

- scharakteryzowanie obiektu,
- obserwację obiektu,
- oględziny całego obiektu,
- rozmowy z użytkownikami obiektu (najemcami lub ich przedstawicielami),
- rozmowy z przedstawicielami administratora obiektu,
- rozmowy z pracownikami ochrony,
- analizę dokumentacji ochronnej.

Posługując się wskazanymi narzędziami badawczymi, można przeprowadzić rzetelny audyt, pozwalający określić błędy i uchybienia, które negatywnie rzutują na bezpieczeństwo obiektu. Do najczęściej spotykanych niebezpieczeństw należą:

- atak aktywnego strzelca,
- podłożenie ładunku wybuchowego,
- rozpylenie toksycznej substancji,
- zamach przy użyciu pojazdu,
- zatrucie żywności,
- zagrożenia kryminalne – kradzież rozbójnicza, kradzież z włamaniem, niszczenie mienia, akty wandalizmu,
- stalking,
- zagrożenia dla życia i zdrowia (będące i niebędące wynikiem działania czynnika ludzkiego),
- zagrożenia związane z działaniami sił natury – wszelkiego rodzaju →klęski żywiołowe [t. 5], pożary,
- zagrożenia związane z atakami przy użyciu bojowych środków trujących (BŚT) i toksycznych środków przemysłowych (TŚP),
- zagrożenia związane ze zdarzeniami typu ROTA (uwolnienie toksycznych substancji w wyniku zdarzenia innego niż atak),
- zagrożenia związane z zaistnieniem aktów terroru kryminalnego,
- nieuprawnione wejście (infiltracja),
- nieuprawniona penetracja terenu chronionego,
- szpiegostwo przemysłowe,
- zagrożenia ekologiczne,
- awarie techniczne,
- ataki terrorystyczne,
- zagrożenia epidemiologiczne.

Przy wykonywaniu audytu bezpieczeństwa należy wziąć pod uwagę prognozowanie zagrożeń dla danego obiektu. Podstawowymi czynnikami mającymi bezpośredni wpływ na charakter potencjalnych zagrożeń są:

- warunki lokalizacyjne,

- charakter danego obiektu i profil jego działalności,
- teren zewnętrzny – otoczenie,
- teren wewnętrzny.

To specyfika obiektów definiuje rodzaj i charakter zagrożeń, jakie mogą wystąpić na jego terenie. Inne rodzaje niebezpieczeństw zagrażają bankom, a zupełnie inne będą dotyczyć zakładów produkcyjnych czy obiektów z obszaru → i n f r a s t r u k t u r y k r y t y c z n e j [t. 2]. Oznacza to, że prawdopodobieństwo wystąpienia konkretnych zagrożeń będzie większe dla jednego rodzaju podmiotów niż dla innego. Ponadto ten sam rodzaj obiektów może być narażony na odmienne niebezpieczeństwa ze względu na lokalizację. Przykładowo inne → z a g r o ż e n i a [t. 4] mogą wystąpić na terenie jednostki położonej na obrzeżach dużej aglomeracji w otoczeniu zabudowy jednorodzinnej, a inne w wypadku obiektu usytuowanego w pobliżu lotniska czy zakładów produkcyjnych stosujących TŚP.

Badaniu audytowemu podlegają także:

- procedury ogólne obiektu,
- procedury poszczególnych najemców danego obiektu,
- dokumentacja prowadzona na terenie obiektu.

Konieczne jest zwrócenie uwagi na procedury czy regulaminy, które określają zasady korzystania z obiektu. Kontrolowane są zarówno procedury ogólne, definiujące codzienne funkcjonowanie obiektu, jak i procedury szczególne, np. → b e z p i e c z e ń s t w a i h i g i e n y p r a c y (BHP), ppoż., sanitarne na wypadek zdarzeń niestandardowych. Sprawdzeniu powinna również podlegać znajomość reguł ze strony użytkowników i administratorów obiektu oraz osób odpowiedzialnych za zapewnianie bezpieczeństwa w jego obrębie.

Kontrola obejmuje dokumentację związaną z funkcjonowaniem audytowanego obiektu. Dotyczy to książek: ewidencji ruchu osobowego, ruchu materiałowego, ewidencji kluczy i kart dostępu, ewidencji ruchu kołowego, ewidencji zdarzeń, instrukcji ochrony, instrukcji bezpieczeństwa pożarowego, planu ewakuacji, planu ochrony, instrukcji obiegu informacji, procedur powiadamiania, procedur współpracy.

Audyt powinien także uwzględniać godziny pracy obiektu oraz przepływ ruchu osobowego. Należy zweryfikować procedury identyfikacji uprawnień ogółu osób do przebywania na terenie danego obiektu, w tym funkcjonowanie systemu identyfikatorów i przepustek. Sprawdzenie obejmuje również awizację: gości, kontrahentów, kontraktorów, najemców. Przy dużym ruchu osobowym jest to istotny element kontroli przepływu osób wewnątrz budynków. Ma to bezpośredni związek z zagrożeniem przedostania się do obiektów i przebywania na ich terenie osób nieuprawnionych. W ramach audytu sprawdzeniu podlega monitoring wizyjny (*closed-circuit television*, CCTV). Jego kontrola powinna objąć rozmieszczenie, ustawienie (występowanie tzw. martwych punktów, czyli miejsc nieobjętych nadzorem poszczególnych kamer) i skonfigurowanie znajdujących się na terenie obiektu kamer. Należy zwrócić uwagę

na ich podłączenie do urządzeń rejestrujących. Trzeba sprawdzić, czy kamery stałe nie są zastępowane mniejszą liczbą kamer obrotowych, które powinny być stosowane przez obsługę stanowiska monitorowania CCTV jedynie jako wsparcie dla tych pierwszych – w sytuacji wykrycia zagrożenia wynikłego np. z pojawienia się na terenie obiektu osoby nieuprawnionej lub stwarzającej zagrożenie. Kamera obrotowa stanowi uzupełnienie, które umożliwia „podążanie za potencjalnym źródłem zagrożenia". Audyt powinien też dotyczyć umiejętności obsługi tych systemów przez osoby je nadzorujące. Pracownicy ochrony zatrudnieni na stanowiskach operatorów systemów telewizji przemysłowej powinni być przygotowani do korzystania z konkretnych rozwiązań wdrożonych w danym obiekcie, a także umieć odtwarzać zapisane zdarzenia i przełączać obrazy z poszczególnych kamer. Badaniu audytowemu podlega też ruch kołowy oraz procesy dostaw towarów. Dotyczy to weryfikacji uprawnień do wjazdu pojazdów kołowych na teren sprawdzanego obiektu, w tym: awizacji pojazdów dopuszczonych do wjazdu na jego teren, systemu przepustkowego oraz identyfikatorów tymczasowych. Audyt powinien również obejmować procedury związane z kontrolą wwożenia materiałów na teren obiektu i wywożenia ich poza jego rejon. Prawidłowość zachodzących w tym obszarze procesów ma bezpośredni związek z przeciwdziałaniem możliwości zaistnienia sytuacji kryminogennych – np. kradzieży z wykorzystaniem pojazdów czy zamachów przy ich użyciu.

Ważnym aspektem audytu jest sprawdzenie zabezpieczeń ppoż. oraz BHP. Weryfikowane są procedury postępowania na wypadek wystąpienia pożaru lub innego zagrożenia, jak również znajdująca się na obiekcie dokumentacja przeciwpożarowa (np. instrukcja bezpieczeństwa pożarowego). Kontroli poddawane jest: wyposażenie obiektu w sprzęt gaśniczy, urządzenia mające wpływ na bezpieczeństwo pożarowe oraz terminowość ich przeglądów. Audyt dotyczy również dróg pożarowych, obecności znaków bezpieczeństwa i ochrony przeciwpożarowej na terenie obiektu.

Kolejny ważny aspekt uwzględniany w trakcie audytu to system kontroli ruchu osobowego (SKD – system kontroli dostępu). Chodzi tu o weryfikację dostosowania SKD do wymagań obiektowych. Należy zwrócić uwagę, czy zamontowane na terenie obiektu techniczne urządzenia kontroli wstępu zapewniają odpowiednią płynność ruchu osobowego (niepowodowanie zatorów komunikacyjnych) przy jednoczesnym zachowaniu bezpieczeństwa dostępu i prawidłowości nadzoru. Ważne jest objęcie kontrolą dostępu miejsc szczególnie newralgicznych, takich jak: przyłącza wody, infrastruktura HVAC (*heating, ventilation, and air conditioning* – całość ogrzewania, wentylacji i klimatyzacji), pomieszczenia BMS (*building management system* – specjalne pokoje służące do zarządzania infrastrukturą i systemami budynku), pomieszczenia ochrony, serwerownie.

Audyt powinien objąć także elementy infrastruktury obiektu i system sygnalizacji włamania i napadu (SSWiN). Wiąże się to ze sprawdzeniem podłączenia do systemu alarmowego kluczowych punktów obiektu, takich jak: ciągi komunikacyjne, windy,

drzwi przeciwpożarowe i ewakuacyjne, drogi ewakuacji, pomieszczenia HVAC, BMS, elementy infrastruktury awaryjnej (hydranty, klapy oddymiające), parkingi, strefy dostaw, strefy wydzielone. Czynności te obejmują również kontrolę pracy grup interwencyjnych oraz działania urządzeń napadowych obsługiwanych przez ochronę danego obiektu. Sprawdzeniu powinien podlegać czas dojazdu grupy interwencyjnej – od załączenia urządzenia sygnalizującego zagrożenie do czasu powiadomienia grupy.

Kluczowym elementem audytu bezpieczeństwa obiektu jest zwrócenie uwagi na kwestię ochrony fizycznej. Należy przede wszystkim ustalić, czy obsada stanowiskowa pracowników ochrony fizycznej jest dostosowana do harmonogramu funkcjonowania danego obiektu – z uwzględnieniem tego, czy nie jest ona zmniejszana w godzinach nocnych mimo braku ograniczenia funkcjonowania obiektu w tej porze. Powinno się również ustalić, czy obsada etatowa pracowników ochrony jest wystarczająca do zapewnienia prawidłowego zabezpieczenia obiektu podczas wykonywanych asyst przy pracach serwisowych.

Należy sprawdzić realizowanie czynności obchodowych, szczególnie w godzinach nocnych. Weryfikacji podlega rodzaj urządzeń wykorzystywanych do ich kontroli. W wypadku urządzeń opartych na czytnikach odbijanych przy punktach kontrolnych w różnych miejscach obiektu pracownicy skupiają się na tym, by jak najszybciej zakończyć obchód. W wyniku tego odnotowywany jest jedynie sam fakt wykonania obchodu, a nie czas jego trwania czy jakość. Dlatego właściwie skonfigurowany system obchodowy powinien opierać się na urządzeniach rejestrujących trasę i czas trwania wykonywanego obchodu.

Sprawdzeniu podlegać powinny kwalifikacje posiadane przez pracowników ochrony zatrudnionych na terenie obiektu, z uwzględnieniem znajomości obiektu, wiedzy dotyczącej przysługujących im uprawnień, znajomości Ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia, Ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej, umiejętności udzielania → p i e r w s z e j p o m o c y [t. 3], posługiwania się przydzielonym sprzętem i wyposażeniem, znajomości języka angielskiego w stopniu komunikatywnym (jeżeli jest ona potrzebna z uwagi na specyfikę obiektu). Pracownicy powinni być okresowo poddawani szkoleniom w zakresie zarówno wymienionych kompetencji, jak i procedur obiektowych, co należy ewidencjonować. Wyposażenie pracowników ochrony to kolejna rzecz, na którą należy zwrócić uwagę. Konieczne jest, by było ono sprawne oraz odpowiednio dobrane do specyfiki obiektu.

Istotne jest ustalenie liczby firm ochrony świadczących usługi ochrony fizycznej na terenie badanego obiektu. Jeżeli jest to więcej niż jeden podmiot, należy sprawdzić, czy istnieją procedury współpracy między tymi firmami oraz między ochroną a najemcami i administracją.

Regularne prowadzenie czynności kontrolnych i audytowych w zakresie bezpieczeństwa obiektów ma wpływ na zarządzanie poziomem zagrożenia. W celu prowadzenia skutecznej profilaktyki oraz zwalczania zagrożeń niezbędne jest ich:

- określanie,
- definiowanie,
- prognozowanie możliwości ich wystąpienia.

Cykliczne wykonywanie audytów bezpieczeństwa obiektów jest niezbędne w celu właściwego ich zabezpieczenia. Przyczynia się to również do zmniejszenia ryzyka wystąpienia na terenie tych obiektów zamachów terrorystycznych czy też aktów terroru kryminalnego. Wynika to z faktu, że obiekty o wyeksponowanej → k u l t u r z e b e z p i e c z e ń s t w a [t. 2] są o wiele mniej atrakcyjne dla potencjalnych zamachowców.

Krzysztof Czop

E. Babuśka, *Audyt wewnętrzny w zarządzaniu przedsiębiorstwem*, [w:] *Controlling i audyt w usprawnianiu zarządzania*, K. Winiarska (red.), Kema, Szczecin 2005; Ł. Czekaj, A. Czop, M. Pietrzyk, *Międzynarodowe, regionalne i lokalne aspekty bezpieczeństwa*, Drukarnia Styl Anna Dura, Kraków 2018; A. Czop, K. Czop, *Poziom przygotowania wielkopowierzchniowych obiektów handlowych do zamachów terrorystycznych ze szczególnym uwzględnieniem ataków z użyciem broni chemicznej*, [w:] *Bezpieczeństwo antyterrorystyczne budynków użyteczności publicznej. Analiza – Diagnoza – Case Study*, B. Wiśniewska-Paź, M. Szostak, J. Stelmach (red.), Wydawnictwo Adam Marszałek, Toruń 2018; K. Czop, *Proponowane zmiany ukierunkowane na podniesienie bezpieczeństwa terrorystycznego na terenie dużych centrów biurowo – usługowych*, „Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate" 2021, nr 11(1); G. Gozdór, *Prywatyzacja bezpieczeństwa.Rola i miejsce prywatnego sektora ochrony w systemie bezpieczeństwa i porządku publicznego*, Wydawnictwo KUL, Lublin 2012; P. Mazur, *Terroryzm islamski*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć, Wydawnictwo Libron, Kraków 2018; Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia, Dz.U. 1997, nr 114, poz. 740; Ustawa z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej, Dz.U. 2013, poz. 628; O. Wasiuta, *ISIS, Państwo Islamskie*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; O. Wasiuta, S. Wasiuta, P. Mazur, *Państwo Islamskie ISIS. Nowa twarz ekstremizmu*, Difin, Warszawa 2018; *The New Oxford Dictionary of English*, J. Pearsall (ed.), Oxford University Press, Oxford 1998.

AUTORYTARYZM I NEOAUTORYTARYZM – pojęcia odnoszące się do → r e ż i m u [t. 3] politycznego, w którym władza jest w dużej mierze skoncentrowana w rękach jednej osoby lub niewielkiej grupy osób. Pierwsze pojęcie ma klasyczny charakter i od dekad obecne jest w naukach społecznych, drugie zaś pojawiło się już po ostatniej fazie demokratyzacji, gdy w wielu państwach świata uwidocznił się znaczący trend odchodzenia od tradycyjnej, liberalnej demokracji w stronę systemów niedemokratycznych. Na ogół autorytarny reżim zakłada, że stoi ponad prawem, a jego funkcjonowanie oparte jest przede wszystkim na osobowości i charyzmie pojedynczego przywódcy lub woli elity, która przejmuje władzę dla własnych celów. Autorytaryzm uznaje nieograniczony autorytet państwa i całkowite posłuszeństwo poddanych, a w niektórych wypadkach może prowadzić do → t o t a l i t a r y z m u [t. 4]. Inaczej niż w przypadku totalitaryzmu, państwo autorytarne nie niszczy porządku politycznego

ani nie charakteryzuje go eliminacja sfery prywatnej, w ramach autorytarnego państwa możliwe jest funkcjonowanie organizacji cieszących się pewną niezależnością od władzy państwa, jeśli nie negują całkowicie systemu politycznego. Do początku lat 60. XX w. istniała zasadnicza dychotomia w rozróżnianiu reżimów politycznych polegająca na określaniu ich albo mianem systemów demokratycznych, albo totalitarnych. Reżimy autorytarne były często traktowane jako typ reżimu totalitarnego. Jednak wraz z upadkiem III Rzeszy i reżimów totalitarnych po II wojnie światowej i w latach 50. XX w., a także późniejszą transformacją ZSRR autorytarne reżimy polityczne stały się dominującą formą niedemokratycznego sposobu sprawowania władzy w państwie.

Pierwszą teorię reżimów autorytarnych zaproponował J.J. Linz, wskazał on, jakie cechy odróżniają je od demokracji i reżimów totalitarnych. Reżimy autorytarne w 2. poł. XX w. zaczęły przyciągać większą uwagę obserwatorów życia politycznego w związku z pojawieniem się wojskowo-biurokratycznych reżimów autorytarnych w znacznej części Ameryki Łacińskiej, a po globalnym odrodzeniu się demokracji w latach 80. i 90., określanym przez S. Huntingtona „trzecią falą demokratyzacji", po wytworzeniu się jeszcze nowszego typu autorytaryzmu, tj. autorytaryzmu wyborczego. Jego charakterystyczną cechą pozostaje to, że sytuuje się w szarej strefie pomiędzy liberalnymi demokracjami a zamkniętymi reżimami, w których nie odbywają się nawet fasadowe wybory.

Pierwszą cechą konstytuującą autorytaryzm jest ograniczony pluralizm, który uwypukla jego odmienność od prawie nieograniczonego pluralizmu liberalnych demokracji i całkowitego braku pluralizmu w reżimach totalitarnych. Skala ograniczenia pluralizmu jest odmienna w różnych przypadkach i podtypach reżimów autorytarnych. Drugim elementem definiującym autorytarne reżimy jest mentalność, a nie silna ideologia. Zdaniem Linza w przeciwieństwie do bardziej sztywnej, systematycznej, racjonalnie rozwiniętej, utopijnej i wszechstronnej natury ideologii mentalność jest mniej systematycznym i bardziej amorficznym sposobem myślenia i odczuwania, bardziej emocjonalnym niż racjonalnym. Chociaż rozróżnienie to nie jest jednoznaczne, wskazać można, że w autorytaryzmach w centrum uwagi stawia się mniej lub bardziej niejednoznacznie rozwinięte wartości takie jak ojczyzna, naród, porządek, hierarchia, tradycja, rasa, pochodzenie etniczne i inne. Kluczową ich cechą polityczną jest to, że właśnie dlatego, że są one niejednoznaczne i nierozwinięte intelektualnie, tworzenie wokół nich szerszych koalicji politycznych w celu budowania podstaw reżimu jest znacznie łatwiejsze niż w przypadku precyzyjnych, rozwiniętych ideologii. Trzeci element konstytuujący autorytaryzm, brak szerokiej mobilizacji politycznej, stanowi o kolejnej zasadniczej różnicy w stosunku do reżimów totalitarnych. Cecha ta jest ściśle powiązana z poprzednią, ponieważ pod nieobecność ideologii trudno jest realizować skuteczną politykę mobilizacji i przyciągać zaangażowanych wyznawców, którzy chcieliby usilnie popierać reżim.

Fakt, iż reżimy autorytarne rozciągają się w szerokim obszarze pomiędzy tymi systemami politycznymi, które już nie są totalitaryzmami, a tymi, które jeszcze nie

są demokracjami, pozwala dostrzegać stopniowalny poziom autorytaryzmu, rozumiany jako zakres jego konsolidacji. Nieskonsolidowany autorytaryzm występuje wszędzie tam, gdzie czy to przez nieudolność rządzących, czy za ich przyzwoleniem istnieje możliwość działania opozycji, choć nie ma pełnej możliwości → a l t e r n a c j i w ł a d z y, a więc opozycja nie zajmie miejsca rządzących. Z kolei skonsolidowany autorytaryzm oznacza takie zbudowanie norm i wartości reżimu politycznego, by bezalternatywność polityczna, wyrażająca się w jednoznacznie określonym braku możliwości zmiany rządzących bez zgody obecnie sprawujących władzę, stanowiła kluczową cechę systemu politycznego. W XXI w. w wielu państwach cechujących się długimi tradycjami demokratycznymi, jak również w niektórych państwach Europy Środkowo-Wschodniej nastąpił znów powrót do idei rządów stawiających się ponad prawem, określany przez badaczy mianem neoautorytaryzmu. Jest on specyficznym reżimem cywilnym, w którym istnieją formalne instytucje demokratyczne i są one postrzegane jako podstawowy sposób sprawowania władzy, ale rządzący nadużywają instytucji państwa dzięki posiadanej przewadze nad politycznymi oponentami. Takie reżimy są konkurencyjne, ponieważ partie opozycyjne używają demokratycznych instytucji, aby poważnie zakwestionować władzę rządzących, ale nie są demokratyczne, ponieważ pole gry jest mocno wypaczone na korzyść sprawujących władzę. Konkurencja jest zatem realna, lecz niesprawiedliwa. Neoautorytaryzm pojawia się w różnych grupach państw z odmiennych przyczyn. W państwach Ameryki Łacińskiej, Afryki lub Azji może on stanowić rodzaj ułomnej demokracji albo etapu przejściowego od systemu autorytarnego do demokracji. W państwach Europy Środkowo-Wschodniej, takich jak Polska czy Węgry, przejawy autorytaryzmu tłumaczy się niedostatecznym poziomem konsolidacji demokracji. Zbyt krótkie tradycje demokratyczne prowadzą w tej grupie państw do trwających niekiedy dłuższy czas rządów populistów lub ugrupowań skrajnych, które wykorzystują nabyte w drodze wyborów możliwości sprawowania władzy do dokonania takich przekształceń systemu politycznego, by uniemożliwić realną alternację władzy podczas kolejnej elekcji. Tendencje prowadzące do neoautorytaryzmu obecne są jednak także w grupie państw określanych jako dojrzałe demokracje zachodnie. W tym przypadku badacze twierdzą, że ich przyczyną jest ogólny → k r y z y s [t. 2] demokracji, partii politycznych oraz wyborów. Te ostatnie ze święta demokracji przekształcają się niejednokrotnie w traumę demokracji. Wyborcy skłonni są głosować raczej przeciw rządzącym niż za określoną ideą czy koncepcją polityczną. Oczekiwania wyborców w państwach zachodnich wiodą w stronę rozwiązań populistycznych, skrajnych, niejednokrotnie główną motywacją głosujących jest rozczarowanie dotychczas rządzącymi, choć też kierunek oczekiwanych dążeń i zmian artykułowanych przez elektorat ma charakter antyideologiczny i trudny do bliższego określenia.

Neoautorytaryzm jest typem hybrydowego reżimu mającego istotne cechy zarówno demokracji, jak i autorytaryzmu. Odróżnia się od pełnego autorytaryzmu tym, że

istnieją kanały konstytucyjne, poprzez które grupy opozycyjne konkurują o władzę wykonawczą. Wybory odbywają się regularnie, a partie opozycyjne nie są prawnie zabronione. Działalność opozycyjna ma charakter jawny: partie opozycyjne mogą otwierać biura, rekrutować kandydatów i organizować kampanie, a politycy rzadko są zatrzymywani lub więzieni. Demokratyczne procedury mają więc wystarczające znaczenie dla grup opozycyjnych, aby traktować je poważnie jako arenę, na której można rywalizować o władzę. Tym, co odróżnia neoautorytaryzm od demokracji, jest jednak fakt, że istniejące nadużycia państwa dotykają wolnych wyborów oraz swobód obywatelskich.

W odniesieniu do wyborów wskazać można, że z jednej strony są one konkurencyjne, ponieważ główni kandydaci opozycji rzadko są wykluczani, partie opozycyjne są w stanie prowadzić kampanie wyborcze i nie występują masowe oszustwa. Z drugiej strony wybory często nie są wolne i prawie zawsze są niesprawiedliwe. W niektórych przypadkach dochodzi do manipulowania listami wyborców, wypełniania kart do głosowania lub fałszowania wyników, tak jak w Dominikanie w 1994 r. lub w Ukrainie w 2004 r. Chociaż takie oszustwo może zmienić wynik wyborów, to nie jest tak poważne, żeby sam akt głosowania był pozbawiony sensu. W systemach neoautorytarnych może dochodzić do zastraszania działaczy opozycji, wyborców i obserwatorów wyborów. Nadużycia te nie są jednak wystarczająco istotne ani usystematyzowane, aby uniemożliwić opozycji prowadzenie kampanii wyborczych.

W reżimach neoautorytarnych swobody obywatelskie są nominalnie gwarantowane i przynajmniej częściowo respektowane. Istnieją niezależne media, a grupy obywatelskie i opozycyjne mogą działać. Przez większość czasu mogą się swobodnie spotykać, a nawet protestować przeciwko rządowi, jednak wolności obywatelskie są często łamane. Opozycyjni politycy, niezależni sędziowie, dziennikarze, działacze na rzecz → p r a w c z ł o w i e k a [t. 3] i inni krytycy rządowi są narażeni na prześladowania, aresztowania, a nawet gwałtowne ataki. Niezależne media są często zastraszane, atakowane, rzadziej zaś zawieszane lub zamykane. W niektórych reżimach jawne represje, w tym aresztowanie liderów opozycji, zabijanie działaczy opozycji i gwałtowne represje wobec protestów są powszechne i spychają te reżimy na krawędź pełnego autorytaryzmu.

W najnowszych badaniach podkreśla się, że wzrost poparcia dla partii autorytarno-populistycznych we współczesnych wyborach zmobilizował opór zaniepokojonych jego potencjalnymi konsekwencjami dla liberalnej demokracji. Jak wskazują czołowi światowi politolodzy, P. Norris i R. Inglehart, skala konsekwencji zwycięstwa D. Trumpa w USA, liczba partii autorytarno-populistycznych, które wygrały wybory parlamentarne i prezydenckie w wielu państwach i wprowadziły swoich przedstawicieli do rządu, m.in. w Austrii, Szwajcarii, Nowej Zelandii, Norwegii, Finlandii, Czechach, Włoszech i Polsce, budzi zaniepokojenie. Od lat 80. XX w. głosowanie na partie autorytarno-populistyczne w Europie wzrosło do najwyższego poziomu odnotowanego od czasu II wojny światowej. Niezwykle trudno ocenić obecnie, jakie działania mogłyby

powstrzymać narastającą falę poparcia dla ugrupowań sceptycznych wobec dotychczasowego modelu demokracji liberalnej.

Jakub Idzik, Rafał Klepka

S. Babones, *The New Authoritarianism: Trump, Populism, and the Tyranny of Experts*, Polity Press, Cambridge 2018; E. Carter, *Right-wing Extremism/Radicalism: Reconstructing the Concept*, „Journal of Political Ideologies" 2018. vol. 23, iss. 2; S.P. Huntington, *The Third Wave: Democratization in the Late Twentieth Century*, University of Oklahoma Press, Norman 1993; R. Klepka, *Autorytaryzm*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; tenże, *Neoautorytaryzm*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; tenże, *Neoautorytaryzm – w poszukiwaniu specyficznych cech reżimów politycznych sytuujących się między demokracją a autorytaryzmem*, „Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate" 2018, nr 8; tenże, *Parlament w państwie federalnym na przykładzie Austrii, Belgii, Niemiec i Szwajcarii*, Wydawnictwo Sejmowe, Warszawa 2013; S. Levitsky, L. Way, *Competitive Authoritarianism: Hybrid Regimes After the Cold War*, Cambridge University Press, Cambridge 2010; J.J. Linz, *Totalitarian and Authoritarian Regimes*, Lynne Rienner, Boulder 2000; B. Margulies, *Falling in with the Wrong Crowd: Linkage in the Age of Populism*, „Canadian Foreign Policy Journal" 2018, vol. 25, iss. 1; P. Norris, R. Inglehart, *Cultural Backlash: Trump, Brexit, and Authoritarian Populism*, Cambridge University Press, Cambridge 2019; G. Palmer, *Europe 2016: The Rhetoric of Unity and the Rise of Neo-Authoritarianism*, „The European Legacy" 2017, vol. 22, iss. 7–8; E. Özbudun, *Authoritarian Regimes*, [w:] *International Encyclopedia of Political Science*, B. Badie, D. Berg-Schlosser, L. Morlino (eds.), Sage, Los Angeles 2011.

AZYL – udzielenie schronienia przed prześladowaniem cudzoziemcowi lub bezpaństwowcowi przez państwo, na którego terytorium dana osoba przebywa.

Początki instytucji azylu sięgają starożytnej Grecji, w której osoby poszukiwały schronienia w miejscach kultu religijnego. Zgodnie z ówcześnie panującymi wierzeniami, takie miejsca podlegały ochronie bogów i dlatego nikt nie miał prawa wyrządzić krzywdy ludziom tam przebywającym. Prawo azylu nie przysługiwało osobom, które popełniły umyślną zbrodnię, oraz uciekinierom. W Rzymie obowiązywały azyl kościelny oraz azyl cesarski, przy czym ten ostatni był związany z istotą kultu cesarza, a nie – z instytucją polityczną: miejscem schronienia okazywała się świątynia wznoszona na cześć władcy bądź jego statua, a ochronie podlegali m.in. niewolnicy uciekający przed złym traktowaniem przez właścicieli. W takiej sytuacji konsekwencją azylu stawało się zobowiązanie do sprzedaży niewolnika.

Instytucja azylu religijnego funkcjonowała w starożytności i średniowieczu. W 1538 r. zniesiono go we Francji, w 1570 r. – w Hiszpanii, a w 1625 – w Anglii. Tworzenie azylu w kościołach było elementem prawa kanonicznego. Świeckie podstawy azylu terytorialnego wyprowadzone z prawa natury i wojen religijnych opracowali Hugo Grocjusz i Emerich de Vattel. Prawo azylu w wymiarze politycznym zostało wyartykułowane po raz pierwszy w konstytucji jakobińskiej z 1793 r., która stanowiła o fakcie udzielania przez naród francuski azylu cudzoziemcom, których w imię wolności wygnano z ojczyzny, i o odmowie udzielenia azylu tyranom.

Po II wojnie światowej prawo do ubiegania się o azyl i korzystania z niego w innych krajach zostało literalnie ujęte w art. 14(1) Powszechnej deklaracji praw człowieka z 1948 r. Zgodnie z art. 14(2) „Na prawo to nie można się powoływać w razie ścigania dotyczącego w istocie przestępstw pospolitych (ang. *non-political crimes*; franc. *un crime de droit commun*) albo działań sprzecznych z celami i zasadami Narodów Zjednoczonych". Deklaracja nie ma charakteru prawnie wiążącego, dlatego też jednostce nie przysługuje prawo roszczenia w tym względzie. Do instytucji azylu nawiązują Akt końcowy Konferencji Pełnomocników ONZ i preambuła konwencji dotycząca statusu → u c h o d ź c y z 1951 r. Mimo że w obu tych dokumentach wspomina się o azylu, to jednak ani konwencja, ani protokół dodatkowy do konwencji z 1967 r. nie formułują prawa przyznawania azylu. O zachowanie polityki azylowej w myśl Powszechnej deklaracji → p r a w c z ł o w i e k a [t. 3], a także Deklaracji o azylu terytorialnym z 14 grudnia 1967 r., apeluje natomiast Wysoki Komisarz ONZ ds. Uchodźców.

Azyl terytorialny polega na zezwoleniu przez dane państwo na wjazd i pobyt na jego terytorium cudzoziemca lub bezpaństwowca, zasadniczo z wyłączeniem ekstradycji takiej osoby. Z kolei azyl dyplomatyczny oznacza udzielenie schronienia na terenie placówki dyplomatycznej danego państwa. W świetle Deklaracji o azylu terytorialnym udzielenie azylu stanowi pokojowy i humanitarny akt działania państwa. Państwa w swoich praktykach – „bez uszczerbku dla istniejących instrumentów dotyczących azylu oraz statusu uchodźców i bezpaństwowców" – powinny m.in.:

- szanować azyl przyznany przez państwo w ramach wykonywania jego suwerenności, osobom uprawnionym do powoływania się na art. 14 Powszechnej deklaracji praw człowieka, w tym – osobom walczącym z kolonializmem;
- mieć na uwadze, że na prawo do ubiegania się o azyl i do korzystania z niego nie może powoływać się żadna osoba, w stosunku do której istnieją poważne powody, aby sądzić, że dopuściła się ona zbrodni przeciwko pokojowi, → z b r o d n i w o j e n n e j [t. 4] lub → z b r o d n i p r z e c i w k o l u d z k o ś c i [t. 4] w rozumieniu międzynarodowych instrumentów opracowanych w celu zabezpieczenia przed takimi przestępstwami;
- odpowiadać za ocenę podstaw udzielenia azylu;
- indywidualnie lub wspólnie lub za pośrednictwem ONZ rozważyć odpowiednie środki w celu zmniejszenia ciężaru państwa, którenapotyka trudności w udzieleniu lub w dalszym udzielaniu azylu;
- nie zezwalać osobom, którym przyznały azyl, na prowadzenie działalności sprzecznej z celami i zasadami ONZ.

Deklaracja stanowi jednocześnie, że osoby uprawnione do powoływania się na art. 14 Powszechnej deklaracji praw człowieka nie mogą być odesłane z granicy lub – jeżeli już wjechały na terytorium, na którym ubiegają się o azyl – na wydalenie lub przymusowy powrót do jakiegokolwiek państwa, w którym mogą być prześladowane,

z wykluczeniem sytuacji →za g r o ż e n i a [t. 4] →b e z p i e c z e ń s t w a n a r o d o w e g o [t. 1] lub w celu ochrony ludności, jak ma to miejsce w przypadku masowego napływu osób.

Ponieważ udzielenie azylu w dużej mierze ma charakter uznaniowy, regulowany prawem wewnętrznym, to w tym kontekście można mówić o prawie państwa do udzielenia azylu. Z kolei prawo jednostki do azylu,poszukiwania ochrony przed prześladowaniem należy rozpatrywać w kontekście art. 14 Powszechnej deklaracji praw człowieka oraz konwencji dotyczącej statusu uchodźców. Azyl jako narzędzie ochrony jest przyznawanyosobom objętym zakresem definicji stanowionej w art. 1A tej konwencji, a więc osobom uznanym za „uchodźców" w myśl porozumień i konwencji sprzed 1951 r., oraz osobom, które z powodu uzasadnionej obawy przed prześladowaniem z powodu swojej rasy, religii, narodowości, przynależności do określonej grupy społecznej lub z powodu przekonań politycznych przebywają poza granicami państwa, którego obywatelstwo posiadają, oraz nie mogą lub nie chcą z tych powodów korzystać z ochrony tego państwa. Dotyczy to również bezpaństwowców znajdujących się w podobnej sytuacji, którzy nie mogą lub nie chcą korzystać z ochrony państwa swojego dawnego stałego zamieszkania.

Do tej pory nie ustanowiono prawnie wiążącej normy międzynarodowej regulującej instytucję azylu. Zasady udzielania azylu dyplomatycznego i terytorialnego uwzględniono m.in. w regionalnych instrumentach prawnych dotyczących np. Ameryki Łacińskiej, taki jak: porozumienie o ekstradycji z Caracas (1911 r.), konwencja o azylu z Hawany (1928 r.), konwencja o azylu politycznym z Montevideo (1933 r.), konwencja o azylu dyplomatycznym z Caracas (1954 r.), konwencja o azylu terytorialnym z Caracas (1954 r.) oraz traktat o międzynarodowym prawie karnym z Montevideo (1989 r.).

W zakresie „azylu" prawo unijne przewiduje 2 formy ochrony międzynarodowej: status uchodźcy i status ochrony uzupełniającej. W 1999 r. Rada Europejska, na posiedzeniu w Tampere w dniach 15–16 października, podjęła decyzję o rozpoczęciu prac w kierunku ustanowienia Wspólnego Europejskiego Systemu Azylowego, opartego na pełnym stosowaniu konwencji genewskiej dotyczącej statusu uchodźców z 1951 r., uzupełnionej protokołem nowojorskim z 1967 r., z uwzględnieniem zasady zakazu wydalania. Cztery lata później przyjęto dyrektywę Rady Unii Europejskiej ustanawiającą minimalne normy dotyczące przyjmowania osób ubiegających się o azyl (2003/9/WE). Zgodnie z pkt 2(b) dyrektywy: wniosek o udzielenie azylu oznacza wniosek złożony przez obywatela państwa trzeciego lub bezpaństwowca, który może być rozumiany jako wniosek o ochronę międzynarodową przez Państwo Członkowskie na podstawie konwencji genewskiej. Każdy wniosek o ochronę międzynarodową jest uznawany za wniosek o udzielenie azylu, chyba że obywatel państwa trzeciego lub bezpaństwowiec wyraźnie wnioskuje o inny rodzaj ochrony, który może być stosowany osobno.

Dyrektywa odnosi się do wszystkich obywateli państw trzecich, do bezpaństwowców, a także do członków ich rodzin, którzy wnioskują o udzielenie azylu

na granicy lub na terytorium państwa członkowskiego, do czasu obowiązującego zezwolenia na pozostanie na jego terytorium jako osoby ubiegające się o azyl – pod warunkiem że są oni objęci wnioskiem o udzielenie azylu zgodnie z prawem krajowym. Dyrektywa nie ma zastosowania do wniosków o udzielenie azylu dyplomatycznego lub terytorialnego składanych w przedstawicielstwach państw członkowskich oraz do sytuacji, w których zastosowanie mają przepisy dyrektywy Rady 2001/55/WE z dnia 20 lipca 2001 r. w sprawie minimalnych standardów przyznawania tymczasowej ochrony na wypadek masowego napływu wysiedleńców oraz środków wspierających równowagę wysiłków między państwami członkowskimi, związanych z przyjęciem takich osób, wraz z jego następstwami. Obecnie Wspólny Europejski System Azylowy tworzą:

- Dyrektywa Parlamentu Europejskiego i Rady 2013/32/UE z dnia 26 czerwca 2013 r. w sprawie wspólnych procedur udzielania i cofania ochrony międzynarodowej, która zapewnia wydawanie decyzji o azylu;
- Dyrektywa Parlamentu Europejskiego i Rady 2013/33/UE z dnia 26 czerwca 2013 r. w sprawie ustanowienia norm dotyczących przyjmowania wnioskodawców ubiegających się o ochronę międzynarodową, zapewniająca humanitarne i materialne warunki przyjmowania osób ubiegających się o azyl;
- Dyrektywa Parlamentu Europejskiego i Rady 2011/95/UE z dnia 13 grudnia 2011 r. w sprawie norm dotyczących kwalifikowania obywateli państw trzecich lub bezpaństwowców jako beneficjentów ochrony międzynarodowej, jednolitego statusu uchodźców lub osób kwalifikujących się do otrzymania ochrony uzupełniającej oraz zakresu udzielanej ochrony, wyjaśniająca podstawy udzielania ochrony międzynarodowej;
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 604/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca (tzw. przekształcone rozporządzenie dublińskie);
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 603/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania rozporządzenia (UE) nr 604/2013 w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca oraz w sprawie występowania o porównanie z danymi Eurodac przez organy ścigania państw członkowskich i Europol na potrzeby ochrony porządku publicznego, oraz zmieniające rozporządzenie (UE) nr 1077/2011 ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi

Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości.

Komisja Europejska 23 września 2020 r. zaproponowała również **nowy pakt o migracji i azylu, mający m.in. tworzyć kompleksowe** europejskie ramy zarządzania migracją i azylem. W związku z → k r y z y s e m [t. 2] migracyjnym KE również proponuje przekształcenie Europejskiego Urzędu Wsparcia w dziedzinie Azylu (EASO) w pełnoprawną unijną agencjęazylową.

W Polsce prawo do azylu zagwarantowano w art. 56 Konstytucji RP: „Cudzoziemcy mogą korzystać z prawa azylu w Rzeczypospolitej Polskiej na zasadach określonych w ustawie. Cudzoziemcowi, który w Rzeczypospolitej Polskiej poszukuje ochrony przed prześladowaniem, może być przyznany status uchodźcy zgodnie z wiążącymi Rzeczpospolitą Polską umowami międzynarodowymi". Na mocy Ustawy z dnia 13 czerwca 2003 r. o udzielaniu cudzoziemcom ochrony na terytorium Rzeczypospolitej Polskiej, art. 90(1) „Cudzoziemcowi można, na jego wniosek, udzielić azylu w Rzeczypospolitej Polskiej, gdy jest to niezbędne do zapewnienia mu ochrony oraz gdy przemawia za tym ważny interes Rzeczypospolitej Polskiej". Pozbawienie azylu następuje w razie ustania przyczyny, dla których został on udzielony, oraz gdy azylant prowadzi działalność skierowaną przeciwko → o b r o n n o ś c i lub →b e z p i e c z e ń s t w u [t. 1] państwa lub bezpieczeństwu i porządkowi publicznemu (art. 91).

Klaudia Cenda-Miedzińska

K. Burczak, *Prawo azylu w ustawodawstwie synodów galijskich V–VII wieku*, Wydawnictwo KUL, Lublin 2005; Constitution of 1793, *Liberty, Equality, Fraternity: Exploringthe French Revolution*, https://revolution.chnm.org/items/show/422,(dostęp 29.11.2021); Dyrektywa Rady 2003/9/WE z dnia 27 stycznia 2003 r. ustanawiająca minimalne normy dotyczące przyjmowania osób ubiegających się o azyl, Dz.Urz. UE wyd. spec. 2004, rozdz. 19, t. 6; EASO, FRONTEX, *Dostęp do procedury azylowej*, Unia Europejska, 2016; Konwencja dotycząca statusu uchodźców,sporządzona w Genewie dnia 28 lipca 1951 r., Dz.U. z 1991 r. nr 119, poz. 515 i 516; P. Kuczma, *Prawo cudzoziemca do ubiegania się o udzielenie azylu terytorialnego*, http://www.repozytorium.uni.wroc.pl/Content/52928/PDF/17_Pawel_Kuczma. pdf (dostęp 29.11.2021); W. Mossakowski, *Azyl w późnym Cesarstwie Rzymskim (confugium ad statuas, confugium ad ecclesias)*, Wydawnictwo UMK, Toruń 2000;Powszechna deklaracja praw człowieka, 10 grudnia 1948, http://libr.sejm.gov.pl/ tek01/txt/onz/1948.html (dostęp 29.11.2021); UN General Assembly, Declaration on Territorial Asylum, 14 December 1967, A/RES/2312(XXII); Ustawa z dnia 13 czerwca 2003 r. o udzielaniu cudzoziemcom ochrony na terytorium Rzeczypospolitej Polskiej, Dz.U. 2003 nr 128, poz. 1176.

B

BAŃKA INFORMACYJNA I ZJAWISKO *ECHO CHAMBER* – terminy odnoszące się do specyfiki funkcjonowania jednostki w świecie → i n f o r m a c j i [t. 2] i mediów, w którym z uwagi na czynniki zewnętrzne (głównie algorytmy internetowe) oraz wewnętrzne (możliwości poznawcze człowieka i sposób ich działania) docierają do jednostki głównie te informacje i treści, które zgodne są z jej oczekiwaniami i nie naruszają dotychczasowych poglądów i przekonań.

Bańka informacyjna (ang. *filter bubble*) jest efektem izolacji intelektualnej, która powstaje w wyniku personalizacji algorytmicznej. Pojęcie zostało spopularyzowane przez internetowego aktywistę E. Parisera za sprawą jego pracy *The Filter Bubble: What the Internet Is Hiding from You* wydanej w 2011 r. Autor dowodził w niej, że za sprawą wyszukiwarek takich jak Google oraz algorytmów wykorzystywanych przez Facebook do odbiorcy docierają tylko takie dane, które będą mu się podobać z uwagi na zgodność z jego oczekiwaniami, poglądami, gustami i opiniami. Taki stan rzeczy sprawia, że użytkownik internetu może mieć poczucie, że wszyscy myślą tak jak on, co prowadzi do silnej polaryzacji i może mieć negatywne konsekwencje w publicznym, szczególnie politycznym dyskursie.

Początkowo internet był medium zapewniającym anonimowość, a wyniki wyszukiwania były niezależne od użytkowników, oferowały im wolność i przejrzystość, której oczekiwali. Ta utopijna wizja wkrótce odeszła jednak do przeszłości. Dostępność ogromnej mocy obliczeniowej i możliwość generowania dużych ilości danych wpłynęła na przejrzystość wyszukiwarek poprzez zastosowanie zindywidualizowanych algorytmów. Sieć ogólnoświatowa może zwiększać stopień autonomii jednostki.

Początkowo wydawało się, że pluralizm i różnorodność punktów widzenia są konieczne do podejmowania dobrze przemyślanych decyzji dotyczących tego, z czym najbardziej się identyfikujemy. Ilość informacji dostępnych online oferowała wybór z szerokiej gamy możliwości, jednak z czasem okazało się, że podejmowanie decyzji nie byłoby możliwe bez pewnego stopnia filtrowania. Aby być skutecznym, konieczne staje się dynamiczne podejmowanie decyzji, co byłoby nie do zniesienia w ogromnym zalewie dostarczanych informacji. W związku z tym człowiek pozostaje ograniczony w podejmowaniu decyzji, ponieważ jego mózg nie jest w stanie przetwarzać każdej dostępnej informacji. Bez filtrowania jednostka może mieć wysoki stopień autonomii przy jednoczesnej trudności w podejmowaniu decyzji.

Ludzka potrzeba filtrowania doprowadziła do powstania personalizacji algorytmicznej. Spersonalizowane algorytmy filtrują zawartość i strukturę treści internetowych, aby dostosować ją do konkretnych potrzeb, celów, zainteresowań i preferencji każdego użytkownika. Wszystko zaczyna się od modelu użytkownika utworzonego

na podstawie wszystkich zachowań użytkownika, takich jak historia kliknięć, lokalizacja, dane osobowe itp. Dzięki ujednoliceniu różnych sygnałów pod jedną, sprofilowaną tożsamością system może przewidzieć, które informacje będą istotne dla danego użytkownika, i odfiltrować te dane, które nie pasują do jego modelu, ułatwiając tym samym mu znalezienie drogi w zalewie informacji online. Algorytmiczna personalizacja nie jest jednak pozbawiona ryzyka, ponieważ może podważyć warunki niezbędne dla osobistej autonomii. W tym kontekście należy zwrócić uwagę na fakt, że zdolność jednostki do samooceny jest znacznie osłabiona. Aby móc określać potrzeby, musi być ona w stanie ocenić, kim jest i kim chce zostać, co jednak staje się trudne, jeśli nie niemożliwe, gdy spersonalizowane filtrowanie ogranicza jej wiedzę o świecie i o sobie. Filtry personalizujące stanowią rodzaj niewidzialnej autopropagandy (zob. → p r o p a g a n d a [t. 3]), indoktrynując nas naszymi własnymi pomysłami, wzmacniając nasze pragnienie rzeczy, które są znajome, i pozostawiając nas nieświadomymi wszelkich rozbieżnych informacji. W rezultacie bańki filtrujące uniemożliwiają użytkownikom uświadomienie sobie, że ich przekonania i pragnienia mogą wymagać przemyślenia, w ten sposób poważnie osłabiają zdolność jednostki do samooceny.

Krytycy dowodzą, że bańki filtrujące nie mają wielu wad, gdyż zgodne z naturą pozostaje, by człowiek aktywnie poszukiwał wiarygodnych informacji i pytał, czy jego przekonania są rzeczywiście uzasadnione. Uwagę zwraca jednak zjawisko znane jako stronniczość potwierdzająca, czyli ludzka tendencja do wierzenia w rzeczy, które wzmacniają zakorzenione już w człowieku poglądy, aby zobaczyć to, co chcemy widzieć. Stronniczość potwierdzająca nie działa tak samo jak bańki informacyjne, gdyż błąd potwierdzenia jest kwestią ludzkiej psychiki, bańki filtrujące zaś nie są. Spersonalizowane algorytmy są narzucane w większym stopniu niż psychologiczne uwarunkowania działań charakterystyczne dla człowieka. Ponadto bańki informacyjne są stosunkowo nowym zjawiskiem, o którym wielu ludzi wciąż nie wie, szczególnie dlatego, że informacje są filtrowane przed dotarciem do użytkownika, co dzieje się w oderwaniu od jego świadomości. Nawet osoba świadoma personalizacji algorytmicznej niewiele może zrobić. Kryterium filtrowania informacji nie jest ani przejrzyste, ani konfigurowalne. Co więcej, wydaje się oczywiste, że aby użytkownicy mogli kontrolować usługi, z których korzystają, muszą wiedzieć, jakie informacje są wykorzystywane do personalizacji i jak wykorzystywane są ich dane. Osiągnięcie takiego stanu jest jednak mało prawdopodobne, zwłaszcza biorąc pod uwagę to, że nawet programiści nie mogą już w pełni wyjaśnić wszystkich danych wyjściowych ze względu na złożoność personalizacji algorytmicznej. Być może zatem jedynym realnym sposobem ochrony naszej zdolności do samooceny i autonomii byłaby rezygnacja z filtrowania, co jednak także jest scenariuszem nierealistycznym, ponieważ ludzki mózg nie jest w stanie samodzielnie przetworzyć potopu informacji online (zob. → p o t o p i n f o r m a c y j n y i j e g o z a g r o ż e n i a [t. 3]).

Uwagę zwraca również inna konsekwencja działania bańki informacyjnej, mianowicie zanik krytycznej refleksji. Aby racjonalnie poprzeć konkretne rozwiązanie, a nie inne, musi wystąpić zdolność do kwestionowania swoich opinii. Staje się to trudne bez sygnałów z zewnątrz, które zachęcałyby do wykorzystywania tej zdolności. W końcu, aby krytycznie zastanowić się nad swoimi dążeniami, musi wystąpić pewien rodzaj sprzeczności, który zainicjowałby ten proces. Spersonalizowane algorytmy oferują wizję świata dostosowanego do indywidualnych potrzeb, która pasuje do nas doskonale. Nigdy się nie nudzimy ani nie denerwujemy. Nasze media są doskonałym odzwierciedleniem naszych zainteresowań i pragnień. Ze względu na tę intelektualną izolację, a zwłaszcza z powodu nieznajomości istoty procesu filtrowania nigdy nie czujemy potrzeby spojrzenia poza swoje osobiste preferencje, nie mówiąc już o krytycznej refleksji nad nimi. Nieświadomość użytkowników w połączeniu z brakiem kontroli oraz przejrzystości spersonalizowanych algorytmów całkowicie odbiera zdolność do analizy krytycznej.

W świecie baniek filtrujących, dzięki ciągłemu dostarczaniu informacji zgodnych z zainteresowaniami użytkownika, personalizacja algorytmiczna zapewnia pewien stopień spójności w tym, czego jednostka pragnie lub w co wierzy. Na przykład osoba będąca wegetarianinem stale dostaje informacje potwierdzające słuszność jej życiowego wyboru. W ten sposób odbiorcy nowoczesnych mediów mają przekonanie, że pozostają w większości, gdyż wszystkie źródła, z którymi mają do czynienia, nie tylko potwierdzają, ale pogłębiają ich sposób myślenia, co silnie kształtuje poglądy na rozmaite tematy i sprzyja ich polaryzacji.

Z kolei zjawisko *echo chamber* zostało opisane w wyniku wzrostu ilości opiniotwórczych i stronniczych treści medialnych. W odniesieniu do treści politycznych zjawisko najczęściej odnosi się do przepływu informacji w sieci i zachowań informacyjnych użytkowników internetu. Wielka liczba stron internetowych o charakterze stronniczym i mnogość politycznie jednostronnych głosów na portalach społecznościowych tworzą ogromną przestrzeń, w której użytkownicy mediów powtarzają to, co powiedzieli już inni. Zjawisko to nie jest zamierzonym efektem ubocznym współczesnej praktyki dziennikarskiej, ale konsekwencją powstawania zamkniętej przestrzeni komunikacyjnej, która może potencjalnie generować nowe wiadomości o podobnej treści i izolować je od jakiejkolwiek formy krytyki.

Zjawisko *echo chamber* zostało wykorzystane do wyjaśnienia produkcji i rozpowszechniania informacji publikowanych przez media informacyjne. W czasach, gdy od dziennikarzy takich mediów oczekuje się publikowania treści 24 godz. na dobę, 7 dni w tygodniu, informacje są stale przetwarzane i ponownie wykorzystywane, ponieważ te same historie i opinie pojawiają się w wielu miejscach jednocześnie. Duże i uznane koncerny medialne, a także mniejsze → m e d i a a l t e r n a t y w n e [t. 3] i dzienniki internetowe odwołują się do siebie, aby promować swoje materiały. Odpowiadając sobie nawzajem na wiadomości i opinie, każde z nich legitymizuje drugie.

Domniemanie istnienia zjawiska echa w zamkniętej przestrzeni medialnej zostało wykorzystane przez K.H. Jamieson i J.N. Cappellę w 2008 r. w badaniu mediów konserwatywnych i ich odbiorców. Dowiedli oni, że w szczególności 3 produkty medialne – radio talk-show Rush Limbaugh, stacja Fox News i strona redakcyjna „Wall Street Journal" – stanowią komorę pogłosową, która skutecznie promuje konserwatywne zasady i Partię Republikańską oraz je broni. Te 3 odrębne podmioty medialne cytują się nie tylko w swoich doniesieniach i relacjach, lecz również tworzą pozytywne sprzężenia zwrotne dla odbiorców, udostępniając linki do treści wzajemnie na swoich stronach internetowych. Jamieson i Cappella doszli do wniosku, że spójność i powtarzalność ich konserwatywnego przekazu tworzą ideologiczną przestrzeń dla konserwatywnej publiczności, ponieważ opinie mediów rezonują z ich obecnymi przekonaniami.

W konsekwencji istnienia zamkniętej przestrzeni komunikacyjnej współcześni odbiorcy mediów mają coraz częściej poczucie, że niemal wszystkie osoby wokół nich myślą podobnie, że znajdują się w większości, a poglądy przeciwne do tych, które wypowiadają, mają charakter niezwykle rzadki. Zwykle w takiej sytuacji wyniki wyborów, referendów czy nawet wyniki badań → o p i n i i p u b l i c z n e j [t. 3] przynoszą zaskoczenie, okazuje się bowiem, że wbrew oczekiwaniom dana jednostka znajduje się w mniejszości, a jej poglądy wcale nie są tak popularne, jak tego oczekiwała. Liczne badania dowodzą, że takie odczucia, a także szeroko pojęte kształtowanie naszych przekonań i opinii nie tylko w odniesieniu do naszych decyzji czy poglądów politycznych, ale również do tego, jak myślą inni, są kreowane lub co najmniej współkreowane przez media.

Interesujących dowodów potwierdzających wspomnianą tezę dostarczają relacje medialne wydarzeń takich jak brexit, wybory w USA wygrane przez D. Trumpa, → w o j n a h y b r y d o w a [t. 4] między Rosją a Ukrainą, fale uchodźców napływające do Europy po → k r y z y s i e [t. 2] syryjskim czy coraz popularniejsze fake newsy. Wyraźnie dowodzą one, że już sam dobór źródeł informacji, z których korzystamy, czy to dokonany przez nas, czy przez wyszukiwarki internetowe i → m e d i a s p o ł e c z n o ś c i o w e [t. 3], a także nasza dotychczasowa wiedza i przekonania mają silny wpływ na postrzeganie i ocenę zjawisk odnoszących się do polityki i → b e z p i e c z e ń s t w a .

Według części takich koncepcji jednostka korzystająca z mediów narażona jest na autocenzurę, kontakt tylko z przefiltrowanymi dla niej informacjami, co sprawia, że w istocie poznaje jedynie postawy i poglądy zbliżone do swoich. W ten sposób obywatel zostaje umieszczony w komorze ze zwielokrotnionym, odbijającym się echem. Ma do dyspozycji wiele kanałów i źródeł informacji, ale sięga – z jednej strony sam, a z drugiej strony za sprawą rozwiązań technologicznych – do tych, które pozwalają mu potwierdzać sądy i odczucia, do których jest przyzwyczajony. Poszukiwane są głównie publikacje dowodzące, że nasze oceny są właściwe, co w konsekwencji prowadzić może do tego, że jednostka znajduje się w metaforycznym pokoju wypełnionym echem, a więc nie docierają do niej poglądy, oceny i opinie polemiczne czy

krytyczne wobec jej stanowiska. Już wybór tytułu prasowego, programu telewizyjnego czy witryny internetowej w przypadku większości użytkowników mediów nie jest dziełem przypadku i nie jest powodowany ciekawością świata, lecz staje się działaniem zgodnym z psychologiczną → s t r a t e g i ą [t. 4] konfirmacyjną, czyli tendencją do preferowania tych źródeł informacji i opinii, które potwierdzają posiadane już oczekiwania czy hipotezy.

Zarysowane uwarunkowania sprawiają, że zwolennicy rządu oglądają głównie programy informacyjne w telewizji publicznej, a głosujący na opozycję – w telewizjach komercyjnych. Osoby konserwatywne, preferujące wartości religijne, sięgają po media katolickie, a widzowie i czytelnicy o poglądach liberalnych korzystają z mediów, które prezentują bliskie im wyobrażenia o świecie. Podobnie w internecie wyszukiwarki i media społecznościowe, wykorzystując wiedzę o tym, co zostało polubione przez danego odbiorcę, a w szczególności o tym, jakie tematy i opinie śledził przez największą ilość czasu, sprawiają, że użytkownik znajduje się zawsze w grupie bliskich mu tematów i punktów widzenia podobnych do jego własnych, nigdy zaś nie zostanie skierowany do odmiennych, niezgodnych z jego systemem wartości. To właśnie sprawia, że widzowie i czytelnicy mają przekonanie, że pozostają w większości, gdyż wszystkie źródła, z którymi mają do czynienia, nie tylko potwierdzają, ale też pogłębiają ich sposób myślenia, co silnie kształtuje poglądy polityczne i sprzyja ich polaryzacji.

Powyższy przykład opisuje publiczność jako pasywnego konsumenta informacji w zdominowanej przez media *echo chamber*. Jednak widzowie mogą również odgrywać bardziej aktywną rolę, gdy uczestniczą w tworzeniu treści w interaktywnych miejscach cyfrowych. Korzystając z serwisów społecznościowych, osobistych dzienników internetowych i innych platform internetowych, które zachęcają do interakcji z odbiorcami, jednostki wzmacniają efekt *echo chamber*, przesyłając treści multimedialne i wyrażając dodatkowe opinie. W szczególności naukowcy i krytycy uznali zdolność sieci społecznościowych do wzmacniania efektów echa za strukturalny element ich projektu. W serwisach społecznościowych użytkownicy szukają kontaktów z osobami, z którymi dzielą podobne przekonania. Przyjaciele i połączenia nakładają się na siebie w większości sieci, a – co za tym idzie – użytkownicy słyszą wciąż te same informacje. Badania sugerują, że ludzie, którzy są wielokrotnie narażeni na te same informacje dostarczane przez różne źródła, w końcu przyjmują te informacje jako prawdę.

Fragmentaryzacja publiczności i jej polaryzacja oraz tworzenie fałszywej iluzji rzeczywistości to tylko jedna z negatywnych konsekwencji, jakie niesie za sobą zjawisko *echo chamber*. Badania w dziedzinie komunikacji i nauk społecznych sugerują, że publiczność poznaje informacje dotyczące polityki, rozpoczynając ich odbiór z istniejącymi już postawami i preferencjami, które chce wzmocnić poprzez wybór kompatybilnych mediów. Technologia internetowa umożliwia użytkownikom selektywne narażanie się na pewne treści i opinie, które rezonują z ich wcześniejszymi przekonaniami. Poprzez ten proces poszukiwania informacji widzowie bronią się przed informacjami,

które podważają ich przekonania, a ostatecznie ich zaangażowanie w stronnicze i dalekie od obiektywizmu echo prowadzi jednostki do przyjęcia bardziej ekstremalnych postaw, które zwiększają polaryzację postaw politycznych.

Niektórzy badacze sugerują, że zjawiska *echo chamber* i *filter bubble* silnie pogłębiają efekty polaryzacyjne, które dodatkowo nasilają się w wyniku postępu technicznych i kulturowych cech internetu. Na przykład organizacje informacyjne i kampanie polityczne coraz częściej zachęcają swoich odbiorców online do formowania grup społecznych i forów dyskusyjnych wokół tematów będących przedmiotem wspólnego zainteresowania. Naukowcy twierdzą, że ta aktywność wytwarza społeczne enklawy ludzi o podobnych poglądach, które ostatecznie uniemożliwiają obywatelom spojrzenie różnych punktów widzenia i dzielenie się wspólnymi doświadczeniami. Internetowe grupy społeczne izolują siebie i swoje opinie od nowych wyzwań, co powoduje poszerzenie przepaści między skrajnymi stronami w kwestiach publicznych.

Jakub Idzik, Rafał Klepka

S.E. Bor, *Echo Chamber Phenomenon*, [w:] *Encyclopedia of Social Media and Politics*, K. Harvey (ed.), Sage, Los Angeles 2011; D. Geschke, J. Lorenz, P. Holtz, *The Triple-Filter Bubble: Using Agent-Based Modelling to Test a Meta-Theoretical Framework for The Emergence of Filter Bubbles and Echo Chambers*, „British Journal of Social Psychology" 2019, vol. 58, no. 1; F. Hamborg, K. Donnay, B. Gipp, *Automated Identification of Media Bias in News Articles: An Interdisciplinary Literature Review*, „International Journal on Digital Libraries" 2019, vol. 20; C. Happer, G. Philo, *The Role of the Media in the Construction of Public Belief and Social Change*, „Journal of Social and Political Psychology" 2013, vol. 1, no. 1; J. Idzik, R. Klepka, *Echo chamber*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; ciż, *Media Coverage of Refugee Crisis: Some Evidence From Poland*, „International Relations Review" 2018, vol. 1; ciż, *Filter bubble*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; ciż, *Voters in the Filter Bubble: Local Government Election Campaign in Polish Opinion Weeklies in the Light of the „Echo Chamber" Concept*, „International Relations Review" 2019, vol. 4; K.H. Jamieson, J.N. Cappella, *Echo Chamber: Rush Limbaugh and the Conservative Media Establishment*, Oxford University Press, New York 2008; D.C. Mutz, *Facilitating Communication Across Lines of Political Difference: The Role of Mass Media*, „American Political Science Review" 2001, vol. 95, no. 1; E. Pariser, *The Filter Bubble: What the Internet Is Hiding from You*, The Penguin Press, New York 2011; D. Sumpter, *Outnumbered: From Facebook and Google to Fake News and Filter-bubbles – The Algorithms That Control Our Lives*, Bloomsbury, London 2018; C.R. Sunstein, *The Law of Group Polarization*, „Journal of Political Philosophy" 2002, vol. 10, no. 2; O. Wasiuta, S. Wasiuta, *Wojna hybrydowa Rosji przeciwko Ukrainie*, Wydawnictwo Arcana, Kraków 2017; F.J. Zuiderveen Borgesius i in., *Should We Worry about Filter Bubbles?*, „Internet Policy Review" 2016, vol. 5, iss. 1.

BARGUZIN – międzykontynentalna kolejowa wyrzutnia → p o c i s k ó w b a l i s t y c z n y c h [t. 5], określana w Rosji jako „bojowy kolejowy kompleks rakietowy" (*bojewoj żeleznodorożnyj rakietnyj kompleks*). Nazwa pochodzi od silnego wschodniego wiatru, który wieje w okolicach jeziora Bajkał. Początki

międzykontynentalnej kolejowej wyrzutni pocisków balistycznych Barguzin sięgają 2013 r., kiedy Siły Zbrojne Federacji Rosyjskiej ogłosiły, że zamierzają przywrócić mobilne systemy w postaci pociągów wyposażonych w pociski balistyczne z głowicami nuklearnymi. Miały one stanowić kontynuację prac prowadzonych w Związku Radzieckim w latach 70. i 80. XX w. Były one odpowiedzią na rosnącą precyzję amerykańskich międzykontynentalnych pocisków balistycznych (ICBM), które były w stanie zniszczyć wszystkie radzieckie podziemne silosy niezależnie od głębokości i poziomu utwardzenia. Dysponując liniami kolejowymi o długości 99 tys. mil, ZSRR planował ukryć mobilne wyrzutnie pocisków balistycznych, zwiększając tym samym szanse na przetrwanie pierwszego amerykańskiego uderzenia atomowego. W 1987 r. uruchomiony został pierwszy kolejowy ICBM Mołodiec, uzbrojony w 77-metrowe pociski RT-23UTTH o masie 104 t, przenoszące po 10 głowic. Aby wystrzelić rakiety, pociąg musiał zatrzymać się na jednym z 200 specjalnie skonstruowanych punktów strzeleckich znajdujących się wzdłuż tras kolejowych, a następnie załoga musiała otworzyć dach wagonu. Aby uniknąć pożarów, zastosowano system „zimnego startu", w trakcie którego pocisk wyrzucany był 200 m w powietrze, a następnie przechylany na jeden z boków, zanim dopalacze ostatecznie się zapaliły.

Łącznie wyprodukowano 10–12 pociągów. Każdy z nich składał się z 3 lokomotyw, 7 wagonów (samochodów) mieszczących moduły dowodzenia, 1 wagonu z paliwem i ze smarami, 3 wagonów z modułem startowym oraz 1 wagonu, w którym znajdował się pocisk. Ze względu na kryzys gospodarczy lat 90. XX w. oraz ograniczenia wynikające z traktatu START II (Treaty Beetween the United States of America and the Russian Federation on the Further Reduction and Limitation of Strategic Offensive Arms [START II], signed at Moscow on 3 January 1993) Rosja wycofała je ze służby.

Barguzin miał być systemem wyposażonym w nowocześniejsze ICBM RS-24 Jars, zbliżone zasięgiem do RT-23 (12,6 tys. km), lecz o 3 m krótsze i znacznie lżejsze. Jest to podstawowa różnica między „nową", a „starą" wersją z czasów sowieckich. Wówczas ze względu na dużą masę międzykontynentalnych rakiet balistycznych zastosowano wagony ze wzmocnionymi zestawami kołowymi, co mogło powodować ich zdemaskowanie. Jeden wagon będący kontenerem transportowym z rakietą ważył nawet 130 t. Obniżenie masy w wypadku Barguzina umożliwi wykorzystanie wagonów towarowych i utrudni obserwatorom znajdujących się na ziemi odróżnienie go od „zwykłych" pociągów. Wystrzelenie pocisku będzie również prostsze, ponieważ nie będzie potrzeby korzystania z punktów strzeleckich. Wystarczy zatrzymanie pociągu w dowolnym miejscu linii kolejowej. Załoga będzie składać się z 70 oficerów i podoficerów. Wagony mają być chronione „elektronicznymi środkami antydostępowymi", a cały system ma być odporny nawet na eksplozję nuklearną w promieniu kilkuset metrów. Jak podkreślali oficerowie Wojsk Rakietowych Przeznaczenia Strategicznego, Barguzin powinien przywrócić lądową triadę nuklearną, składającą się z podziemnych silosów, w których znajdują się międzykontynentalne pociski balistyczne, pocisków

montowanych na samochodach ciężarowych i pocisków znajdujących się na platformach kolejowych.

Powodem podjęcia decyzji o wznowieniu prac nad mobilnymi międzykontynentalnymi pociskami balistycznymi miała być rozbudowa amerykańskiej tarczy antyrakietowej w Europie oraz projekt Conventional Prompt Global Strike realizowany przez Departament Obrony USA, zakładający możliwość przeprowadzenia konwencjonalnych uderzeń rakietowych na dowolny punkt na świecie w czasie krótszym niż godzina. W samej Rosji panowało powszechne przekonanie, że mobilne międzykontynentalne pociski balistyczne dają zupełnie nowe możliwości odstraszania przez karanie. Są one znacznie trudniejsze do wykrycia, w przeciwieństwie do pocisków balistycznych znajdujących się w podziemnych silosach. Mniejsze pociski, takie jak RS-24 Jars, mogą być również umieszczane w pojedynczych wagonach, co daje możliwość wkomponowania ich w cywilne pociągi towarowe. Przewidywano, że pojedynczy pociąg będzie mógł przewozić do 6 międzykontynentalnych pocisków balistycznych i będzie odpowiednikiem jednego pułku. Liczba głowic miała być znacznie większa niż liczba pocisków. Każdy z nich miał rzekomo przenosić do 10 głowic. W rzeczywistości jednak liczba ta mogła być nieco mniejsza, ponieważ wśród nich mogły być atrapy głowic i „zakłócacze radarów". Nie zmienia to faktu, że Rosjanie planowali użycie pocisków z dużą liczbą głowic. Rozwiązanie takie ma kilka zalet. Po pierwsze, posiadanie mniejszej liczby międzykontynentalnych pocisków balistycznych jest tańsze w utrzymaniu. Po drugie, w czasie wymiany ciosów nuklearnych wystrzelenie 10 głowic w kierunku wroga utrudnia zestrzelenie wszystkich. Poza 6 wagonami z rakietami w skład atomowego pociągu miały wchodzić wagony z centrum dowodzenia, łączności, kwaterami dla → ż o ł n i e r z y [t. 4] i ochrony oraz zapleczem technicznym w postaci zapasów żywności i generatorów prądu. Wojsko rosyjskie planowało wystawić jedną dywizję rakietową składającą się z 5 pułków o łącznej liczbie 120 głowic nuklearnych. Zakładano również, że w ciągu doby pociąg będzie mógł przemieścić się na odległość ponad 2 tys. km i wystrzelić rakietę z dowolnego miejsca na trasie, czyniąc wykrycie takiego miejsca bardzo problematycznym. Według obliczeń Stany Zjednoczone musiałyby rozmieścić nad terytorium Rosji co najmniej 18 nowych satelitów obserwacyjnych, aby śledzić składy kolejowe, na których może poruszać się Barguzin.

Prace nad nowym system uzbrojenia zaczęły się bardzo intensywnie.

W grudniu 2013 r. dowódca Wojsk Rakietowych Przeznaczenia Strategicznego generał pułkownik Siergiej Karakajew poinformował, że wstępny projekt ma być ukończony w pierwszej połowie 2014 r. Jak podały media rosyjskie, w grudniu 2015 r. rozpoczęło się opracowanie dokumentacji. Zakładano wówczas, że termin powstania Barguzina nie przekroczy 2020 r. Zgodnie z informacją z 2017 r. ambitny plan rosyjskiego wojska został zawieszony z powodów finansowych. Trwający wówczas kryzys rosyjskiej gospodarki związany z nałożeniem sankcji przez państwa zachodnie po → a n e k s j i [t. 1] Krymu skutkował przełożeniem przyjęcia krajowego programu

uzbrojenia z 2015 na 2017 r. Ponadto drastycznie zmniejszone zostało finansowanie programu z 55 bln do 19 bln rubli (z 928 mld do 290 mld dolarów). Ostatecznie, w przeciwieństwie do pocisków balistycznych Sarmat i Rubież, Barguzin nie znalazł się na liście przewidzianych do badań i rozwoju systemów uzbrojenia. Reaktywacja mobilnych wyrzutni pocisków balistycznych na platformach kolejowych już wcześniej spotykała się z poważną krytyką. W 2019 r. pojawiły się jednak kolejne doniesienia, wskazujące, że Kreml nie zrezygnował całkowicie z nowych mobilnych międzykontynentalnych pocisków balistycznych i zamierza wrócić do prac w sytuacji, w której uzna to za konieczne.

Od momentu rozpoczęcia prac nad Burguzinem zdania na temat międzykontynentalnych kolejowych wyrzutni pocisków balistycznych w rosyjskich środowiskach eksperckich były podzielone. Aleksandr Konowałow – prezes → t h i n k t a n k u [t. 5] Instytutu Oceny Strategicznej – podkreślił, że jest to powrót do kłopotliwych i przestarzałych sowieckich koncepcji. Jego zdaniem zagrożenie ze strony amerykańskiej tarczy antyrakietowej w Europie Środkowo-Wschodniej jest przesadzone, a środki, jakie Ministerstwo Obrony Narodowej planuje przeznaczyć na rozwój programu Barguzin, powinny być wydane na systemy komunikacyjne, bezzałogowe statki powietrzne i amunicję precyzyjną. W 2011 r. generalny projektant Moskiewskiego Instytutu Techniki Cieplnej Jurij Solomonow przyznał, że uruchomienie systemu Barguzin wymagałoby modernizacji infrastruktury kolejowej, w tym budowy nowych zajezdni. Barguzin byłby narażony również na wykolejenie, ataki terrorystyczne oraz → k a t a s t r o f y n a t u r a l n e [t. 2], takie jak osuwiska. Przeszkodą w jego rozwoju były zapisy traktatu → N o w y S T A R T (New START) z 2010 r. (*Treaty Between the United States of America and The Russian Federation on Measures for the Further Reduction and Limitation of Strategic Offensive Arms, signed in Prague on 8 April 2010*), które z jednej strony nie zabraniają rozwoju tego rodzaju broni, z drugiej jednak narzucają ograniczenia ilościowe i regularne kontrole, co pozbawiłoby Rosję możliwości skutecznego ukrycia broni. Podobnego zdania był Robert Beckhusen, który podkreślił, że ograniczenia związane z traktatami START, dotyczące liczby aktywnie rozmieszczonej broni jądrowej, prawdopodobnie zmusiłyby Rosjan do utrzymywania pociągów Barguzin w schronach lub innych zamkniętych obiektach do momentu wzrostu napięcia międzynarodowego poprzedzającego wybuch → w o j n y [t. 4]. Oznacza to sytuację, w której może on nie zdążyć opuścić swojego miejsca i zostać zniszczony z zaskoczenia.

Jak podkreślają inni zachodni eksperci, liczba ograniczeń związanych z użyciem Barguzina jest znacznie dłuższa. Jedną z nich są duże miasta położone przy liniach kolejowych. W czasie pierwszej fazy wojny atomowej strony koncentrują się przede wszystkim na zniszczeniu potencjału → b r o n i m a s o w e g o r a ż e n i a [t. 1] przeciwnika. W związku z tym pociągi typu Barguzin będą musiały unikać dużych ośrodków miejskich i centrów przemysłowych, aby nie stały się one celem ataku nuklearnego.

Przemieszczanie odbywa się po torach kolejowych, więc wyrzutnie te są o wiele mniej mobilne niż wyrzutnie znajdujące się na platformach poruszających się po drogach i łatwiej jest je zlokalizować. Zniszczenie torów kolejowych za pomocą ładunku jądrowego lub ładunku wybuchowego zdetonowanego przez żołnierza sił specjalnych bądź partyzanta może doprowadzić do wykolejania się maszyny lub, w najlepszym wypadku, ograniczenia w poruszaniu się. W środkowej i we wschodniej części Rosji przeszkodą może być nawet zalegający przez wiele miesięcy na torach śnieg.

Mimo pojawiających się co pewien czas wypowiedzi rosyjskich wojskowych, podkreślających, że siły zbrojne tego kraju nie rezygnują z rozwoju systemu Barguzin, wydaje się to mało prawdopodobne. Rozwijany w latach 80. XX w. kolejowy ICBM Mołodiec był jednym z najdroższych projektów zbrojeniowych Związku Radzieckiego. Należy przypuszczać, że podobnym wyzwaniem dla współczesnej Rosji byłby Barguzin.

Tomasz Wójtowicz

R. Beckhusen, *Say Goodbye to Russia's Nuclear-Armed Doomsday Train*, 6.12.2017, https://warisboring.com/say-goodbye-to-russias-nuclear-armed-doomsday-train/ (dostęp 30.03.2022); M. Dura, *Rosja wraca do pociągów z wyrzutniami rakiet balistycznych*, 30.12.2014, https://defence24.pl/siły-zbrojne/rosja-wraca-do-pociagow-z-wyrzutniami-rakiet-balistycznych (dostęp 5.04.2023); K. Mizokami, *All Aboard Russia's Nuclear Weapon Apocalypse Train*, 27.02.2017, https://www.popularmechanics.com/military/weapons/a25423/all-aboard-russias-apocalypse-train/ (dostęp 5.04.2023); T. Newdick, *The Soviet Union's Railway-based Intercontinental Ballistic Missile Had an Inflatable Nosecone*, 9.03.2021, https://www.thedrive.com/the-war-zone/39685/the-soviet-unions-railway-based-intercontinental-ballisticmissile-had-an-inflatable-nosecone (dostęp 30.03.2022); S. Roblin, *Russia Almost Built a Nuclear Missile Train*, 8.12.2020, https://nationalinterest.org/blog/reboot/ russia-almost-built-nuclear-missile-train-174059 (dostęp 5.04.2023); *RS-24/SS-32/ Barguzin. New Rail-Mobile ICBM*, https://www.globalsecurity.org/wmd/world/ russia/rs-24-barguzin.htm (dostęp 30.03.2022); M. Starchak, *Russia Terminates Development of New Rail-Mobile Ballistic Missile*, 13.12.2017, https://jamestown.org/ program/russia-terminates-development-new-rail-mobile-ballistic-missile/ (dostęp 30.03.2022); М. Ходаренок, *Ядерные ракеты на запасном пути*, 22.11.2016, https://www.gazeta.ru/army/2016/11/22/10358843.shtml (dostęp 5.04.2023).

BARIERY I ZAGROŻENIA W DOSTĘPIE DO INFORMACJI – przeszkody utrudniające lub uniemożliwiające korzystanie z → i n f o r m a c j i [t. 2] bądź jej rozpowszechnianie. W literaturze opisywane są bariery w dostępie do informacji, bariery w komunikacji, bariery w przepływie informacji, a także tzw. klatki dostępności do źródeł informacji, czyli ograniczenia, które uniemożliwiają, utrudniają lub deformują postrzeganie rzeczywistości (opisywanych obiektów), czy tzw. klatki językowe lub klatki wiedzy ograniczające generowanie informacji w systemach społeczno-gospodarczych, wynikające ze sposobu (modeli) opisu potrzeb informacyjnych, sposobu odwzorowania rzeczywistości, rodzajów źródeł informacji i sposobów pozyskiwania informacji ze źródeł informacji. Ograniczenia w fazie wytwarzania informacji wpływają na zakres informacji możliwej do generowania w danym → p r o c e s i e

i n f o r m a c y j n y m [t. 3]. Zniesienie tych ograniczeń wymaga usunięcia barier ograniczających każdą z tych klatek. Twórcy informacji i gestorzy systemów informacyjnych adresowanych do użytkowników powinni dostosować procesy informacyjne do ich potrzeb. W praktyce jednak przepływ informacji napotyka wiele barier, począwszy od etapu formułowania potrzeb informacyjnych, przez gromadzenie informacji, tworzenie zbioru informacyjnego, dostępu do tego zbioru, na wykorzystaniu informacji w nim zgromadzonych skończywszy. Zaliczyć do nich można: bariery społeczne utrudniające dostęp do danych i źródeł, bez których jest niemożliwe zaspokajanie potrzeb informacyjnych w systemie społecznym; bariery instytucjonalne wynikające z niezdolności do zaspokajania potrzeb przez instytucje odpowiedzialne za obieg informacji; ekonomiczne (finansowe), techniczne, bariery językowe, bariery ideologiczne itp.

Bariery informacyjne mogą dotyczyć dostępu do informacji, ale też przepływu wiedzy lub przeszkód występujących w procesie komunikacji. Bariery informacyjne jako przeszkody, które zakłócają proces przepływu informacji od jej twórców do adresatów, mogą oddziaływać na użytkownika niezależnie od jego świadomości (bariery obiektywne) lub poprzez tę świadomość (bariery subiektywne). Według *Lexikon Information und Documentation* bariery informacyjne występują, gdy informacje nie są wykorzystywane z powodu niewiedzy użytkownika o ich istnieniu lub z powodu niekorzystania ze znanych źródeł informacji, albo z powodu utrudnionego dostępu do tych źródeł informacji. Jednak zgodnie z definicją D.E. Haaga „pojawiają się zawsze wtedy, gdy występuje rozbieżność między idealną a aktualną dostępnością opublikowanej informacji, i powodują utrudnienie, opóźnienie, uniemożliwienie dostępu do informacji".

Bariery wynikające z utrudnień dostępu do informacji dotyczą głównie problemów niemożności dotarcia do dokumentu lub niemożności wykorzystania treści w nim zawartych. Według Ch. Borgmanna istnieją 3 zasadnicze przeszkody związane z zapewnieniem dostępu do informacji: wynikające z braku połączenia z siecią komputerową; z braku dostępu do treści i serwisów informacyjnych; związane z niemożnością wykorzystania technologii informacyjnych i wykorzystania treści zawartych w dokumentach. Z kolei dostęp do informacji wg R.E. Rice'a i Shan-Ju L. Changa może być utrudniony, jeżeli brak: dostępu do wiedzy, dostępu do technologii i mediów, dostępu wynikającego z nieumiejętności wykorzystania informacji (pojmowania, rozumienia i przyswajania treści), dostępu wynikającego z władzy nad przepływem informacji (nadrzędna kontrola), dostępu do informacji jako towaru, dostępu do rządowych serwisów informacyjnych (znajomość praw umożliwiających aktywny udział w demokratycznym społeczeństwie).

W literaturze opisano różne typologie barier informacyjnych. Najczęściej dzielone są one na bariery obiektywne i subiektywne, na bariery zewnętrzne i wewnętrzne oraz makrobariery (uwzględniające warunki ekonomiczne i geopolityczne na świecie) i mikrobariery (uwzględniające cechy psychologiczne użytkownika). Jak stwierdza

M. Świgoń, bariery informacyjne tworzą kompleks zależnych od siebie i wzajemnie przenikających się zjawisk, dlatego w praktyce niemożliwe jest wyznaczenie wyraźnej granicy pomiędzy różnymi ich rodzajami i formami. Przykładowo typologia Haaga obejmuje 51 typów barier informacyjnych zestawionych w 3 zespołach: barier związanych z publikowaniem informacji, barier związanych z organizacją i przetwarzaniem informacji, barier związanych z korzystaniem z informacji opublikowanej. Z kolei typologia barier, na które można natknąć się w procesie komunikacji, zaproponowana przez W. Przelaskowskiego obejmuje aż 14 barier: braku rozeznania, braku łączności, językową, konceptualną (wewnątrzjęzykową), semiotyczną (między językiem a myślą), braku erudycji, efektu pierwszeństwa, efektu ostatniego, subiektywnej oceny hipotez, minimalizacji dystansu między hipotezą a stanem adekwatnym, poszukiwania reguły i prawidłowości, barierę wynikającą ze sprzeczności między teoretycznym poziomem poznania a uświadomieniem go w kategoriach filozoficznych, barierę informacyjną między nauką a techniką, barierę informacji niepełnej.

Najbardziej znana jest w literaturze typologia barier informacyjnych sporządzona na podstawie schematu T.D. Wilsona. Obejmuje ona 4 zasadnicze grupy barier: bariery związane z użytkownikiem informacji, bariery interpersonalne, bariery środowiskowe (otoczenie użytkownika) i bariery związane ze źródłami informacji (tworzone przez biblioteki lub przez autorów i wydawców informacji pośredniej i bezpośredniej). Przykładowo do barier związanych z użytkownikiem informacji zalicza się: barierę nieświadomości, barierę braku wiedzy, barierę terminologiczną, barierę języków obcych, barierę niewystarczającego przygotowania do wyszukiwania informacji, barierę oporu psychicznego przed korzystaniem z komputerowych baz danych, barierę oporu psychicznego przed proszeniem o pomoc w wyszukiwaniu informacji, barierę pasywnej postawy, barierę braku systematyczności, barierę braku wystarczającej ilości czasu na poszukiwanie informacji naukowej, barierę obawy związanej z korzystaniem z instytucji gromadzących informacje. Z kolei bariery środowiskowe obejmują bariery prawne (wynikające z ochrony praw własności intelektualnej i przemysłowej, ochrony przed naśladownictwem i konkurencją), bariery finansowe (wynikające z niedoboru środków finansowych), bariery ekonomiczne (bariera wartości czasu, jaki należy poświęcić na wyszukanie informacji, bariera wysokich kosztów publikacji, bariera wysokich kosztów dostępu do informacji i korzystania z niej), bariery geograficzne (bariera dystansu, izolacja geograficzna, izolacja od dużych ośrodków naukowych, odległość do miejsc udostępniania informacji), bariery polityczne (wynikające z obrony państwowych interesów, z cenzurowania (zob. → c e n z u r a) informacji, utajniania wyników badań, → m a n i p u l a c j i i n f o r m a c j ą [t. 3], działań ideologicznych).

Bariery informacyjne stanowiące przeszkodę w prawidłowym obiegu informacji mogą hamować rozwój organizacji i doprowadzić do jej upadku. T. Galewski, analizując system informacyjny przedsiębiorstwa, zwraca uwagę na szkodliwość wybranych barier z grupy informacyjnych *sensu stricto*, psychologicznych, socjologicznych,

organizacyjnych i ekonomicznych. Do pierwszej grupy zalicza bariery związane z pozyskiwaniem informacji złej jakości i niespełniającej kryteriów użyteczności w sensie zaspokajania potrzeb informacyjnych podmiotów. Z punktu widzenia ekonomiki informacji należą do nich: brak informacji, niedoskonałości generowania informacji, niska jakość informacji, czyli niski stopień jej użyteczności dla odbiorcy. Bariery psychologiczne powstają w sytuacji niewystarczającego czasu do namysłu nad otrzymaną informacją, zależą od dotychczas posiadanej wiedzy, kontekstu, stanu emocjonalnego użytkownika, okoliczności odbioru informacji.

Do barier tych zalicza się tzw. klatkę wiedzy, która oznacza ograniczenia człowieka w procesie generowania informacji. Każdy obserwator danego obiektu ma pewną wiedzę, która wpływa na jego postrzeganie świata, przez co wygenerowana informacja nie jest obiektywna. Bariera ta jest trudna do pokonania, ponieważ podmiot generujący informację ograniczony jest swoim horyzontem informacyjnym i może nie zdawać sobie sprawy z tego, iż tkwi we własnej klatce wiedzy.

Inne bariery z tej grupy mogą być generowane w związku ze złą interpretacją informacji i odwzorowania danego fragmentu rzeczywistości; wynikać z → p r z e c i ą ż e n i a i n f o r m a c y j n e g o [t. 3], czyli z otrzymywania nadmiernej ilości danych, których odbiorca nie jest w stanie przyswoić; z „paradoksu przesytu informacyjnego", oznaczającego stan braku pożądanej informacji przy ogólnej nadprodukcji informacji; z koncepcji „dominującej logiki firmy" C.K. Prahalada i R.A. Bettisa, która oparta jest na założeniu, że nie wszystkie informacje są wykorzystywane na najwyższych szczeblach zarządzania. Bariera ta wynika z zachowań menedżerów opartych na schematach poznawczych, które nabyli wraz z doświadczeniem zawodowym, i uniemożliwia zmianę procesu podejmowania przez nich decyzji; z niedocenienia znaczenia *information literacy*, czyli umiejętności, które warunkują odpowiednie posługiwanie się informacją i ich wykorzystanie; ze stosowania uproszczonych heurystyk w celu uniknięcia niedogodności podczas analizy informacji, np. heurystyki dostępności, zakotwiczenia, reprezentatywności.

Kolejną grupę stanowią bariery socjologiczne – wg J. Unolda, mimo że każda jednostka teoretycznie ma potencjalną zdolność do samodzielnej obserwacji i interpretacji świata, to w rzeczywistości tworzy ten obraz na podstawie przyjętych powszechnie norm społecznych, które ograniczają jej procesy percepcji i wpływają na sposób oceny obserwowanych zjawisk. Należy zatem przyjąć, że to, jak dany obiekt czy proces jest postrzegany przez daną grupę pracowników, ma wpływ na procesy informacyjne w firmie. Duże znaczenie ma tutaj kwestia podejmowania decyzji w grupie, jednorodność tej grupy i typ kultury organizacyjnej. Każdy z uczestników grupy stara się wpłynąć na percepcję, intencje, oceny, decyzje i konkretne działania pozostałych członków danej zbiorowości, tworząc bariery w prawidłowym obiegu informacji.

Czwarta grupa barier informacyjnych dotyczy złej organizacji i niedoskonałości zasobów technicznych. Zalicza się do nich bariery wynikające z niedopracowanej

metainformacji, w której zawarte są niepełne informacje na pytania: jakie informacje są dostępne w systemie? ile razy była wykorzystywana dana informacja? jaki sprzęt jest używany? jakie są potrzeby informacyjne użytkowników? Należy uwzględnić tu także bariery wynikające ze stosowania nieodpowiednich i złych kanałów informacyjnych służących do komunikacji między nadawcą a odbiorcą. Dobry kanał informacyjny nie powoduje zniekształcenia informacji, która jest przez niego przesyłana. Zły kanał generuje szumy informacyjne, takie jak: szumy techniczne (wadliwe działanie sprzętu), organizacyjne (błędne przekazywanie informacji), osobowościowe (psychofizyczne ograniczenia użytkowników), celowe. Ostatnia grupa barier informacyjnych powstaje w wyniku braku środków na implementację optymalnego systemu informacyjnego i skutkuje powstawaniem wielu „luk", które z kolei powodują złe zarządzanie informacją w firmie – są to bariery ekonomiczne. Niedoinwestowanie najczęściej wpływa na powstawanie innych rodzajów barier.

Część z wymienionych barier występuje także w systemach obronności i → b e z p i e c z e ń s t w a , szczególnie w zakresie zaspokajania potrzeb informacyjnych na poszczególnych szczeblach dowodzenia. G. Michalewski do istotnych utrudnień zalicza konieczność dokonywania ocen i prognoz → z a g r o ż e n i a [t. 4] w sytuacjach niepewności, czyli dużego niedoboru informacji, jaki charakteryzuje działalność operacyjną. Do barier informacyjnych szczególnie utrudniających ten proces zalicza brak jasno określonych procedur tworzenia ujednoliconych baz danych, co skutkuje stosowaniem indywidualnych zasad organizacji zasobów informacyjnych i utrudnieniami w sprawnym przepływie informacji.

Zgodnie z modelem zachowań informacyjnych Wilsona bariery informacyjne powstają w takim samym kontekście jak potrzeby informacyjne użytkowników informacji. Mogą być związane z ich cechami osobowymi (bariery personalne), z rolą społeczną, jaką pełnią (bariery interpersonalne), z warunkami zewnętrznymi (bariery środowiskowe). Bariery informacyjne wywierają negatywny wpływ nie tylko na potrzeby informacyjne i zachowania informacyjne związane z poszukiwaniem informacji, ale na przebieg całego procesu informacyjnego. Bez względu na miejsce występowania barier, tj. na etapie identyfikacji potrzeb, na etapie poszukiwania informacji czy na etapie jej użytkowania, wszystkie bariery można rozpatrywać łącznie, jedne wynikają z drugich, a pokonanie ich przyczynia się do powstawania nowego kontekstu potrzeb informacyjnych dla podmiotu, który przystępując do rozwiązywania kolejnych zadań informacyjnych, musi usunąć kolejne bariery informacyjne. Jest więc to model kontinuum.

Bariery informacyjne stanowią zagrożenie dla społecznego ładu informacyjnego, ponieważ zakłócają system komunikowania się poszczególnych osób i grup społecznych i uniemożliwiają swobodny obieg informacji między wszystkimi podmiotami procesu komunikacyjnego. Wzmacniają „nieład informacyjny" na każdym z etapów procesu informacyjnego. Zakłócają spójność ładu informacyjnego, czyli kompleksowość, aktualność, niesprzeczność norm, procesów, systemów i zasobów informacyjnych. Tymczasem

obywatelskie prawo do informacji oznacza nie tylko zapewnienie każdemu obywatelowi dostępu do jakościowo dobrej informacji potrzebnej mu do funkcjonowania w społeczeństwie i państwie, ale i pomoc w przezwyciężaniu barier informacyjnych ograniczających i utrudniających dostęp do rzetelnej i obiektywnej informacji. Zadaniem demokratycznego państwa jest usuwanie barier informacyjnych w celu zapewnienia społecznego ładu i → b e z p i e c z e ń s t w a i n f o r m a c y j n e g o .

Katarzyna Batorowska

W. Abramowicz, *Filtrowanie informacji*, Wydawnictwo Akademii Ekonomicznej w Poznaniu, Poznań 2008; M. Banacka, *Współczesne bariery w dostępie do informacji – kilka uwag w związku z ich typologiami i rodzajami*, 29.11.2004, e-Pedagogiczna.edu.pl (dostęp 12.02.2020); K. Batorowska, *Bariery informacyjne*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; T. Galewski, *Bariery informacyjne w przedsiębiorstwie*, „Zarządzanie i Finanse" 2012, R. 10, nr 1, cz. 1; J. Jaworski, *Bariery informacyjne w funkcjonowaniu małego przedsiębiorstwa*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług" 2011, nr 80; J. Oleński, *Ekonomika informacji*, PWE, Warszawa 2001; tenże, *Infrastruktura informacyjna państwa w globalnej gospodarce*, Uniwersytet Warszawski, Warszawa 2006; M. Popiołek, *Bariery rozwoju e-administracji w Polsce*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług" 2013, nr 105; *Procesy informacyjne w obronności i bezpieczeństwie. Teoria i praktyka*, M. Wrzostek (red.), AON, Warszawa 2017; J. Sobielga, *Psychologiczne aspekty barier informacyjnych – badania wśród studentów*, „Praktyka i Teoria Informacji Naukowej i Technicznej" 1997, nr 4; B. Stefanowicz, *Informacja*, Oficyna Wydawnicza SGH, Warszawa 2010; M. Świgoń, *Bariery informacyjne*, Wydawnictwo SBP, Warszawa 2006; taż, *Bariery informacyjne w środowisku naukowym. Badania pilotażowe*, „Przegląd Biblioteczny" 2003, t. 71; taż, *Zarządzanie wiedzą i informacją: podstawy teoretyczne, badania w wymiarze indywidualnym*, Wydawnictwo Uniwersytetu Warmińsko-Mazurskiego, Olsztyn 2012; J. Unold, *Teoretyczno-metodologiczne podstawy przetwarzania informacji w cyberprzestrzeni*, Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu, Wrocław 2011.

BAYRAKTAR – potoczna nazwa tureckiego bezzałogowego statku powietrznego. To → d r o n [t. 2] średniego pułapu o długim czasie lotu, zdolny do wykonywania lotów zdalnie sterowanych lub autonomicznych. Statek i jego uzbrojenie są kontrolowane przez załogę w naziemnej stacji kontroli. Producentem jest turecka firma wojskowa Baykar Makina Sanayi ve Ticaret A.Ş., założona w 1986 r. jako przedsiębiorstwo zajmujące się montażem części samochodowych. Od 2000 r. skupiła się na produkcji bezzałogowych statków powietrznych. Dron został nazwany na cześć założyciela firmy, Özdemira Bayraktara (tur. *bayraktar* oznacza 'ten który niesie flagę, sztandarowy'). Statki powietrzne występują w 3 klasach: lekkiej, średniej i ciężkiej. Najbardziej znanym modelem jest Bayraktar TB2. Może on latać przez 27 godzin bez przerwy i trafiać cele na odległość ponad 10 km. Cena jednego bezzałogowego statku waha się od 1 mln do 2,5 mln dolarów. Koszt zestawu obejmującego: 6 dronów, 2 mobilne naziemne punkty kontrolne, komplet broni oraz programów szkoleniowych dla operatorów i inżynierów to 30–70 mln dolarów.

Największym operatorem dronów TB2 jest armia turecka, ale model eksportowy został sprzedany armiom wielu krajów. Umowy na dostawy zostały już podpisane z 28 państwami. Obecnie drony TB2 są powszechnie używane przez Siły Zbrojne Ukrainy w wojnie rosyjsko-ukraińskiej. Pierwsze bezzałogowe statki powietrze tego typu zostały zakupione przez Ukrainę w 2018 r. We wrześniu 2019 r. w bazie szkoleniowej i produkcyjnej firmy Baykar rozpoczął się 3-miesięczny program szkoleniowy dla ukraińskich → ż o ł n i e r z y [t. 4] z obsługi i konserwacji systemu. Kursy, które obejmują część zarówno teoretyczną, jak i praktyczną, wymaganą do obsługi drona, zostały przewidziane w umowie podpisanej między Ukrainą a Turcją.

Podczas pierwszego kursu zostało przeszkolonych ponad 30 specjalistów – instruktorów, techników, operatorów, specjalistów naziemnego terminala danych i naziemnej stacji kontroli. Systemy Bayraktar TB2 zostały wprowadzone do służby bojowej w Ukrainie wiosną 2021 r. Od marca tego roku okazały się skuteczne w rozpoznaniu i dostarczały praktycznych danych na temat wroga. Systemy patrolowały nie tylko Donbas, lecz także południe i północ Ukrainy. 26 października 2021 r. media doniosły o pierwszym bojowym użyciu drona przez Ukrainę. Według Sztabu Generalnego Sił Zbrojnych Ukrainy w godzinach 14.25–15.15 bateria haubic D-30 rosyjskich sił ostrzelała pozycje armii ukraińskiej w pobliżu wsi Hranitne w obwodzie dniepropietrowskim. Wraz z początkiem ostrzału za pośrednictwem Specjalnej Misji Monitorującej OBWE wystosowano pilne żądanie zawieszenia broni, jednak zostało ono bez odpowiedzi. Aby zmusić wroga do przerwania ognia, głównodowodzący Sił Zbrojnych Ukrainy Wałerij Załużny nakazał użycie Bayraktara. Bezzałogowy statek powietrzny zniszczył haubicę rosyjską za pomocą bomby kierowanej MAM-C.

Na początku rosyjskiej → i n w a z j i [t. 2] na Ukrainę w lutym 2022 r. Ukraina miała ok. 20 dronów typu Bayraktar TB2 gotowych do wykonywania misji bojowych. Większość analityków wojskowych wątpiła w ich skuteczne wykorzystanie, uznając, że urządzenia zostaną szybko zestrzelone przez rosyjską obronę powietrzną. Praktyka pokazała jednak, że Bayraktary są bardzo skuteczne i odporne. 28 lutego ukraińskie siły powietrzne potwierdziły 2 ataki na rosyjskie cele za pomocą dronów, zlikwidowano wtedy konwój rosyjskiego sprzętu w obwodzie chersońskim. 2 marca 2022 r. Bayraktary zniszczyły ok. 180 sztuk rosyjskiego sprzętu w obwodzie sumskim. Dzięki atakowi drona ukraińskie wojsko było w stanie przechwycić i zbadać samobieżny przeciwlotniczy system rakietowy i działowy Pantsyr. 12 marca bezzałogowy statek zniszczył rosyjski system rakietowy Uragan.

Amerykański ekspert ds. zwalczania dronów Samuel Bendett w odniesieniu do Bayraktarów w Ukrainie zauważył, że Rosji jak dotąd nie udało się właściwie wykorzystać przeciwko dronom swoich systemów obrony powietrznej. To stwierdzenie potwierdziło się podczas operacji na Morzu Czarnym, kiedy to Bayraktar zakłócił obronę powietrzną rosyjskiego okrętu Moskwa, w wyniku czego został on trafiony przez ukraińskie rakiety. 8 maja 2022 r. dowództwo operacyjne sił rosyjskich Wostok

opublikowało nagranie wideo, na którym ukraiński Bayraktar TB2 zniszczył rosyjski śmigłowiec Mi-8 podczas próby lądowania rosyjskich wojsk na wyspie Zmijinyj. Do 12 września 2022 r. co najmniej 95 sztuk rosyjskiego sprzętu zostało zniszczonych przez bezzałogowe statki powietrzne.

Bayraktar jest obecnie jedynym ukraińskim dronem szturmowym tej klasy. Ma rozmiar małego samolotu, jest wyposażony w kamery i może być uzbrojony w 2 pociski przeciwpancerne UMTAS, które są naprowadzane laserowo (zasięg startu: 0,5–8 km), lub 4 precyzyjne bomby lotnicze, które mogą trafić cele w odległości 1 km. Dane techniczno-taktyczne drona przedstawiają się następująco:

- długość – 6,5 m,
- ładowność – 55 kg,
- maksymalna masa startowa – 650 kg,
- rozpiętość skrzydeł – 12 m,
- prędkość maksymalna – 222 km/h,
- prędkość przelotowa – 130 km/h,
- zasięg w zależności od wersji: pierwsza wersja – 150 km, zaktualizowana wersja – 300 km,
- autonomia – 24 h,
- pułap – 8200 m.

Bayraktar TB2 jest sterowany ze stacji naziemnej transportowanej pojazdem, wyposażonej w przesuwne szafy, klimatyzator, system filtracji powietrza NBC, zasilacze, systemy łączności bezprzewodowej i interkom. Stacje są w stanie wzajemnie przechwytywać sterowanie dronami, co pozwala na szybką zmianę → t a k t y k i [t. 5]. Zasięg operacyjny Bayraktarów obliczany jest nie od punktu startu, a od najbliższej stacji dowodzenia i kontroli.

Na wyposażeniu armii ukraińskiej znajdują się 2 wersje bezzałogowych statków Bayraktar TB2 o zasięgu 150 km i 300 km. Cechą wyróżniającą te drony jest precyzyjny optyczny system celowniczy wyposażony w kamery elektronooptyczne na podczerwień i dalmierz laserowy. Wykorzystanie Bayraktarów ma na celu rozpoznanie lub atak. Obecność głowicy optoelektronicznej pozwala na użycie dronów jako systemu rozpoznania powietrznego dalekiego zasięgu, co nie tylko zwiększa świadomość sytuacyjną dowództwa, ale także pozwala na zdalne dostosowanie ognia artyleryjskiego z jednoczesną oceną skuteczności ognia i strat wroga. Największą jednak zaletą drona jest jego zdolność do przenoszenia do 4 tureckich bomb MAM-L i MAM-C (naprowadzanych laserowo) na zewnętrznym podwieszeniu skrzydeł. Teoretycznie Bayraktar może trafić do 4 celów podczas 1 misji bojowej, atakując je zarówno jednocześnie, jak i sekwencyjnie. Może to być kilka wozów bojowych w tym samym czasie, np. z baterii obrony przeciwlotniczej, w marszu i podczas postoju. Jeżeli założyć, że Siły Zbrojne Ukrainy używały co najmniej 3 dronów dziennie, to w ciągu pierwszych 25 dni wojny mogły

one zniszczyć do 300 sztuk sprzętu wroga. Co ważne, wszystkie ataki następowały z zaskoczenia, głównie za liniami wroga.

W dostarczenie dronów zaangażowały się organizacje pozarządowe i wolontariusze, którzy organizowali zbiórki pieniędzy na rzecz Sił Zbrojnych Ukrainy. Najbardziej znaną akcją była zbiórka fundacji Serhija Prytuły. Pierwsza o zasięgu międzynarodowym odbyła się w czerwcu 2022 r. pod hasłem „Ludowy Bayraktar", jej celem było zebranie 500 mln hrywien (ok. 60 mln zł) na 3 drony szturmowe dla Sił Zbrojnych Ukrainy. W ciągu zaledwie 3 dni na rachunku było 600 mln hrywien (70 mln zł). Do zbiórki aktywnie dołączyli też obywatele polscy, którzy w ramach osobnej akcji uzbierali 7 mln zł. Przedstawiciele tureckiej firmy zbrojeniowej Baykar, którzy byli pod ogromnym wrażeniem tych działań, odmówili przyjęcia pieniędzy i przekazali drony za darmo. Za zebrane pieniądze została zakupiona satelita ICEYE, która robi zdjęcia miejsc dyslokacji przeciwnika i przekazuje je w zaledwie godzinę.

Bezzałogowe statki powietrzne Bayraktar TB2 od początku inwazji na pełną skalę odgrywają niezwykle ważną rolę w niszczeniu rosyjskich punktów dowodzenia i kontroli, obiektów obrony powietrznej, a także miejsc dyslokacji rosyjskich sił na linii frontu. Ponadto drony są aktywnie wykorzystywane przez marynarkę wojenną.

Ważnym przełomem dla producenta dronów było podpisanie umowy między Ukrainą a Turcją dotyczącej produkcji tych maszyn na terytorium Ukrainy. Porozumienie zostało podpisane w sierpniu 2021 r. Przedstawiciele firmy Baykar oświadczyli, że mimo pewnych przeszkód wynikających z trwającej wojny zakładają ukończenie budowy zakładu mechanicznego w Ukrainie w ciągu 2 lat.

Ukraina zajmuje ważne miejsce w łańcuchu dostaw Baykar, zwłaszcza gdy chodzi o nowy ciężki dron Akıncı i bezzałogowy myśliwiec Kızılelma, który jest obecnie w fazie opracowania. Do produkcji dronów wykorzystuje się ukraińskie silniki Motor Sicz i Iwczenko-Progress. „W rzeczywistości są to szeregowi, którzy idą naprzód, próbując zniszczyć obronę powietrzną rosyjskich wojsk, a za nimi podąża lotnictwo, które pomaga wspierać siły z powietrza" – wyjaśnia ekspert wojskowy i szef Centrum Studiów Wojskowych i Prawnych Ołeksandr Musienko. Główną jednak funkcją tych dronów jest nadal pozyskiwanie informacji wywiadowczych i dostarczanie instrukcji celowania dla innych środków rażenia, takich jak → a r t y l e r i a [t. 1]. Mimo tak ważnych zadań, które spełniają w Ukrainie bezzałogowe statki powietrzne, obecnie najwyższym priorytetem nadal jest obrona przeciwlotnicza i ciężka artyleria, która jest w stanie i zniszczyć cele na większych odległościach.

Anna Netreba

A. Maciejewski, *Bayraktar TB2 jako system operacyjny*, „Wojsko i Technika" 2021, nr 6; Ministerstwo Obrony Narodowej, *Bezzałogowce BAYRAKTAR TB2*, https://www.gov.pl/web/obrona-narodowa/bezzalogowce-bayraktar-tb2 (dostęp 20.05.2023); M. Strembski, *Bayraktar TB2 rozwija skrzydła,* „Lotnictwo" 2021, nr 6; tenże, *Bojowe powietrzne bezzałogowce w tureckim wydaniu*, „Nowa Technika Wojskowa" 2016, nr 2; D. Winkie, *Ukraine Receives More Armed*

Drones Amid Russian Invasion, 4.03.2022, https://www.militarytimes.com/flashpoints/ukraine/2022/03/03/ukrainereceives-more-armed-drones-amid-russian-invasion/ (dostęp 20.05.2023); Т. Мележик, *Що таке „Байрактар": основні характеристики, де використовується,* 9.03.2022, https://tsn.ua/ato/scho-take-bayraktar-osnovni-harakteristiki-de-vikoristovuyetsya-2004037.html (dostęp 20.05.2023); *На що здатні турецькі БПЛА Bayraktar TB2 і як їх використовує Україна у війні з рашистами*, 24.04.2022, https://defence-ua.com/weapon_and_tech/smert_z_neba_vijskovi_eksperti_pro_ mozhlivosti_bayraktar_tb2_u_borotbi_z_rosijeju-7062.html (dostęp 20.05.2023).

BAZA LĄDOWA (ang. *ground base*) – pojęcie różnie definiowane, sięgające starożytności. Dla części badaczy baza lądowa to miejsce lub obszar przeznaczone – w miarę możliwości – do wszechstronnego zabezpieczenia działalności bojowej, zaopatrzenia i stacjonowania wojsk, z którego prowadzi się lub wspiera operacje. Bywają w niej zlokalizowane regionalne lub ogólnokrajowe centra dowodzenia. W bazie lądowej prowadzi się również szkolenie oddziałów. Wycofanym do niej oddziałom baza lądowa ułatwia odtworzenie zdolności bojowej i powrót na linię frontu. Musi być więc wyposażona m.in. w odpowiednią infrastrukturę, urządzenia i materiały niezbędne do funkcjonowania bazy, zapewniania wsparcia logistycznego dla jednostek walczących z wrogiem, a także musi zapewnić im w trakcie operacji ciągłość zasilania materiałowego. Baza lądowa zawiera m.in. koszary, magazyny (m.in. uzbrojenia oraz paliw), warsztaty remontowe, poligony, wyrzutnie, szpitale, składy żywności oraz umocnienia i zapory inżynieryjne. W tym samym czasie w tak definiowanej bazie lądowej można także spotkać np. sklepy z bronią i boiska.

Badacze postrzegają omawiane pojęcie też nieco inaczej, jako odpowiednio przygotowany i wyposażony obiekt wojskowy. Przeznaczony jest do okresowego lub stałego przebywania w nim wojska.

Dla jednych badaczy bazy lądowe mogą wykorzystywać tylko → w o j s k a l ą d o w e [t. 4] (np. bez wojsk inżynieryjnych czy chemicznych), drudzy uznają, że decydującym kryterium jest stały ląd, na którym usytuowana jest baza. Próbując dopasować terminologię do rzeczywistości, część naukowców słusznie uznaje, że w jednej bazie lądowej mogą równocześnie stacjonować jednostki kilku rodzajów sił zbrojnych. Nieco bardziej kontrowersyjne jest wliczanie przez niektórych badaczy do baz lądowych znajdujących się na lądzie baz sił powietrznych, baz → m a r y n a r k i w o j e n n e j [t. 3] oraz wykorzystywanych przez wojsko baz rzecznych. W tej interpretacji bazy lądowe obejmują zdecydowaną większość wszystkich baz wykorzystywanych przez wojsko. Do wyjątków można by wówczas zaliczyć np. bazy pływające. Dla tych naukowców baza lądowa jest organizowana oraz utrzymywana na lądzie w zależności od sytuacji przez różne rodzaje wojsk: lądowe, marynarkę wojenną i lotnictwo. Poszczególne rodzaje wojsk mogą tu współpracować lub tworzyć bazę samodzielnie (przykładem są bazy lotnicze morskie). Słabą stroną takiego zdefiniowania analizowanego pojęcia jest fakt, że w obręb bazy morskiej wchodzi także przyległy akwen.

Z drugiej jednak strony można wyobrazić sobie bazę, przez której środek przepływa niewielka rzeka.

Sytuację dodatkowo komplikuje spotykany w literaturze podział baz lądowych na bazy materiałowo-techniczne (uznawane przez część badaczy za równorzędne bazom lądowym w ramach pojęcia → b a z w o j s k o w y c h), remontowe (przeznaczone do naprawy uzbrojenia i sprzętu technicznego) i przeładunkowe (przemieszczające zaopatrzenie np. z samochodów na transport kolejowy).

W literaturze przedmiotu pojawiają się także inne terminy, które ze względu na ogólnikowość najszerszej definicji analizowanego pojęcia można również zaliczyć do baz lądowych. Przykładem są bazy logistyczne (niekiedy traktowane jako pojęcie równorzędne bazie lądowej), bazy zaopatrzenia i bazy materiałowe. Te pierwsze pełnią ważną funkcję wojskową przy magazynowaniu i dystrybucji. Zawierają m.in. zapasy sprzętu wojskowego i środków materiałowych. Z baz logistycznych przepływ środków zaopatrzenia kierowany jest do pododdziałów rozlokowanych w danej części kraju i/lub walczących na froncie. Prowadzą one także działalność obsługowo-remontową. W ich skład wchodzą więc np. warsztaty techniczne i związany z nimi stacjonarny i mobilny potencjał obsługowo-naprawczy. Bazy logistyczne wpływają też na działalność wojskowych oddziałów gospodarczych. Częstotliwość napraw w bazie logistycznej zależy m.in. od intensywności działań bojowych, jakości sprzętu, jego stopnia zużycia i daty wyprodukowania.

Wpływ na wykorzystywanie baz lądowych w zakresie zaopatrzenia mają m.in.: przewidywanie lub rozpoczęcie konfliktu zbrojnego, położenie geograficzne miejsca stacjonowania danej jednostki wojskowej, miejsce zaopatrywania (kraj, konflikt zagraniczny) oraz wielkość środków finansowych, które przeznaczają na bazy władze państwowe.

Na poziom wyposażenia i gotowości baz lądowych danego państwa wpływa m.in. polityka jego władz, uwarunkowania geograficzne, sprawność systemu logistycznego oraz poziom → k o r u p c j i [t. 2].

Jeśli państwo dysponuje odpowiednią liczbą nowoczesnych samolotów, misją bazy powietrznej jest, jak wskazuje M. Boulègue, zapewnienie państwu wielowarstwowej obrony powietrznej w danym regionie. Analogiczną funkcję na innych polach pełnią pozostałe bazy zaliczane do baz lądowych. Odpowiednie strategicznie rozmieszczenie baz lądowych ułatwia także egzekwowanie praw państwa na danym terytorium.

Stanowi równocześnie pokaz siły państwa i ułatwia pilnowanie jego granic. W czasie działań wojennych wykorzystanie baz lądowych ułatwia realizację działań siłom głównym zarówno podczas ataku, jak i obrony. Sprzyjają np. stawianiu skutecznego oporu nacierającym wojskom przeciwnika i utrzymaniu ważnego strategicznie obszaru. Bazy lądowe są także oparciem dla potencjalnych operacji wojskowych państw sojuszniczych.

Wielkość bazy lądowej może być bardzo różna. Przykładowo baza na poziomie taktycznym na zapleczu sił przeciwnika może być tworzona również przez bardzo

nieliczne oddziały. Należą do nich struktury, które zostały odcięte od sił głównych, zostały na obszarze, z którego wycofały się siły główne, lub które zostały specjalnie skierowane do działań w zgrupowaniu na zapleczu przeciwnika. W takich przypadkach baza lądowa bywa podstawowym elementem pozwalającym przetrwać zgrupowanym w tych jednostkach → ż o ł n i e r z o m [t. 4]. Na tym poziomie S. Heberski i D. Kozerawski wyróżniają bazy główne, stałe, zapasowe i przejściowe. Zbliżonym pojęciem do tak usytuowanych baz lądowych jest rejon bazowy. Jest on definiowany jako przygotowany inżynieryjnie i uzbrojony obszar na zapleczu sił przeciwnika. Rozmieszczonym w nim wojskom ma umożliwić skuteczną i długotrwałą walkę. W świetle niektórych opisanych wyżej interpretacji rejon bazowy także można zaliczyć do baz lądowych.

Utrzymanie połączenia działających na froncie jednostek wojskowych z bazami lądowymi to zadanie linii komunikacyjnych. W omawianym przypadku pojęcie to obejmuje wszystkie drogi lądowe, a w wypadku wielu baz lądowych też powietrzne i wodne. Za ich pośrednictwem jest dostarczane na front zaopatrzenie i uzupełnienia. Układ linii komunikacyjnych oraz odległość od frontu poważnie wpływają na zmiany znaczenia danej bazy dla jednostek walczących na froncie. Patrząc w dłuższej perspektywie czasowej, bazy lądowe także pod wieloma względami są przecież zależne od zaopatrzenia z zewnątrz.

W części baz lądowych tworzy się centra działań obronnych. Skupiają się one na zagadnieniach dowodzenia, planistycznych, zabezpieczenia logistycznego itp. Obrona bazy (i troska o jej → b e z p i e c z e ń s t w o wewnątrz) jest koordynowana przez dowódcę bazy lub dowódcę zespołu baz lądowych. Ważną rolę w realizacji powyższego odgrywa rozpoznanie techniczne. Zajmuje się ono m.in. ustaleniem stanu infrastruktury technicznej i obiektów ją otaczających.

Jak wskazuje L.M. Coulter, obrona bazy jest bardzo istotna w przypadku wypełnionych samolotami baz lotniczych. Biorąc pod uwagę ograniczoną obecnie liczebność sił powietrznych poszczególnych państw, poprzez nagły, skuteczny atak przeciwnik jest w stanie zadać bardzo dotkliwe straty. Zdaniem wielu badaczy w XXI w. zmalało znaczenie wojskowe baz lądowych, czego najważniejszymi przyczynami są rozwój → techniki wojskowej [t. 4] i zmiany taktyki w XXI w. Nadal jednak stanowią one najważniejszą część zabezpieczenia materiałowo-technicznego. W części przypadków zachowały duże znaczenie strategiczne. Nieprzypadkowo w ostatnim pięcioleciu zbudowano nowe bazy lądowe w graniach państwa (np. w Rosji) i poza jego granicami (np. pierwsza baza chińska) czy rozbudowano istniejące (baza japońska w Dżibuti).

Przynależność baz lądowych do baz wojskowych (baz wojennych) jest w literaturze sporna. Część specjalistów uznaje bowiem, że pojęcie bazy wojskowej dotyczy tylko baz danego państwa zbudowanych poza jego granicami.

Część pojęcia bazy lądowej pokrywa się z pojęciami wojskowej bazy obsługowo-naprawczej, → i n f r a s t r u k t u r y w o j s k o w e j [t. 2] i infrastruktury

technicznej. Omawiane pojęcie jest równocześnie czymś odrębnym od bazy mobilizacyjnej jednostki wojskowej. Mniej jednoznaczne są relacje z pojęciem bazy operacyjnej. Dla jednych badaczy jest ona pojęciem odrębnym od baz lądowych, inni bazy strategiczne wyróżniają w ramach baz morskich. Przy tak dużych rozbieżnościach odnośnie do zakresu pojęcia nie dziwi, że pojęcie bazy lądowej jest stosunkowo rzadko używane w literaturze przedmiotu.

Tomasz Skrzyński

M. Boulègue, *Military Infrastructure and Logistics in the Russian Arctic*, [w:] tegoż, *Russia's Military Posture in the Arctic: Managing Hard Power in a „Low Tension" Environment*, Hatham House, The Royal Institute of International Affairs, London 2019; L.M. Coulter, *You Own It: The Commander's Responsibility for Air Base Defense*, [w:] *Defending Air Bases in an Age of Insurgency*, vol. 2, S.W. Caudill, T.H. Deale, B.D. Spacy (eds.), Air University Press, Montgomery 2019; M.A. Hassan, *Growing China-India Competition in the Indian Ocean*, „Strategic Studies" 2019, vol. 39, no. 1; A.J. Vick, *Air Base Attacks and Defensive Counters: Historical Lessons and Future Challenges*, RAND Corporation, Santa Monica 2015; S. Haberski, D. Kozerawski, *Baza w działaniach taktycznych*, „Przegląd Wojsk Lądowych" 1996, nr 12; R. Jakubczak, *Działania operacyjne obrony terytorialnej na rzecz ochrony tyłów oraz administracji terenem, zasobami, rezerwami, infrastrukturą i zabezpieczeniem materiałowo-technicznym. Terytorialna ochrona strefy tyłowej (baz i garnizonów)*, „Myśl Wojskowa" 2004, nr 1 (630); M. Kalwasiński, C. Wojdat, M. Morawski, *Podsystem materiałowy*, [w:] *System logistyczny Sił Zbrojnych Rzeczypospolitej Polskiej. Raport 2019*, T. Jałowiec i in. (red.), Akademia Sztuki Wojennej, Warszawa 2019; D. Nagrabski, *Podsystem techniczny*, [w:] *System logistyczny Sił Zbrojnych Rzeczypospolitej Polskiej. Raport 2019*, T. Jałowiec i in. (red.), Akademia Sztuki Wojennej, Warszawa 2019; *Przedmiot badań i system pojęć współczesnej sztuki wojennej. Materiały z konferencji naukowej*, A. Czupryński (red.), AON, Warszawa 2006.

BAZA WOJSKOWA – obiekt powstały w celu wspierania logistyki i operacji wojskowych, stanowiący własność wojska i przez nie zarządzany. Bazy wojskowe dzieli się zwykle na lądowe (zob. → b a z a l ą d o w a), powietrzne i morskie. W zależności od ich specyficznych funkcji bazy wojskowe mogą pełnić funkcję magazynu zapasów broni, stanowiska wywiadowczego, miejsca testowania broni, planowania operacji wojskowych oraz stanowić zaplecze gospodarcze dla korpusu wojskowego. Bazy wojskowe są także określane jako instalacje rutynowo używane przez siły zbrojne, teren, na którym się znajdują, kapitał w postaci statycznych urządzeń, zapasów i sprzętu. W bazach stale stacjonuje określony zasób pracowników, od → ż o ł n i e r z y [t. 4], przez pracowników paramilitarnych, po cywilów. Bazy wojskowe dzieli się również na wewnętrzne, funkcjonujące na terenie danego państwa oraz zagraniczne.

Zagraniczna baza wojskowa jest także instrumentem mającym strategiczne znaczenie w stosunkach międzynarodowych, nie ma wątpliwości co do istotności zagranicznych baz wojskowych dla zwiększania → b e z p i e c z e ń s t w a m i ę d z y n a r o d o w e g o i stabilności oraz ich wpływu na równowagę sił w globalnej → g e o p o l i t y c e [t. 2]. Mimo że zakończenie → z i m n e j w o j n y [t. 4] przyniosło zmiany w polityce → b e z p i e c z e ń s t w a, które stworzyły silną potrzebę

współpracy i budowania zaufania między państwami na całym świecie, zagraniczne bazy wojskowe nie straciły na znaczeniu. Kluczowy jest tu interes strategiczny uzgadniany przez państwo przyjmujące i państwo tworzące bazę wojskową, co uzasadnia perspektywę tworzenia dalszych sojuszy i jest wykorzystywane jako zabezpieczenie przed przyszłymi → z a g r o ż e n i a m i b e z p i e c z e ń s t w a [t. 4]. Tworzenie baz zagranicznych jest w dużej mierze zdeterminowane przez międzynarodową strukturę systemu stosunków międzynarodowych, w którym duże państwa mają silniejszy głos.

Obecnie USA mają prawdopodobnie największy zbiór baz wojskowych w historii świata, w sumie ponad 5,3 tys. na całym świecie, z czego szacuje się, że ponad 1 tys. baz poza własnym terytorium, przy czym istnienie niektórych z nich nie jest jawne. Krytycy wskazują, że masowe rozmieszczenie sił USA na suwerennym terytorium innych państw pozwala określić USA mianem imperium baz wojskowych. Oficjalnie ponad 190 tys. żołnierzy i 115 tys. pracowników cywilnych jest zgromadzonych w 909 obiektach wojskowych w 46 krajach i na terytoriach zależnych. Wojsko USA jest właścicielem lub wynajmuje ponad 3200 tys. km^2 ziemi, 26 tys. budynków i budowli o wartości 146 mld USD. Te oficjalne liczby nie wyczerpują wiedzy o skali amerykańskiego zaangażowania w budowę i rozwój baz wojskowych, gdyż nie obejmują masowej budowy i obecności wojsk w Iraku i Afganistanie w ciągu wielu ostatnich lat, a także tajnych lub niepotwierdzonych obiektów w Izraelu, Kuwejcie, na Filipinach i w wielu innych miejscach na świecie. W ciągu zaledwie 3 lat trwania wojen w Iraku i Afganistanie wydano 2 mld USD na budowę baz wojskowych. Tylko jeden obiekt w Iraku, port lotniczy Al-Bakr w mieście Balad, funkcjonujący jako amerykańska baza lotnicza, kwaterował 30 tys. żołnierzy i 10 tys. innych pracowników, rozciągając się na 41 km^2 z dodatkowym „obwodem bezpieczeństwa" o powierzchni 31 km^2.

Zagraniczne bazy wojskowe są często tworzone tam, gdzie dane państwo ma szczególne interesy, gdzie chce bezpośrednio lub w inny sposób budować imperium, wykorzystać instrumenty polityki zagranicznej, prawa i gospodarki innego państwa. Bazy wojskowe mogą więc także służyć realizacji strategicznych racjonalnych celów politycznych, a nie tylko militarnych. Utrzymywanie zagranicznych baz wojskowych poza → N A T O [t. 3] umożliwia państwom przyjmującym obronę przed eskalacją → z a g r o ż e ń [t. 4] atakami, zapewnienie bezpieczeństwa innym państwom, ale może też pozwolić na ingerencję w procesy gospodarcze. Na przykład Portugalczycy w XVI w. zajęli porty wzdłuż indyjskiego wybrzeża i stworzyli tam swoje bazy wojskowe, ustanowili patrole morskie i zbudowali fortyfikacje, aby zagwarantować sobie monopol w handlu przyprawami. Mieszkańcy próbujący przedostać się przez ufortyfikowane porty zostali zmuszeni do zapłaty za przejazd. Według najnowszych badań zagraniczne bazy wojskowe były często wykorzystywane do kontrolowania życia gospodarczego i politycznego państw przyjmujących. Na przykład zagraniczne bazy wojskowe USA w Korei służyły sprawowaniu kontroli nad koreańską polityką

zagraniczną i ich siłami zbrojnymi w czasie → w o j n y [t. 4], umożliwiając w ten sposób siłom amerykańskim uzyskanie kluczowego wsparcia wojskowego i politycznego podczas niektórych operacji wojskowych, np. w Syrii i Wietnamie.

Amerykańskie instalacje wojskowe, na co zwrócono już uwagę, są rozproszone po całych USA i reszcie świata, jednak większa niż gdzie indziej koncentracja baz występuje w południowo-zachodniej i południowo-wschodniej części USA i wzdłuż wybrzeża środkowego Atlantyku. Bazy te są zróżnicowane, od stosunkowo niewielkich obiektów takich jak skupisko budynków dla lokalnej jednostki Gwardii Narodowej, aż do dużych baz, których obsada jest porównywalna z populacją średnich miast, niektóre z liczbą ponad 100 tys. żołnierzy i pracowników. Wiele baz wojskowych posiada znaczne zasoby ziemi, które mogą stanowić bufor wokół wrażliwych lub hałaśliwych obiektów wojskowych takich jak pasy startowe na lotniskach albo składy amunicji, mogą mieć też krytyczne znaczenie dla ćwiczeń szkoleniowych z wykorzystaniem ostrej amunicji, strzelnic, testów broni i innego rodzaju intensywnych działań wojskowych.

H.E. Balbach i in. badacze baz wojskowych w USA analizowali zmieniające się historycznie powody lokalizacji baz i stwierdzili, że początkowo były one umiejscowione tam, gdzie mogły zapewnić ochronę portów, żeglownych rzek, dróg lądowych i kolei. Następnie, w XX w., ponieważ bazy rozmieszczano zazwyczaj poza USA, zdolność do szybkiego i skutecznego użycia siły stawała się coraz ważniejszym kryterium lokalizacji, dlatego dostęp do lotnisk, linii kolejowych, dróg międzystanowych i portów zyskał na znaczeniu. Lokalizację baz wojskowych w USA niekiedy porównuje się z lokalizacją miast w USA, które są skoncentrowane we wschodniej części kraju. Grupowanie ośrodków miejskich w odległości 100 km od linii brzegowej i bardzo silnie zurbanizowanego regionu wzdłuż korytarza Waszyngton–Boston ilustruje tendencję do lokalizacji miast i instalacji wojskowych w południowo-wschodniej i środkowo-zachodniej części USA, co częściowo odzwierciedla fakt, że rozwój urbanistyczny miast nastąpił wokół instalacji wojskowych po ich ustanowieniu. Obecnie często na takich obszarach znajduje się wspólna infrastruktura miejska.

W ostatnich dziesięcioleciach w USA powstało niewiele nowych baz, a wiele z nich zamknięto lub zdecydowano o innym ich zastosowaniu. Kilka baz rozszerzyło swoje granice, tak jak Fort Carson w Kolorado – gdzie dodano duży obszar treningowy (Pinon Canyon) w latach 80. – i Fort Irwin na pustyni Mojave w Kalifornii, który powiększono w latach 90. Zmiany zwiększające obszar baz są jednak wyjątkami wynikającymi z konieczności dostosowania się do dużych wymagań związanych z prowadzeniem szkoleń z wykorzystaniem dużych pojazdów lądowych. Zamknięcia i ekspansje baz odzwierciedlają zmieniające się priorytety misji, ale też lokalne opinie społeczne na temat obecności wojska, która w jednym miejscu jest postrzegana jako kamień węgielny gospodarki, podczas gdy w innym jest potępiana za zajmowanie cennych nieruchomości, które mogłyby zostać ulepszone i bardziej racjonalnie użytkowane w przypadku przekształcenia we własność prywatną.

Ochrona sieci komunikacyjnych, gromadzenia danych oraz sieci dowodzenia i kontroli stała się decydującym czynnikiem dla lokalizacji nowych obiektów wojskowych. Instalacje wojskowe mogą znajdować się w krytycznych węzłach sieci danych, telekomunikacji, energii i żeglugi. Chociaż lokalizacja geograficzna jest nadal ważna, krajobraz lokalizacji nie wiąże się tylko z szerokością i długością geograficzną, lecz także obejmuje przestrzeń wirtualną, mobilną i pozaziemską. Te zmiany uwarunkowań lokalizacyjnych mogą w krótkim okresie mieć niewielki wpływ na bazy wojskowe, ale w ciągu kolejnych dziesięcioleci mogą radykalnie zmienić wykorzystanie i potrzebę istnienia baz tradycyjnych.

Zurbanizowane bazy wojskowe, nie tylko w USA, są podobne do miast, którymi tak jak bazami wojskowymi zarządza się jak zasobami publicznymi. Na bazy wojskowe często składają się strefy mieszkalne, handlowe, biurowe, rekreacyjne i przemysłowe – jak w miastach. Jednak w przypadku instalacji wojskowej dowódca jest odpowiedzialny za wszystkie aktywa i operacje – ziemię, personel, obiekty i usługi – w jej granicach wyznaczanych przez ogrodzenie. Bazy wojskowe mogą mieć bardzo znaczną populację z ogromną liczbą pracowników, więc obecność i żywotność tych instalacji może silnie wpływać na społeczności lokalne, które są w określonym stopniu zaangażowane także w kluczowe decyzje dotyczące samej bazy.

Obecność wojsk na obcych ziemiach to zjawisko znane od starożytności i nie należy wiązać baz wojskowych jedynie z obecną ich rolą w polityce zagranicznej. Bazy wojskowe aktualnie służą głównie realizacji długoterminowych zadań sił zbrojnych, co może wynikać ze stacjonowania wojsk, rezolucji ONZ, dwustronnych lub wielostronnych porozumień obronnych i pokojowych. Przed wojnami napoleońskimi Wielka Brytania jako pierwsza stworzyła globalną sieć baz wojskowych, obejmującą wiele punktów. W szczytowym momencie Imperium Brytyjskie rozwinęło swoją główną bazę → m a r y n a r k i w o j e n n e j [t. 3], tworząc placówki w miejscach takich jak Gibraltar, Kapsztad, Mauritius, Singapur, Hongkong, Malta, Suez czy Aden. Całe wybrzeże Morza Śródziemnego od dawna stanowi obszar konkurencji o dostęp do baz. Podczas szczytu zimnej wojny główne amerykańskie bazy morskie i powietrzne w Rocie (Hiszpania), Sigonelli (Sycylia), La Maddalenie (Sardynia), Neapolu, Pireusie, Sudzie (Kreta) i Izmirze (Turcja) były zrównoważone przez dostęp radziecki do Annaby (Algieria), Trypolisu (Libia), Aleksandrii i Port Said. Nawet po zakończeniu zimnej wojny bazy pozostały ważne, chociaż strategiczne względy związane z instalacją baz wojskowych nabrały innego znaczenia. Kontrowersyjną kwestią związaną z bazami wojskowymi, zwłaszcza z potęgami postkolonialnymi w byłych koloniach, jest to, czy stoją one w sprzeczności z zasadą → s u w e r e n n o ś c i p a ń s t w a [t. 4]. Niektórzy eksperci twierdzą, że bazy wojskowe nie mogą naruszać suwerenności państwa, którą należy szanować za wszelką cenę. Inni – wręcz przeciwnie – twierdzą, że jeśli państwo uzyskało prawo do rozmieszczania swoich sił w granicach innego państwa za zgodą państwa przyjmującego, państwo wysyłające

ma wyłączną jurysdykcję nad swoimi siłami, a nie ma zwierzchnictwa nad żadną ich częścią państwo przyjmujące.

Jakub Idzik

L. Andersson, J. Lundberg, M. Sjöström, *Regional Effects of Military Base Closures: The Case of Sweden*, „Defence and Peace Economics" 2007, vol. 18, no. 1; G. Duman, V. Ferlengez, *Setting Up Overseas Military Bases In Line With International Security*, „İstanbul Aydın Üniversitesi Dergisi" 2018, vol. 10 (3); E. Fitz-Henry, *US Military Bases and Anti-Military Organizing: An Ethnography of an Air Force Base in Ecuador*, Palgrave Macmillan, New York 2015; B.A. Harmon, W.D. Goran, R.S. Harmon, *Military Installations and Cities in the Twenty-First Century: Towards Sustainable Military Installations and Adaptable Cities*, [w:] *Sustainable Cities and Military Installations*, I. Linkov (ed.), Springer, Dordrecht 2012; S. Kawana, *Base Politics and the Hold-up Problem*, [w:] *The Influence of Sub-state Actors on National Security: Using Military Bases to Forge Autonomy*, M. Takahashi (ed.), Springer, Cham 2019; C. Lutz, *Introduction: Bases, Empire, and Global Response*, [w:] *The Bases of Empire: The Global Struggle against US Military Posts*, C. Lutz (ed.), Pluto Press, London 2009; E.A. Martini, *Proving Grounds: Militarized Landscapes, Weapons Testing, and the Environmental Impact of U.S. Bases*, University of Washington Press, Seattle–London 2015; *Military Bases: Historical Perspectives, Contemporary Challenges*, L.N. Rodrigues, S. Glebov (eds.), IOS Press, Amsterdam 2009; A. Stergiou, *The Exceptional Case of the British Military Bases on Cyprus*, „Middle Eastern Studies" 2015, vol. 51, no. 2; D. Vine, *Island of Shame: The Secret History of the U.S. Military Base on Diego Garcia*, Princeton University Press, Princeton 2009.

BELLINGCAT – zarejestrowany w Holandii anglojęzyczny i dostępny także w języku rosyjskim serwis internetowy specjalizujący się w dziennikarstwie śledczym i w sprawach międzynarodowych. Został oficjalnie założony 14 lipca 2014 r. w Leicester w środkowej Anglii (Wielka Brytania) przez Eliota Higginsa, wówczas blogera, pracownika biurowego, który sam nazywał siebie maniakiem gier komputerowych. Na koniec 2020 r. serwis miał 18 pełnoetatowych pracowników i 30 współpracowników w ponad 20 krajach na całym świecie. Misję serwisu Eliot Higgins opisał w sposób następujący:

> Nasza dyscyplina jest tak nowa, że nawet nie ma jednolitej nazwy. Najczęściej używanym określeniem jest biały wywiad, czyli zdobywanie informacji z ogólnie dostępnych źródeł, tak zwany OSINT (ang. open-source intelligence). Jest to jednak pojęcie wywodzące się z rządowych służb wywiadowczych, których tajne metody odbiegają od jawnej i publicznej misji Bellingcat. Bardziej trafne określenie to internetowe dziennikarstwo śledcze. Ale nasze działania znacznie wykraczają poza zwykłe poszukiwania w sieci. Walczymy z siłami, które wypaczają fakty i wprowadzają społeczeństwo w błąd. Kładziemy nacisk na gromadzenie dowodów. Pokazujemy zwykłym obywatelom, jak ujawniać przestępstwa i domagać się odpowiedzialności od możnych i wpływowych.

Nazwa serwisu jest bezpośrednio związana z jego misją. Od 2011 r. na swoim blogu, koncie na Twitterze i forum „Guardiana" Eliot Higgins jako Brown Moses dzielił się swoimi odkryciami m.in. na temat → w o j n y d o m o w e j [t. 4] w Syrii

między siłami prezydenta Baszszara al-Asada a opozycją. Jego pseudonim pochodził od piosenki Franka Zappy. Nazwa Bellingcat została wybrana w sposób bardziej przemyślany: nawiązuje do popularnej bajki i kreskówki „Belling the cat", która opowiada historię kota będącego postrachem myszy. Mimo że gryzonie biegały szybciej od ssaka, ten stanowił dla nich → z a g r o ż e n i e [t. 4], ponieważ nie wiedziały, kiedy nadchodzi. Postanowiły więc zawiesić mu na szyi dzwoneczek. Problemembyło jedynie znalezienie odważnej jednostki, która podejmie się zadania. „To było to – nasza nazwa i nasza misja. Zawieszanie dzwoneczków na szyjach drapieżnych kotów" – tłumaczy Higgins.

Internetowi dziennikarze śledczy, wśród których znajdują się wolontariusze z całego świata, zgodnie z mottem serwisu Bellingcat „Odkrywać. Weryfikować. Nagłaśniać" ujawniają sprawy pominięte przez → o p i n i ę p u b l i c z n ą [t. 3] lub możliwe do znalezienia w sieci. Weryfikują dowody w celu późniejszego nagłośnienia wszystkich zdobytych → i n f o r m a c j i [t. 2]. Ustalenia powstałe w ten sposób są łatwe do zweryfikowania. Bellingcat wykorzystuje platformy powszechnie dostępne dla internautów, jak branżowe fora internetowe, blogi, → m e d i a s p o ł e c z n o ś c i o w e [t. 3], takie jak Twitter, Instagram, Facebook czy VKontakte i komunikatory jak Telegram, Discord czy WhatsApp. Zaczerpnięte z nich informacje są weryfikowane dzięki takim narzędziom jak Google Maps, Google Earth, Google Translate, SunCalc czy Truecaller.

Jedno z pierwszych śledztw Bellingcat dotyczyło 298 ofiar śmiertelnych pasażerów samolotu MH17 linii Malaysia Airlines zestrzelonego 17 lipca 2014 r. w obwodzie donieckim nad wschodnią Ukrainą, czyli 3 dni po powstaniu serwisu. W trakcie dziennikarskiego śledztwa Bellingcat odkrył kluczowe informacje, które odpowiedzialnością za te wydarzenia obarczały Rosję. Ujawnił (co później potwierdzili międzynarodowi śledczy), że wyrzutnia do pocisków rakietowych Buk została sprowadzona na wschodnią Ukrainę z Rosji, a po zestrzeleniu Boeinga 777 przez prorosyjskich separatystów wróciła do Rosji. Higgins wyjaśniał: „Kiedy pracowaliśmy nad Ukrainą, co zaczęło się od sprawy zestrzelenia samolotu MH17 malezyjskich linii lotniczych 17 lipca 2014 r., to doprowadziło nas do odkrycia zaangażowania Rosji w konflikt na Ukrainie. A dzięki temu dowiedzieliśmy się, że młodzi → ż o ł n i e r z e [t. 4], którzy jeździli z Rosji na Ukrainę potajemnie walczyć po stronie separatystów, dosyć swobodnie udostępniali informacje w mediach społecznościowych. Ci żołnierze byli rekrutami, młodymi chłopakami, którzy po prostu robią takie rzeczy, a to doprowadziło nas do wielu odkryć, które inaczej byłyby niemożliwe […]. Oprócz tego było też wielu lokalnych mieszkańców, Rosjan i Ukraińców, którzy nagrywali lub robili zdjęcia sprzętowi wojskowemu i żołnierzom. W niektórych przypadkach pozwalało nam to połączyć ze sobą jakąś jednostkę albo wóz wojskowy, który był na Ukrainie, a wcześniej znajdował się w Rosji. Dokładnie tak prześledziliśmy trasę wyrzutni rakiet, która zestrzeliła MH17".

Bellingcat zdemaskował również 3 podejrzanych o próbę otrucia za pomocą nowiczoka Siergieja Skripala, podwójnego agenta MI6, oraz jego córki Julii w Salisbury w marcu 2018 r. Wskazane osoby okazały się wysokimi rangą oficerami rosyjskiego → w y w i a d u [t. 4] wojskowego. W 2021 r. Republika Czeska oskarżyła Rosjan o spowodowanie wybuchów w 2 składach amunicji. Do eksplozji doszło w 2014 r. w rejoniemiejscowości Vrbětice, we wschodnich Czechach, blisko w granicy ze Słowacją. W zdarzeniach śmierć poniosły 2 osoby. Bellingcat poinformował, że wybuchy w czeskim składzie amunicji, próba zamachu na bułgarskiego biznesmena Christo Gebrewa oraz wybuchy w bułgarskich magazynach amunicji w 2015 r. są ze sobą powiązane i stanowiły część operacji GRU, mającej na celu utrudnienie Ukrainie zdobycia broni niezbędnej do wykorzystania w Donbasie przeciwko prorosyjskim separatystom i żołnierzom rosyjskim. Według serwisu w operację w Czechach zaangażowanych było co najmniej 6 agentów z jednostki 29155 GRU, a nadzorował ją osobiście gen. Andriej Władimirowicz Awerianow. Bellingcat pisał także na temat roli Kremla w nieudanym → p u c z u [t. 3] w Czarnogórze.

Z powodu swojej działalności Eliot Higgins i serwis Bellingcat są – o czym szczegółowo pisze Jessika Aro w książce *Trolle Putina* – przedmiotem ataku m.in. rosyjskich mediów rządowych i samej administracji Władimira Putina. We wrześniu 2013 r., po ujawnieniu przez Higginsa, że al-Asad użył w Syrii → b r o n i c h e m i c z n e j [t. 1], dziennikarzem zainteresowała się stacja telewizyjna RT Londyn – pierwotnie działająca pod nazwą Russia Today, a niezmiennie reprezentująca interesy Kremla. Niezgodnie z prawdą poinformowała ona, że Higgins o użycie broni chemicznej oskarżył przeciwników al-Asada. Krytyka w → RT [t. 3] nasiliła się po publikacji przez Higginsa tekstów o rosyjskiej odpowiedzialności za zestrzelenie samolotu MH17. Według Jessiki Aro serwis Russia Insider, powielający → d e z i n f o r m a c j ę [t. 2] Kremla, pisał o dziennikarzu ponad 100 razy. Autorka *Trolli Putina* pisze:

> W żadnym z ponad 100 artykułów prawdziwość obraźliwych twierdzeń nie została udowodniona, nie zrobiono tego również w tekstach, w których nie wyzywa się blogera wprost. Zasadą normalnego dziennikarstwa jest, że krytykowana osoba może przedstawić swoje stanowisko – Russia Insider nigdy o nic Higginsa nie zapytał. Być może dlatego, że nie chodzi o dziennikarstwo obywatelskie, tylko o operację wpływu.

W październiku 2021 r. serwis Bellingcat został wpisany przez władze Rosji na listę „zagranicznych agentów", na której znajdowało się dotąd ponad 150 serwisów informacyjnych, organizacji pozarządowych i organizacji charytatywnych. Dzień po tym zainteresowanie serwisem wzrosło w Rosji 2,5-krotnie, o czym Eliot Higgins poinformował na Twitterze – ironicznie podziękował prezydentowi Putinowi za jego decyzję. Założyciel serwisu Bellingcat tłumaczy:

> Gdyby Rosjanie nie kłamali, nie mielibyśmy o czym pisać. Pojawiło się przekonanie, że to mistrzowie propagandy – a to nieprawda. Oni kłamią, a zachodnie media

nie patrzą na ich kłamstwa wystarczająco krytycznie. Powinny robić to od lat, ale wielu dziennikarzy mówi: „To takie trudne, nie damy rady tego sprawdzić" albo „Istnieją dwa punkty widzenia na sprawę i prawda zawsze leży gdzieś pośrodku". Przedstawianie różnych perspektyw w dziennikarstwie działa tylko jeśli wszystkie odpowiadają rzeczywistości.

Na temat E. Higginsa i Bellingcat pisano także wielokrotnie w rosyjskim serwisie Sputnik. Przedstawiano tam blogera jako stronniczego amatora, pracującego dla rządów Stanów Zjednoczonych i Ukrainy oraz rozpowszechniającego fałszywe informacje. Dziennikarze Bellingcat stali się ofiarami prowokacji CyberBerkutu, grupy podejrzewanej o powiązania z aparatem służb bezpieczeństwa Rosji: 24 lutego 2016 r. → h a k e r z y [t. 2] włamali się na stronę Bellingcata i opublikowali na niej treści mające zdyskredytować rosyjskiego dziennikarza serwisu Rusłana Lewiewa (nazwanego seksualnym perwersem).

Śledztwa Bellingcat nie skupiają się jedynie na Rosji. Serwis pisał o kręgu ukraińskich neonazistów (→ n e o n a z i m [t. 3]), którego celem są m.in. środowiska LGBT+, działacze feministyczni oraz przedstawiciele mniejszości narodowych, a także zidentyfikował osoby, które w 2017 r. wywołały zamieszki i starcia białych rasistów i radykalnej prawicy z kontrmanifestantami i policją w Charlottesville w stanie Wirginia w USA.

Lista fundatorów Bellingcat jest jawna i została opublikowana na stronie serwisu. Bellingcat nie przyjmuje funduszy i składek bezpośrednio od żadnego rządu krajowego, może jednak przyjąć środki od fundacji wspieranej przez rząd, pod warunkiem że pozostaje ona od niego niezależna. Serwis gwarantuje sobie pełną niezależność redakcyjną i zapewnia, że przyjęcie finansowania nie ogranicza go do ujawnienia wszelkich nieprawidłowości, które mogą mieć wpływ na fundatora. W 2021 r. informował również, że ok. 35 proc. jego budżetu generują warsztaty prowadzone przez niego i organizowane na całym świecie.

Dziennikarze Bellingcat i sam serwis będący częścią Global Investigative Journalism Network byli wielokrotnie wyróżniani prestiżowymi nagrodami dziennikarskimi. W 2017 r. Christiaan Triebert otrzymał European Press Prize (Europejską Nagrodę Prasową) w kategorii „Innowacje" za opublikowany w serwisie Bellingcat tekst o tureckim → z a m a c h u s t a n u w 2016 r. W 2019 r. zespół śledczych pod kierunkiem Christo Grozeva otrzymał Europejską Nagrodę Prasową w kategorii dziennikarstwa śledczego za pracę nad sprawą próby otrucia Skripalów. Na początku 2019 r. komisje spraw zagranicznych parlamentów 3 krajów bałtyckich – Łotwy, Litwy i Estonii – wspólnie wysunęły kandydaturę Bellingcata do Nagrody Pulitzera, prestiżowej amerykańskiej nagrody dla dziennikarzy.

Sukcesy serwisu Bellingcat przełożyły się na popularność metod OSINT-owych, coraz częściej wykorzystywanych przez dziennikarzy na całym świecie. Przykładem ich użycia może być – opublikowany na łamach serwisu OKO.press – artykuł,

w których Dominika Sitnicka przygląda się fotografiom pokazanym podczas konferencji prasowej w sprawie migrantów na polsko-białoruskiej granicy, w trakcie której głos zabrali minister obrony narodowej Mariusz Błaszczak i minister spraw wewnętrznych i administracji Mariusz Kamiński. Dzięki wykorzystaniu ogólnodostępnych narzędzi ujawniono, że zdjęcie o charakterze zoofilskim znalezione rzekomo na telefonie → u c h o d ź c ó w w rzeczywistości pochodzi z materiału wideo udostępnionego w sieci.

Należy jednak zauważyć, że śledztwa internetowe nie zawsze kończą się sukcesem. Powstałe w ostatnim czasie określenie „digiletantyzm", przywoływane również przez Higginsa, odwołuje się do nieumiejętnego śledztwa w sieci, które dodatkowo przyczynia się do szerzenia dezinformacji.

Łukasz Grzesiczak

J. Aro, *Trolle Putina. Prawdziwe historie z frontów rosyjskiej wojny informacyjnej*, tłum. M. Laskowska, SQN, Kraków 2020; *Bellingcat*, https://www.bellingcat.com (dostęp 18.11.2021); *European Press Prize*, https://www.europeanpressprize.com/ shortlists/year-2017/ (dostęp 18.11.2021); E. Higgins, *Bellingcat. Ujawniamy prawdę w czasach postprawdy*, tłum. R. Madejski, Sonia Draga, Katowice 2021; O. Kundra, J. Spurný, *Za výbuchem ve Vrběticích je šest členů ruského komanda včetně jeho velitele*, https://www.respekt.cz/agenda/bellingcat-a-respekt-za-vybuchem-ve-vrbeticich-jesest-clenu-ruskeho-komanda-vcetne-jeho-velitele (dostęp 18.11.2021); A. Mackinnon, *Bellingcat Can Say What U.S. Intelligence Can't*, https://foreignpolicy.com/2020/12/17/ bellingcat-can-say-what-u-s-intelligence-cant/ (dostęp 18.11.2021); *More Mice Belling the Cat?*, https://euvsdisinfo.eu/more-mice-belling-the-cat/ (dostęp 18.11.2021); B. Pawłowski, E. Higgins, *Eliot Higgins z Bellingcat o dziennikarstwie śledczym z domu: rozmowa*, https://demagog.org.pl/analizy_i_raporty/eliot-higgins-z-bellingcat-o-dziennikarstwie-sledczym-z-domu-rozmowa/ (dostęp 18.11.2021); A. Roth, *Russia Names Bellingcat Reporting Partner a 'Foreign Agent'*, https://www.theguardian. com/world/2021/jul/23/russia-brands-local-bellingcat-reporting-partner-as-foreign-agent (dostęp 18.11.2021); D. Sitnicka, *„Krowa Kamińskiego" to stare nagranie z internetu. A w dodatku to klacz*, https://oko.press/krowa-kaminskiego-to-stare-nagranie-z-internetu-a-w-dodatku-to-klacz/ (dostęp 18.11.2021).

BEZPIECZEŃSTWO – stan, który daje poczucie pewności i gwarancje jego zachowania oraz szansę na doskonalenie. Jest jedną z podstawowych potrzeb człowieka, najwyżej cenionych i najbardziej chronionych, która dotyczy niemal wszystkich sfer jego działalności. Jest to sytuacja odznaczająca się brakiem ryzyka utraty czegoś, co człowiek szczególnie ceni, np. zdrowia, pracy, szacunku, uczuć, dóbr materialnych. Jest to wartość, do jakiej dążą zarówno całe narody, mniejsze społeczności lokalne, jak i jednostki. Zagadnienie bezpieczeństwa jest bardzo szerokie i obejmuje wiele aspektów. Współczesne pojmowanie bezpieczeństwa ma znacznie szerszy kontekst niż w przeszłości, zawierają się w nim nie tylko aspekty polityczne i militarne, ale także ekonomiczne, gospodarcze, ekologiczne, społeczne, kulturowe i humanitarne. Aktualnie do zakresu bezpieczeństwa należą też takie czynniki jak zachowanie narodowej tożsamości, poszanowanie → p r a w c z ł o w i e k a [t. 3], respektowanie praw i swobód obywatelskich itd. Bezpieczeństwo to wartość, która jest rozumiana

i definiowana na różne sposoby, jak również rozmaicie pojmowana jest jej rola we współczesnym świecie. W naukach społecznych bezpieczeństwo, w najogólniejszym znaczeniu, obejmuje zaspokojenie potrzeb takich jak istnienie, przetrwanie, tożsamość, niezależność, spokój, posiadanie i pewność rozwoju. Jego brak wywołuje niepokój i poczucie → z a g r o ż e n i a [t. 4]. A.H. Maslow uplasował bezpieczeństwo na drugim miejscu w piramidzie potrzeb, którą tworzy 5 podstawowych grup. W porządku hierarchicznym są to potrzeby: fizjologiczne, bezpieczeństwa, przynależności, uznania, samorealizacji.

Pojęcie bezpieczeństwa pochodzi od wyrażenia przyimkowego *bez pieczy*, które oznaczało „bez troskliwości", „bez bojaźni", podobnie ang. *security* wywodzi się od łac. *sine cura* lub *securus* oznaczających „bez pieczy",

„bez niepokoju", „bez troski". W literaturze przedmiotu nie została wypracowana jedna, uzgodniona i przyjęta definicja bezpieczeństwa, a w definicjach stosowanych w → n a u k a c h o b e z p i e c z e ń s t w i e [t. 3] pojęcie to zawiera takie elementy jak:

- stan niezagrożenia, spokoju, pewności, braku zagrożeń i ochrony przed niebezpieczeństwami;
- stan, który daje poczucie pewności i gwarancję jego zachowania oraz szansę na doskonalenie, brak ryzyka utraty czegoś, co człowiek szczególnie ceni, np. zdrowia, pracy, szacunku, uczuć, dóbr materialnych;
- stan poczucia stabilności, niezagrożenia, pewności doskonalenia i rozwoju, przeciwstawność zagrożeń czy ochrona przed nimi;
- teoria i praktyka zapewniania możliwości przetrwania (egzystencji) i realizacji własnych interesów przez dany podmiot, w szczególności poprzez wykorzystywanie szans (okoliczności sprzyjających), podejmowanie wyzwań, redukowanie ryzyka oraz przeciwdziałanie (zapobieganie i przeciwstawianie się) wszelkiego rodzaju zagrożeniom dla podmiotu i jego interesów;
- naczelna potrzeba państw i systemów międzynarodowych, gwarantująca stabilizację i rozwój życia politycznego, ekonomicznego i społecznego.

Definicje słownikowe określają bezpieczeństwo jako podstawową potrzebę człowieka, stan poczucia stabilności, niezagrożenia, pewności doskonalenia i rozwoju, przeciwstawność zagrożeń czy ochronę przed nimi. Wyodrębniają również 2 elementy bezpieczeństwa: wewnętrzny i zewnętrzny. W aspekcie wewnętrznym wyróżniają stabilność i harmonijność danego organizmu bądź systemu (podmiotu zbiorowego), natomiast w aspekcie zewnętrznym brak zagrożenia ze strony innych podmiotów. Oba składają się na ogólne bezpieczeństwo danego podmiotu. Jednocześnie wielu autorów rozszerza znaczenie tego pojęcia, w którym podkreśla, iż bezpieczeństwo to:

- ciągła działalność jednostek, społeczności lokalnych, państw czy organizacji międzynarodowych w tworzeniu pożądanego stanu bezpieczeństwa;

- zdolność do kreatywnej aktywności podmiotu, oznaczającej holistyczną i dynamiczną sytuację obiektywną polegającą na braku zagrożenia, odczuwaną subiektywnie przez jednostki lub grupy społeczne;
- zmienny w czasie stan określający możliwość zaspokojenia potrzeb społecznych związanych z trwaniem i rozwojem podmiotu w warunkach istnienia realnych lub potencjalnych zagrożeń, świadomość tego stanu oraz aktywność zmierzająca do osiągnięcia pożądanego poziomu tego stanu;
- dynamizm i aktywność, która zmierza do zapewnienia przetrwania, rozwoju i swobody realizacji interesów w danych uwarunkowaniach poprzez wykorzystywanie szans, podejmowanie wyzwań, redukowanie ryzyka oraz przeciwdziałanie wszelkiego rodzaju zagrożeniom dla podmiotu i jego interesów.

Bezpieczeństwo jest postrzegane wieloznacznie i wieloaspektowo jako stan i proces. Pierwotne znaczenie etymologiczne pojęcia „bezpieczeństwo" określało je jako stan (np. stan niezagrożenia, stan pokoju, stan pewności, stan wolności od zagrożeń itp.). Bezpieczeństwo rozpatrywane jako stan odnosi się zatem do konkretnej sytuacji i oznacza stan braku zagrożeń, stan pewności, spokoju, zabezpieczenia oraz jego poczucia, co wskazuje, że oznacza ono brak zagrożenia oraz ochronę przed niebezpieczeństwami. Należy podkreślić, że stan bezpieczeństwa jest niemierzalny (brak bowiem kryteriów jego mierzalności), ważne jest jego postrzeganie przez społeczeństwo i władze państwa. Może ono przybierać postacie:

- stanu braku bezpieczeństwa, wtedy gdy występuje duże rzeczywiste zagrożenie, a postrzeganie tego zagrożenia jest prawidłowe;
- stanu obsesji, wtedy gdy nieznaczne zagrożenie jest postrzegane jako duże;
- stanu fałszywego bezpieczeństwa, wtedy gdy zagrożenie jest poważne, a postrzegane bywa jako niewielkie,
- stanu bezpieczeństwa, wtedy gdy zagrożenie zewnętrzne jest nieznaczne, a jego postrzeganie prawidłowe.

Postrzeganie bezpieczeństwa jako procesu współcześnie jest bardziej właściwe ze względu na dynamiczny charakter wewnętrznych i zewnętrznych uwarunkowań bezpieczeństwa. Bezpieczeństwo jako proces należy rozumieć jako nieustanne działania podejmowane przez określony podmiot (czyli człowieka, daną społeczność, konkretne państwo, organizację międzynarodową itp.) w celu osiągnięcia pożądanego stanu bezpieczeństwa. Proces bezpieczeństwa polega na tym, że jego podmioty dążą do udoskonalenia mechanizmów zapewniających im poczucie bezpieczeństwa, a stan bezpieczeństwa i jego organizacja podlegają dynamicznym zmianom uwarunkowań bezpieczeństwa. Zakres pojęcia bezpieczeństwa postrzeganego jako proces zmienia się w miarę rozwoju podmiotu bezpieczeństwa. Zakres ten rozszerzał się wraz z postępem cywilizacyjnym, który przyniósł nieznane wcześniej zagrożenia oraz metody ich eliminacji. W przeszłości zagadnienie bezpieczeństwa wiązano przede wszystkim ze sferą militarną – uważano wówczas, że podstawowymi wartościami chronionymi

przed zagrożeniami powinny być integralność terytorialna, niezależność polityczna, → s u w e r e n n o ś ć [t. 4], przetrwanie państwa i narodu, a ochrona tych wartości jest możliwa tylko wtedy, gdy państwo jest samowystarczalne i dysponuje odpowiednim potencjałem militarnym – lecz współcześnie oprócz nich na poczucie bezpieczeństwa wpływają czynniki o charakterze ekonomicznym, ekologicznym, politycznym, demograficznym itp., które rodzą nowe rodzaje zagrożeń dla bezpieczeństwa. Konsekwentnie więc bezpieczeństwo rozumiane jedynie jako brak zagrożeń nie ma stanowić wyłącznie gwarancji fizycznego przetrwania, lecz równocześnie zapewnić realizację minimum pozostałych potrzeb społecznych. W dzisiejszych czasach, charakteryzujących się szybkim rozwojem cywilizacji i postępem technicznym, pojęcie bezpieczeństwa rozpatrywane jest na 2 płaszczyznach. Pierwszą jest bezpieczeństwo w skali makro, która obejmuje sprawy o zasięgu globalnym – całego świata, kontynentu czy konkretnego państwa. Druga płaszczyzna, z perspektywy której definiuje się bezpieczeństwo, to skala mikro odnosząca się do spraw dotyczących np. społeczności lokalnych zamieszkujących gminy, powiaty, województwa itp. oraz do każdego człowieka. Współczesne pojęcie bezpieczeństwa ma szerszy wymiar aniżeli w przeszłości, obejmuje wszystkie dziedziny życia, w których może wystąpić zagrożenie, i jest wieloaspektowe. Uwzględnia aspekty polityczne, wojskowe, czynniki gospodarcze i technologiczne, ekologiczne, społeczne i humanitarne. Do jego zakresu włącza się również zachowanie narodowej tożsamości oraz eksponowanie

„ludzkiego wymiaru" bezpieczeństwa, czyli poszanowania podstawowych praw i swobód obywatelskich. Wiele spraw, które w przeszłości kwalifikowano do wewnętrznych kompetencji państwa, staje się przedmiotem uregulowań ponadnarodowych.

O złożoności pojęcia bezpieczeństwa świadczy też różnorodność kryteriów jego klasyfikacji oraz ilość rodzajów bezpieczeństwa, wyodrębnianych w wielu analizowanych typologiach. W zależności od przyjętego kryterium wyróżnia się rozmaite rodzaje bezpieczeństwa. Ich zbiór jest otwarty i nie można stwierdzić, która z analizowanych typologii jest optymalna. Jednocześnie analiza typologii bezpieczeństwa pozwala zauważyć tendencję powstawania nowych przedmiotowych rodzajów bezpieczeństwa, uwzględniających czynniki ekonomiczne, ekologiczne, żywnościowe, demograficzne, energetyczne, informacyjne czy społeczne. Poszerzanie się pojęcia bezpieczeństwa jest związane z tworzeniem warunków nie tylko do przetrwania, ale również zapewnienia rozwoju podmiotu, jego poczucia pewności stanu posiadania i funkcjonowania oraz ochrony przed zagrożeniami. W piśmiennictwie polskim funkcjonuje głównie podział zaproponowany przez R. Ziębę. Dzieli on bezpieczeństwo wg następujących kryteriów:

- podmiotowych – na → b e z p i e c z e ń s t w o n a r o d o w e i → b e z p i e c z e ń s t w o m i ę d z y n a r o d o w e;
- przedmiotowych – na → b e z p i e c z e ń s t w o p o l i t y c z n e, bezpieczeństwo wojskowe, bezpieczeństwo gospodarcze, → b e z p i e c z e ń s t w o s p o ł e c z n e, → b e z p i e c z e ń s t w o k u l t u r o w e,

→ bezpieczeństwo ideologiczne, → bezpieczeństwo ekologiczne, → bezpieczeństwo informacyjne;
- przestrzennych – na bezpieczeństwo lokalne, bezpieczeństwo subregionalne, bezpieczeństwo regionalne, ponadregionalne i globalne;
- czasu – na stan bezpieczeństwa i proces bezpieczeństwa;
- sposobu organizowania – na indywidualne (unilateralne), hegemonizm mocarstwowy, izolacjonizm, → neutralność [t. 3], niezaangażowanie, sojusze (system blokowy), system bezpieczeństwa kooperacyjnego, system bezpieczeństwa zbiorowego.

Należy podkreślić, że bezpieczeństwo jest pojęciem wieloznacznym i wieloaspektowym, stosowane jest do opisu i charakterystyki podmiotów bezpieczeństwa, aspektów egzystencjalnych, stanu stabilności i pewności. Kluczowym celem bezpieczeństwa jest zapewnienie przetrwania oraz podstawowych potrzeb i rozwoju podmiotu, jego poczucia pewności stanu posiadania oraz funkcjonowania, a jego istotą jest funkcjonowanie podmiotu bez zagrożenia. Bezpieczeństwo jest stanem, którego nie można zbudować raz na zawsze, jest procesem, który jest związany z rozwojem podmiotu bezpieczeństwa. Podmiotem bezpieczeństwa mogą być pojedyncze osoby, różne grupy społeczne, narody, a nawet cała ludzkość. Bezpieczeństwo przejawia się we wszystkich dziedzinach aktywności podmiotu. Jest uzależnione od tego, co dzieje się w otoczeniu podmiotu bezpieczeństwa, od relacji podmiotu z tym otoczeniem oraz od zbudowanej ochrony przed zagrożeniami, które mogą pochodzić z tego otoczenia. Zagrożenia mogą również pochodzić z wewnątrz podmiotu bezpieczeństwa. Bezpieczeństwo jest traktowane jako jedna z podstawowych wartości i potrzeb podmiotu bezpieczeństwa, do których zbioru zalicza się m.in.: pewność istnienia i przetrwania, gwarancję rozwoju podmiotu bezpieczeństwa, niezakłóconą możliwość posiadania oraz tożsamość i niezależność polityczną. Pomimo pewnej uniwersalności nie jest to zbiór stały i jest on związany w określonym zakresie z podmiotem bezpieczeństwa. Przedmiotowy zbiór wymaga zapewnienia ochrony przed realnymi lub potencjalnymi zagrożeniami, co jest realizowane m.in. za pomocą stosownych systemów bezpieczeństwa.

Janusz Falecki

T. Berliński, *Różnorodność postrzegania zagrożeń*, [w:] *Zarządzanie bezpieczeństwem. Międzynarodowa Konferencja Naukowa, Kraków 11–13 maja 2000 r.*, P. Tyrała (red.), Wydawnictwo Profesjonalnej Szkoły Biznesu, Kraków 2000; J. Falecki, *Bezpieczeństwo*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka. R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; tenże, *Dylematy zarządzania kryzysowego w Rzeczypospolitej Polskiej*, Oficyna Wydawnicza „Humanitas", Sosnowiec 2016; J. Stańczyk, *Współczesne pojmowanie bezpieczeństwa*, Instytut Studiów Politycznych PAN, Warszawa 1996; A. Wawrzusiszyn, *Teoretyczne aspekty bezpieczeństwa*, [w:] *Studia i materiały*, CSGG, Kętrzyn 2009; B. Wiśniewski, *System bezpieczeństwa państwa. Konteksty teoretyczne i praktyczne*, Wydawnictwo Wyższej Szkoły Policji w Szczytnie, Szczytno 2013; *Współczesne bezpieczeństwo*, W. Fehler (red.), Wydawnictwo Adam Marszałek, Toruń 2003; R. Zięba, *Instytucjonalizacja bezpieczeństwa europejskiego*, Wydawnictwo Naukowe

Scholar, Warszawa 2004; tenże, *Pojęcie i istota bezpieczeństwa w stosunkach międzynarodowych*, „Sprawy Międzynarodowe" 1989, nr 10; R. Zięba, J. Zając, *Budowa zintegrowanego systemu bezpieczeństwa Polski. Ekspertyza*, Ministerstwo Rozwoju Regionalnego, Warszawa 2010.

BEZPIECZEŃSTWO CAŁOŚCIOWE (inaczej całościowe podejście do bezpieczeństwa) – w głównej mierze utożsamiane z wszelkimi sposobami na wzmocnienie odporności (→ r e z y l i e n c j i) państwa i społeczeństwa na presję zewnętrzną oraz z zagwarantowaniem korzystnych warunków dla działań obronnych w sytuacjach realnych zagrożeń. W swoim podstawowym zakresie odnosi się zarówno do militarnych, jak i niemilitarnych aspektów → b e z p i e c z e ń s t w a n a r o d o w e g o [t. 1], jednocześnie jest związane z problematyką → z a r z ą d z a n i a k r y z y s o w e g o [t. 4] i → o b r o n y c y w i l n e j [t. 3]. Koncepcja bezpieczeństwa całościowego potwierdza zatem wielosektorowość bezpieczeństwa państwa w ogóle. W XX w., po rozpadzie bipolarnego ładu światowego, nastąpiła istotna zmiana paradygmatu bezpieczeństwa, wymuszona niejako pojawieniem się nowych rodzajów zagrożeń, które zrewolucjonizowały koncepcję międzynarodowego → ś r o d o w i s k a b e z p i e c z e ń s t w a [t. 4], implikując tym samym rekonfigurację ładu światowego. Wówczas na arenie międzynarodowej pojawiły się nowe podmioty polityczne, gospodarcze oraz społeczne o wyraźnie odmiennych interesach, co sprawiło, że dotychczas obowiązujące klasyczne teorie stosunków międzynarodowych, zwłaszcza realizm strukturalny, stały się niewystarczającymi i nieefektywnymi koncepcjami kreowania reguł ich wzajemnych relacji. Zauważalna różnorodność celów, potrzeb, a także sił i środków służących ich osiąganiu i zaspokajaniu, wymusiła odwołanie się do bardziej całościowego nurtu badawczego, któryw pełni określiłby mechanizmy partycypacji państw i innych podmiotów w obszarze szeroko pojętych stosunków międzynarodowych.

Głównym zarzutem stawianym neorealizmowi było eksponowanieznaczenia presji systemu stosunków międzynarodowych przy jednoczesnym lekceważeniu – kluczowych przecież dla polityki zagranicznej i bezpieczeństwa – subiektywnych czynników wewnętrznych, kulturowych i społecznych. Jednym z remediów na zrozumienie nowych okoliczności i zmian zachodzących w obrębie otoczenia systemu bezpieczeństwa globalnego miało stać się podejście strategiczne, wprowadzające do dyskursu naukowego termin → „k u l t u r a s t r a t e g i c z n a" [t. 2].

Wpisuje się ona niewątpliwie w koncepcję bezpieczeństwa całościowego. Kultura strategiczna wymaga usystematyzowania tzw. warunków bezpieczeństwa – wyzwań, → r y z y k a , zagrożeń oraz szans – w konkretnym dokumencie strategicznym. Podobnie kreowanie bezpieczeństwa całościowego również nie jest możliwe bez uwzględnienia specyficznej dla danego podmiotu kultury strategicznej, m.in. przez określenie wspomnianych wyzwań, ryzyka, zagrożeń, a także szans. Ustalenie istotnychpriorytetów w zakresie → b e z p i e c z e ń s t w a [t. 1], a w konsekwencji celów

strategicznych i interesów, określa poniekąd status państwa oraz decyduje o sposobach radzenia sobie z ewentualnymi problemami.

Samo bezpieczeństwo całościowe stanowi skomplikowaną kategorię, uwzględnia bowiem militarne i niemilitarne czynniki kształtujące bezpieczeństwo narodowe, więc dotyczy aktywności w zakresie → o c h r o n y l u d n o ś c i [t. 3], obrony cywilnej i zarządzania kryzysowego. Zatem tworzenie właściwych ram bezpieczeństwa całościowego wymaga zaangażowania wielu podmiotów odpowiedzialnych ustawowo za zagwarantowanie bezpieczeństwo państwa w czasie pokoju, → k r y z y s u [t. 2] oraz → w o j n y [t. 4].

Z perspektywy kultury strategicznej zapewnienie bezpieczeństwa całościowego nie jest możliwe bez uprzedniej wnikliwej analizy warunków bezpieczeństwa oraz właściwego doboru dostępnych sił i środków służących osiąganiu określonych celów strategicznych. Dlatego też omawiając charakterystyczne dla konkretnych państw modele bezpieczeństwa całościowego, nie sposób nie odwołać się bezpośrednio do ich kultury strategicznej, która przez uwzględnianie wypływu wielu kluczowych czynników, takich jak: doświadczenia historyczne, położenie geopolityczne oraz uwarunkowania wewnętrzne i zewnętrzne, stale kształtuje określoną wizję bezpieczeństwa całościowego.

Geneza strategii całościowego podejścia do bezpieczeństwa wywodzi się głównie z doktryny → o b r o n y t o t a l n e j [t. 3], kojarzonej przede wszystkim z → z i m n ą w o j n ą [t. 4]. Zgodnie z ówczesną koncepcją obrona totalna miała angażować przede wszystkim siły zbrojne, nie pomijając jednocześnie istotnej roli instytucji publicznych i komponentu cywilnego. Działania zbrojne miały aktywować całe społeczeństwo, które zgodnie wyrażało wolę walki, ponieważ ewentualnym działaniom armii był podporządkowany potencjał ludzki. Obrona totalna sprowadzała się zatem do szybkiej mobilizacji sił zbrojnych przy jednoczesnym wykorzystaniu obrony terytorialnej i obrony cywilnej. Wspomniana koncepcja była kierowana przede wszystkim do państw o ograniczonym potencjale obronnym, krajów prowadzących politykę neutralną, znajdujących się poza rywalizującymi ze sobą ówczesnymi blokami. Koncepcja ta uwzględniała gwarancje ochrony narodu i majątku państwowego. Państwa forsujące model obrony totalnej wykazywały daleko idącą gotowość do działań defensywnych, nawet w sytuacji znacznych dysproporcji wobec potencjału narodowego, obronnego i możliwości przeciwnika.

O obronie totalnej jako synonimie → o b r o n y n a r o d o w e j [t. 3] i obrony powszechnej wspomina Waldemar Kitler, utożsamiając ją z wojskowymi i cywilnymi rozwiązaniami na rzecz zapewnienia bezpieczeństwa państwa i społeczeństwa w obliczu potencjalnych zagrożeń. W opinii Przemysława Wywiała przez obronę totalną należy rozumieć nie tylko działania obligatoryjne z punktu widzenia przygotowań państwa do przeciwstawienia się zagrożeniom zewnętrznym, lecz także proces zreorganizowania i adaptacji społeczeństwa do warunków wojny. Widoczne jest tu

podobieństwo w rozumieniu obrony totalnej i wywodzącej się z tej koncepcji strategii bezpieczeństwa całościowego.

Bezpieczeństwo całościowe, jako odpowiedź na → z a g r o ż e n i a [t. 4], stało się istotnym elementem w budowaniu współczesnych systemów bezpieczeństwa. Trend ten obserwujemy zwłaszcza w państwach regionu nordycko-bałtyckiego, przede wszystkim w Szwecji, Finlandii i Estonii. Powrót do rozwiązań charakterystycznych dla obrony totalnej, jednakże w nowej odsłonie, może świadczyć o kryzysie układów regionalnych gwarantujących bezpieczeństwo. Co więcej, potwierdza potrzebę przebudowy dotychczas funkcjonujących układów i strategii bezpieczeństwa. Niestety, kres zimnej wojny spowodował, że w relacjach na arenie międzynarodowej uwidoczniła się tendencja niesłusznego bagatelizowania przez elity polityczne i opinię publiczną kwestii obrony totalnej. Przy pozornie minimalnym zagrożeniu atakiem militarnym lub wykorzystaniem broni atomowej idea pokojowego rozwiązywania sporów i integracji na rzecz → b e z p i e c z e ń s t w a r e g i o n a l n e g o [t. 1] wręcz całkowicie wyparła racjonalne podejście do ochrony ludności, obrony cywilnej i reakcji na kryzysy. Wiek XXI uwidocznił nowe wyzwania natury hybrydowej, konieczna okazała się więc rewizja dotychczasowych strategii bezpieczeństwa, m.in. w kierunku implementacji rozwiązań właściwych dla koncepcji obrony totalnej w nowym wydaniu, a zatem bezpieczeństwa całościowego.

Bezpieczeństwo całościowe jako kontynuacja obrony totalnej w nowej odsłonie jest wypadkową działań podejmowanych w 3 istotnych dziedzinach: zarządzania kryzysowego, obrony cywilnej oraz odporności państwa na ewentualną → a g r e s j ę [t. 1] innych podmiotów. W koncepcji bezpieczeństwa całościowego zarządzanie kryzowe koncentruje się wokół aktywności organów administracji publicznej na rzecz przeciwdziałania → s y t u a c j o m k r y z y s o w y m [t. 4], przygotowania do przejmowania nad nimi kontroli, reagowania na pojawiające się już kryzysy, a także ograniczania i usuwania ich skutków z jednoczesnym procesem odtwarzania utraconych zasobów, a przede wszystkim kluczowej dla bezpieczeństwa państwa → i n f r a s t r u k t u r y k r y t y c z n e j [t. 2]. Zarządzanie kryzysowe sprowadza się również do działalności planistycznej (przed wystąpieniem sytuacji kryzysowych). Z kolei obrona cywilna w koncepcji bezpieczeństwa całościowego skupia się na ochronie ludności, zakładów pracy i urządzeń użyteczności publicznej oraz dóbr kultury, ratowaniu i udzielaniu pomocy poszkodowanym w czasie wojny, a także na współdziałaniu w zwalczaniu → k l ę s k ż y w i o ł o w y c h [t. 5] i zagrożeń środowiska, nie wyłączając działań polegających na usuwaniu ich skutków. Trzeci element bezpieczeństwa całościowego, tzw. odporność państwa, jest utożsamiany ze zdolnościami do przeciwstawienia się sytuacjom kryzysowym (zarówno w czasie pokoju, jak i w trakcie wojny) oraz przywróceniem stanu sprzed ich wystąpienia. Kluczowymi elementami odporności państwa są potencjały cywilny i wojskowy, a ich uwzględnienie w koncepcji bezpieczeństwa całościowego gwarantuje zachowanie ciągłości administracji i kluczowych usług publicznych.

Koncepcja bezpieczeństwa całościowego, implementowana współcześnie chociażby w republikach nadbałtyckich, a wzorująca się na podejściu fińskim, bazuje na znanych już rozwiązaniach obrony totalnej, które zostały uzupełnione koniecznością budowy nowych zdolności sektora społecznego i militarnego jako realnej odpowiedzi na potencjalne i wysoce nieprzewidywalne → z a g r o ż e n i a h y b r y d o w e [t. 4]. W obliczu obecnych kryzysów i zagrożeń nękających państwa europejskie obligatoryjna stała się rewizja dotychczasowych sposób zapewnienia bezpieczeństwa. Za podstawę modelu bezpieczeństwa całościowego możemy uznać: 1) filar militarny; 2) wsparcie cywilne dla sił zbrojnych; 3) konkretne działania na arenie międzynarodowej (podnoszące prestiż i status państwa); 4) utrzymywanie → b e z p i e c z e ń s t w a w e w n ę t r z n e g o [t. 1]; 5) zagwarantowanie → b e z p i e c z e ń s t w a u s t r o j o w e g o [t. 1] przez zapewnienie ciągłości funkcjonowania władz państwowych i społeczeństwa; 6) propagowanie rozwiązań z zakresu obrony cywilnej; 7) budowanie odporności (rezyliencji) państwa i społeczeństwa (wraz z → e d u k a c j ą d l a b e z p i e c z e ń s t w a [t. 2] na rzecz wzmacniania świadomości obywateli w zakresie radzenia sobie w sytuacjach kryzysowych); 8) obronę psychologiczną. Ze względu na złożoność problematyki i potrzebę synchronizacji wielu kluczowych obszarów bezpieczeństwa proces implementacji konkretnego modelu bezpieczeństwa całościowego jest długofalowy, stopniowyi wymaga znacznych nakładów finansowych, a przede wszystkim zaangażowania obywateli.

Julia Anna Gawęcka

W. Kitler, *Obrona narodowa w wybranych państwach demokratycznych*, AON, Warszawa 2001; Ł. Smalec, *Kultura strategiczna a paradygmat realistyczny. Krytyka, rywalizacja i perspektywy współpracy*, „Kwartalnik Naukowy OAP UW e-Politikon" 2012, nr 2; P. Szymański, *Nowe pomysły na obronę totalną. Bezpieczeństwo całościowe w Finlandii i Estonii*, Ośrodek Studiów Wschodnich im. Marka Karpia, Warszawa 2020; P. Wywiał, *Obrona totalna*, [w:] *Encyklopedia bezpieczeństwa*, t. 3, O. Wasiuta, S. Wasiuta (red.), Wydawnictwo Libron, Kraków 2021.

BEZPIECZEŃSTWO DANYCH OSOBOWYCH – zapewnienie → b e z p i e c z e ń s t w a danych pozwalających na identyfikację osób fizycznych, w tym wszelkich procesów ich przetwarzania, poprzez stosowanie odpowiednich środków technicznych i organizacyjnych. Obecnie podstawowym celem i wyzwaniem tak rozumianej działalności jest stworzenie skutecznych systemów ochrony prywatności osób fizycznych odpowiadających wyzwaniom współczesnego, zglobalizowanego i zinformatyzowanego świata.

Filozoficzne podstawy ochrony danych osobowych należy wiązać z rozwojem idei → p r a w c z ł o w i e k a [t. 3], szczególnie w kontekście ich tzw. pierwszej generacji (prawo do życia, wolności i własności). Są one kategorią moralną, w ramach której człowiek traktowany jest jako wartość. Ich fundamentem jest przyrodzona godność osoby ludzkiej. Są to prawa uniwersalne i powszechne, przysługujące

każdemu człowiekowi na mocy faktu bycia człowiekiem, niezależnie od miejsca urodzenia czy zamieszkania. W odniesieniu do powyższego podstawowe prawa, takie jak prawo do prywatności, prawo do bycia niezależnym, prawo do kontroli → i n f o r m a c j i [t. 2] na własny temat oraz prawo do bycia pozostawionym w spokoju, składają się na tzw. autonomię informacyjną jednostki. Historia tworzenia rozwiązań systemowych w przedmiocie bezpieczeństwa danych osobowych na świecie rozpoczęła się od postulatów ochrony życia prywatnego osób znanych publicznie, przez dostosowywane w miarę rozwoju cywilizacyjnego rozwiązania mające chronić dane dotyczące osób fizycznych, w tym w szczególności odpowiadające tworzonym i rozwijającym się wielkim bazom danych w systemach informatycznych, aż po próby zapewnienia ochrony przetwarzania informacji w tym zakresie w skali międzynarodowej (globalnej). Można w tym obszarze wskazać najważniejsze momenty przełomowe:

- koniec XIX w. – pierwsze postulaty realizacji prawa do ochrony życia prywatnego w USA w związku z rozwojem technologii w dziedzinie fotografii i umożliwieniem po raz pierwszy sporządzania wizerunku osób bez konieczności pozowania (dyskusji dał początek artykuł autorstwa L. Brandeisa i S. Warrena pt. *The Right to Privacy*, który ukazał się w 1890 r. na łamach czasopisma „Harvard Law Review" i który zawierał argumentację na rzecz uznania prawa do bycia pozostawionym samemu sobie, ang. *right to be let alone*);
- 1948 r. – zawarcie zapisów dotyczących m.in. ochrony godności jednostek, życia prywatnego, rodzinnego, domowego, korespondencji w Powszechnej deklaracji praw człowieka (ONZ);
- 1950 r. – podobne zapisy w Europejskiej konwencji praw człowieka (Rada Europy, RE);
- 1970 r. – pierwszy akt prawny na świecie wprost odnoszący się do ochrony danych osobowych (ustawa o ochronie danych osobowych w Hesji, związana z rozpoczęciem komputerowego przetwarzania danych osobowych);
- 1973 r. – rezolucja nr 22 RE dotycząca ochrony danych osób fizycznych w elektronicznych bankach danych w odniesieniu do sektora prywatnego;
- 1974 r. – rezolucja nr 29 RE zawierająca podobne postanowienia w zakresie sektora publicznego;
- 1980 r. – wytyczne Organizacji Współpracy Gospodarczej i Rozwoju (Organisation for Economic Cooperation and Development, OECD), stanowiące próbę uregulowania ochrony prywatności i przepływu danych między państwami;
- 1981 r. – Konwencja RE nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych (uznawana jest za jeden z najstarszych i podstawowych prawnych instrumentów ochrony danych osobowych);
- 1995 r. – Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady (UE) – zobowiązanie państw członkowskich UE do ujednolicenia systemów ochrony danych

osobowych w ramach Europejskiego Obszaru Gospodarczego (EOG); dokument miał również fundamentalne znaczenie dla tworzenia systemów ochrony danych w państwach starających się o członkostwo w UE, a wskazane w nim przesłanki legalności przetwarzania danych pozostają aktualne do dziś;
- 2000 r. – ujęcie praw dotyczących ochrony danych osobowych w Karcie praw podstawowych UE;
- 2016 r. – wejście w życie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119/1 z 4.05.2016 r.), najczęściej określanego jako RODO lub rozporządzenie 2016/679; jest bezpośrednio stosowane i egzekwowane w państwach członkowskich UE od 25 maja 2018 r.

W Polsce zagadnienia ochrony danych osobowych były istotnym elementem zachodzących przemian systemowych rozpoczętych na przełomie lat 80. i 90. XX w., ukierunkowanych na tworzenie i rozwijanie mechanizmów demokratycznych oraz przystępowanie do zachodnioeuropejskich i euroatlantyckich struktur bezpieczeństwa i współpracy. Podstawowe rozwiązania systemowe w tym przedmiocie zawarte zostały w szczególności w następujących aktach prawnych:
- Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. – w rozdziale II wskazane zostały podstawowe prawa, wolności i obowiązki człowieka i obywatela, w tym m.in. zasada poszanowania i ochrony wolności człowieka, zasada ochrony życia prywatnego oraz ochrona informacji o osobie.
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych – implementacja Dyrektywy 95/46/WE oraz innych wytycznych i zasad określonych w obowiązujących dokumentach międzynarodowych.

Wraz z wydanymi na jej podstawie stosownymi rozporządzeniami była podstawą tworzenia systemów ochrony danych osobowych w sektorze publicznym i prywatnym (m.in. regulowała funkcjonowanie organu właściwego w sprawach ochrony danych, czyli Generalnego Inspektora Ochrony Danych Osobowych (GIODO), obowiązki podmiotów prywatnych i publicznych w przedmiocie zabezpieczenia i ochrony oraz zgodnego z prawem przetwarzania danych osobowych, tzw. administratorów danych osobowych (ADO), jak również administratorów bezpieczeństwa informacji (ABI), których ADO mogli powoływać w celu efektywniejszej realizacji swoich obowiązków). Obowiązywała aż do rozpoczęcia bezpośredniego stosowania RODO w 2018 r., gdy została najpierw w znacznej części, a później w całości uchylona.
- RODO – bezpośrednie stosowanie od 25 maja 2018 r. w państwach członkowskich UE, w tym również w Polsce; określa podstawowe zasady i procesy związane z przetwarzaniem danych osobowych w sektorze publicznym i prywatnym;

stanowi bezpośredni akt prawny, który obowiązuje bezpośrednio wszystkie podmioty biorące udział w procesach przetwarzania danych.

- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018, poz. 1000 z późn. zm.) – zawiera ogólne, zgodne z RODO rozwiązania systemowe dotyczące ochrony danych osobowych w Polsce.
- Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. 2019, poz. 125) – stanowi doprecyzowanie systemu w kontekście pewnych aspektów funkcjonowania organów i służb odpowiedzialnych za realizację zadań z zakresu zapobiegania i zwalczania przestępczości (implementacja Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW, Dz. Urz. UE.L 119/2016, s. 89).

Zgodnie z powyższymi ustaleniami podstawowym aktem prawa, który obecnie reguluje prawa i obowiązki osób i instytucji włączonych w szeroko rozumiane procesy przetwarzania danych osobowych w odniesieniu do sektora publicznego i prywatnego, jest RODO. Wprowadzenie tego aktu prawnego w skali całej UE było wydarzeniem bez precedensu, jeżeli chodzi o zakres i powszechność jego oddziaływania. Podstawowym celem, jaki przyświecał prawodawcy w tym zakresie, było sprostanie szybkim zmianom w obszarze nowych technologii, upowszechnienia się ich w społeczeństwach, wręcz masowego wymiaru ich wykorzystania, co z kolei miało zapewniać większe bezpieczeństwo obywateli w kontekście pojawiających się nowych lub zmieniających swój charakter → z a g r o ż e ń [t. 4].

Same dane osobowe są definiowane w RODO jako:

> wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Przetwarzanie danych osobowych obejmuje natomiast wszelkie operacje z ich wykorzystaniem, takie jak:

> zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie

poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

Można wyróżnić tzw. dane osobowe zwykłe (podstawowe dane o osobie fizycznej, jak np. imię i nazwisko, adres zamieszkania, numer telefonu, adres poczty elektronicznej) oraz dane osobowe wrażliwe (sensytywne), obejmujące tzw. szczególne kategorie danych (m.in. ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne bądź światopoglądowe, przynależność do związków zawodowych, dane genetyczne i biometryczne, dane dotyczące zdrowia, seksualności albo orientacji seksualnej) oraz dane o → c z y n a c h z a b r o n i o n y c h i wyrokach skazujących.

Głównym założeniem RODO było stworzenie systemu bardziej elastycznego i dopasowanego do specyfiki i charakteru funkcjonowania poszczególnych organizacji, pozwalającego odpowiednio dobierać środki bezpieczeństwa, adekwatnie do specyfiki, kontekstu, zakresu i celów przetwarzania danych w ramach prowadzonej działalności. W miejsce obowiązujących wcześniej odgórnych wytycznych odnośnie do sposobów zabezpieczenia procesów przetwarzania danych określone zostały ogólne obowiązki ADO, którzy mieli niejako urealnić system ochrony w kontekście swoich potrzeb i możliwości, rzeczywiście zabezpieczyć dane i procesy przetwarzania adekwatnie do stopnia ryzyka, zapewnić zgodność przetwarzania z przepisami prawa oraz monitorować te procesy. Ponadto postawiono przed nimi obowiązki w przedmiocie spełnienia obowiązków informacyjnych dotyczących przetwarzania danych względem osób fizycznych (podmiotów danych) oraz realizowania ich praw, a także wymogu wykazania spełnienia tych obowiązków.

Przewodnią ideą i fundamentem nowego systemu jest tzw. podejście oparte na ryzyku (z ang. *risk-based approach*), które bazuje na szacowaniu, ocenie i bieżącym monitorowaniu ryzyka procesów przetwarzania danych. Co istotne, chodzi tutaj nie tylko o ryzyko związane z przetwarzaniem danych dla organizacji (ADO), ale przede wszystkim o ryzyko z punktu widzenia praw i wolności osób, których dane dotyczą. Na tej podstawie powinny być dobierane stosownie do stwierdzonego stopnia ryzyka zabezpieczenia.

Nowy system ochrony danych osobowych na gruncie RODO został oparty na 2 podstawowych, ogólnych zasadach przewodnich:

- ochrony danych w fazie projektowania (z ang. *privacy by design*) – konieczności uwzględniania ochrony danych osobowych już na etapie projektowania rozwiązań technicznych i organizacyjnych,
- domyślnej ochrony danych (z ang. *privacy by default*) – konieczności wbudowania ochrony danych w konstrukcję tworzonych rozwiązań.

Ponadto przetwarzanie danych osobowych musi odbywać się z uwzględnieniem kolejnych, bardziej szczegółowych i czasami przenikających się wzajemnie zasad, w szczególności:

- zasady legalności – przetwarzanie musi być zgodne z prawem (konieczność spełnienia co najmniej jednej z przesłanek legalności przetwarzania, określonych w art. 6 i 9 RODO oraz zgodności z pozostałymi przepisami prawa);
- zasady integralności i poufności – dane muszą być w odpowiedni sposób zabezpieczone przed ich niezgodnymi z prawem ujawnieniem, utratą lub modyfikacją;
- zasady rzetelności – przetwarzanie danych musi odbywać się w sposób uczciwy i rzetelny (staranny), w szczególności z uwzględnieniem interesów i oczekiwań osób, których dane dotyczą, a także zmian technologicznych odnoszących się do stosowanych rozwiązań;
- zasady przejrzystości – operacje przetwarzania danych powinny być transparentne dla podmiotów danych, które muszą być odpowiednio informowane w tym zakresie (w postaci tzw. klauzul informacyjnych);
- zasady ograniczenia celu – dane mogą być zbierane jedynie w konkretnych i wyraźnych celach i przetwarzane dalej tylko zgodnie z tymi celami;
- zasady minimalizacji danych – przetwarzanie danych powinno się odbywać w jak najmniejszym zakresie, niezbędnym do osiągnięcia celu; dane zbierane mogą być tylko wtedy, gdy celu nie można osiągnąć w inny sposób;
- zasady prawidłowości (merytorycznej poprawności) – przetwarzane dane powinny być prawidłowe oraz w razie potrzeby i możliwości na bieżąco uaktualniane, usuwane lub sprostowane;
- zasady ograniczenia przechowywania (retencji danych) – dane mogą być przechowywane jedynie przez okres nie dłuższy, niż jest to niezbędne dla realizacji celów, w których są przetwarzane; jeżeli dane nie są już potrzebne, powinny zostać usunięte lub zanonimizowane;
- zasady rozliczalności – administrator danych (ADO) musi być w stanie wykazać spełnienie spoczywających na nim obowiązków prawnych oraz odpowiedniego zabezpieczenia procesów przetwarzania danych.

Wśród najważniejszych obowiązków formalnych nałożonych na administratorów danych należy wskazać w szczególności:

- konieczność przeprowadzenia dla określonych procesów oceny skutków dla ochrony danych (pogłębiona ocena ryzyka, tzw. DPIA – z ang. *Data Protection Impact Assessment*),
- prowadzenie tzw. uprzednich konsultacji z organem nadzorczym,
- prowadzenie określonych rejestrów (m.in. rejestrowanie czynności i kategorii czynności przetwarzania, rejestrowanie naruszeń ochrony danych),
- zgłaszanie naruszeń ochrony danych organowi nadzorczemu w terminie 72 godz. od stwierdzenia naruszenia,
- spełnienie obowiązku informacyjnego oraz realizacji praw podmiotów danych w określonym terminie.

W ramach rozwiązań systemowych dotychczasowy GIODO zastąpiony został przez Prezesa Urzędu Ochrony Danych Osobowych (PUODO), który jest organem właściwym w sprawie ochrony danych osobowych (organem nadzorczym). Z kolei dotychczasowy ABI zastąpiony został w nowych warunkach przez Inspektora Ochrony Danych (IOD). Dla pewnych kategorii podmiotów jego wyznaczenie i zgłoszenie do UODO stało się obowiązkowe (dotyczy przede wszystkim podmiotów publicznych oraz przetwarzających na dużą skalę szczególne kategorie danych). Na wszystkich podmiotach publicznych i prywatnych spoczywa natomiast odpowiedzialność za bezpieczeństwo danych osobowych. Można w tym zakresie wyróżnić niejako 2 oddzielne, ale powiązane ze sobą procesy, z których pierwszy dotyczy zapewnienia bezpieczeństwa danych osobowych jako informacji (zasobów informacyjnych i środków je zabezpieczających), drugi natomiast odnosi się do zapewnienia realizacji praw osób, których dane dotyczą.

Zapewnienie bezpieczeństwa informacji związane jest z działaniami w ramach tzw. podstawowych atrybutów bezpieczeństwa informacji, tj. przede wszystkim:

- poufności – zachowanie danych w tajemnicy (zapewnienie, żeby dane nie były ujawniane podmiotom i procesom do tego nieuprawnionym),
- integralności – zachowanie dokładności i kompletności danych (zapewnienie, aby dane nie zostały zniszczone lub zmienione w sposób niezgodny z prawem przez podmioty albo procesy do tego nieuprawnione),
- dostępności – zachowanie dostępu do danych (zapewnienie, żeby dane były dostępne dla uprawnionych podmiotów w odpowiednim czasie i miejscu).

Realizacja praw osób, których dane dotyczą (podmiotów danych), związana jest z jednym z podstawowych, przysługujących jednostkom praw, mianowicie z prawem do kontroli informacji na własny temat. Obejmuje ono – w zależności od przesłanki legalizującej przetwarzanie i uwarunkowań prawnych – w szczególności takie prawa jak m.in.:

- prawo do informacji na temat przetwarzanych danych,
- prawo dostępu do danych, ich poprawiania i sprostowania,
- prawo sprzeciwu wobec przetwarzania,
- prawo do usunięcia danych (tzw. prawo do bycia zapomnianym),
- prawo do ograniczenia przetwarzania,
- prawo do wycofania zgody na przetwarzanie danych osobowych,
- prawo do przenoszenia danych w określonych przypadkach,
- prawo skargi do organu nadzorczego na przetwarzanie niezgodne z prawem.

W celu odpowiedniego (adekwatnego do stwierdzonego ryzyka) zabezpieczenia danych osobowych oraz procesów ich przetwarzania, w tym również spełnienia obowiązków prawnych ciążących na ADO, stosowane powinny być różnego rodzaju środki bezpieczeństwa, zarówno w odniesieniu do danych przetwarzanych w formie elektronicznej (z wykorzystaniem systemów informatycznych), jak i w formie tradycyjnej (papierowej).

Można wskazać następujące przykłady zabezpieczeń w ramach 4 ich rodzajów:

- organizacyjne (m.in. polityki bezpieczeństwa, instrukcje zarządzania systemami informatycznymi, procedury nadawania uprawnień do pracy w systemach informatycznych, procedury zgłaszania incydentów bezpieczeństwa i naruszeń ochrony danych osobowych, rejestrowanie czynności przetwarzania, rejestrowanie incydentów bezpieczeństwa, regulaminy korzystania ze sprzętu teleinformatycznego, system obiegu dokumentów, umowy powierzenia przetwarzania danych, szkolenia itp.);
- techniczne (m.in. programy antywirusowe, segmentacja sieci, kopie zapasowe, zasilacze awaryjne, zapory sieciowe – *firewall*, UTM, szyfrowanie itp.);
- fizyczne (m.in. fizyczna ochrona budynku, monitoring, wydzielenie stref ochronnych, systemy alarmowe, punkty przeciwpożarowe, elektroniczna kontrola dostępu, plombowanie pomieszczeń i miejsc, szafy zamykane na klucz, sejfy itp.);
- personalne (m.in. upoważnienia do przetwarzania danych osobowych, weryfikacja uprawnień do pracy w systemach informatycznych, indywidualne loginy i hasła, klauzule o zachowaniu danych w poufności itp.).

Piotr Swoboda

Agencja Praw Podstawowych UE, Rada Europy, Kancelaria Europejskiego Trybunału Praw Człowieka, *Podręcznik europejskiego prawa o ochronie danych*, Urząd Publikacji UE, Luksemburg 2014, FRA.Europa.eu (dostęp 19.02.2020); Generalny Inspektor Ochrony Danych Osobowych, *Jak stosować podejście oparte na ryzyku? Poradnik RODO. Podejście oparte na ryzyku*, cz. 1–2, GIODO 2017; M. Jabłoński, S. Jarosz-Żukowska, *Prawa człowieka i systemy ich ochrony. Zarys wykładu*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2004; L. Kępa, *Ochrona danych osobowych. Praktyczny przewodnik dla przedsiębiorców*, C.H.Beck, Warszawa 2018; Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz. Urz. UE L 119/1 z 4.05.2016 z późn. zm.; M. Sakowska-Baryła, *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, C.H.Beck, Warszawa 2018; P. Swoboda, *Bezpieczeństwo danych osobowych*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz. U. 2018, poz. 1000 z późn. zm.; Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, Dz. U. 2019, poz. 125; Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, t.j. Dz. U. 2016, poz. 922 z późn. zm.

BEZPIECZEŃSTWO DEFENSYWNE – rozumiane jest jako → s t r a t e g i a [t. 4] prowadzenia polityki → b e z p i e c z e ń s t w a państwa traktująca obronność, a nie atak czy → i n w a z j ę [t. 2], jako priorytet w kreowaniu instrumentów, decyzji i podejmowanych działań. Główną ideą bezpieczeństwa defensywnego jest → o d s t r a s z a n i e [t. 3] obronne. Oznacza to, że przygotowania obronne mają na celu powstrzymanie inwazji. Odstraszanie zakłada pobudzenie w potencjalnym przeciwniku lub agresorze świadomości, która pomimo jego możliwej przewagi militarnej

i przewidywalnie dużych szans na sukces zmusi go do zaniechania prowadzenia działań podbojowych głównie z powodu dysproporcji kosztów i zysków wynikających z takiej operacji. Odstraszanie obronne jest zatem ściśle defensywne w przeciwieństwie do innych strategii obronnych, które przewidują coś więcej niż tylko możliwość odparcia inwazji. W szczególności należy to skontrastować z działaniem odwetowym, którego intencją jest powstrzymanie potencjalnych agresorów poprzez groźbę kontrataku. Chociaż odwetowe odstraszanie może mieć charakter obronny w tym sensie, że jego celem jest raczej zapobieganie inwazji niż rozpoczęcie → a g r e s j i wojennej, co polega na → z a g r o ż e n i u [t. 4] kontratakiem, to jednak oznacza, że musi ono uwzględniać zdolność do ofensywnych operacji wojskowych, takich jak atak na siły wroga, instalacje wojskowe, a może nawet miasta i tereny przemysłowe. Odstraszanie obronne wymaga położenia nacisku na różne rodzaje broni do odwetowego odstraszania: pocisków przeciwczołgowych zamiast czołgów, pocisków ziemia–powietrze i myśliwców zamiast bombowców i samolotów uderzeniowych, lekkich patroli przybrzeżnych oraz trałowców i okrętów podwodnych zamiast lotniskowców. Należy zaznaczyć, że nie ma wyraźnego rozróżnienia między bronią defensywną i ofensywną, stąd podział ten nie tłumaczy istoty bezpieczeństwa defensywnego, np. pociski przeciwpancerne można wykorzystać w ataku na pozycję wroga. Niemniej jednak określony dobór uzbrojenia sygnalizuje tendencję do strategii ściśle defensywnej lub odwetowej. Idea odstraszania zaczęła coraz ściślej kojarzyć się z odstraszaniem nuklearnym – badacze mówią o → b r o n i n u k l e a r n e j jako o działaniu odstraszającym. W świetle dyskusji na temat sprzeciwu wobec walki i niemoralności masowego zabijania odstraszanie nuklearne wydaje się nie do przyjęcia. Jednak niekoniecznie oznacza to, że idea odstraszania jest negatywnym fenomenem. Każda szczególna forma odstraszania będzie akceptowalna, jeśli groźba odwetu byłaby moralnie dopuszczalna, a sam system odstraszania nie stwarza niebezpieczeństwa, któremu powinien zapobiec. Odstraszanie jądrowe uznać można za zawodzące w obu przypadkach, co wynika z istnienia groźby pozbawienia życia milionów ludzi.

Gdyby istniała pewność, że zagrożenie nigdy nie zaistnieje, stworzenie niepewności mogłoby być moralnie uzasadnione. Skoro jednak nie ma takiej pewności, a wystąpienie zagrożenia i podjęte działania byłyby najbardziej przerażającym aktem, jaki można sobie wyobrazić, odstraszanie nuklearne jest moralnie dyskusyjne. Pojawiają się jednak argumenty, że system wzajemnego odstraszania faktycznie przyczynia się do stworzenia zagrożenia, jakim jest → w o j n a [t. 4] nuklearna, i daje początek nuklearnemu wyścigowi zbrojeń. Potęgi nuklearne starają się nadążyć za sobą, wprowadzając nową broń i wzbudzając w ten sposób wzajemne podejrzenia i nieufność. Ten samonapędzający się proces może znacznie zwiększyć prawdopodobieństwo tego, że wojna nuklearna rozpocznie się albo przez błędne obliczenie, albo przez wypadek. Można z przekonaniem stwierdzić, że polityka odstraszania obronnego zmniejszyłaby prawdopodobieństwo wojny. Na pewnym poziomie dotyczyłoby to również

bezpieczeństwa defensywnego w szerszym znaczeniu. Gdyby wszystkie państwa stosowały defensywną politykę, nie byłoby wojen, nigdy nie byłoby okazji do udziału w prewencyjnych działaniach lub kontratakach. Niemniej jednak defensywne polityki, ponieważ uwzględniają zdolność do szerszych form działań wojskowych, są prowokujące. Niezależnie od zapewnień udzielanych przez państwa zgodnie z ideą polityki defensywnej faktem jest, że ich siły zbrojne mogą zostać wykorzystane także do agresywnych celów. Zamierzeniem odstraszania obronnego jest odstraszanie za pomocą zdolności wojskowych, które mają nie tylko celowy charakter obronny, ale też nie mogą być interpretowane przez inne państwa jako potencjalnie agresywne. Nie powinno ono sygnalizować innym państwom konieczności budowania zdolności ofensywnej, a tym samym nie powinno podsycać obaw i napięć, które prowadzą do wojny. Odstraszanie obronne jest zatem działaniem o charakterze pokojowym, będącym polityką, która nie tylko mówi, kiedy i jak należy stosować wojnę w danych okolicznościach, ale także oferuje perspektywę zniwelowania potrzeby uciekania się do wojny. Uproszczeniem byłoby sugerować, że niepokoje i napięcia wywołane wyścigami zbrojeń są jedynymi przyczynami wojny. Państwa i rządy decydują się na prowadzenie wojen, ponieważ postrzegają je jako korzyść polityczną lub gospodarczą. Zwolennicy bezpieczeństwa defensywnego uznają odstraszanie obronne za część szerszej strategii mającej na celu stworzenie takiego świata, w którym coraz mniej celów można osiągnąć za pomocą wojny. Oznacza to w szczególności popieranie tendencji do większej współzależności gospodarczej państw. Im bardziej jedno państwo jest ekonomicznie zależne od współpracy z innym państwem, tym bardziej sprzeczne z jego interesami będzie prowadzenie wojny z tym drugim. Podobnie tworzenie procedur dyplomatycznych i instytucji, które oferują państwom mniej kosztowne sposoby realizacji ich interesów politycznych, jest działaniem charakterystycznym dla realizacji idei bezpieczeństwa defensywnego.

Podkreśla się, że bezpieczeństwo defensywne zakłada, iż wojna może być nieunikniona, gdy obrona militarna jest zinstytucjonalizowaną formą oporu wobec agresji, a ludzie nie mają innego wyboru niż walka. W tej perspektywie czysto obronna reakcja wojskowa na agresję jest bardziej akceptowalna niż polityka odwetowego kontrataku. Kierowanie obroną przed siłami inwazyjnymi jest także reakcją militarną, o której można powiedzieć, że nie było nieunikniona. Opieranie się agresji środkami militarnymi jest w tym przypadku równoznaczne z opieraniem się siłom zbrojnym, które tej agresji dokonują. Bezpieczeństwo defensywne zakłada zatem, że jeśli do dochodzi do ataku, wojska atakującego przekraczają granicę lub lądują na terenie państwa, to wówczas nie ma innego wyjścia niż walka z nimi. Jeśli samoloty wroga prowadzą naloty i bombardują, siły broniące nie mają innego wyjścia, niż spróbować je zestrzelić. Bezpieczeństwo defensywne wyklucza jednak zemstę na państwie najeźdźców poprzez bombardowanie ich fabryk, elektrowni czy miast i uzasadnienie tego tezą, że nie było innego wyboru.

Krytycy idei bezpieczeństwa defensywnego podkreślają trudności stosowania jedynie odstraszania obronnego, gdyż może ona oznaczać powstrzymywanie się od działań niezbędnych, aby wygrać. Argumentują, że oczekiwanie na atak może oznaczać utratę szansy skutecznego oporu. Konieczne może być rozpoczęcie ataku zapobiegawczego przeciwko siłom wroga, aby skutecznie się obronić. Jeśli po rozpoczęciu wojny obronnej ogranicza się działania tylko do odpierania ataków, bez przeprowadzania kontrataku na wojskowe instalacje wroga, pozwala mu się na dalsze ataki, co może prowadzić do porażki. Ponadto jeśli dojdzie do utraty terytorium w wojnie obronnej, jedyną możliwością jego odzyskania może być kontratak. Co więcej, istnieją nowoczesne formy broni, przed którymi nie ma obrony innej niż groźba odwetu. Wskazuje się także wątpliwość, czy możliwe jest utrzymanie wyraźnego rozróżnienia między obroną a atakiem. Pojawia się pytanie o to, czy bombardowanie wrogiego czołgu lub zatopienie wrogich statków mają charakter obrony czy kontrataku. Konkretne typy uzbrojenia nie mogą, w sposób abstrakcyjny, być klasyfikowane jako ofensywne lub defensywne. Należy uwzględnić ogólną koncepcję całokształtu uzbrojenia rozmieszczonego w danym państwie. Na przykład pociski przeciwpancerne mogą być używane podczas ataku, ale jeśli nie są one częścią arsenału, który obejmuje dużą liczbę czołgów i jednostek desantowych oraz samolotów uderzeniowych, ich użycie będzie koniecznie ograniczone do roli czysto obronnej. Chociaż nie ma żadnych ostrych granic, możliwe jest rozróżnienie między państwami, których uzbrojenie kładzie nacisk na zdolność obronną, a tymi, które mają zdolność ofensywną. Analogicznie do rodzajów uzbrojenia można ujmować także konkretne operacje wojskowe. Państwo prowadzące wojnę obronną może być zmuszone do kontrataku przeciwko wojskom inwazyjnym, które przedostały się na jego terytorium. Niemniej jednak będzie można określić ogólną strategię, w której bezpieczeństwo defensywne uznane zostanie za kluczowy cel i kierunek polityki państwa.

Jakub Idzik

Ch. Bellamy, *The Evolution of Modern Land Warfare: Theory and Practice*, Routledge, New York–London 2015; G. Caforio, D.S. Hong, *Some Historical Notes*, [w:] *Handbook of the Sociology of the Military*, G. Caforio, M. Nuciari (eds.), Springer, Cham 2018; B. Chapman, *Military Doctrine: A Reference Handbook*, ABC-CLIO, Santa Barbara–Denver–Oxford 2009; R. Elias, *Violence as Solution, Culture of*, [w:] *Encyclopedia of Violence, Peace & Conflict*, L.R. Kurtz (ed.), Elsevier, Oxford 2008; R. Kopeć, P. Mazur, *Odstraszanie militarne w XXI wieku: Polska – NATO – Rosja*, Uniwersytet Pedagogiczny im. KEN w Krakowie, Kraków 2017; P. Lawler, *Peace Studies*, [w:] *Security Studies: An Introduction*, P.D. Williams (ed.), Routledge, London–New York 2013; R. Norman, *Ethics, Killing and War*, Cambridge University Press, New York 1995; S. Tang, *A Theory of Security Strategy for Our Time: Defensive Realism*, Palgrave Macmillan, New York 2010.

BEZPIECZEŃSTWO DEMOGRAFICZNE – część → b e z p i e c z e ń s t w a n a r o d o w e g o, stan ochrony państwa, społeczeństwa i ochrona rynku pracy przed → z a g r o ż e n i a m i [t. 4] demograficznymi, zapewniający rozwój z uwzględnieniem

całości zrównoważonych interesów demograficznych państwa, społeczeństwa i jednostki; stan procesów demograficznych, który jest wystarczający dla odtwarzania społeczeństwa/populacji i zabezpieczenie zasobami ludzkimi interesów geopolitycznych państwa (→ g e o p o l i t y k a [t. 2]); to również funkcjonowanie i rozwój populacji w parametrach wieku, płci i etnicznych, jej korelacja z narodowymi interesami państwa, które mają zapewnić jego integralność, niepodległość, → s u w e r e n n o ś ć [t. 4] i utrzymanie istniejącego statusu geopolitycznego. Bezpieczeństwo demograficzne państwa to taka sytuacja demograficzna, w której jakościowy i ilościowy rozwój społeczny i indywidualny są zgodne z priorytetami rozwoju i bezpieczeństwa narodowego. Dzięki temu umacnia się bezpieczeństwo narodowe i ekonomiczne państwa, co z kolei przyczynia się do bezpiecznego i → z r ó w n o w a ż o n e g o r o z w o j u [t. 4] demograficznego państwa, czyli takiej sytuacji demograficznej, która pod względem różnych wskaźników strukturalnych pomoże osiągnąć w perspektywie czasu reprodukcję populacji wyższej jakości, aby zapewnić przewidywalność i kontrolowanie głównych procesów demograficznych. To zapewnienie takiej kombinacji warunków wewnętrznych i zewnętrznych w kraju, która będzie najbardziej korzystna dla rozwoju demograficznego.

Bezpieczeństwo demograficzne wiąże się z takimi pojęciami, jak: przetrwanie, wyludnienie, wyginięcie, samowystarczalne odtworzenie, rozwój demograficzny, → k r y z y s [t. 2] demograficzny, polityka demograficzna, depopulacja itp. Głównym zagrożeniem dla bezpieczeństwa demograficznego jest możliwe wyginięcie na skutek długotrwałej i głębokiej depopulacji –należy wskazać, że depopulacja obejmuje tylko naturalny ruch ludności – wskaźnik urodzeń i umieralności; gdy naturalny spadek jest rekompensowany przez imigrację, prowadzi to nie do zachowania populacji, ale do jej zmiany wraz ze wszystkimi etniczno-kulturowymi i społecznymi konsekwencjami, a w takim przypadku etniczne i genetyczne oblicze kraju z czasem się zmienia.

Czynnik demograficzny jest jednym z najważniejszych służących zapewnieniu zrównoważonego i bezpiecznego rozwoju państwa. Problemy optymalnego rozwoju demograficznego powinny być postrzegane jako priorytet interesów państwowych oraz jako czynnik, a także jako wynik jego działania. Od charakterystyki demograficznej populacji zdolnej do pracy i wskaźników rozwoju demograficznego zależy rozwój potencjału państwa i wielkość dochodu narodowego.

W wielu regionach świata populacja rośnie w tempie, za którym nie mogą nadążyć dostępne surowce i zasoby energetyczne, oczekiwany postęp w budownictwie mieszkaniowym, opiece zdrowotnej, bezpieczeństwie żywnościowym. Czynniki demograficzne, wraz z ekonomicznymi i politycznymi, stały się jedną z przyczyn rosnących nierówności w dobrobycie krajów rozwiniętych i rozwijających się, gdzie wysoka śmiertelność jest równoważona jeszcze wyższym wskaźnikiem urodzeń. Jednocześnie w wielu krajach rozwiniętych zmniejsza się liczba mieszkańców.

Główne cechy sytuacji demograficznej to: wielkość populacji i tempo jej zmian, struktura wiekowa i procesy migracyjne. Niestabilna sytuacja demograficzna stwarza realne zagrożenie dla → i n t e r e s ó w n a r o d o w y c h [t. 2] i bezpieczeństwa państwa. Brak siły roboczej, zmniejszenie wydajności pracy, wyludnienie, zmniejszenie dochodu narodowego mogą doprowadzić nawet do utraty suwerenności i państwowości.

Poważnym problemem społeczno-demograficznym jest nie tyle spadek liczby ludności, ile przekształcenie jej struktury wiekowej, w szczególności wzrost odsetka osób starszych. Starzenie się społeczeństwa prowadzi do wzrostu obciążenia ekonomicznego osób pracujących.

W aspekcie demograficznym stopniowy wzrost odsetka osób starszych wpływa na charakter wskaźnika urodzeń i odtwarzanie się populacji, pogorszenie struktury płci i wieku oraz zmniejszenie wskaźnika urodzeń. W aspekcie ekonomicznym oddziałuje na wzrost obciążeń osób zdolnych do pracy przez osoby starsze. Gdy grupa ludzi gotowych do pracy nie uzupełnia się w wystarczającym stopniu w sposób naturalny, rodzą się problemy na ścieżce rozwoju społecznej produkcji. W aspekcie społecznym w związku ze starzeniem się społeczeństwa istnieje potrzeba dodatkowej opieki dla osób starszych, których liczba rośnie bardzo szybko. Występuje wzrost nieproduktywnych kosztów społeczeństwa, tj. koszt utrzymania i obsługi emerytów.

Główne uwarunkowania bezpieczeństwa demograficznego to:

- ekonomiczne czynniki bezpieczeństwa demograficznego;
- społeczny wymiar bezpieczeństwa demograficznego;
- sytuacja ekologiczna;
- czynniki naturalne i klimatyczne;
- kształtowanie stanu zdrowia;
- czynniki prawne i polityka społeczno-demograficzna w systemie bezpieczeństwa demograficznego;
- duchowy i kulturowy stan społeczeństwa;
- etniczno-narodowe cechy w zakresie kształtującym bezpieczeństwo demograficzne.

Główne zagrożenia bezpieczeństwa demograficznego to:

- depopulacja i starzenie się społeczeństwa;
- degradacja instytucji rodziny;
- pogorszenie stanu zdrowia i przedwczesna umieralność;
- reprodukcyjne straty populacji;
- zagrożenia związane z procesami migracji.

Jeśli chodzi o kierunki rozwoju bezpieczeństwa demograficznego, zapobieganie i przeciwdziałanie katastrofie demograficznej powinny stanowić jedną ze strategicznych misji państwa, obejmującą kompleks przedsięwzięć w sferze społecznej, ekonomicznej, edukacyjnej i kulturowej, takich jak:

- uświadamianie znaczenia trwałości rodziny i macierzyństwa (przyrostu naturalnego) dla państwa i społeczeństwa, w tym dla bezpieczeństwa narodowego;

- przywrócenie rangi tradycyjnej rodzinie, pełniącej funkcję prokreacyjną, socjalizacyjną, patriotyczno-obywatelską i usługowo-opiekuńczą;
- powrót do modelu rodziny wielodzietnej i wielopokoleniowej jako gwaranta wykształcenia więzi społecznych i międzyludzkich;
- zapewnienie prawnych gwarancji socjalno-bytowych dla rodzin, obejmujących m.in.:
  - obniżenie kosztów pobytu dzieci w żłobkach i przedszkolach oraz zwiększenie możliwości korzystania z nich,
  - obniżenie podatku w rodzinach wielodzietnych,
  - obniżenie kosztów edukacji dzieci i młodzieży,
  - wsparcie państwa dla młodych rodzin, np. w postaci zagwarantowania bezpieczeństwa pracy dla matki po urlopie macierzyńskim oraz możliwości płynnej regulacji wymiaru przepracowanych w ciągu tygodnia godzin;
- zachowanie i poprawa stanu zdrowia ludności jako elementu bezpieczeństwa demograficznego;
- minimalizacja zagrożeń migracyjnych.

Globalny trend wskaźnika zmniejszenia urodzeń wynika z wielu przyczyn – ekonomicznych, społecznych, psychologicznych i biologicznych. Nawiasem mówiąc, czynnik ekonomiczny, o czym świadczą wyniki badań, nie zawsze odgrywa decydującą rolę. Na przykład we Francji, gdzie – jak wiadomo – poziom dobrobytu jest znacznie wyższy, rodzina ma średnio 1,1 dziecka, czyli podobnie jak w Polsce.

Polska w ślad za większością państw UE weszła w fazę załamania demograficznego, która ma określone konsekwencje dla → b e z p i e c z e ń s t w a s p o ł e c z n e g o – ograniczenie podaży pracy, trudności w powiększaniu PKB, zagrożenie dla stabilności systemu finansów publicznych czy wreszcie ograniczenie zdolności obronnych państwa. Od końca lat 90. XX w. obserwujemy w Polsce stałą tendencję do spadku liczby urodzeń, co prowadzi do powstania groźnego niżu demograficznego, który zasadniczo wpływa na możliwość przetrwania i rozwoju naszego państwa.

Czynnik demograficzny jest jednym z kluczowych, zapewniających stabilny i bezpieczny rozwój kraju. Demografię należy uznać za czynnik, a zarazem za skutek funkcjonowania państwa.

W ostatnich latach sytuacja demograficzna w Polsce jest wyjątkowo niekorzystna. Przyrost naturalny nadal znajduje się pod kreską, liczba zgonów przewyższa liczbę urodzeń. Około 2010 r. osiągnęliśmy najwyższy odsetek liczby osób w wieku produkcyjnym w populacji. Łącznie w pierwszym półroczu 2017 r. liczba zgonów zwiększyła się o 7% w stosunku do analogicznego okresu rok wcześniej. Oznacza to, że dziennie umiera aż o 75 Polaków więcej niż 12 miesięcy temu. Sytuacja demograficzna Polski jest trudna i nie widać symptomów jej poprawy. Dane statystyczne za 2017 r. pokazują, iż jako naród wymieramy i największe straty są dopiero przed nami. Główny Urząd Statystyczny (GUS) szacuje, iż liczba ludności Polski na koniec 2017 r. wyniosła

38,434 mln, a to oznacza mikroskopijny wzrost o 1 tys. względem stanu sprzed roku. Co ciekawe, nie oznacza to wcale, że liczba urodzeń przewyższyła liczbę zgonów. Tych ostatnich bowiem zanotowano ok. 500 więcej. Oba wskaźniki zbliżyły się do siebie w stopniu pozwalającym stwierdzić, iż rodziło się nas niemal tyle samo, ile umierało.

Jak zauważa GUS, współczynnik dzietności jest bardzo niski. Oznacza on liczbę urodzonych dzieci przypadających na jedną kobietę w wieku rozrodczym (15–49 lat). W 2016 r. wyniósł 1,36, w 2019 r. 1,43, w 2000 r. było to zaś 1,37. Jest to liczba katastrofalnie mała, ponieważ zastępowalność pokoleń gwarantuje dopiero współczynnik na poziomie 2,1. W UE gorzej pod tym względem wypadła jedynie Portugalia. Statystyka urodzeń uwzględnia przede wszystkim współczynnik dzietności, co oznacza, że bez napływu imigrantów spoza kontynentu i przy zachowaniu obecnych trendów w dłuższej perspektywie liczba ludności Europy będzie malała.

W 2017 r. wzrosła liczba rozwodów. Zjawisko to dotknęło 65 tys. par małżeńskich, czyli o ok. 1,5 tys. więcej niż w 2016 r. Oznacza to, że już co trzecie małżeństwo w Polsce się rozpada. Jeśli doliczyć do tego liczbę separacji, z których wg GUS niemal wszystkie prędzej czy później kończą się rozwodem, wówczas obraz polskich rodzin wygląda wręcz tragicznie. Demografowie przewidują, iż do 2050 r. przy tak niskim wskaźniku dzietności nastąpi stopniowy spadek ludności Polski z 38,7 mln do ok. 27,3 mln obywateli. Następstwem spadku liczby urodzonych dzieci będzie niewątpliwie szybki proces starzenia się polskiego społeczeństwa. Zacznie lawinowo rosnąć liczba emerytów. Grozi to całkowitym załamaniem systemu emerytalnego, w którym obecnie na 5 pracujących osób przypada 1 emeryt; za 30–50 lat na 1 emeryta będzie pracować już tylko 1 osoba. Przewidywane przez GUS niekorzystne zmiany zarówno liczby, jak i struktury wieku kobiet w wieku rozrodczym spowodują, iż mimo założonego wzrostu dzietności liczba urodzeń będzie malała. W 2050 r. spodziewane jest zaledwie 277,6 tys. urodzeń. W perspektywie najbliższych dwudziestu kilku lat GUS spodziewa się także znacznego wzrostu liczby zgonów. Z prognozy wynika, że liczba zgonów będzie rosła stopniowo do 2043 r., gdy osiągnie maksymalny poziom ok. 444 tys.

Sergiusz Wasiuta

Bezpieczeństwo społeczne. Pojęcia – uwarunkowania – wyzwania, A. Skrabacz, S. Sułkowski (red.), Dom Wydawniczy Elipsa, Warszawa 2012; *Demografia i bezpieczeństwo społeczne krajów Unii Europejskiej*, I. Sobczak, M. Wyrzykowska-Antkiewicz (red.), Wyższa Szkoła Bankowa, CeDeWu, Gdańsk–Warszawa 2013; A. Durasiewicz, *Bezpieczeństwo demograficzne na przykładzie wybranych państw*, [w:] *Polityka społeczna dla bezpiecznego rozwoju*, M. Leszczyński, M. Kubiak (red.), Instytut Politologii Uniwersytetu Gdańskiego, Gdańsk 2015; M. Kawalec, J. Wróbel, *Bezpieczeństwo demograficzne*, [w:] *Ekonomika bezpieczeństwa państwa w zarysie. Zarządzanie bezpieczeństwem*, J. Płaczek (red.), Wydawnictwo Difin, Warszawa 2014; M. Łakomy, *Bezpieczeństwo demograficzne a potęga państw*, „Przegląd Geopolityczny" 2017, nr 19; tenże, *Demografia polityczna i możliwości dla polityki pronatalistycznej w Polsce*, „Studia Demograficzne" 2016, t. 169, nr 1; *Polska w liczbach*, Główny Urząd Statystyczny, Warszawa 2017; P. Warchoł,

Zmiany demograficzne jako zagrożenie dla bezpieczeństwa. Analiza na przykładzie Japonii, „Przegląd Strategiczny" 2015, nr 8; S. Wasiuta, *Bezpieczeństwo demograficzne*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018.

BEZPIECZEŃSTWO DZIECKA – o odrębnym traktowaniu → b e z p i e c z e ń s t w a dzieci zaczęto mówić dopiero pod koniec XIX w., wykorzystując pojęcie ochrony dzieciństwa, które traktowano jako wszelkie działania państwa, samorządów i organizacji społecznych mających za zadanie zapewnienie dziecku niezbędnych warunków do prawidłowego rozwoju. Sam termin „dzieciństwo" sformułował w 1762 r. J.-J. Rousseau w traktacie *Emil, czyli o wychowaniu*. Znaczący wpływ na uwrażliwienie na kwestię bezpieczeństwa dzieci miał przypadek 10-letniej M.E. McCormack mieszkającej na Manhattanie, która w 1873 r. zwróciła uwagę sąsiadów. Dziewczynka była zaniedbana i posiniaczona, dlatego poinformowali oni departament sprawujący nadzór nad przytułkami, ośrodkami dla umysłowo chorych, sierocińcami, więzieniami i szpitalami publicznymi (Department of Public Charities and Correction). Nie istniały wówczas żadne regulacje prawne chroniące dziecko przed → p r z e m o c ą [t. 3] fizyczną ze strony rodziców, z tego powodu E.A. Wheeler, będąca pracownikiem socjalnym w sprawie dziewczynki, powiadomiła lokalny oddział Amerykańskiego Towarzystwa Zapobiegania Okrucieństwu wobec Zwierząt (The American Society for the Prevention of Cruelty to Animals, ASPCA).

H. Bergh, założyciel ASPCA, prawnik E. Gerry'ego, który oskarżył przybraną matkę o znęcanie się nad dziewczynką, oraz filantrop J.D. Wright stworzyli w 1874 r. Towarzystwo Zapobiegania Okrucieństwu wobec Dzieci (The New York Society for the Prevention of Cruelty to Children), pierwszą na świecie organizację działającą na rzecz dzieci zaniedbywanych i maltretowanych. W 1892 r. powstało Międzynarodowe Stowarzyszenie Opieki nad Dzieckiem (International Kindergarten Union, obecnie Association for Childhood Education International), a w 1919 Save the Children i jej szwedzka sekcja Rädda Barnen.

Deklaracja praw dziecka z 1959 r. nie określała limitu wieku, zgodnie z którym osobę należy traktować jako dziecko, wskazywała jednak na kryterium braku dojrzałości fizycznej i umysłowej, warunkującej konieczność otoczenia dzieci szczególną opieką i troską, w tym właściwą ochroną prawną, zarówno przed urodzeniem, jak i po urodzeniu. Kryterium wieku w określaniu „dziecka" ma jednak zasadnicze znaczenie z uwagi na brak jego pełnej zdolności do czynności prawnych. Przyjmuje się zatem wykładnię Konwencji o prawach dziecka, w której art. 1 dziecko „oznacza każdą istotę ludzką w wieku poniżej 18 lat, chyba że zgodnie z prawem odnoszącym się do dziecka uzyska ono wcześniej pełnoletność". Niemniej poza terminem „dziecko" normy prawa posługują się również innymi pojęciami. Międzynarodowy pakt praw gospodarczych, społecznych i kulturalnych używa pojęć „dzieci na utrzymaniu" oraz „dzieci i młode osoby". Terminem „osoby poniżej 18. roku życia" posługuje się Międzynarodowy pakt

praw obywatelskich i politycznych oraz Konwencja genewska o ochronie osób cywilnych podczas wojny. W odniesieniu do dzieci będących w konflikcie z prawem stosuje się termin „nieletni" – *juvenile* (z ang.). W tej formie funkcjonuje w rezolucjach Zgromadzenia Ogólnego i Rady Praw Człowieka, Deklaracji z Limy w sprawie sprawiedliwości naprawczej nieletnich, we Wskazaniach ONZ dotyczących zapobiegania przestępczości nieletnich (tzw. wskazania rijadzkie), Regułach Narodów Zjednoczonych odnoszących się do ochrony nieletnich pozbawionych wolności oraz w Międzynarodowej konwencji o ochronie praw wszystkich pracowników migrujących i członków ich rodzin. Jednocześnie w Międzynarodowym pakcie praw obywatelskich i politycznych termin *juvenile* jest tłumaczony jako „młodociany" i dotyczy osoby oskarżonej o popełnienie przestępstwa lub uznanej winną popełniania przestępstwa. Minimalne standardy Narodów Zjednoczonych zawierające zasady działania administracji sądownictwa wobec nieletnich (tzw. reguły pekińskie) używają bardzo szerokiej definicji nieletniego, uznając za niego dziecko lub osobę młodą, która w danym systemie prawnym może być pociągnięta do odpowiedzialności za przestępstwo na innych zasadach niż dorosły lub za czyny określane mianem demoralizacji. W tym przypadku granice wiekowe uzależnia się od każdego systemu prawnego, co sprawia, że grupy wiekowe objęte definicją nieletniego mają zakres od 7 do 18 lat lub powyżej.

Kryterium małoletności stosowane w określaniu dziecka odpowiada również postulatom, jakie w odniesieniu do poszczególnych sfer, etapów rozwoju i potrzeb dziecka są formułowane przez lekarzy, pedagogów, socjologów i psychologów.

W warstwie biologicznej bezpieczeństwo oznacza zapewnienie dziecku właściwej pielęgnacji, odpowiednich składników odżywczych, wyrównywania ewentualnych niedoborów w organizmie, wykrywania i leczenia stanów chorobowych, stymulowania rozwoju z wykorzystaniem odpowiednich warunków środowiska. Prawidłowy rozwój społeczny wymaga odpowiedniego środowiska domowego, szkolnego i pozaszkolnego, a także organizowania sytuacji sprzyjających kształtowaniu odpowiednich relacji interpersonalnych, przyjęcia i dostosowania się dziecka do akceptowanych norm społecznych oraz przezwyciężania sytuacji niekorzystnych. Z kolei rozwój kulturalny pociąga za sobą konieczność przyswajania przez dziecko modelu kultury wolnego od przemocy, dyskryminacji, nienawiści, fanatyzmu, niesprawiedliwych stosunków społecznych czy stereotypowego postrzegania ról w społeczeństwie. Bezpieczeństwo dziecka jest zatem stanem, w którym potrzeby zmieniające się w zależności od sfery i stopnia osiąganego rozwoju i dojrzałości dziecka są zaspokojone; stanem, w którym kontrolowane są → z a g r o ż e n i a [t. 4] prowadzące do szkód fizycznych, psychicznych, emocjonalnych i materialnych dziecka, co służy stworzeniu odpowiednich warunków dla jego zdrowego, wielopłaszczyznowego rozwoju. Bezpieczeństwo traktowane jako proces podlega ciągłemu umacnianiu przez inne podmioty, np. rodzinę, szkołę, państwo. O jego dynamice świadczą zagrożenia, które ulegają przeobrażeniom, zmieniają intensywność oddziaływań. Bezpieczeństwo dziecka można rozpatrywać jako

wolność od zagrożeń chronicznych, czyli od głodu, choroby, represji, oraz jako ochronę przed nagłymi i szkodliwymi zakłóceniami w modelach życia codziennego, tj. w domu, instytucjach opieki, szkole, społeczności. Obejmuje ono działania organizacyjne i prawne realizowane przez rodziców, społeczeństwo, instytucje edukacyjne, opiekuńcze, wychowawcze, podmioty rządowe i pozarządowe krajowe, zagraniczne i międzynarodowe, które mają za zadanie zapewnienie odpowiednich warunków dla rozwoju psychicznego, fizycznego, socjo-kulturowego i duchowego dziecka oraz niedopuszczenie do jego marginalizacji. O bezpieczeństwie dzieci decydują względnie stałe czynniki, które w zasadniczy sposób implikują decyzję władz co do eliminacji ryzyka i poprawy warunków rozwoju. Podyktowane są rodzajami zagrożeń, stanem państwowości, w tym elit politycznych, zobowiązaniami międzynarodowymi, religią i kulturą. Na bezpieczeństwo wpływa także stopień świadomości społecznej, poziom rozwoju kraju oraz konflikt zbrojny.

→ Z a g r o ż e n i a b e z p i e c z e ń s t w a [t. 4] dzieci stanowią wszelkie potencjalne i rzeczywiste działania, sytuacje, zjawiska i warunki, które naruszają dobrostan dziecka, powodują niebezpieczeństwo dla jego zdrowia, życia, rozwoju fizycznego, psychicznego, społecznego, emocjonalnego oraz warunków socjalnych. Wywołują je naturalne czynniki wewnętrzne samego dziecka, np.: uszkodzenia układu nerwowego, oddechowego czy choroby wrodzone lub nabyte, czynniki polityczne, ekonomiczne, kultura, religia, siły natury. Źródło zagrożeń stanowią sytuacje społeczne (np.: patologie, bezrobocie), militarne (działalność sił i grup zbrojnych, → t e r r o r y z m [t. 4]), →t e c h n o l o g i e i n f o r m a c y j n o - k o m u n i k a c y j n e [t. 4], natura (powodzie, susze, lawiny, trzęsienia ziemi, osunięcia gruntu). Zagrożone może być dziecko, ale i konkretne grupy dzieci: dzieci ulicy, niepełnosprawne, dzieci wewnętrznie przesiedlone, dzieci osierocone, dzieci z plemion koczowniczych itd. Zagrożenia generuje zarówno najbliższe dziecku środowisko, jakim jest rodzina, jak i lokalna społeczność, szkoła, rówieśnicy, państwo. Szczególnym zagrożeniem bezpieczeństwa dziecka jest konflikt zbrojny. → R a d a B e z p i e c z e ń s t w a O N Z [t. 3] identyfikuje 6 głównych naruszeń (ang. *six grave violations*) podczas konfliktu zbrojnego:

- zabijanie i okaleczanie dzieci,
- rekrutację lub wykorzystywanie dzieci jako → ż o ł n i e r z y [t. 4],
- przemoc seksualną wobec dzieci,
- ataki na szkoły i szpitale,
- odmowę dostępu do pomocy humanitarnej dla dzieci,
- uprowadzenia dzieci.

Naruszenie stanowią także przymusowe przesiedlenia, przymusowa praca i inne formy niewolnictwa.

Zapewnienie bezpieczeństwa i odpowiednich warunków rozwoju dziecka spoczywa przede wszystkim na jego rodzicach/opiekunach. Państwo nie wyręcza rodziców w ich powinnościach, ale może ich wspierać i interweniuje w sytuacji, gdy bezpieczeństwo dziecka jest zagrożone. Brak zaspokojenia potrzeby bezpieczeństwa, miłości

i przynależności powoduje u dziecka skutki psychiczne na każdym etapie rozwoju. W konsekwencji, zdaniem M. Łopatkowej, w wieku przedszkolnym mogą wystąpić opóźnienia w rozwoju, „imbecylizm uczuciowy", brak koncentracji, nadpobudliwość. W wieku szkolnym może się to objawiać zamknięciem się w sobie, biernością, wycofaniem się z kontaktów społecznych, powierzchownością, agresywnością, roszczeniowością, niechęcią do nauki i szkoły, zaniżonym poziomem myślenia logicznego i abstrakcyjnego, nieszanowaniem rzeczy, a także pogłębieniem postawy konsumpcyjnej. Z kolei u młodzieży może dojść do zaniku ambicji, samodzielności, odpowiedzialności za siebie i innych, wczesnego rozpoczęcia życia seksualnego, skłonności do alkoholu.

Deklaracja praw dziecka z 1924 r. obligowała kobiety i mężczyzn do zapewnienia dziecku normalnego rozwoju fizycznego i duchownego, opieki, pomocy w czasie klęski i zabezpieczenia przed wszelkim wyzyskiem. Deklaracja praw dziecka przyjęta przez Zgromadzenie Ogólne ONZ w 1956 r. podkreślała, iż dziecko powinno mieć pierwszeństwo w pomocy oraz ochronie przed wszelkim zaniedbaniem, okrucieństwem i wyzyskiem, a jego dobro winno być celem nadrzędnym przy uchwalaniu ustaw. Pakty praw człowieka z 1966 r. przyznały dziecku prawo do środków ochrony, jakich wymaga status małoletniego, ze strony rodziny, społeczeństwa i państwa, zwracając szczególną uwagę na ochronę dzieci i młodzieży przed wyzyskiem ekonomicznym i społecznym. W 1989 r. uchwalono Konwencję o prawach dziecka, która przyznała dzieciom prawa cywilne, socjalne i kulturalne oraz w niewielkim stopniu prawa polityczne (wolność pokojowych zgromadzeń) i ekonomiczne (praca). Konwencja obliguje państwa strony do podejmowania:

> […] wszelkich kroków w dziedzinie ustawodawczej, administracyjnej, społecznej oraz wychowawczej dla ochrony dziecka przed wszelkimi formami przemocy fizycznej bądź psychicznej, krzywdy lub nadużyć, zaniedbania bądź niedbałego traktowania lub wyzysku, a w tym wykorzystywania w celach seksualnych dzieci pozostających pod opieką rodzica/ów, opiekuna/ów prawnego/ych lub innej osoby sprawującej opiekę nad dzieckiem.

W 2000 r. przyjęto 2 Protokoły fakultatywne do Konwencji o prawach dziecka, tj. w sprawie handlu dziećmi, dziecięcej prostytucji i dziecięcej pornografii oraz w sprawie angażowania dzieci w konflikty zbrojne. Trzeci protokół fakultatywny do Konwencji o prawach dziecka w sprawie procedury składania zawiadomień do Komitetu praw dziecka na naruszenia praw dzieci przyjęto dopiero w 2011 r. Do konwencji Rady Europy, które mają duże znaczenie dla kształtowania bezpieczeństwa dzieci, należy zaliczyć: Konwencję o ochronie praw człowieka i podstawowych wolności (1950) wraz z protokołami dodatkowymi, Europejską kartę społeczną (1961) i Zrewidowaną europejską kartę społeczną (1996), Protokół dodatkowy do Europejskiej karty społecznej wprowadzający system skarg zbiorowych (1995), Europejską konwencję o przysposobieniu dzieci (1967), Europejską konwencję o statusie prawnym dziecka pozamałżeńskiego (1975), Europejską konwencję o uznawaniu i wykonywaniu orzeczeń

dotyczących pieczy nad dzieckiem oraz o przywracaniu pieczy nad dzieckiem (1980), Europejską konwencję o zapobieganiu torturom oraz nieludzkiemu lub poniżającemu traktowaniu albo karaniu (1987), Europejską konwencję o wykonywaniu praw dzieci (1996), Europejską konwencję o obywatelstwie (1997), Konwencję o cyberprzestępczości (2001), Konwencję w sprawie kontaktów z dziećmi (2003), Konwencję w sprawie działań przeciwko handlowi ludźmi (2005), Konwencję o ochronie dzieci przed ich seksualnym wykorzystywaniem i znieważaniem (2007).

Klaudia Cenda-Miedzińska

K. Cenda-Miedzińska, *Bezpieczeństwo dziecka*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; taż, *Międzynarodowe działania na rzecz poprawy bezpieczeństwa komunikacyjnego dzieci i młodzieży w cyberprzestrzeni*, [w:] *Komunikowanie społeczne w globalizującym się świecie: szanse i zagrożenia dla edukacji*, G. Andrzejewska, K. Czerwiński, M. Schneider (red.), Wydawnictwo Adam Marszałek, Toruń 2010; taż, *Problematyka ochrony praw dziecka w konwencjach Rady Europy*, „Ruch Pedagogiczny" 2008, nr 5–6; taż, *Bezpieczeństwo fizyczne a prawa dzieci*, [w:] *Edukacja dla bezpieczeństwa wobec wyzwań współczesności*, Z. Kwiasowski, K. Cenda-Miedzińska (red.), Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2012; taż, *Współczesne konflikty zbrojne a bezpieczeństwo dzieci – polityka władz Islamskiej Republiki Afganistanu wobec dzieci-żołnierzy*, [w:] *Jednostki, grupy i społeczeństwa*, t. 2, M. Kopczewski, A. Kurkiewicz, S. Mikołajczak (red.),Wydawnictwo Wyższej Szkoły Bezpieczeństwa, Poznań 2015; taż, *Wybrane aspekty bezpieczeństwa społecznego dzieci*, [w:] *„Jestem nie po to, aby mnie kochać i podziwiać, ale po to, abym ja działał i kochał" – dzieło i życie Janusza Korczaka*, M. Lubińska-Bogacka, M. Banach (red.), Impuls, Kraków 2014; taż, *Zakaz stosowania kar cielesnych wobec dzieci na przykładzie ustawodawstwa wybranych krajów*, [w:] *Pracownik socjalny wobec wyzwań współczesności*, T.W. Gierat, A. Grudziński, E. Kucharska (red.), Scriptum, Kraków 2012; *International Instruments Relevant to the Security and Protection of Children. The Choice of Source Texts*, vol. 1: *Treaties and Protocols, Rules, Guidelines, Guiding Principles*, vol. 2: *Declarations, Recommendations, Resolutions*, K. Cenda-Miedzińska (ed.), Scriptum, Cracow 2014; M. Łopatkowa, *Samotność dziecka*, WSiP, Warszawa 1983.

BEZPIECZEŃSTWO EKOLOGICZNE – element →b e z p i e c z e ń s t w a n a r o d o w e g o , który zapewnia ochronę żywotnych interesów społeczeństwa ludzkiego, środowiska naturalnego i stanów rzeczywistych lub potencjalnych → z a g r o ż e ń [t. 4] stwarzanych przez sztuczne albo naturalne czynniki oddziaływania na środowisko. Bezpieczeństwo ekologiczne jest kategorią społeczną, która jest nieodłączną częścią społeczeństwa ludzkiego i która tworzy się w ramach stosunków społecznych. Można je charakteryzować przede wszystkim jako odwieczną wartość ludzkiej społeczności, która opiera się na systemie gwarancji bezpieczeństwa ekologicznego współistnienia środowiska naturalnego i człowieka. Dotyczy bezpieczeństwa człowieka w procesach: interakcji ze środowiskiem naturalnym, z substancjami niebezpiecznymi (radioaktywnymi, chemicznymi, toksycznymi itd.), stosowania destrukcyjnych i niebezpiecznych technologii. Może być powiązane również z niekontrolowanymi przez człowieka procesami i zjawiskami (siły natury).

Przy zapewnieniu bezpieczeństwa ekologicznego są brane pod uwagę prawa natury, wg których rozwijają się obiekty ekologiczne. Oprócz tego pieczę nad bezpieczeństwem ekologicznym sprawuje państwo, które tworzy system organów wyspecjalizowanych. Podstawy prawne zapewnia zaś dla niego prawo ochrony środowiska jako odrębny zbiór przepisów. Przepisy służące dbaniu o bezpieczeństwo ekologiczne są jednymi z podstawowych praw.

Definicja bezpieczeństwa ekologicznego zmieniała się w ciągu ostatnich 40 lat. Pierwsze nawiązywały do potrzeby działań na rzecz likwidacji lub zmniejszenia do minimum zagrożeń spowodowanych przez skażenia i dewastację środowiska i podkreślały głównie zapobieganie zjawiskom zachodzącym nagle. Nie nawiązywały zaś do działań mających na celu zabezpieczenie funkcjonowania przyrody i środowiska, w jakim żyje człowiek. Lata obserwacji i badań środowiska naturalnego wykazały, że nie można traktować bezpieczeństwa ekologicznego przez pryzmat tylko bezpieczeństwa człowieka. Okazało się, że istnieje ścisły związek między tym, co dzieje się w przyrodzie, a tym, czym zajmuje się człowiek.

Obecnie bezpieczeństwo ekologiczne pojmuje się jako trwały i ciągły proces zmierzający do osiągnięcia pożądanego stanu ekologicznego, zabezpieczający spokojną i zdrową egzystencję wszystkich elementów ekosystemu, przy użyciu różnych środków zgodnych z zasadami współżycia wewnętrznego państwa i społeczności międzynarodowych.

Bezpieczeństwo ekologiczne to również zbiór działań, stanów i procesów, które bezpośrednio lub pośrednio nie prowadzą do poważnego uszkodzenia (bądź zagrożenia wystąpienia takich szkód) środowiska naturalnego, człowieka albo ludzkości w ogóle; to także działania i wydarzenia, które zapewniają równowagę ekologiczną na Ziemi i w każdym z regionów na poziomie, do którego ludzkość fizycznie, społeczniegospodarczo, technologicznie i politycznie jest gotowa się adaptować.

Bezpieczeństwo ekologiczne jest realizowane na poziomie globalnym, regionalnym, lokalnym, w tym na terytorium państwa lub oddzielnych regionów. W rzeczywistości charakteryzuje ekosystemy wszystkich hierarchicznych rang – od biocenozy (agro-, urbo-) do biosfery jako całości. Ograniczają je rozmiar i czas przeprowadzonych akcji: krótkoterminowy efekt zmian ekologicznych może być stosunkowo bezpieczny i nawet niewyczuwalny, natomiast długotrwały – niebezpieczny, lokalne zmiany mogą nie wpłynąć na poziom bezpieczeństwa ekologicznego, ale zmiany procesów ekologicznych zachodzące na dużą skalę mogą przynieść fatalne albo nawet śmiertelne konsekwencje.

Globalny poziom bezpieczeństwa ekologicznego obejmuje prognozowanie i śledzenie procesów w biosferze jako całości i jej obszarach składowych. Od 2. poł. XX w. procesy wyrażają się w globalnych zmianach klimatu, powstaniu efektu cieplarnianego, niszczeniu warstwy ozonowej, tworzeniu się nowych pustyń i zanieczyszczeniu oceanów. Istotą globalnej kontroli i zarządzania jest zachowanie i przywrócenie naturalnego mechanizmu biosfery środowiska naturalnego, który jest częścią biosfery żywych organizmów.

Zarządzanie globalnym bezpieczeństwem ekologicznym leży w obszarze stosunków międzynarodowych na poziomie ONZ, → U N E S C O [t. 4], UNEP (Programu Środowiskowego ONZ, United Nations Environment Programme) i innych organizacji międzynarodowych. Metody zarządzania na tym poziomie obejmują przyjęcie międzynarodowych regulacji dotyczących ochrony środowiska w całej biosferze, realizację międzynarodowych programów ochrony środowiska, stworzenie międzyrządowych jednostek w celu wyeliminowania katastrof ekologicznych, które mają naturalny lub antropogeniczny charakter. Na poziomie globalnym wyeliminowano szereg problemów. Wielkim sukcesem społeczności międzynarodowej jest zakaz prób nuklearnych, porozumienie w sprawie wprowadzenia światowego zakazu połowu wielorybów i prawnej regulacji międzypaństwowego wyłowu ryby oraz innych owoców morza, stworzenie międzynarodowych Czerwonych Ksiąg w celu zachowania bioróżnorodności, wspólne badanie Arktyki i Antarktydy jako obszarów przyrodniczych biosfery nietkniętych ingerencją człowieka.

Zakres regionalny bezpieczeństwa ekologicznego obejmuje duże obszary geograficzne lub ekonomiczne, a czasami terytorium kilku państw. Monitorowanie i kontrola odbywają się na poziomie państwa i stosunków międzyrządowych. System zarządzania bezpieczeństwem ekologicznym obejmuje wtedy: ekologizację gospodarki, nowe, przyjazne dla środowiska technologie; tempo rozwoju gospodarczego, które nie utrudnia odtworzenia środowiska naturalnego i wspierania racjonalnego wykorzystania zasobów naturalnych.

Zakres lokalny bezpieczeństwa ekologicznego obejmuje miasta, powiaty, przedsiębiorstwa metalurgiczne, chemiczne, naftowe, górnicze oraz kompleks obronny, a także kontrole emisji, gospodarki odpadami i inne. Zarządzanie bezpieczeństwem ekologicznym odbywa się w ramach administracji miasta, powiatu, przedsiębiorstw z udziałem agencji odpowiedzialnych za warunki sanitarne i ochronę środowiska. Rozwiązania konkretnych problemów lokalnych decydują o możliwości osiągnięcia celu zarządzania bezpieczeństwem ekologicznym na szczeblu regionalnym i globalnym. Cel ten osiąga się przy poszanowaniu zasady przekazywania → i n f o r m a c j i [t. 2] o stanie środowiska naturalnego od poziomu lokalnego do regionalnego i globalnego.

Niezależnie od zakresu zarządzania bezpieczeństwem ekologicznym obiektem zarządzania zawsze jest środowisko naturalne. Dlatego w systemie zarządzania bezpieczeństwem ekologicznym na każdym poziomie musi być przedstawiona analiza gospodarcza, finansowa, prawna, administracyjna, edukacji, kultury i zasobów naturalnych.

Obiektem bezpieczeństwa ekologicznego jest wszystko to, co ma duże znaczenie dla bezpieczeństwa: prawa, materialne i duchowe potrzeby jednostki, zasoby naturalne i środowisko naturalne jako materiał rozwoju państwowego i społecznego. Przedmiotem bezpieczeństwa ekologicznego jest człowiek, społeczeństwo, biosfera i państwo.

Mówiąc o rodzajach bezpieczeństwa ekologicznego, należy powiedzieć, że klasyfikacje bezpieczeństwa ekologicznego można analizować wg różnych zasad: źródeł

zagrożeń, podziału terytorialnego, skali negatywnych skutków, sposobów i środków zapewnienia bezpieczeństwa, szkodliwej dla środowiska działalności człowieka.

W zależności od źródeł zagrożeń rozróżniamy:

- te, które wystąpiły jako efekt wpływu działalności gospodarczej człowieka na środowisko naturalne (społeczne, polityczne, wojskowe, katastrofy spowodowane działalnością technologiczną człowieka), w związku z którymi pojawiają się naturalne zagrożenia, takie jak klęski i katastrofy żywiołowe (trzęsienia ziemi, wybuchy wulkanów, powodzie itp.);
- cywilizacyjne – materialne zanieczyszczenia różnego rodzaju i typu wprowadzane do otoczenia w wyniku działalności człowieka.

Na skutek katastrofy przemysłowej czy klęski żywiołowej może powstać nagłe nadzwyczajne zagrożenie życia i zdrowia ludzi lub środowiska przyrodniczego, w wyniku pojawienia się w środowisku czynników biologicznych, chemicznych, atomowych, powodziowych, pożarowych bądź technicznych. Rezultatem jest degradacja albo dewastacja środowiska, a w skrajnym przypadku – klęska ekologiczna (taka jak w Czarnobylu w 1986 r. czy w Japonii po trzęsieniu ziemi u wybrzeży Honsiu w 2011 r.).

Najogólniej rzecz ujmując, zagrożenia ekologiczne to zdarzenia, w których istnieje możliwość wystąpienia trwałego (nieodwracalnego w sposób naturalny) uszkodzenia lub zniszczenia dużego obszaru środowiska przyrodniczego, wpływającego negatywnie (pośrednio albo bezpośrednio) na zdrowie lub życie ludzi. Do tego typu zdarzeń można zaliczyć:

- → k a t a s t r o f y n a t u r a l n e [t. 2] i przemysłowe;
- niekontrolowaną eksploatację zasobów naturalnych;
- zanieczyszczenie wody, powietrza i gleby na skalę masową;
- brak gospodarki odpadami komunalnymi, przemysłowymi, nuklearnymi;
- stosowanie niebezpiecznych technologii przemysłowych;
- naruszenie stosunków wodnych w środowisku;
- chaotyczną urbanizację;
- próby nuklearne i testy nowych typów broni.

Bezpieczeństwo ekologiczne ze względu na skalę terytorialną dzieli się na:

- globalne (międzynarodowe),
- narodowe (państwowe),
- regionalne,
- lokalne,
- oddzielne obiekty ochrony środowiska.

Według skali negatywnych skutków można wyróżnić ogólne bezpieczeństwo ekologiczne, które obejmuje globalne, krajowe, lokalne i osobiste bezpieczeństwo ekologiczne obywateli. Według kryterium sposobów i środków zapewnienia bezpieczeństwa wyróżnia się:

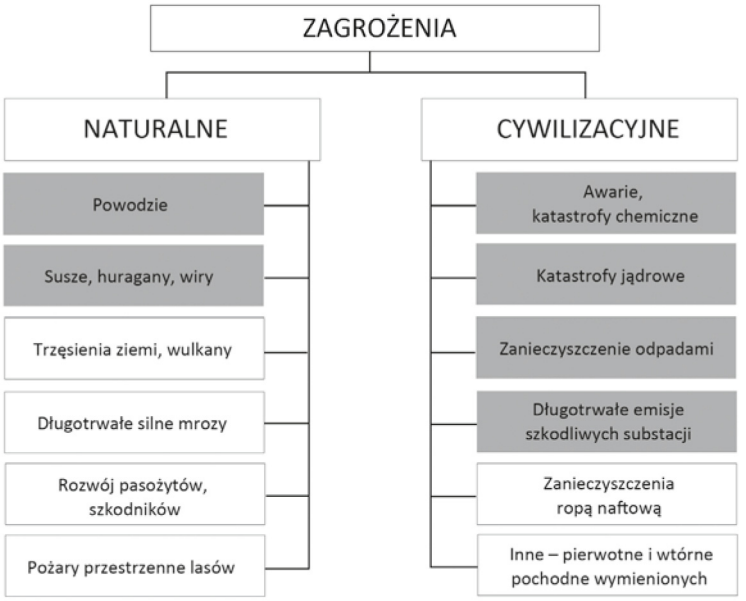
- bezpieczeństwo technologiczno-ekologiczne,

- radiologiczne,
- społeczno-ekologiczne,
- środowiskowe,
- gospodarczo-ekologiczne.

Bezpieczeństwo ekologiczne dzieli się też wg kryterium szkodliwej dla środowiska działalności człowieka na: techniczne, chemiczne, toksyczne, biologiczne, radioaktywne, jądrowe, konstrukcje hydrauliczne i inne.

Bezpieczeństwo ekologiczne przewiduje – za sprawą postępu naukowego i technologicznego – optymalizację lub zmniejszenie wykorzystania zasobów naturalnych, negatywnych wpływów antropologicznych i technogennych, poprawę naturalnych i społecznych warunków życia, a także zachowania różnorodności środowiska. Prawidłowy rozwój oraz życie obywateli powinny przebiegać w czystym, zdrowym i nieskażonym środowisku naturalnym, dlatego też należy racjonalnie połączyć procesy rozwoju państwa przy zachowaniu równowagi przyrodniczej i ekologicznej.

Zagrożenie dla bezpieczeństwa Polski w sferze ekologicznej stanowią: negatywne skutki katastrof ekologicznych wewnątrz kraju i w państwach ościennych; rozmieszczenie w kraju obiektów gospodarki stwarzających zagrożenie awariami; transport niebezpiecznych środków, materiałów i technologii; ujemny wpływ działalności gospodarczej na środowisko naturalne; nieefektywne wykorzystywanie zasobów naturalnych; stosowanie ekologicznie szkodliwych technologii.



Ryc. 1. Składowe bezpieczeństwa ekologicznego – kolorem szarym oznaczono te, które występują na terenie Polski. Oprac. aut.

Z dokumentu *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* z 2014 r. wynika, że nadrzędnym celem naszego państwa w zakresie bezpieczeństwa ekologicznego jest podjęcie szeregu działań mających na celu zmniejszenie zagrożeń. Cele te będą osiągnięte poprzez poprawę stanu środowiska, zachowanie różnorodności biologicznej oraz adaptację do zmian klimatu, w szczególności po uwzględnieniu konieczności zapewnienia odpowiedniego poziomu inwestycji w źródła niskoemisyjne. W ramach ochrony środowiska kontynuowane będą działania na rzecz poprawy czystości powietrza, wód, gleb oraz właściwej gospodarki odpadami. Adaptacja do zmieniających się uwarunkowań klimatycznych i hydrologicznych wymaga wdrożenia nowych rozwiązań systemowych, ukierunkowanych m.in. na minimalizowanie skutków klęsk żywiołowych i ekstremalnych zjawisk pogodowych. Szczególne znaczenie w tym kontekście ma realizacja działań przeciwpowodziowych oraz usprawnienie →s y s t e m u z a r z ą d z a n i a k r y z y s o w e g o [t. 4]. Istotne jest też prowadzenie kampanii edukacyjnych upowszechniających ochronę środowiska, zachowanie różnorodności biologicznej oraz adaptację do zmian klimatu. Gospodarka wodna musi stać się priorytetem w skali gospodarki całego kraju.

W ciągu ostatnich lat przybliżyło się widmo katastrofy ekologicznej spowodowanej działalnością człowieka, a zwłaszcza rozwojem gospodarczym, lawinowym wzrostem konsumpcji surowców, paliw i żywności. Naukowcy z wielu państw potwierdzili istnienie związku między gospodarczą działalnością człowieka a coraz częściej występującymi klęskami żywiołowymi takimi jak ekstremalne susze, powodzie czy huragany. Następuje degradacja gleb, ubywa ozonu, a funkcjonowanie wielu ekosystemów jest zagrożone. Największe niebezpieczeństwa dla ludzkości w XXI w. to zagrożenia wynikające ze zmiany klimatu, niedoboru wody, zamierania lasów, zanieczyszczenia wody i powietrza. Większość zagrożeń, jakie pojawiają się w naszym otoczeniu, jest wynikiem działalności człowieka. Coraz częściej mają one zasięg globalny. Uwalniane w czasie produkcji gazy przemysłowe zatruwają powietrze, a odpady komunalne, poprodukcyjne, rozmaite substancje chemiczne oraz śmieci z gospodarstw domowych zanieczyszczają ziemię.

Aleksander Wasiuta

Bezpieczeństwo ekologiczne regionu. Teoria i praktyka: działy wybrane, E. Krasowski (red.), Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, Lublin 2013; *Bezpieczeństwo w perspektywie ekologicznej*, M. Kubiak, M. Tołwiński (red.), ASPRA-JR, Siedlce–Warszawa 2017; P. Korzeniowski, *Bezpieczeństwo ekologiczne jako instytucja prawna ochrony środowiska*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2012; A. Kramek, *Bezpieczeństwo ekologiczne obszarów zurbanizowanych*, „Przegląd Prawno-Ekonomiczny" 2017, nr 39; M. Pietraś, *Bezpieczeństwo ekologiczne w Europie: studium politologiczne*, Wydawnictwo UMCS, Lublin 2000; A. Wasiuta, *Ekonomiczne instrumenty polityki ekologicznej w kontekście zarządzania środowiskowego*, [w:] *Współdziałanie systemu zarządzania i inżynierii produkcji. Teoria i praktyka*, T. Noch, J. Saczuk (red.), Wydawnictwo Gdańskiej Szkoły Wyższej, Gdańsk 2015; tenże, *Ekonomiczne uwarunkowania rozwoju energetyki wiatrowej*, Wydział Dziennikarstwa i Nauk

Politycznych, Uniwersytet Warszawski, Warszawa 2014; tenże, *Labor Market in Poland in the Context of Renewable Energy Sector Development*, „Ekonomia i Środowisko" 2018, nr 1 (64); S. Wasiuta, *Ukraine before and after Chernobyl: Social and Medical Aftermath of the Disaster in Chernobyl as a Result of Soviet Ecological Policy*, [w:] *Globalne i regionalne problemy ochrony środowiska*, W. Pawlak, T. Noch (red.), Wydawnictwo Gdańskiej Wyższej Szkoły Administracji, Gdańsk 2006; *Współczesne bezpieczeństwo ekologiczne*, M. Kubiak, M. Lipińska-Rzeszutek (red.), ASPRA-JR, Warszawa 2017; О. Васюта, С. Васюта, Г. Філіпчук, *Екологічна політика: національні та глобальні реалії*, т. 4, Зелена Буковина, Чернівці 2003–2004.

BEZPIECZEŃSTWO EKONOMICZNE – jeden z najważniejszych elementów → b e z p i e c z e ń s t w a n a r o d o w e g o, co odzwierciedla związek przyczynowy między siłą ekonomiczną kraju, jego potencjałem wojskowym, gospodarczym i → b e z p i e c z e ń s t w e m n a r o d o w y m. Zachowanie bezpieczeństwa ekonomicznego stało się jednym z głównych celów polityki wewnętrznej i zagranicznej państw. W najbliższych latach to właśnie na tej płaszczyźnie będzie się toczyć rywalizacja między państwami, w przestrzeni ekonomicznej jako rynkach zbytu towarów i inwestycji. Analiza bezpieczeństwa ekonomicznego państwa ujmowanego jako jedna z części składowych prowadzonej polityki bezpieczeństwa jest ważna ze względu na siłę, jakiej we współczesnym świecie nabierają → z a g r o ż e n i a [t. 4] asymetryczne.

W literaturze naukowej istnieje wiele poglądów na temat definicji bezpieczeństwa ekonomicznego państwa. Propozycje ekspertów krajowych i zagranicznych opierają się na różnych podejściach i znacznie odbiegają od siebie. Terminem bezpieczeństwa ekonomicznego jako pierwszy posługiwał się prezydent USA F.D. Roosevelt podczas wielkiego → k r y z y s u [t. 2]. W przeszłości zagadnienie bezpieczeństwa ekonomicznego omawiali wybitni amerykańscy naukowcy, D. Kenan i H. Morgenthau. Główne zadania związane z osiągnięciem bezpieczeństwa ekonomicznego widzieli oni w zwiększaniu konkurencyjności produkcji krajowej oraz handlu, zapewnianiu korzyści gospodarczych na rynkach światowych oraz ochronie interesów państwa w dziedzinach technologicznych.

Dla japońskich badaczy z kolei typowe jest podejście humanistyczne. Widzą oni w bezpieczeństwie ekonomicznym państwa takie zachowanie, dzięki któremu kraj nie miałby wrogów (S. Okita). W ramach dążenia do tego stanu należy stworzyć korzystne warunki dla importu, wzmocnienia narodowej waluty, rozwoju strategicznej polityki inwestycyjnej.

Ciekawe definicje bezpieczeństwa ekonomicznego znajdujemy w badaniach naszych wschodnich sąsiadów. W przeciwieństwie do Anglosasów nauka rosyjska i ukraińska dość późno zajęła się tymi zagadnieniami, choć dziś posiada w tym zakresie pokaźny dorobek. Kwestie bezpieczeństwa ekonomicznego po raz pierwszy pojawiły się w tamtym kręgu w połowie lat 90. XX w.

Szeroki zakres podmiotowy i przedmiotowy badanego problemu nie pozwala na utworzenie jednej całościowej definicji. Trudności te bezpieczeństwo ekonomiczne

odziedziczyło po pojęciu bezpieczeństwa państw. Definicje bezpieczeństwa ekonomicznego można podzielić na następujące grupy:

- opierające się na zagrożeniu (E.M. Green, A. Lubbe, S. Michałowski, E. Frejtag-Mika) – tradycyjnie odwołują się do zapewnienia bezpieczeństwa w sferze ekonomicznej w celu zapewnienia bezpieczeństwa w sferze militarnej i koncentrują się na nim;
- łączące zagrożenia i możliwości (J. Sperling, E. Kirchner, P. de Souza);
- odwołujące się do zdolności państwa do funkcjonowania (Ch. Dent, K. Księżopolski; bogactwo – R. Thakur);
- definicje jednostronne (C.R. Neu i Ch. Wolf).

Na podstawie tego podziału można wyróżnić definicje pozytywne i negatywne bezpieczeństwa ekonomicznego. Do pierwszej grupy należy zaliczyć te, w których nacisk kładzie się poza sferą potrzeb egzystencjalnych i zwraca uwagę na rolę rozwoju. Definiowanie negatywne skupia się na potrzebie odparcia zagrożeń, co zapewnia prostą formę przeżycia. Takie podejście opiera się na konkretyzacji zagrożeń i możliwości ich odparcia. Niejako z tego podziału wynika inny, wyróżniający bezpieczeństwo rozpatrywane na płaszczyźnie ogólnoekonomicznej oraz na płaszczyźnie ekonomiczno-obronnej.

Bezpieczeństwo ekonomiczne tradycyjnie ma najwyższy priorytet w polityce państwa. Pojęcie bezpieczeństwa ekonomicznego nabywa wyjątkowego znaczenia jako argument za kształtowaniem właściwej polityki i podejmowaniem odpowiednich decyzji. System bezpieczeństwa ekonomicznego przewiduje zapewnienie ciągłego monitorowania procesów społeczno-gospodarczych w zakresie ich wpływu na stan bezpieczeństwa ekonomicznego, przepisów prawnych i analizy skuteczności obecnych rozwiązań w dziedzinie polityki gospodarczej.

Bezpieczeństwo ekonomiczne każdego kraju to zatem ogólnonarodowy cykl działań zmierzających do → z r ó w n o w a ż o n e g o r o z w o j u [t. 4] dla dobrobytu obywateli i poprawy stanu gospodarki, które muszą obejmować również mechanizm tworzenia przeciwwagi dla zagrożeń zewnętrznych i wewnętrznych lub ryzyka, które państwo ponosi jako podmiot stosunków finansowych. Jest to także stan gospodarki krajowej, która zapewnia ochronę → i n t e r e s ó w n a r o d o w y c h [t. 2], odporność na zagrożenia wewnętrzne i zewnętrzne, zdolność do rozwoju i ochrony żywotnych interesów osób, społeczeństwa i państwa. Interesy te oznaczają w tym kontekście zestaw potrzeb, których realizacja umożliwia istnienie i stopniowy rozwój jednostki, społeczeństwa i państwa. Bezpieczeństwo ekonomiczne jest częścią bezpieczeństwa narodowego, która obejmuje również obronę, bezpieczeństwo ekologiczne itp.

Bezpieczeństwo ekonomiczne to także zdolność gospodarki do zagwarantowania, że potrzeby społeczne na poziomie krajowym i międzynarodowym zostaną odpowiednio zaspokojone. Innymi słowy, łączy ono wewnętrzne i zewnętrzne warunki ułatwiające skuteczny i dynamiczny rozwój gospodarki narodowej i jej zdolność

do zaspokojenia potrzeb społeczeństwa, państwa oraz jednostki w celu zapewnienia konkurencyjności na rynkach krajowych i zagranicznych. Można wyciągnąć z tego 2 wnioski. Po pierwsze bezpieczeństwo ekonomiczne kraju musi być zapewnione efektywnością gospodarki – dzięki środkom ochronnym podejmowanym przez państwo musi cechować się ona wysoką wydajnością pracy, jakością produktów itp. Po drugie zapewnienie bezpieczeństwa ekonomicznego kraju nie jest przywilejem jednej instytucji państwowej, musi być wspierane przez cały system organów państwowych oraz całą strukturę gospodarki.

Rozumienie bezpieczeństwa ekonomicznego może znacznie różnić się w zależności od możliwości i funkcji gospodarki narodowej – jej potencjału, stabilności, stopnia otwartości. Na tworzenie krajowych koncepcji bezpieczeństwa ma wpływ całość warunków współfunkcjonowania gospodarki krajowej z gospodarką światową, poglądy grup rządzących, państwowa ideologia, obecność potencjału wojskowego. Mogą one wpływać na podejmowanie politycznych i gospodarczych decyzji przez podmioty światowej polityki i gospodarki.

Głównymi celami bezpieczeństwa ekonomicznego są m.in.:

- zapewnienie proporcjonalnego i stałego wzrostu gospodarczego,
- ograniczenie inflacji i bezrobocia,
- tworzenie skutecznej struktury gospodarki i rozwiniętego rynku papierów wartościowych,
- ograniczenie deficytu budżetowego i długu publicznego,
- zabezpieczenie społecznej ochrony i poprawy jakości życia,
- utrzymanie stabilności waluty.

Zadania te określają → s t r a t e g i ę [t. 4] bezpieczeństwa gospodarczego jako formowania i uzasadnienia strategicznych priorytetów i interesów narodowych, środków i mechanizmów likwidacji pojawiających się problemów.

W analizie makroekonomicznej bezpieczeństwa ekonomicznego można wyróżnić następujące elementy:

- niezależność ekonomiczną,
- odporność i stabilność gospodarki narodowej,
- zdolność do samodzielnego rozwoju i postępu. Bezpieczeństwo ekonomiczne państwa charakteryzuje się:
- poziomem rozwoju całej gospodarki,
- obecnością i poziomem zagrożenia państwa, społeczeństwa i jednostki,
- skutecznością polityki gospodarczej i państwowej regulacji gospodarki,
- kompletnością realizacji funkcji państwa.

Podstawowymi elementami strukturalnymi bezpieczeństwa ekonomicznego, które trzeba stosować w analizie bezpieczeństwa ekonomicznego, są:

- bezpieczeństwo surowcowo-energetyczne,
- → b e z p i e c z e ń s t w o e n e r g e t y c z n e ,

- → bezpieczeństwo finansowe,
- → bezpieczeństwo społeczne,
- bezpieczeństwo innowacyjne i technologiczne,
- bezpieczeństwo żywnościowe,
- bezpieczeństwo zewnętrzno-gospodarcze. Części składowe bezpieczeństwa ekonomicznego:
- zewnętrzno-ekonomiczna,
- makroekonomiczna,
- naukowo-technologiczna,
- inwestycyjna,
- finansowa,
- produkcyjna,
- energetyczna,
- społeczna,
- demograficzna,
- spożywcza.

Rozwój bezpieczeństwa ekonomicznego podąża tą samą drogą co bezpieczeństwo ogólne: wraz ze zmieniającym się światem przekształca się jego zakres przedmiotowy i podmiotowy. Przedmiotami bezpieczeństwa ekonomicznego są państwo, które wykonuje swoje zadania w tym obszarze poprzez instytucje ustawodawcze, wykonawcze i sądownicze, a także społeczeństwo, ludzie, firmy, instytucje i organizacje, terytoria, poszczególne komponenty bezpieczeństwa ekonomicznego. Zakres przedmiotowy opiera się głównie na środkach i mechanizmach, jakie państwo wykorzystuje w celu realizacji swej racji stanu. W tym aspekcie można powiedzieć, że bezpieczeństwo wyraża się poprzez bilans potrzeb i możliwości ich zaspokojenia. Taki tok rozumowania każe zwrócić uwagę na takie aspekty bezpieczeństwa ekonomicznego jak kategorie żywnościowe, kredytowo-płatnicze, technologiczne, socjalne, ekologiczne, związane z szerszą aktywnością państwa. Bezpieczeństwo ekonomiczne w swoim zakresie podmiotowym dotyczy głównie rozwoju krajowego systemu gospodarczego, wykorzystania zasobów naturalnych – w tym przede wszystkim surowcowych – zgodnie z ich potencjałem, przeciwstawiania się ingerencji podmiotów zewnętrznych przy jednoczesnym rozwijaniu wielostronnych relacji integracyjnych w zakresie gospodarczym. Opiera się tym samym na zagwarantowaniu pewności istnienia i wyeliminowaniu elementów zagrażających żywotnym interesom państwa.

W systemie bezpieczeństwa ekonomicznego decydującą rolę odgrywają narodowe interesy gospodarcze oraz ich priorytety. Aby określić interesy gospodarcze państwa, konieczne są:

- analiza aktualnej sytuacji gospodarczej i określenie trendów rozwoju;
- modelowanie i prognozowanie rozwoju społeczno-gospodarczego;

- regulacja rządowych działań w celu osiągnięcia pożądanych celów. Do najbardziej priorytetowych interesów gospodarczych należą:
- stworzenie samowystarczalnej gospodarki zorientowanej społecznie;
- konserwacja i rozwój potencjału naukowo-technicznego;
- zapewnienie bezpiecznych warunków rozwoju społeczeństwa;
- budowa równych i wzajemnie korzystnych stosunków gospodarczych z innymi krajami.

Ocenić bezpieczeństwo ekonomiczne można przez parametry, kryteria i wskaźniki określające kluczowe znaczenie funkcjonowania systemu gospodarczego. Główne z nich to poziom i jakość życia, tempo inflacji, poziom bezrobocia, wskaźniki makroekonomiczne, deficyt budżetowy i stan środowiska naturalnego. Sytuację bezpieczeństwa ekonomicznego można określić jako ideał, do którego musimy dążyć. Głównym kryterium bezpieczeństwa ekonomicznego jest zdolność gospodarki narodowej do utrzymania lub szybkiego przywrócenia krytycznego poziomu reprodukcji społecznej w sytuacji zawieszenia dostaw zewnętrznych albo kryzysów wewnętrznych. Innymi kryteriami są: struktura PKB, poziom i tempo rozwoju przemysłowego, zakres i dynamika inwestycji; surowcowo-energetyczny i naukowo-technologiczny potencjał kraju; efektywność wykorzystania zasobów; konkurencyjność gospodarcza na rynkach krajowych i zagranicznych; tempo inflacji; stopa bezrobocia; jakość życia, poziom zróżnicowania dochodów, dostępność dóbr materialnych oraz usług publicznych; deficyt budżetowy i dług publiczny; zależność energetyczna; integracja z gospodarką światową.

Przede wszystkim jednak trzeba klasyfikować zagrożenia biorące się z działań państwa, jak również wynikające z funkcjonowania gospodarki. Przez → z a g r o ż e n i a b e z p i e c z e ń s t w a [t. 4] ekonomicznego rozumiemy zbiór warunków i czynników, które uniemożliwiają lub znacznie utrudniają realizację narodowych interesów gospodarczych, zagrażają żywotnym interesom indywidualnym, społeczeństwa i państwa, tworząc zagrożenie dla utrzymania i zabezpieczenia państwa, jego systemów społeczno-gospodarczego i politycznego. Identyfikacja zagrożeń i ich usuwanie powinny być priorytetami polityki gospodarczej.

Zagrożenia dla bezpieczeństwa ekonomicznego państwa dzieli się na wewnętrzne i zewnętrzne. Pierwsze z nich opiera się na zapewnieniu stabilności systemu gospodarczego, struktury podmiotowej i przedmiotowej gospodarki, PKB, inflacji, mechanizmów gospodarowania. Drugie natomiast – ujmowane w ramach definicji negatywnej – polegać będzie na odpieraniu zagrożeń zewnętrznych, w tym ingerencji państw trzecich, w ujęciu pozytywnym będzie zaś oznaczało wykorzystanie możliwych współzależności w celu jak najpełniejszego rozwoju gospodarczego.

Głównymi zagrożeniami wewnętrznymi są:

- w dziedzinie nauki i technologii:
  - zniszczenie potencjału naukowo-technologicznego,

  - zmniejszenie potencjału kluczowych dziedzin nauki, niepewność państwowej naukowo-technologicznej polityki,
  - emigracja naukowców lub ich przechodzenie do innych sfer działalności;
- w sferze gospodarczej:
  - spadek produkcji w głównych sektorach,
  - zerwanie stosunków gospodarczych,
  - monopolizacja gospodarki,
  - kryminalizacja społeczeństwa,
  - istnienie strukturalnych nierówności,
  - duży dług krajowy,
  - wysoki poziom amortyzacji środków trwałych,
  - kryzys energetyczny,
  - niska wydajność pracy i działalności inwestycyjnej,
  - wysoka inflacja i bezrobocie,
  - wzrost szarej strefy,
  - niski popyt wewnętrzny społeczeństwa,
  - dysproporcje cenowe pomiędzy przemysłem i rolnictwem,
  - groźba utraty żywnościowej niezależności państwa,
  - masowe oszustwa podatkowe;
- w sferze społecznej:
  - pogłębienie zróżnicowania dochodów,
  - ubóstwo,
  - pogorszenie struktury spożywczej,
  - ograniczony dostęp do edukacji i opieki zdrowotnej,
  - pogorszenie jakości życia,
  - brak bezpieczeństwa socjalnego,
  - znaczny spadek liczby ludności,
  - wzrost śmiertelności,
  - niekontrolowane migracje.

Do zewnętrznych zagrożeń zaliczamy:

- ekonomiczne uzależnienie od importu,
- ujemne saldo handlu zagranicznego,
- irracjonalną strukturę eksportu, np. nadmierny eksport surowców,
- utratę pozycji na rynkach zagranicznych,
- wzrost zadłużenia zewnętrznego, nieefektywne wykorzystanie kredytów zagranicznych,
- niekontrolowane przerzucanie środków dewizowych za granicę, umieszczanie ich w bankach zagranicznych,
- migrację siły roboczej za granicę.

Na podstawie priorytetowych interesów narodowych i zagrożeń dla bezpieczeństwa ekonomicznego państwa określa się środki polityki państwowej dla bezpieczeństwa ekonomicznego w obszarach: naukowo-technicznym, gospodarczym, społecznym, wojskowym, ochrony środowiska, informacyjnym, politycznym.

Można wskazać 4 powiązane ze sobą i współzależne od siebie wymiary bezpieczeństwa ekonomicznego:

- finansowy,
- surowcowo-energetyczny,
- żywnościowy,
- dostępu do czystej wody.

W celu zapewnienia bezpieczeństwa ekonomicznego kraju w warunkach światowego kryzysu gospodarczego konieczne jest podjęcie pilnych działań dla wzmocnienia systemu ekonomicznego kraju, spośród których należy wyróżnić zwłaszcza:

- ogromne inwestycje w modernizację gospodarki, wielokrotnie przewyższające jej potencjał akumulacji;
- wprowadzenie kredytów dla realnego sektora gospodarczego i projektów infrastrukturalnych;
- bezpośrednie kredyty Narodowego Banku Polskiego dla strategicznych przedsiębiorstw: hutniczych, naftowych i przemysłu węglowego;
- inteligentną restrukturyzację gospodarki;
- inteligentne planowanie deficytu budżetowego;
- realistyczne planowanie emerytur, zasiłków i stypendiów;
- stworzenie skutecznych mechanizmów realizacji tego programu oraz kontroli i odpowiedzialności.

Aleksander Wasiuta

Bezpieczeństwo ekonomiczne państw, T. Guz, P. Marzec, K.A. Kłosiński (red.), Polihymnia, Lublin–Tomaszów Mazowiecki 2006; *Bezpieczeństwo ekonomiczne państwa. Uwarunkowania, procesy, skutki*, A. Jackiewicz, A. Trzaskowska-Dmoch (red.), CeDeWu, Warszawa 2017; *Bezpieczeństwo ekonomiczne w perspektywie politologicznej – wybrane problemy*, K.M. Księżopolski, K. Pronińska (red.), Dom Wydawniczy Elipsa, Warszawa 2012; M. Bojańczyk, *Bezpieczeństwo ekonomiczne w niestabilnej gospodarce światowej*, Wydawnictwo Akademii Finansów i Biznesu Vistula, Warszawa 2014; J. Kostecki, *Wpływ czynników zewnętrznych i wewnętrznych na bezpieczeństwo ekonomiczne Polski*, „Kwartalnik Naukowy Uczelni Vistula" 2016, nr 3; K.M. Księżopolski, *Ekonomiczne zagrożenia bezpieczeństwa państw. Metody i środki przeciwdziałania*, Dom Wydawniczy Elipsa, Warszawa 2004; H.E.S. Nesadurai, *Conceptualising Economic Security in an Era of Globalisation: What Does the East Asian Experience Reveal?*, „CSGR Working Paper" 2005, no. 157/05; G. Rejda, *Social Insurance and Economic Security*, Routledge, New York–London 2015; *The Economic Security of Business Transactions: Management in Business*, K. Raczkowski, F. Schneider (eds.), Chartridge Books Oxford, Oxford 2013; A. Wasiuta *Bezpieczeństwo ekonomiczne*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; tenże, *Ekonomiczne instrumenty polityki ekologicznej w kontekście zarządzania środowiskowego*, [w:] *Współdziałanie systemu zarządzania i inżynierii produkcji. Teoria i praktyka*, T. Noch,

J. Saczuk (red.),Wydawnictwo Gdańskiej Szkoły Wyższej, Gdańsk 2015; tenże, *Ekonomiczne uwarunkowania rozwoju energetyki wiatrowej*, Wydział Dziennikarstwa i Nauk Politycznych, Uniwersytet Warszawski, Warszawa 2014; tenże, *Labor Market in Poland in the Context of Renewable Energy Sector Development*, „Ekonomia i Środowisko" 2018, nr 1 (64); *Współczesne bezpieczeństwo ekonomiczne. Wymiar międzynarodowy*, M. Gębska, M. Kubiak (red.), Akademia Sztuki Wojennej, Warszawa 2016.

BEZPIECZEŃSTWO ENERGETYCZNE (ang. *energy security*) – pojęcie stosowane m.in. w ekonomii, → n a u k a c h o b e z p i e c z e ń s t w i e [t. 3], politologii i energetyce. Mimo że dyskusje nad → b e z p i e c z e ń s t w e m energetycznym prowadzone są od wielu lat, a związana z nim problematyka jest postrzegana jako jedna z kluczowych dla bezpieczeństwa gospodarczego regionów i często podejmowana przez polityków, to nie ma jego jednoznacznej, globalnej definicji. Najczęściej jest traktowane jako ochrona obywateli, społeczeństwa, państwa i gospodarki przed → z a g r o ż e n i a m i [t. 4] niedoboru.

Walka o zasoby na świecie jest ostra; zabezpieczenie krajowego bezpieczeństwa energetycznego stało się dla każdego państwa kwestią twardej, realnej polityki (niem. *Realpolitik*). Bezpieczeństwo energetyczne państwa/sojuszu państw to kategoria obejmująca całość problematyki związanej z kwestiami zapewniania ich funkcjonowania oraz swobody realizacji własnych → i n t e r e s ó w n a r o d o w y c h [t. 2] w niepewnym lub jawnie nieprzyjaznym (niebezpiecznym, ryzykownym) środowisku energetycznym, głównie poprzez wykorzystywanie szans, podejmowanie wyzwań, redukowanie ryzyka i przeciwdziałanie zagrożeniom energetycznym.

Międzynarodowa Agencja Energetyczna (International Energy Agency) określa bezpieczeństwo energetyczne jako „dostępność źródeł energii po przystępnej cenie". Amerykańskie Centrum Studiów Strategicznych i Międzynarodowych (Center for Strategic and International Studies) ujmuje bezpieczeństwo energetyczne jako ciągłą zdolność państwa do utrzymywania swego funkcjonowania bez poważnych zaburzeń.

W szerszym ujęciu bezpieczeństwo energetyczne można określić także jako zaspokojenie zapotrzebowania odbiorców na paliwa i energię w sposób zapewniający jednocześnie:

- bezpieczeństwo technologiczne (praca urządzeń i instalacji);
- opłacalność inwestycji z punktu widzenia rynku i kapitału;
- ciągłość/niezawodność dostaw o odpowiednich standardach;
- akceptowalny poziom cen dla odbiorców indywidualnych, który nie stanowi nadmiernego obciążenia budżetów gospodarstw domowych, w odniesieniu zaś do odbiorców przemysłowych taki, który nie powoduje nieopłacalności produkcji.

Centrum Badań Energetycznych Azji i Pacyfiku w Tokio (Asia Pacific Energy Research Centre) uznaje bezpieczeństwo energetyczne za:

> zdolność gospodarki do zagwarantowania dostępności dostaw zasobów energetycznych w sposób zrównoważony i terminowy z ceną energii na poziomie, który nie będzie miał niekorzystnego wpływu na wyniki ekonomiczne gospodarki.

Z kolei badacze brytyjscy wskazują 4 aspekty, które muszą być brane pod uwagę odnośnie do bezpieczeństwa energetycznego. Chodzi m.in. o dostępność nośników energetycznych mierzoną stosunkiem posiadanych zasobów do wydobycia/produkcji danego surowca/paliwa. Według nich ważna jest także dosięgalność związana z → g e o p o l i t y k ą i skalą inwestycji w stosowną infrastrukturę. Szczególne znaczenie ma również dopuszczalność łącząca się ze skutkami wykorzystywania surowców energetycznych dla środowiska. Nie można pominąć też przystępności cenowej związanej z kosztami inwestycyjnymi.

Z punktu widzenia odbiorcy finalnego bezpieczeństwo energetyczne to przede wszystkim dostępność rozumiana w 2 aspektach: poziomu cen za energię oraz gwarancji niezawodności dostaw energii.

Bezpieczeństwo energetyczne jest związane także z zapewnieniem: dostaw surowców, zdolności wytwórczych elektrowni, elektrociepłowni i ciepłowni funkcjonujących w państwie oraz zdolności przesyłowych systemu – dostarczenia energii do odbiorców.

Według innego podejścia to stan gospodarki umożliwiający pokrycie zapotrzebowania na paliwa i energię obecnie oraz w perspektywie wieloletniej, w sposób technicznie uzasadniony, z dbałością o środowisko, trafny z ekonomicznego punktu widzenia.

Zwolenników ma też nieco inna definicja: to stan gospodarki umożliwiający pokrycie zapotrzebowania na paliwa i energię – stale, po korzystnej cenie, przy braku zależności od poszczególnych paliw, dostawców oraz tras przesyłu surowca/energii.

Według A. Podrazy definicja bezpieczeństwa energetycznego obejmuje: „energię, wzrost gospodarczy i władzę polityczną". Jak twierdzi badacz, to uzyskanie „niezależności energetycznej poprzez podejmowanie działań przez poszczególne państwa". Działania te będą się różnić w zależności od obowiązującego w danym kraju systemu energetycznego.

W literaturze można też spotkać ujęcia globalne. Bezpieczeństwo energetyczne w takiej skali jest rozumiane jako długoterminowe, niezawodne i konkurencyjne połączenie różnych rodzajów energii dla → z r ó w n o w a ż o n e g o r o z w o j u [t. 4] społeczno-gospodarczego świata przy minimalnym oddziaływaniu na środowisko przyrodnicze. Jak pisze Podraza, uwzględnia ono i wskazuje konieczność dążenia do minimalizacji „niestabilności w globalnych dostawach energii", do ochrony środowiska oraz brania pod uwagę zmian klimatycznych.

Ogólna definicja bezpieczeństwa energetycznego w Polsce zawarta została w 3 różnych dokumentach, mianowicie: w *Doktrynie zarządzania bezpieczeństwem energetycznym*, w Ustawie z dnia 10 kwietnia 1997 r. – Prawo energetyczne oraz w *Polityce*

energetycznej Polski do roku 2030 (w 2015 r. było planowane przyjęcie nowej polityki energetycznej do 2050 r., obecnie trwają konsultacje projektu tej polityki do 2040 r.). W *Doktrynie zarządzania bezpieczeństwem energetycznym* sformułowano następującą definicję:

> Bezpieczeństwo energetyczne to zdolność do zaspokojenia w warunkach rynkowych popytu na energię pod względem ilościowym i jakościowym, po cenie wynikającej z równowagi popytu i podaży, przy zachowaniu warunków ochrony środowiska.

Z kolei art. 3 pkt 16 ustawy określa je jako:

> stan gospodarki umożliwiający pokrycie bieżącego i perspektywicznego zapotrzebowania odbiorców na paliwa i energię w sposób technicznie i ekonomicznie uzasadniony, przy zachowaniu wymagań ochrony środowiska.

Zróżnicowanie definicji bezpieczeństwa energetycznego wynika z trudności ujęcia wielopłaszczyznowości zagadnienia w jednej zwartej regule. W dzisiejszym świecie bezpieczeństwo energetyczne jest jednym z najważniejszych elementów bezpieczeństwa narodowego, bardzo istotnym elementem bezpieczeństwa wewnętrznego i zewnętrznego państwa, jest ściśle związane ze → s t r a t e g i ą [t. 4] państwa, pozwalającą na zapewnienie krajowi zrównoważonego rozwoju i dobrobytu.

Poszczególni uczestnicy globalnego rynku energii jednak w rozmaity sposób postrzegają kwestię bezpieczeństwa energetycznego. Wynika to m.in. z charakteru tych podmiotów oraz ich miejsca w łańcuchu energetycznym. Zdaniem J. Gryza podejście do omawianego bezpieczeństwa jest odmienne w 5 typach państw: w liberalnych demokracjach; konkurencyjnych kapitalistycznych państwach autorytarnych; biurokratycznym kapitalizmie państwowym, socjaldemokratycznym kapitalizmie oraz w państwach niekapitalistycznych.

Jak podkreśla S. Wasiuta, istnieją bardziej kompletne podziały uczestników globalnego rynku energii. Przykładowo dla rządów w rozwiniętych ekonomicznie państwach importujących najważniejsze są: ryzyko zakłóceń dostaw, zagrożenia odpowiedniej części → i n f r a s t r u k t u r y k r y t y c z n e j [t. 2], poziom modernizacji infrastruktury, rezerwy strategiczne, nadmiar mocy w systemie energetycznym. Dla Chin i Indii bezpieczeństwo energetyczne to możliwość szybkiego dostosowania się do nowej zależności od rynków światowych. Dla Japonii jest to zniwelowanie ostrego niedoboru zasobów krajowych poprzez dywersyfikację, handel i inwestycje. W UE najważniejsza dyskusja koncentruje się na tym, jak najlepiej kontrolować uzależnienie od importu gazu ziemnego. W części krajów europejskich dyskutuje się także nad perspektywami budowy nowych elektrowni atomowych oraz wielkością wydobycia i wykorzystania węgla.

W odniesieniu do strategii państw importerów na globalnym rynku energii mówi się o potrzebie zwiększenia konkurencyjności gospodarki, obniżenia jej energochłonności;

zwiększania eksportu do krajów, z których importuje się surowce; zagwarantowania stałego dopływu surowców. Przy strategii wolnorynkowej ceny co prawda reguluje rynek, ale importerzy muszą się liczyć z reakcją państw.

Dla państw eksporterów resursów energetycznych kluczowy jest poziom zapotrzebowania odbiorców oraz bezpieczeństwo dochodów. Kraje te koncentrują się na zachowaniu dogodnych rynków zbytu obecnie i w perspektywie wieloletniej (zapotrzebowanie, poziom cen). Na przykład Rosja dąży do przywrócenia pełnej kontroli państwa nad znajdującymi się w obrębie jej terytorium zasobami strategicznymi, a także nad głównymi rurociągami i kanałami dystrybucji.

Kraje rozwijające się będące importerami surowców energetycznych są zaniepokojone tym, jak zmiany cen energii wpływają na ich bilans płatniczy. Za podstawowe wyzwania w tym zakresie uznają zdolność do regulowania należności oraz zagrożenie szokami cenowymi. To ostatnie nie dziwi. J. Adamkiewicz zwraca uwagę, że jeśli w państwach o dobrej kondycji gospodarki wzrost cen ropy naftowej o 10 USD za baryłkę powoduje spadek ich PKB o 1,5%, to w krajach trzeciego świata osłabienie to może być nawet 3 razy wyższe.

Z kolei dla firm opartych na dostawach energii i indywidualnych konsumentów kluczowa jest cena i brak zakłóceń dostaw. Inne będzie postrzeganie zagadnienia przez firmy wydobywające surowce energetyczne. Dla nich najważniejsza będzie stabilność systemów inwestycyjnych, rozbudowa infrastruktury oraz dostęp do nowych zasobów. Z kolei dla innej grupy przedsiębiorstw energetycznych kluczowa jest integralność sieci przesyłowych.

Wieloaspektowość bezpieczeństwa energetycznego przejawia się tym, że można je również rozpatrywać pod względem szeregu kryteriów o przeciwstawnym charakterze, np. ekonomicznym, środowiskowym czy społecznym. Wszystko to sprawia, iż analiza bezpieczeństwa energetycznego obarczona jest problemem subiektywności doboru definicji. Jest ona uzależniona każdorazowo od ważności poszczególnych komponentów określających fragmentarycznie badane zagadnienie.

Ponadto definicje mogą odnosić się do różnych aspektów bezpieczeństwa energetycznego. Inaczej jest ono definiowane podczas analizy kwestii krótkoterminowych takich jak np. ryzyko wstrzymania dostaw nośników energii przez głównych producentów.

Główną przyczyną pogorszenia się sytuacji w zakresie zapewnienia globalnego bezpieczeństwa energetycznego w ostatnich 2 dekadach jest:

- znaczący wzrost popytu w zakresie energii podstawowej szczególnie w krajach poza Organizacją Współpracy Gospodarczej i Rozwoju (OECD);
- wyczerpywanie się stosunkowo tanich naturalnych zasobów energetycznych w większości regionów świata, które generuje potrzebę opracowania droższych rozwiązań, co z kolei może powodować konieczność znacznych inwestycji w sektorze energetycznym.

W przypadku tego drugiego należy jednak pamiętać, że rezerwy źródeł energii są znaczne. Dzięki intensywnym poszukiwaniom w ciągu ostatnich 20 lat w skali globalnej wielkość potwierdzonych rezerw ropy naftowej wzrosła o 1/3. W tym czasie potwierdzone rezerwy gazu ziemnego wzrosły o niemal 1/3, z tego w Chinach 4-krotnie. Niektórzy badacze – np. Gryz – uznają, że wyczerpanie się źródeł energii w skali globalnej w perspektywie długoterminowej jest jednak mało prawdopodobne. Nastąpił też radykalny wzrost – niemal na całym świecie – wykorzystania energii odnawialnej (od UE po Chiny).

Po 11 września 2001 r. → t e r r o r y z m [t. 4] zaczął być postrzegany jako znaczące zagrożenie również dla omawianego bezpieczeństwa. Dotyczy to nie tylko → c y b e r a t a k ó w na sieci energetyczne państwa. W obecnej dekadzie przykładem mogą być ataki na infrastrukturę gazową w Algierii (wzięto znaczną liczbę zakładników, zob. → w z i ę c i e z a k ł a d n i k a [t. 4]) czy w Rosji (Tatarstan). Z nieco starszych można wymienić atak na elektrownię atomową w RPA w 2007 r. (zamachowcy dotarli aż do sterowni). Wymusza to większą ochronę strategicznych obiektów związanych z bezpieczeństwem energetycznym i powoduje wzrost zainteresowania zaawansowanymi elektronicznymi systemami ochrony.

Jeszcze do niedawna bezpieczeństwo energetyczne analizowane było w wielu krajach niemalże wyłącznie w odniesieniu do surowców importowanych (ropy naftowej i gazu ziemnego) oraz energii atomowej. Sytuacja w skali globalnej ulega jednak zmianie. Przykładowo kierunki polityki energetycznej UE oraz wydarzenia z przełomu 2007 i 2008 r. (problemy z dostawą energii elektrycznej, strajki górnicze) skłoniły państwa Unii do poszerzenia dyskusji o bezpieczeństwie energetycznym o kwestie związane z ewentualnym dalszym wykorzystaniem paliw stałych (węgla kamiennego i brunatnego) oraz stanem infrastruktury energetycznej.

W obecnej dekadzie znaczenie bezpieczeństwa energetycznego wzrosło także w związku z kilkoma poważnymi wypadkami, które miały miejsce na różnych kontynentach. Łącznie w ciągu ostatnich 40 lat w energetycznych systemach świata wystąpiło ponad 40 poważnych systemowych awarii, przy czym połowa z nich w USA. Najważniejszym powodem tych wypadków są dążenia do pełnego osiągnięcia wyznaczonych celów biznesowych bez uwzględnienia możliwości technologicznych sieci elektrycznych, co prowadzi do ich przeciążenia i awarii. Rozpowszechnienie takich wypadków obserwowano również ze względu na problemy w dziedzinie → b e z p i e c z e ń s t w a i n f o r m a c y j n e g o , w tym nieprawidłowości w telekomunikacji i sieciach komputerowych.

Zagrożenia dla stabilnych dostaw wynikają z negatywnych skutków naturalnych, technologicznych, menedżerskich, społecznych, gospodarczych, wewnętrznych i zewnętrznych. Różne czynniki mają ważne, a nawet decydujące znaczenie dla bezpieczeństwa energetycznego w zależności od przynależności do danej grupy państw, a niekiedy nawet regionu. Zwykle najważniejsza jest niewystarczająca dostępność energii lub niekonkurencyjne albo zbyt niestabilne ceny.

Do najważniejszych uwarunkowań bezpieczeństwa energetycznego zalicza się także m.in.:

- poziom wydobycia zasobów energetycznych;
- przetwarzanie zasobów energetycznych i pozyskiwanie z nich energii;
- dystrybucję energii i związaną z tym infrastrukturę;
- rynek producentów energii (przepisy prawne, stopień innowacyjności, wizję przyszłości);
- zapotrzebowanie konsumentów. Ważne są również:
- formy wykorzystania energii;
- ocena przyszłych potrzeb przesyłowych, przyszłego zużycia energii;
- techniczne i technologiczne innowacje związane z bezpieczeństwem energetycznym;
- poziom zagrożenia awariami technicznymi.

Na bezpieczeństwo energetyczne wpływa brak możliwości rzeczywistej dywersyfikacji źródeł surowców energetycznych. Przyczyną tego ostatniego mogą być m.in. warunki geograficzne, poziom cen, stan infrastruktury przesyłowej oraz niemożność istotnego zwiększenia wydobycia danego surowca na terenie kraju. Często ten ostatni problem występuje na terenie kraju w postaci dylematu: albo bezpieczeństwo energetyczne, albo „rozsądne" koszty. Zły stan techniczny infrastruktury przesyłowej może znacznie zmniejszyć przepustowość oraz generować ogromne straty surowca w trakcie jego przesyłania. Wyzwanie stanowi także infrastruktura niepozwalająca na przechowywanie odpowiednich zapasów danego surowca. Przyczyną mogą być tu np. zbyt małe magazyny, nieodpowiedni układ sieci przesyłowej oraz uwarunkowania geograficzne i geologiczne. Problemem są też ograniczenia możliwości wykorzystania innych źródeł energii niż dominujące dotąd na danym obszarze. Przyczyną bywają również zbyt wysokie koszty wykorzystania w gospodarce na szeroką skalę źródeł odnawialnych, a także przyzwyczajenia odbiorców czy rozmieszczenie infrastruktury. Niekiedy problem stanowi też niska wydajność przeważających na terenie danego kraju systemów energetycznych; dominacja nieefektywnych metod wydobywania i przetwarzania surowców oraz skala niedoinwestowania sektora energetycznego.

Istotny jest także poziom wrażliwości systemów energetycznych na zakłócenia. Ich źródła są różne. Przyczynami mogą być nie tylko wrogie działania innych państw, ale również zjawiska naturalne takie jak ostre zimy, powodzie albo trzęsienia ziemi. Źródłem zakłóceń bywają ponadto katastrofy i awarie przemysłowe występujące przy wydobyciu, transporcie i wykorzystaniu surowców energetycznych. Na przykład zbyt duże stężenie wysokometanowego gazu ziemnego w powietrzu grozi wybuchem. Odrębną kategorię stanowią wspomniane wyżej zamachy terrorystyczne. Źródłem zakłóceń mogą być także konflikty zbrojne, można tu wspomnieć np. niedawny atak na ropociąg w czasie → w o j n y [t. 4] w Syrii.

Do tego należy doliczyć zjawiska ogólnogospodarcze (niszczenie procesu inwestycyjnego itp.), społeczno-polityczne (strajki, konflikty etniczne itp.). Te ostatnie czynniki zdecydowały np. o radykalnej zmianie sytuacji Libii w zakresie bezpieczeństwa energetycznego. Zagrożenia te mogą mieć oczywiście także przyczyny zewnętrzne. Zalicza się do nich nie tylko sygnalizowane wyżej przyczyny geopolityczne, ale także makroekonomiczne i koniunkturalne.

Takie uwarunkowania i zagrożenia są związane z ryzykiem utraty stabilności gospodarczej albo politycznej, pogorszeniem sytuacji społeczno-gospodarczej państw, spowolnieniem lub powstrzymaniem wzrostu gospodarczego i rozwoju społecznego.

Godny uwagi jest pogląd, że poziom bezpieczeństwa energetycznego zależy od:

- wielkości i zróżnicowania krajowej bazy surowców energetycznych;
- stopnia dywersyfikacji oraz wykorzystania krajowych i zagranicznych źródeł zaopatrzenia w surowce energetyczne;
- stanu technicznego systemu zaopatrzenia oraz form własności jego infrastruktury;
- sytuacji ekonomicznej przedsiębiorstw energetycznych;
- możliwości magazynowania paliw, rozwoju krajowych i międzynarodowych połączeń systemów energetycznych;
- wewnętrznej i międzynarodowej polityki gospodarczej.

Wartość wspomnianej wyżej dywersyfikacji źródeł surowców energetycznych dostrzeżono już ponad 100 lat temu. Przykładowo W. Churchill dostrzegał zalety poszukiwania różnych źródeł energii, podkreślając:

„Stabilność i wiarygodność sektora dostaw ropy naftowej opierają się wyłącznie na zróżnicowaniu i tylko zróżnicowaniu źródeł". Dywersyfikacja powinna być rozpatrywana w kontekście minimum 4 czynników, mianowicie: obniżenia kosztów energii; zróżnicowania wykorzystywanych nośników energii; uniezależnienia się od głównego dostawcy; większej troski o przyrodę. Działania władz państw komplikuje fakt, że wymienione perspektywy odnośnie do poszczególnych surowców energetycznych często są ze sobą sprzeczne. W wielu krajach nie da się więc ich zrealizować równocześnie, a zastąpienie na dużą skalę w gospodarce jednego surowca energetycznego innym wymaga znacznych, czasochłonnych i kapitałochłonnych inwestycji.

→ Zagrożenia bezpieczeństwa [t. 4] energetycznego można analizować z punktu widzenia surowcowo-produktowego, infrastrukturalnego, politycznego oraz kapitału ludzkiego. W ostatnim przypadku chodzi o deficyt fachowców niezbędnych do wykonywania prac w danym państwie w obszarze bezpieczeństwa energetycznego.

W XXI w. obserwuje się kolejne fale dyskusji dotyczącej bezpieczeństwa energetycznego. Warto zauważyć, że ich wzmaganie się pokrywa się ściśle z okresami gwałtownych wzrostów cen nośników energii. Ponadto z czasem toczone dyskusje zyskują coraz szerszy zasięg, często na szczeblu międzynarodowym, a podejmowane decyzje mają na celu podwyższenie poziomu bezpieczeństwa energetycznego rozwiniętych

gospodarek światowych. Sytuacja ta jest wynikiem nakładania się kilku czynników: kluczowego wpływu surowców energetycznych na rozwój gospodarczy; wpływu cen nośników energii na gospodarki państw; świadomością co do siły przetargowej, jaką posiadają kraje zasobne w surowce energetyczne; eskalacją coraz nowszych zagrożeń mających wpływ na bezpieczeństwo energetyczne; wzrostu świadomości co do wyczerpywalności w dłuższej perspektywie dostępnych (także przez względy technologiczne) światowych zasobów ropy naftowej, gazu ziemnego i węgla.

Bez względu jednak na różnice w podejściu do kwestii bezpieczeństwa energetycznego elementem podstawowym i wspólnym jest troska o zabezpieczenie dostaw energii pod różną postacią w ilości pokrywającej zgłaszany w danym regionie popyt. Coraz częściej w definicjach wskazuje się na konieczność zapewnienia dostaw w wysokości gwarantującej trwały rozwój gospodarczy regionu, na konieczność zapewnienia dostaw do finalnych odbiorców, a biorąc pod uwagę historyczne gwałtowne wzrosty cen nośników energii, w tym głównie ropy naftowej (i powiązanego z nią cenowo gazu ziemnego), definicja bezpieczeństwa energetycznego uzupełniana jest o czynnik cenowy oraz o konieczność utrzymania infrastruktury kluczowej dla zaopatrzenia odbiorców w energię, jak również zagwarantowania bezpieczeństwa kluczowych elementów infrastruktury. Stosowane są rozmaite instrumenty mające na celu minimalizację zagrożeń w omawianej sferze. Różnie są one definiowane z punktu widzenia biznesu i z punktu widzenia polityki.

Dla większości krajów uprzemysłowionych bezpieczeństwo energetyczne związane jest przede wszystkim z zapewnieniem długoterminowych, nieprzerwanych dostaw energii z zewnętrznych źródeł na rozsądnych warunkach gospodarczych. Dlatego też w tych krajach szczególną wagę przywiązuje się do zapewnienia bezpieczeństwa dostaw ropy naftowej i gazu ziemnego, jak również do zapobiegania negatywnym, nieprzewidzianym okolicznościom, które mogą mieć wpływ na podaż surowców energetycznych, oraz do zapobiegania lub ograniczania zagrożeń politycznych, gospodarczych, technicznych i innych. Ważne są także wystarczające rezerwy paliw i innych zasobów energii.

Bezpieczeństwo energetyczne może być krótkoterminowe, średnioterminowe i długoterminowe. Krótkoterminowe bezpieczeństwo energetyczne koncentruje się na zdolności systemu energetycznego do niezwłocznego reagowania na nagłe zmiany w ramach równowagi podaży i popytu. Bezpieczeństwo energetyczne długoterminowe zajmuje się przede wszystkim inwestycjami dostarczania energii w zgodzie z rozwojem gospodarczym i zrównoważonymi potrzebami środowiskowymi. Bezpieczeństwo średniookresowe jest planowane i przewidywane na najbliższe kilka lat (zazwyczaj od 5 do 10). W okresie tym weryfikowany jest potencjał krajowych zasobów energetycznych oraz przeprowadzane są inwestycje przesyłowe i magazynowe.

Można też wyróżnić płaszczyzny bezpieczeństwa energetycznego: polityczną, ekonomiczną oraz techniczną. Przydatniejszy jednak wydaje się jego podział na poziomy:

międzynarodowy, bloku ekonomicznego i/lub wojskowego, państwa, części państwa i poszczególnych obywateli (zob. → N A T O [t. 3] w zapewnieniu bezpieczeństwa energetycznego i ochrony infrastruktury energetycznej). Nieprzypadkowo niektórzy badacze wyróżniają jako węższe pojęcie bezpieczeństwa energetycznego państwa.

E. Żywucka-Kozłowska dzieli bezpieczeństwo energetyczne na bezpieczeństwo elektroenergetyczne i paliwowo-surowcowe. Podział ten z różnych względów nie jest na razie stosowany przez innych badaczy, warto jednak odnotować pojawiające się w literaturze pojęcie znaczeniowo węższe od bezpieczeństwa energetycznego, mianowicie bezpieczeństwo surowcowe.

Równocześnie bezpieczeństwo energetyczne w bardzo poważny sposób wpływa na modernizację i rozwój sił zbrojnych, w tym na bezpieczeństwo militarne państwa. Większość wyposażenia wojska potrzebuje bowiem energii, by mogła funkcjonować. Przykładowo w Polsce do infrastruktury krytycznej bezpieczeństwa energetycznego zaliczane są: składy i magazyny paliw; przedsiębiorstwa związane z pozyskaniem i transportem, składowaniem i dystrybucją energii i surowców energetycznych; sieci transportu, przesyłu oraz dystrybucji paliw. W części państw w ramach sił zbrojnych istnieją specjalne struktury dbające m.in. o zapewnienie odpowiedniego poziomu bezpieczeństwa energetycznego kompleksów wojskowych, w tym dostosowania istniejącej infrastruktury paliwowej. W Polsce jest to Wojskowa Inspekcja Gospodarki Energetycznej.

Bezpieczeństwo energetyczne uznaje się najczęściej za rodzaj bezpieczeństwa ekonomicznego, choć Żywucka-Kozłowska nie jest osamotniona w poglądzie, że w aspekcie podmiotowym są one równorzędne. Takie podejście wzmacnia wyróżnianie przez część badaczy 3 głównych aspektów przedmiotowych bezpieczeństwa w omawianym kontekście: energetycznego, ekonomicznego (rynkowego) i ekologicznego.

Pojęciem pokrewnym do bezpieczeństwa energetycznego jest międzynarodowa polityka energetyczna, będąca – jak zauważył Adamkiewicz – siecią połączonych zależności, interesów i priorytetów poszczególnych krajów, które dążą do zachowania wewnętrznej stabilności gospodarczej. Kształtowana jest często na bieżąco przez poszczególne państwa, grupy państw lub inne podmioty polityki międzynarodowej.

Aleksander Wasiuta, Tomasz Skrzyński

J. Adamkiewicz, *Wybrane problemy globalnego bezpieczeństwa energetycznego*, [w:] *Bezpieczeństwo energetyczne: rynki surowców i energii. Energetyka – szanse, wyzwania i zagrożenia*, B. Ćwik, P. Kwiatkiewicz, R. Szczerbowski (red.), Fundacja na Rzecz Czystej Energii, Poznań 2016; *Bezpieczeństwo energetyczne. Gospodarka. Społeczeństwo – wybrane zagadnienia*, M. Ilnicki, Z. Nowakowski (red.), Towarzystwo Naukowe Powszechne, Warszawa 2016; *Bezpieczeństwo energetyczne. Koncepcje, wyzwania, interesy*, J. Gryz, A. Podraza, M. Ruszel (red.), Wydawnictwo Naukowe PWN, Warszawa 2018; *Bezpiecznie czy niebezpiecznie? Wybrane aspekty globalnej i polskiej polityki bezpieczeństwa na przełomie XX i XXI wieku*, J.J. Piątek, R. Podgórzańska (red.), Wydawnictwo Naukowe Uniwersytetu Szczecińskiego, Szczecin 2007; P. Czerpak, *Bezpieczeństwo energetyczne*, [w:] *Bezpieczeństwo międzynarodowe.*

Teoria i praktyka, K. Żukrowska, M. Grącik (red.), Szkoła Główna Handlowa, Warszawa 2006; E. Cziomer, M. Łasoń, *Podstawowe pojęcia i zakres międzynarodowego bezpieczeństwa energetycznego*, [w:] *Międzynarodowe bezpieczeństwo energetyczne w XXI wieku*, E. Cziomer (red.), Krakowskie Towarzystwo Edukacyjne, Oficyna Wydawnicza AFM, Kraków 2008; E. Kochanek, *Bezpieczeństwo energetyczne*, [w:] *Ekonomika bezpieczeństwa państwa w zarysie. Zarządzanie bezpieczeństwem*, J. Płaczek (red.), Wydawnictwo Difin, Warszawa 2014; T. Młynarski, *Bezpieczeństwo energetyczne i ochrona klimatu w drugiej dekadzie XXI wieku. Energia – środowisko – klimat*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2017; T. Młynarski, M. Tarnawski, *Źródła energii i ich znaczenie dla bezpieczeństwa energetycznego w XXI wieku*, Wydawnictwo Difin, Warszawa 2016; S. Müller-Kraenner, *Bezpieczeństwo energetyczne. Nowy pomiar świata*, tłum. K. Jankowska, Wydawnictwo Z Naszej Strony, Szczecin 2009; T. Skrzyński, *In the Face of the Rising Importance of Natural Gas to the Polish Economy*, „Public Governance" 2019, nr 1 (47); B. Soliński, *Proces zarządzania bezpieczeństwem energetycznym w ujęciu systemowym*, „Acta Pomerania. Problemy Bezpieczeństwa" 2013, nr 3; P. Szlagowski, *Polityka energetyczna Polski*, [w:] *Bezpieczeństwo energetyczne państw Grupy Wyszehradzkiej. Jak zmieniają się relacje energetyczne w Europie*, J. Świątkowska (red.), Instytut Kościuszki, Kraków 2011; A. Wasiuta, *Bezpieczeństwo energetyczne*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; tenże, *Globalne problemy surowcowo-energetyczne a bezpieczeństwo państwa*, [w:] *Współczesne problemy bezpieczeństwa państwa*, O. Wasiuta, P. Mazur (red.), Katolicki Uniwersytet Lubelski Jana Pawła II w Lublinie, Stalowa Wola 2017; tenże, *Labor Market in Poland in the Context of Renewable Energy Sector Development*, „Ekonomia i Środowisko" 2018, nr 1 (64); A. Wasiuta, J. Rokitowska, *Ekonomiczne i społeczne aspekty bezpieczeństwa sektora energetycznego w kontekście zrównoważonego rozwoju*, Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2019; A. Wasiuta, M. Malinowski, *Wybrane uwarunkowania bezpieczeństwa energetycznego Polski w kontekście zrównoważonego rozwoju*, [w:] *Bezpieczeństwo współczesnego państwa. Część 1: Wymiar międzynarodowy*, J. Falecki, P. Łubiński (red.), Wydawnictwo Drukarnia Styl, Kraków 2019; S. Wasiuta, *Rola NATO w zapewnieniu bezpieczeństwa energetycznego i ochrony infrastruktury energetycznej*, „Przegląd Geopolityczny" 2016, nr 16; E. Żywucka-Kozłowska, *Bezpieczeństwo energetyczne*, [w:] *Prawne i gospodarcze podstawy bezpieczeństwa*, S. Kamosiński, T. Kuczur, J. Laskowska (red.), Wydawnictwo UKW, Bydgoszcz 2015.

BEZPIECZEŃSTWO EUROATLANTYCKIE – związane z bezpieczeństwem Europy oraz Ameryki Północnej (w szczególności USA), z zachodnim społeczeństwem i jego wartościami; inaczej bezpieczeństwo euroamerykańskie. Obszar euroatlantycki jest obszarem szerszym niż obszar transatlantycki. O wspólnym → b e z p i e c z e ń s t w i e Europy i Północnego Atlantyku można mówić już od czasów walki o niepodległość USA, kiedy to przy władzy chcieli pozostać kolonizatorzy z Europy. Wkrótce po wojnie nawiązano jednak współpracę. Szczególnie uwidoczniła się ona w czasie I wojny światowej, gdy Europa uzyskała od USA wsparcie polityczne i materialne, które przejawiało się głównie w dostarczaniu sprzętu i udzielaniu pożyczek na jego zakup.

Współpracę euroatlantycką można obserwować już na przykładzie działań z 28 czerwca 1919 r. Z inicjatywy prezydenta USA W. Wilsona na paryskiej konferencji pokojowej podpisano Statut Ligi Narodów. Stał się on jedną ze składowych traktatu

wersalskiego i wszedł w życie po zakończeniu procesu ratyfikacji – 10 stycznia 1920 r. Liga Narodów to przykład organizacji, której utworzenie było motywowane ogromem strat poniesionych przez państwa w czasie I wojny światowej. Uświadamiała ona bezcelowość uciekania się przez państwa do rozwiązań siłowych i realizowania w ten sposób planów politycznych.

Wydarzeniem, które również potwierdziło wzajemną współpracę w dziedzinie bezpieczeństwa między USA i Europą, było podpisanie 27 sierpnia 1927 r. paktu Brianda–Kellogga. Francuski minister spraw zagranicznych A. Briand oraz sekretarz stanu USA F.B. Kellogg wraz z państwami sygnatariuszami postanowili odstąpić od stosowania siły w prowadzonej przez siebie polityce zagranicznej. Mimo to 1 września 1939 r. Niemcy jako jedno z państw sygnatariuszy zaatakowały Polskę – która również związana był z tym paktem – i rozpoczęły II wojnę światową. Wydarzenia rozgrywające się w tym czasie są kolejnym przykładem zacieśniania stosunków między Europą i USA. Dzięki pomocy USA II wojnę światową wygrali alianci.

Współpracę między USA i Europą zapewnia również Organizacja Narodów Zjednoczonych. Została utworzona 24 października 1945 r. w miejsce Ligi Narodów, która okazała się zupełnie nieefektywna. Do głównych zadań ONZ należy: ochrona → p r a w c z ł o w i e k a [t. 3], przestrzeganie pokoju oraz zapewnianie → b e z p i e c z e ń s t w a m i ę d z y n a r o d o w e g o . Kraje Europy Zachodniej zaczęły propagować w tym czasie wartości związane z wolnością, demokracją, pluralizmem oraz wolnym rynkiem. Po II wojnie światowej z USA zaczęła napływać pomoc mająca na celu odbudowę gospodarek krajów Europy. Plan Marshalla w latach 1948–1952 oferował pomoc rzeczową, której wartość w ostatecznym rozrachunku wyniosła ponad 14 mld USD (wg dzisiejszych wartości 140 mld USD). Z tej pomocy w największym stopniu skorzystała Francja i Wielka Brytania. W latach powojennych USA w ramach kształtującego się systemu bipolarnego rozpoczęły wyścig o pozycję światowego mocarstwa. Był to kraj, który w najmniejszym stopniu został dotknięty zniszczeniami w trakcie II wojny światowej. Dzięki temu był w stanie zaopatrywać inne kraje w niezbędny sprzęt, technologie czy nawet żywność, co w bardzo dużym tempie napędzało ich gospodarkę. Państwa europejskie w dużej mierze utraciły swoje kolonie, w związku z czym zmniejszyły się ich zyski, co – obok wycieńczenia Europy wojną – pozwalało USA coraz mocniej narzucać innym krajom swoje warunki.

W 1949 r. utworzono → N A T O [t. 3] – organizację polityczno-wojskową, która miała za zadanie przeciwstawiać się → z a g r o ż e n i o m [t. 4] płynącym ze strony państw bloku wschodniego (od 1955 r. w strukturach Układu Warszawkiego). Głównym celem NATO było wzajemne zapewnianie bezpieczeństwa członkom organizacji. Duże znaczenie ma art. 5 traktatu północnoatlantyckiego w brzmieniu:

> Strony zgadzają się, że zbrojna napaść na jedną lub więcej z nich w Europie lub Ameryce Północnej będzie uznana za napaść przeciwko nim wszystkim i dlatego zgadzają się, że jeżeli taka zbrojna napaść nastąpi, to każda z nich, w ramach

wykonywania prawa do indywidualnej lub zbiorowej samoobrony, uznanego na mocy artykułu 51 Karty Narodów Zjednoczonych, udzieli pomocy Stronie lub Stronom napadniętym, podejmując niezwłocznie, samodzielnie, jak i w porozumieniu z innymi Stronami, działania, jakie uzna za konieczne, łącznie z użyciem siły zbrojnej, w celu przywrócenia i utrzymania bezpieczeństwa obszaru północnoatlantyckiego.

Dzięki NATO w okresie → z i m n e j w o j n y [t. 4] nie doszło do wybuchu kolejnego globalnego konfliktu. USA poprzez swoją potęgę zdobyły dominującą pozycję w NATO oraz ONZ.

Wpływ na wzajemne relacje miało także powstanie Organizacji Bezpieczeństwa i Współpracy w Europie (KBWE) i w późniejszym czasie Organizacji Bezpieczeństwa i Współpracy w Europie (OBWE), do których należały również państwa bloku wschodniego. KBWE miała stanowić alternatywę dla zapewniania bezpieczeństwa w Europie. Organizacje te dążyły do stabilizacji i umocnienia bezpieczeństwa. Rzeczywista zmiana zależności między Europą a USA stała się widoczna po zakończeniu zimnej wojny. Narastający po II wojnie światowej wpływ USA na politykę i bezpieczeństwo państw europejskich został częściowo zahamowany przez integrację w ramach kształtującej się UE.

Po zakończeniu zimnej wojny i upadku ZSRR w Europie zwiększyło się znaczenie państw zachodnich. W tym czasie większą rolę zaczęło odgrywać wyznawanie wspólnych wartości. Wraz ze spadającym zagrożeniem ze strony Rosji zastanawiano się nad redefinicją partnerstwa atlantyckiego. Kluczowe stało się sformułowanie nowej roli USA i NATO. Znaczący wpływ miało także ustalenie spójnych, jasnych zasad współpracy w dziedzinie gospodarki oraz pomocy przy zapobieganiu i rozwiązywaniu konfliktów. W ramach KBWE uzgodniono, aby rozwiązywać konflikty w sposób pokojowy bądź przekazywać je do rozstrzygnięcia → R a d z i e B e z p i e c z e ń s t w a O N Z [t. 3]. Potwierdzono, że wojska państwa członkowskiego mogą stacjonować na terenie innego kraju, jednak zgodnie ze swobodnie zawartymi umowami i obowiązującymi przepisami prawa międzynarodowego. Szczyt w Helsinkach 9–10 lipca 1992 r. doprowadził do podpisania tzw. *Wyzwań czasu przemian*, które odnosiły się do przyszłej wizji rozwoju KBWE oraz wyposażenia jej struktur w możliwość przeprowadzania działań prewencyjnych i interwencyjnych. W Budapeszcie 5–6 grudnia 1994 r. KBWE przekształcono w OBWE, które gwarancje bezpieczeństwa opiera wyłącznie na postanowieniach traktatowych.

Inna sytuacja jest w NATO, gdzie państwa członkowskie do dyspozycji mają ochronę wspólnej armii. Siły NATO podzielone są na:

- Siły reagowania (Reaction Forces) – mobilne jednostki, obejmują wszystkie rodzaje wojsk, zdolne do natychmiastowej reakcji. Podzielone zostały dodatkowo na Siły Natychmiastowego Reagowania (Immediate Reaction Forces) i Siły Szybkiego Reagowania (Rapid Reaction Forces).

- Główne Siły Obrony (Main Defence Forces) – regularne jednostki obejmujące wszystkie rodzaje wojsk. Są to formacje o podwyższonym i zwykłym stopniu gotowości bojowej. Stanowią trzon struktury wojskowej NATO.
- Siły Wzmocnienia (Augmentation Forces) – obejmują jednostki o różnym stopniu gotowości bojowej, przygotowane są do wykorzystania w różnych rejonach NATO. Składają się w większości z → w o j s k l ą d o w y c h [t. 4] i lotniczych USA, które gotowe są do szybkiego przerzutu na obszar Europy.
- Rozwijane są także Siły Szybkiego Reagowania NATO (NATO Response Force), które tworzone są od szczytu NATO w Pradze w 2002 r. W swoich działaniach wspomagają również funkcjonowanie sił szybkiego reagowania utworzonych w ramach UE. W 2003 r. siły NATO po raz pierwszy przeprowadziły operację poza regionem euroatlantyckim. Były to działania przeprowadzone w Afganistanie w ramach przejętego dowództwa nad Międzynarodowymi Siłami Wsparcia Bezpieczeństwa (International Security Assistance Force, ISAF).

USA kształtowanie bezpieczeństwa w regionie upatrują w zwiększaniu liczby wojsk stacjonujących w krajach europejskich. Jednak nie wszystkie państwa akceptują tę politykę. Niektóre kraje uważają, że dominująca rola USA może doprowadzić do izolacjonizmu, a także stanowić zagrożenie dla bezpieczeństwa politycznego krajów europejskich. Związane jest to z postępującym od lat 90. XX w. procesem europeizacji. Dotyczy on głównie państw członkowskich UE i wiąże się z kształtowaniem wspólnej polityki, która staje się integralną częścią każdego kraju przynależącego do UE. Należy jednak pamiętać, że aby utrzymywać wspólną politykę państw tworzących euroatlantycką przestrzeń bezpieczeństwa, niezbędne jest stosowanie dyplomacji. Umożliwia ona kierowanie zrównoważoną współpracą, która odpowiada na potrzeby państw członkowskich.

Obecnie państwa euroatlantyckie podejmują próby odnajdowania nowych typów zagrożeń i przeciwdziałania im. Koncentrują się na kwestiach związanych z kulturą, ekologią, energetyką, szeroko pojętą → i n f o r m a c j ą [t. 2] itp. Duże znaczenie mają także → z a g r o ż e n i a m i l i t a r n e [t. 4], które związane są z prowadzonymi przez członków NATO operacjami zbrojnymi, misjami pokojowymi (zob. → m i s j a p o k o j o w a [t. 3]) czy konfliktami występującymi w bezpośrednim sąsiedztwie (np. wojny Rosji z Ukrainą). Wspomnieć należy też o konfliktach na tle religijnym i etnicznym, które również mogą stanowić niebezpieczeństwo dla krajów euroatlantyckich, przykład stanowić może tutaj konflikt w byłej Jugosławii w latach 90. XX w. Obecnie szczególną uwagę zwraca się na konflikt izraelsko-palestyński.

Istotną rolę odgrywają także zagrożenia asymetryczne, a wśród nich przede wszystkim → t e r r o r y z m [t. 4]. W państwach należących do euroatlantyckiego obszaru bezpieczeństwa ataki terrorystyczne organizowane są m.in. przez dżihadystów i fundamentalistów islamskich.

Inne zagrożenia dla obszaru euroatlantyckiego związane są z rozszerzającą się technologią i teleinformatyką. Mowa tutaj o atakach cybernetycznych i cyberterroryzmie.

Wielokrotnie dochodzi do kradzieży danych osób prywatnych, firm i instytucji państwowych, a także do różnego typu blokad stron internetowych, systemów i aplikacji sieciowych. Przykładem może być wirus Stuxnet (zob. →złośliwe oprogramowanie [t. 4]), który w czerwcu 2010 r. użyty został do szpiegowania i przeprogramowania instalacji przemysłowych. Zaatakował on m.in. 45 tys. przemysłowych systemów kontroli wyprodukowanych przez firmę Siemens, najpoważniejsze zagrożenie stanowiło zainfekowanie komputerów przemysłowych w irańskich elektrowniach atomowych.

Z gospodarką związane są natomiast problemy surowców energetycznych (ropy naftowej, gazu ziemnego, węgla kopalnego). Państwa, które stają w obliczu niedoborów energii, często wspierają się importem. Duże zagrożenie stanowić mogą pogarszające się stosunki międzynarodowe z państwami eksportującymi, a także zmiany cen tych surowców na światowych rynkach. Druga kwestia to malejące światowe zasoby energetyczne. Ciągły wzrost zapotrzebowania jest efektem rozwoju gospodarczego, aby sprostać tym wymaganiom, niezbędne jest wprowadzanie produkcji energii z innych źródeł. W tej sprawie podnosi się argumenty na temat dbałości o środowisko i jego ochrony oraz inwestowania w alternatywne źródła energii. Istotne jest prowadzenie polityki proekologicznej i podejmowanie działań w obliczu → sytuacji kryzysowych [t. 4] oraz zagrożeń powstałych w wyniku działania sił natury.

Przykładem działań, w które zaangażowały się państwa euroatlantyckie, jest konflikt w państwach byłej Jugosławii. NATO w 1999 r. przeprowadziło operację pod kryptonimem Allied Force w celu stabilizacji sytuacji w regionie, zaprzestania czystek etnicznych i wprowadzenia procesów demokratyzacyjnych. W ramach ciągłego wzmacniania bezpieczeństwa na opisywanym obszarze misja pokojowa w Kosowie jest ciągle przedłużana. Po zamachach terrorystycznych z 11 września 2001 r. na World Trade Center w Nowym Jorku zawiązano koalicję antyterrorystyczną. Ustalono, że odpowiedzialna ze te wydarzenia jest Al-Kaida wspierana w Afganistanie przez rząd talibów. Na mocy Rezolucji Rady Bezpieczeństwa ONZ nr 1368 (2001) z 12 września 2001 r. zadecydowano o przeprowadzeniu operacji Enduring Freedom. Do tej pory, podobnie jak w Kosowie, w Afganistanie stacjonują → żołnierze [t. 4] Sojuszu i prowadzą misję stabilizacyjną. Jest ona ciągle przedłużana ze względu na nadal dobrze funkcjonującą partyzantkę talibów.

Podobna sytuacja ma miejsce w Iraku. USA przekonywały o zagrożeniu płynącym z rządów S. Husajna oraz posiadaniu przez Irak → broni masowego rażenia. Wszczęcie działań zbrojnych możliwe było dzięki wydanym rezolucjom Rady Bezpieczeństwa ONZ: nr 678 z 1990 r., 687 z 1991 r. oraz 1441 z 2002 r. Mimo że część sił (w tym polskie) została wycofana po osiągnięciu przez Irak względnej stabilizacji, to w dalszym ciągu przebywają tam żołnierze USA.

Bardzo duże zagrożenie w ostatnich latach płynie ze strony Rosji, która w 2014 r. zaanektowała Krym. Jest to szczególnie istotne, dlatego że Ukraina graniczy

bezpośrednio z Polską, której granica wschodnia jest zarazem granicą UE i NATO. USA i państwa sojusznicze nie uznały aneksji Krymu. Zastosowały wobec Rosji wiele → s a n k c j i [t. 4] politycznych i finansowych. Ich działania skupiały się także na izolacji tego państwa na arenie międzynarodowej.

Obecnie na obszarze euroatlantyckim bezpieczeństwo regulowane jest w największym stopniu przez 2 organizacje: UE i NATO. Z biegiem lat obszar ten może zostać poddany próbie,wynikającej z występowania kolejnych zagrożeń. Ich ilość i zakres mogą się zmieniać, a rozwój niektórych spośród nich może być określany jako dynamiczny. Wydarzenia, którymi dotknięte zostaną państwa tworzące euroatlantycką przestrzeń bezpieczeństwa, mogą występować na różnych obszarach, z różną intensywnością. Będzie to zmuszało państwa do poszukiwania nowych, skuteczniejszych metod i środków mających na celu przeciwdziałanie i różnego typu zagrożeniom i ich zwalczanie.

Paulina Rus

J. Czaja, *Bezpieczeństwo euroatlantyckie: nowe zagrożenia, nowe wyzwania*, „Krakowskie Studia Międzynarodowe" 2004, nr 4; J.M. Fiszer, *System euroatlantycki oraz jego miejsce i rola w multipolarnym ładzie międzynarodowym*, [w:] *System euroatlantycki i bezpieczeństwo międzynarodowe w multipolarnym świecie. Miejsce i rola Polski w euroatlantyckim systemie bezpieczeństwa*, J.M. Fiszer (red.), Instytut Studiów Politycznych PAN, Warszawa 2013; S. Koziej, *NATO i UE: dwa euroatlantyckie filary bezpieczeństwa Polski*, [w:] *System euroatlantycki w wielobiegunowym ładzie międzynarodowym*, J.M. Fiszer, P. Olszewski (red.), Dom Wydawniczy Elipsa, Warszawa 2013; J. Pawłowski, *Bezpieczeństwo euroatlantyckie a nowa Koncepcja Strategiczna NATO*, „Zeszyty Naukowe Akademii Sztuki Wojennej" 2011, nr 2 (83); I. Protasowicki, *Wybrane współczesne zagrożenia euroatlantyckiej przestrzeni bezpieczeństwa*, [w:] *Dylematy bezpieczeństwa współczesnego państwa: księga jubileuszowa dedykowana profesorowi Kazimierzowi Rajchelowi*, M. Polinceusz, M. Pomykała (red.), Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2015; M. Wróblewska-Fysik, *Nowy Sojusz na nowy wiek – analiza głównych wyzwań stojących przed wspólnotą euroatlantycką na progu XXI wieku*, [w:] *Współczesne relacje transatlantyckie*, J. Cisek (red.), Instytut Multimedialny, Kraków 2010.

BEZPIECZEŃSTWO EUROPEJSKIE – obecnie w dużej mierze opiera się na funkcjonowaniu Unii Europejskiej (powstałej 1 listopada 1993 r. na mocy podpisanego 7 lutego 1992 r. traktatu z Maastricht) oraz podejmowanych przez nią i jej członków działań. Niebagatelne znaczenie ma tutaj także traktat północnoatlantycki, na podstawie którego powstało → N A T O [t. 3]. Organizacja ta, funkcjonująca jako układ wojskowy, od 1949 r. objęła już państwa europejskie takie jak Belgia, Dania, Francja, Holandia, Islandia, Kanada, Luksemburg, Norwegia, Portugalia, Wielka Brytania, Włochy (1949), Grecja (1952), RFN (1955, od 1990 r. jako Niemcy), Hiszpania (w 1982). 12 marca 1999 r. do NATO przystąpiły Czechy, Polska i Węgry. Następnie w 2004 r. do tych państw dołączyła Bułgaria, Estonia, Litwa, Łotwa, Rumunia Słowacja, Słowenia, w 2009 r. Albania i Chorwacja, a w 2017 r. Czarnogóra.

Decydujący i najważniejszy artykuł traktatu północnoatlantyckiego to art. 5 w brzmieniu:

> Strony zgadzają się, że zbrojna napaść na jedną lub więcej z nich w Europie lub Ameryce Północnej będzie uznana za napaść przeciwko nim wszystkim, i dlatego zgadzają się, że jeżeli taka zbrojna napaść nastąpi, to każda z nich, w ramach wykonywania prawa do indywidualnej lub zbiorowej samoobrony, uznanego na mocy artykułu 51 Karty Narodów Zjednoczonych, udzieli pomocy Stronie lub Stronom napadniętym, podejmując niezwłocznie, samodzielnie, jak i w porozumieniu z innymi Stronami, działania, jakie uzna za konieczne, łącznie z użyciem siły zbrojnej, w celu przywrócenia i utrzymania bezpieczeństwa obszaru północnoatlantyckiego.

W Europie już od lat 50. XX w. istniała koncepcja współpracy w zakresie → b e z p i e c z e ń s t w a , planowano powołać Europejską Wspólnotę Obronną, której celem miało być stworzenie europejskiej armii. Miała ona zawierać 40 narodowych dywizji, składających się z 13 tys. → ż o ł n i e r z y [t. 4] każda (w jednakowym umundurowaniu). Współtworzyć miały ją Belgia, Francja, Holandia, Luksemburg, Niemcy i Włochy. Plany te jednak nie doszły do skutku.

Na podstawie układów paryskich z 22 października 1954 r. powstała Unia Zachodnioeuropejska (UZE). Opisywana międzynarodowa organizacja wojskowa nie odegrała znaczącej roli, a jej aktywność wojskowa spłynęła w ręce NATO. Mimo że kompetencje UZE wykraczały poza obręb art. 5 traktatu północnoatlantyckiego, nie pełniła ona funkcji operacyjnych. Dopiero w latach 1987–1988 przeprowadziła pierwszą akcję militarną. Miała ona miejsce w cieśninie Ormuz po zakończeniu → w o j n y [t. 4] iracko-irańskiej i wiązała się z rozminowywaniem kanału morskiego. Lata 90. XX w. wymusiły na organizacji większą aktywizację, czego skutkiem było utworzenie Korpusu Europejskiego oraz rozszerzenie współpracy z NATO. Jednak już w 1999 r. Rada Europejska zawnioskowała o wygaszenie UZE. Jej kompetencje przejęła nowo powstała Wspólna Europejska Polityka Bezpieczeństwa i Obrony (WPBiO), która rozpoczęła działalność w ramach Wspólnej Polityki Zagranicznej i Bezpieczeństwa (WPZiB). Unia Zachodnioeuropejska rozwiązana została w marcu 2010 r., w związku z wejściem w życie traktatu lizbońskiego. Jej działalność wygaszono w czerwcu 2011 r.

Wspomniana WPZiB formowana jest od 1992 r. Kwestie z nią związane uregulowane zostały w art. 21–46 traktatu z Maastricht i kolejno rozwinięte w traktatach: z Amsterdamu (1997 r.), Nicei (2001 r.) i Lizbony (2007 r.). Do jej najważniejszych celów zaliczyć można: ochronę wspólnych interesów i wartości na obszarze Unii, wzmacnianie bezpieczeństwa i pokoju w Unii i na świecie, rozszerzanie współpracy międzynarodowej, ochronę → p r a w c z ł o w i e k a [t. 3] i umacnianie zasad demokratycznych. Wszelkie działania podejmowane w ramach tego programu finansuje budżet UE. Państwa członkowskie zobligowane są przekazywać na swoje siły zbrojne ustaloną część PKB oraz utrzymywać je na odpowiednim poziomie.

Od 1992 r. na obszarze UE i poza nią formowany jest Europejski Obszar Gospodarczy (EOG). Państwa niebędące członkami UE i należące do EOG obowiązane są przepisami prawa stanowiącymi o strefie wolnego handlu i wspólnym rynku. Oparte są one na swobodnym przepływie ludzi, kapitału, usług oraz towarów.

Wymieniony wcześniej Korpus Europejski, inaczej Eurokorpus, sformowano w 1993 r., pełną zdolność bojową osiągnął w 1995 r. Za jego cel obrano wyznaczenie tożsamości obronnej UE, a także jej zdolności wojskowych. Korpus dowodzony jest rotacyjnie przez państwa ramowe, do których należą Niemcy, Francja, Belgia, Hiszpania i Luksemburg. Obserwatorami natomiast są Polska, Grecja, Turcja, Włochy, Rumunia. Opisywana struktura wojskowa oparta jest na uczestnictwie żołnierzy z wielu krajów, są to siły szybkiego reagowania stacjonujące w Strasburgu (Francja). Zostały one powołane na potrzeby UE i NATO w celu uczestniczenia w operacjach kryzysowych, humanitarnych czy ratunkowych oraz wymuszania i utrzymywania pokoju. Kwestie te uwzględnione i zapisane zostały w misjach petersberskich z 1992 r. Dowództwo korpusu stanowi ok. 1 tys. żołnierzy, jest zdolne do kierowania 60 tys. żołnierzy i prowadzenia różnego typu akcji w odmiennych strefach klimatycznych. Jako przykład ich działań można podać kierownictwo w operacji NATO w 2000 r. w Kosowie (KFOR II) czy dowództwo na przełomie 2004 i 2005 r. w Afganistanie nad operacją ISAF6 Force. Natomiast w 2012 r. członkowie Eurokorpusu stanowili trzon dowództwa sił ISAF w Kabulu. Eurokorpus nie podlega żadnej strukturze wojskowej, udział w operacjach i misjach zatwierdzany jest przez tzw. Komitet Wspólny, wśród jego członków znajdują się szefowie obrony i ministrowie spraw zagranicznych. Siły Eurokorpusu mogą być wykorzystywane na potrzeby państw ramowych.

W 1999 r. na szczycie w Helsinkach ustanowiono Europejską Politykę Bezpieczeństwa i Obrony (EPBiO). Na jej czele stanął Komitet Polityczny i Bezpieczeństwa. Główne zadania EPBiO miały polegać na zwiększaniu zdolności do samodzielnego prowadzenia działań operacyjnych oraz przystępowania do działań w obliczu → k r y z y s u [t. 2]. W tym zakresie potwierdzono również decyzję o rozwijaniu europejskich sił szybkiego reagowania (European Rapid Reaction Force).

W 2000 r. wprowadzono w formie deklaracji tzw. Kartę Praw Podstawowych, która obowiązuje członków UE i ma gwarantować poszanowanie praw człowieka. Składa się ona z 7 rozdziałów namawiających do przestrzegania i poszanowania godności człowieka, wolności, solidarności, praw obywatelskich, prawa do rzetelnego procesu sądowego itp.

22 stycznia 2001 r. Rada UE utworzyła Sztab Wojskowy Unii Europejskiej (European Union Military Staff, EUMS) w ramach funkcjonowania EPBiO. Jest to departament, który funkcjonuje przy Sekretariacie Rady UE. Tworzą go eksperci z dziedziny wojskowości, których delegują kraje członkowskie. Na przewodniczącego wybrany może być generał, który ma przynajmniej 3 gwiazdki. Najważniejsze zadania EUMS to analiza sytuacji międzynarodowej w zakresie bezpieczeństwa i obrony, wczesne

ostrzeganie o kryzysach, planowanie strategiczne misji petersberskich, wykonywanie decyzji, które podejmuje Sztab Wojskowy UE.

4 kwietnia 2001 r., również w ramach działania Europejskiej Polityki Bezpieczeństwa i Obrony, powołano Komitet Wojskowy UE. W skład tego organu UE wchodzą szefowie obrony państw członkowskich, którzy w Brukseli reprezentowani są przez wyznaczonych przedstawicieli. Na przewodniczącego wybrany zostać może jedynie generał mający 4 gwiazdki. Komitet Wojskowy UE wyznacza wskazówki Komitetowi Politycznemu i Bezpieczeństwa, a także gwarantuje zwierzchnictwo nad Sztabem Wojskowym UE.

Komitet Polityczny i Bezpieczeństwa jako instytucja pomocnicza działa przy Radzie UE w dziedzinach wspólnej polityki zagranicznej i bezpieczeństwa oraz wspólnej polityki bezpieczeństwa i obrony UE. Zadania komitetu określa art. 38 (dawny art. 25 TUE) Traktatu o funkcjonowaniu Unii Europejskiej:

> Komitet Polityczny i Bezpieczeństwa obserwuje sytuację międzynarodową w dziedzinach objętych wspólną polityką zagraniczną i bezpieczeństwa oraz przyczynia się do określania polityk, wydając opinie dla Rady – na jej żądanie, na żądanie Wysokiego Przedstawiciela Unii ds. zagranicznych i polityki bezpieczeństwa lub z inicjatywy własnej. Czuwa on również nad wprowadzaniem w życie uzgodnionych polityk, bez uszczerbku dla uprawnień wysokiego przedstawiciela. W zakresie objętym niniejszym rozdziałem Komitet Polityczny i Bezpieczeństwa sprawuje, pod kierunkiem Rady i wysokiego przedstawiciela, kontrolę polityczną i kierownictwo strategiczne nad operacjami zarządzania kryzysowego, o których mowa w art. 43 Traktatu o Unii Europejskiej. Rada może upoważnić Komitet do podjęcia, w celu i na czas trwania operacji zarządzania kryzysowego, określonych przez Radę decyzji dotyczących kontroli politycznej i kierownictwa strategicznego nad operacją.

Członkami Komitetu Politycznego i Bezpieczeństwa są przeważnie wysokiej rangi przedstawiciele państw członkowskich, zazwyczaj ambasadorowie. Komitet obraduje przeważnie 2 razy w tygodniu, ma charakter stały.

Kolejnym ważnym dokumentem regulującym kwestię bezpieczeństwa w Europie jest *Europejska Strategia Bezpieczeństwa* (ESB). Została przyjęta 12 grudnia 2003 r., jej założeniem jest obrona kontynentu europejskiego przed różnego typu czynnikami destabilizującymi. Wymienia w tym zakresie przede wszystkim → t e r r o r y z m [t. 4], który zagraża życiu ludności, stanowi zwiększające się → z a g r o ż e n i e [t. 4] strategiczne dla Europy, powoduje zmniejszanie się otwartości i tolerancji wobec innych społeczeństw, stanowi o zwiększaniu wydatków. Inne zagrożenia dostrzega się w rozprzestrzenianiu → b r o n i m a s o w e g o r a ż e n i a, konfliktach religijnych, rozpadzie państwowości (→ k o r u p c j a [t. 2], nadużycia władzy itp.), rozszerzającej się → p r z e s t ę p c z o ś c i z o r g a n i z o w a n e j [t. 3]. UE, aby zapewniać bezpieczeństwo, stawia przed sobą 3 główne zadania: odpowiedź na zagrożenia i przeciwdziałanie im (przeciwdziałanie rozprzestrzenianiu się broni masowego rażenia, rozwiązywanie konfliktów regionalnych, zwalczanie terroryzmu, wprowadzenie

europejskiego nakazu aresztowania), budowanie bezpieczeństwa w sąsiedztwie, dbanie o porządek międzynarodowy oparty na skutecznym multilateralizmie. Określa, że siły zbrojne wykorzystane mogą być w akcjach stabilizacyjnych, humanitarnych, ratowniczych, zapobiegania rozwoju konfliktów oraz wymuszania pokoju (np. Kosowo). W 2008 r. w ramach aktualizacji ESB do zagrożeń dołączono → b e z p i e c z e ń s t w o e n e r g e t y c z n e , cybernetyczne, zmiany klimatu oraz ubóstwo mogące wpływać na stabilność regionów.

Od 2003 r. można mówić także o Europejskiej Polityce Sąsiedztwa, która reguluje współpracę państw członkowskich UE z krajami sąsiadującymi. Uwzględnia ona działania w dziedzinie polityki, bezpieczeństwa, ekonomii, handlu, ochrony środowiska, transportu, energetyki, współpracy naukowej oraz kulturalnej.

W 2004 r. powstała Europejska Agencja Obrony, która udziela wsparcia państwom członkowskim (bez Danii) w zwiększaniu potencjału zasobów wojskowych. Jej działania skupiają się głównie na przekazywaniu fachowej wiedzy, planowaniu budżetowym, a przede wszystkim elastycznym dostosowywaniu wsparcia dla różnych krajów. Pomoc ta uzależniona ma być od potrzeb, jakie przedstawia dane państwo.

Następnie należy wspomnieć traktat lizboński, który wszedł w życie 1 grudnia 2009 r. Wprowadził klauzulę solidarności i wzajemnej pomocy państw członkowskich w brzmieniu:

> Jeżeli Państwo Członkowskie stało się przedmiotem ataku terrorystycznego lub ofiarą klęski żywiołowej lub katastrofy spowodowanej przez człowieka, na prośbę jego władz inne Państwa Członkowskie udzielają mu pomocy. W tym celu Państwa Członkowskie koordynują swoje działania w ramach Rady.

Traktat ten ustanowił UE – poprzez zniesienie Wspólnoty Europejskiej – organizacją międzynarodową, zlikwidował również podział Unii na filary.

W czerwcu 2016 r. przedstawiono kolejne działania w ramach WPBiO. Wprowadzono w tym czasie globalną → s t r a t e g i ę [t. 4] na rzecz polityki zagranicznej i bezpieczeństwa UE. Nakreślono wówczas 5 najważniejszych priorytetów prowadzenia polityki zagranicznej, mianowicie: bezpieczeństwo Unii, opracowanie wspólnego podejścia do konfliktów, wsparcie państw i społeczeństw na wschodzie i południu UE, utrzymywanie ładu regionalnego oraz ładu globalnego. Wprowadzanie tej strategii podlega corocznemu przeglądowi i konsultacjom (przez Radę, Komisję oraz Parlament). W ramach WPBiO Parlament Europejski:

> organizuje debaty, wysłuchania i warsztaty poświęcone takim zagadnieniom jak cywilne i wojskowe misje w ramach WPBiO, kryzysy mię dzy narodowe mające konsekwencje dla bezpieczeństwa i obrony, wielostronne ramy w zakresie bezpieczeństwa, kontrola zbrojeń i kwestia nierozprzestrzeniania broni, walka z terroryzmem i przestępczością zorganizowaną, najlepsze praktyki w celu poprawy skuteczności bezpieczeństwa i obrony oraz zmiany prawne i instytucjonalne w UE w tych dziedzinach.

Parlament Europejski bierze również udział w Zgromadzeniu Parlamentarnym NATO, co pokazuje, jak ważne dla bezpieczeństwa europejskiego jest uczestnictwo w NATO. WPBiO związana jest także z Europejskim Planem Działań w Sektorze Obrony, który ustanowił Europejski Fundusz Obronny. Fundusz ten wspiera badania nad obronnością oraz rozwój zdolności obronnych.

W marcu 2017 r. w ramach WPBiO Rada Europejska powołała nową strukturę – Komórki Planowania i Prowadzenia Operacji Wojskowych. Jej główne zadanie opiera się na zwiększaniu zdolności UE do szybszego, skuteczniejszego reagowania w ramach prowadzenia misji wojskowych. Obecnie są one prowadzone w Mali, Republice Środkowoafrykańskiej oraz Somalii. Od 2018 r. wdrażany jest program PESCO, umożliwiający państwom członkowskim UE zacieśnienie współpracy w obszarze bezpieczeństwa i obrony. W tym samym roku powołano także Europejski program rozwoju przemysłu obronnego, którego celem jest wspieranie konkurencyjności i innowacyjności przemysłu obronnego UE.

W Europie działa również wiele organizacji regionalnych. Zaliczyć można do nich chociażby → G r u p ę Wy s z e h r a d z k ą [t. 2], która powstała w 1991 r. Zrzesza ona Polskę, Czechy, Słowację i Węgry. W tym samym roku powstał też tzw. Trójkąt Weimarski, którego członkami są Polska, Niemcy i Francja. W 2015 r. utworzono kolejną organizację o charakterze gospodarczo-politycznym – Trójmorze. W jej skład wchodzą: Austria, Chorwacja, Czechy, Estonia, Litwa, Łotwa, Polska, Rumunia, Słowacja, Słowenia i Węgry. Kraje europejskie należą także do innych organizacji międzynarodowych (np. ONZ, WHO).

Kwestiami bezpieczeństwa w Europie zajmuje się również organizacja G6, która powstała w 2003 r. i zrzesza w swoich kręgach Hiszpanię, Francję, Włochy, Niemcy, Polskę i Wielką Brytanię. Grupa ma na celu współdziałanie m.in. w walce z terroryzmem, kontrolowaniu granic, wymianie danych operacyjnych, przeciwdziałaniu nielegalnej imigracji, zapobieganiu i zwalczaniu przestępczości zorganizowanej.

Obecnie Europa upatruje →z a g r o ż e n i a b e z p i e c z e ń s t w a [t. 4] m.in. w terroryzmie, który ułatwia postępująca globalizacja, multikulturowość oraz polityka otwartych granic (układ z Schengen). Związany jest on również z kryzysem migracyjnym i brakiem → a s y m i l a c j i, w szczególności muzułmańskich imigrantów. Z drugiej strony przyjmowanie imigrantów, także z Ukrainy, wspomaga procesy demograficzne w Europie i zapobiega i tak już daleko posuniętemu procesowi starzenia się społeczeństwa. Innym zagrożeniem jest rozprzestrzenianie broni masowego rażenia. Rada Europejska w grudniu 2003 r. przyjęła deklarację o nieproliferacji broni masowego rażenia. Do działań UE w najbliższym czasie należeć będzie wpływanie na politykę nuklearną innych państw na świecie. Kolejnych zagrożeń upatrywać można w konfliktach regionalnych (np. była Jugosławia, Hiszpania). W obliczu takich zdarzeń niezbędne jest monitorowanie sytuacji i zapobieganie rozprzestrzenianiu się konfliktów. Ważne będzie również umacnianie stabilizacji na takich obszarach i pomoc

w prowadzeniu procesów demokratycznych. Obecnie duże znaczenie ma rozpoczęty w 2014 r. konflikt między Rosją a Ukrainą, w którego wyniku Rosja zaanektowała Krym. UE i NATO nałożyły na Rosję szereg → s a n k c j i [t. 4]. Były to m.in. wykluczenie z grupy G8, odmówienie członkostwa w Organizacji Współpracy Gospodarczej i Rozwoju (OECD), wprowadzenie embarga na uzbrojenie i technologie militarne, wstrzymanie przewozu zaawansowanych technologii do Rosji i inne. NATO i UE zwiększyły wydatki na zakup nowego uzbrojenia oraz zintensyfikowały ćwiczenia wojskowe. Dodatkowo w Polsce i w krajach bałtyckich rozmieszczono Siły Odpowiedzi NATO. Duże zagrożenie nieść za sobą może także przestępczość zorganizowana, powiązana z transgranicznym handlem narkotykami, bronią i ludźmi (np. kobietami czy migrantami o nieuregulowanym statusie prawnym). Ułatwieniami dla przestępczości zorganizowanej są błyskawiczna łączność (GPS, internet), mobilność, szybkość i łatwość dokonywania transakcji finansowych oraz dostęp do zaawansowanych technologii. W ostatnich latach zagrożenie mogą stanowić również ataki cybernetyczne i wycieki danych z firm i instytucji państwowych. Z gospodarką związany jest problem surowców energetycznych (ropy naftowej, gazu ziemnego, węgla i innych surowców kopalnych) – wizja przyszłej Europy opiera się przede wszystkim na wykorzystywaniu źródeł alternatywnych. Jest to też koncepcja połączona z postulatami mówiącymi o ochronie środowiska i ograniczeniu skutków zmian klimatycznych.

Paulina Rus

A. Ciupiński, *Wspólna Polityka Bezpieczeństwa i Obrony Unii Europejskiej. Geneza, rozwój, funkcjonowanie*, Wydawnictwo Difin, Warszawa 2013; A. Dziewulska, *Strategie bezpieczeństwa Unii Europejskiej*, „Studia Europejskie – Studies in European Affairs" 2016, nr 4; Eurocorps.org (dostęp 27.01.2020); *Europejska Strategia Bezpieczeństwa. Bezpieczna Europa w lepszym świecie*, Urząd Publikacji Unii Europejskiej, Luksemburg 2009; M. Joks, *Zagrożenia bezpieczeństwa Europy w aspekcie Europejskiej Strategii Bezpieczeństwa*, „Zeszyty Naukowe Akademii Sztuki Wojennej" 2017, nr 4 (109); D.J. Mierzejewski, *Bezpieczeństwo europejskie w warunkach przemian globalizacyjnych*, Wydawnictwo Adam Marszałek, Toruń 2011; M. Pala, *Wyzwania i zagrożenia dla środowiska bezpieczeństwa europejskiego*, „Doctrina. Studia Społeczno-Polityczne" 2015, nr 12; A. Rossa, *Bezpieczeństwo europejskie – historia niedokończona. Analiza historyczna koncepcji bezpieczeństwa europejskiego w kontekście budowy zdolności obronnych przez Unię Europejską*, „Słupskie Studia Historyczne" 2010, nr 16; I. Sokolska, E. Pavy, *Traktat z Lizbony*, 2020, EuroParl.Europa.eu/factsheets.pl (dostęp 28.02.2020); *Strategia bezpieczeństwa wewnętrznego Unii Europejskiej. Dążąc do europejskiego modelu bezpieczeństwa*, Urząd Publikacji Unii Europejskiej, Luksemburg 2010; Traktat Północnoatlantycki sporządzony w Waszyngtonie dnia 4 kwietnia 1949 r., Dz. U. 2000, nr 87, poz. 970; Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską, sporządzony w Lizbonie dnia 13 grudnia 2007 r., Dz. U. 2009, nr 203, poz. 1569; Wersja skonsolidowana Traktatu o funkcjonowaniu Unii Europejskiej, Dz. Urz. UE C 326/47 z 26.10.2012.

BEZPIECZEŃSTWO FINANSOWE – element szerzej rozumianego → b e z p i e c z e ń s t w a e k o n o m i c z n g o, które z kolei jest częścią → b e z p i e c z e ń s t w a n a r o d o w e g o państwa. Istotą bezpieczeństwa finansowego jest

brak → z a g r o ż e ń [t. 4] w kilku najważniejszych sferach, w jakich rozpatrywać można finanse, a mianowicie w obszarze finansów publicznych, finansów przedsiębiorstw, ubezpieczeń, bankowości oraz finansów osobistych gospodarstw domowych. W każdej z tych sfer inne czynniki determinują istnienie zagrożeń oraz poczucie → b e z p i e c z e ń s t w a , choć istnieje także gama determinant, która mają charakter wspólny dla wszystkich sfer bezpieczeństwa finansowego.

Analiza finansów odnosząca się do idei bezpieczeństwa jest wyrazem włączenia dyskursu dotyczącego procesów ekonomicznych, podobnie jak wielu innych sfer działania społeczno-politycznego w ciągu ostatnich kilkunastu lat, do sekurytyzacji, a więc procesu rozumienia, analizy i postrzegania świata, którego punktem centralnym jest bezpieczeństwo. Badacze wskazują na szereg istotnych cech, które łączą te zagadnienia, przy czym za kategorię najistotniejszą należy uznać ryzyko, będące jedną z centralnych kategorii zarówno analiz odnoszących się do bezpieczeństwa, jak i do finansów.

Bezpieczeństwo finansowe na poziomie państwa mierzone jest zwykle przy użyciu ratingów, które określają możliwość danego państwa w zakresie wywiązywania się ze swoich zobowiązań finansowych. Na świecie istnieje ok. 100 agencji ratingowych, jednak za najbardziej profesjonalne i wiarygodne uznaje się Moody's Investor Service, Standard & Poor's oraz Fitch Ratings. Procedura oceny jest wielowymiarowa, jest też często poddawana krytyce. Inną znaną metodą oceny bezpieczeństwa finansowego państwa jest stosunek długu publicznego w relacji do produktu krajowego brutto (PKB). Przyjmuje się, że państwo, które wyemitowało i wprowadziło na rynek mniej papierów dłużnych, jest mniej zadłużone i ponosi niższe koszty obsługi zadłużenia. Bezpieczeństwo finansowe w państwie wiąże się na ogół z dyscypliną finansów publicznych, którą osiąga się poprzez racjonalizację wydatków i skuteczne realizowanie dochodów budżetowych. W przypadku przedsiębiorstw bezpieczeństwo finansowe zasadniczo rozumiane jest jako możliwość realizowania przez przedsiębiorstwo podstawowego celu, jakim jest generowanie zysku. Objawami zagrożeń dla bezpieczeństwa finansowego przedsiębiorstw są przypadki m.in.:

- niekorzystnego kształtowania się wartości wskaźników finansowych,
- niezdolności do terminowej spłaty zobowiązań, zwłaszcza kredytów,
- wycofania zasilania finansowego przez banki lub dostawców,
- zastępowania przez dostawców sprzedaży kredytowej przez transakcje gotówkowe,
- braku środków na inwestycje lub nawet na odtwarzanie wartości środków trwałych,
- braku możliwości sfinansowania uruchomienia produkcji ważnych, nowych wyrobów lub szczególnie ważnych inwestycji,
- finansowania działalności głównie z kredytu kupieckiego,
- występowania poważnych strat z działalności operacyjnej (zwłaszcza powtarzających się w kolejnych latach),

- istotnie ujemnych wartości przepływów środków pieniężnych netto,
- niewypełniania ustalonych z bankiem warunków umów kredytowych,
- przekroczenia limitów kredytowych.

Zagrożenie dla bezpieczeństwa finansowego przedsiębiorstwa utożsamia się najczęściej z jego pogarszającą się kondycją finansową, która prowadzi do trwałej utraty płynności finansowej. Przez pojęcie kondycji finansowej przedsiębiorstwa należy rozumieć sytuację czy pozycję finansową przedsiębiorstwa, która jest rezultatem podejmowanych decyzji gospodarczych i związanych z tym perspektyw. Ponadto oznacza stan osiągniętych i oczekiwanych rezultatów oraz uwarunkowań finansowych dotyczących danego momentu. Wśród czynników wymienianych jako warunkujące kondycję finansową przedsiębiorstwa wymienia się m.in.:

- strukturę finansową przedsiębiorstwa,
- płynność finansową,
- wypłacalność,
- zdolności adaptacyjne przedsiębiorstwa,
- posiadane zasoby ekonomiczne, w tym potencjał produkcyjny,
- zdolność do generowania zysku,
- zdolność do maksymalizacji wartości rynkowej przedsiębiorstwa. Do najpopularniejszych i najczęściej stosowanych metod pomiaru kondycji finansowej przedsiębiorstwa umożliwiających ocenę poziomu jego bezpieczeństwa finansowego należy analiza wskaźnikowa. Polega ona na różnokierunkowych przekształceniach i powiązaniach danych liczbowych zawartych w sprawozdaniach finansowych. Ogólnie wskaźniki finansowe obrazujące kondycję finansową przedsiębiorstwa można zakwalifikować do 4 grup, są to:
- wskaźniki płynności,
- wskaźniki zadłużenia,
- wskaźniki sprawności działania,
- wskaźniki rentowności.

Narzędziem umożliwiającym bardziej zaawansowaną ocenę poziomu bezpieczeństwa finansowego przedsiębiorstwa jest system wczesnego ostrzegania, którego rolą jest jednak nie tylko wykorzystywanie sygnałów z otoczenia przedsiębiorstwa i jego wnętrza umożliwiających wczesną identyfikację zagrożeń finansowych, lecz również identyfikacja szans, by tym samym minimalizować ryzyko działalności lub wzmacniać potencjalny sukces przedsiębiorstwa.

W przypadku gospodarstw domowych bezpieczeństwo finansowe definiuje się i ocenia odmiennie, określając je jako możliwość dostępu do środków finansowych w celu utrzymania odpowiedniego poziomu życia. Istnieją wskaźniki finansowe będące narzędziami analitycznymi służącymi do oceny bezpieczeństwa finansowego i dobrobytu gospodarstw domowych. Wykorzystuje się w nich parametry takie jak adekwatność środków na wydatki nadzwyczajne, ogólne stopy oszczędności, wydatki

medyczne i na składki ubezpieczeniowe, poziom zadłużenia i ryzyko niewypłacalności oraz koszty mieszkaniowe i przystępność cenową.

Najczęściej jako wskaźniki bezpieczeństwa finansowego przyjmuje się narzędzia umożliwiające udzielenie odpowiedzi na pytania:

- czy gospodarstwo domowe jest w stanie utrzymać odpowiedni poziom płynności na wypadek → s y t u a c j i k r y z y s o w y c h [t. 4]?
- czy gospodarstwo domowe może uniknąć nadmiernego zadłużenia?
- jakie konkretne progi lub punkty zaniechania wydatkowania są sugerowane przy ocenie bezpieczeństwa finansowego gospodarstwa domowego?

Wśród czynników determinujących poziom bezpieczeństwa finansowego gospodarstw domowych wskazuje się cechy demograficzne członków gospodarstwa domowego takie, jak: wiek, stan cywilny i rasa, pochodzenie etniczne, kompetencje finansowe, czyli umiejętność unikania błędów w podejmowaniu decyzji finansowych, ograniczenia kredytowe, możliwość dostępu do instytucji finansowych determinująca decyzje finansowe takie jak oszczędzanie, zaciąganie pożyczek i akumulacje aktywów, postawy finansowe wpływające na decyzje finansowe gospodarstw domowych takie jak tolerancja ryzyka oraz nawyki dotyczące oszczędzania i wydawania pieniędzy.

Bezpieczeństwo finansowe jest także rozpatrywane na poziomie indywidualnym. Istnieją powody, by sądzić, że bezpieczeństwo finansowe rozumiane jako poczucie, że jednostka może sobie pozwolić na rzeczy, których potrzebuje, teraz i w dającej się przewidzieć przyszłości, powinny wspierać zdolność ludzi do znalezienia satysfakcji i sensu życia. Szereg teoretycznych koncepcji sugeruje, że rozwój jednostki zależy od zaspokojenia podstawowych ludzkich potrzeb, a bezpieczeństwo finansowe może pomóc ludziom w zaspokojeniu wielu z nich. Środki finansowe umożliwiają zaspokojenie podstawowych potrzeb związanych z przetrwaniem, ponieważ można je wymienić na schronienie, jedzenie i czystą wodę pitną. Jednak badania wskazują, że potrzeby psychologiczne można również zaspokoić środkami ekonomicznymi. Według niektórych badań już sama obecność pieniędzy budzi poczucie autonomii i samodzielności. Wydawanie pieniędzy na doświadczenia, takie jak jedzenie w restauracji, chodzenie na koncerty, może wzmocnić poczucie przynależności. Bogactwo ekonomiczne jest powszechnie postrzegane jako wskaźnik kompetencji osobistych, a zdobywanie i wydawanie pieniędzy może być sposobem na uzyskanie poczucia własnej wartości lub zrekompensowania niskiej samooceny.

Wobec tego, że pieniądze mogą pomóc ludziom w zaspokojeniu szeregu potrzeb psychologicznych, utrzymanie bezpieczeństwa finansowego jest ważnym elementem funkcjonowania społecznego i rozwoju psychicznego. W przeciwieństwie do tego niepewność finansowa – definiowana jako niepewność, czy ktoś jest w stanie sobie pozwolić na rzeczy, których potrzebuje teraz i w dającej się przewidzieć przyszłości – okazuje się pogarszać kondycję psychiczną jednostki. Ponadto badania wskazują, że niepewność finansowa może prowadzić do deficytu w funkcjonowaniu poznawczym

oraz że niepewność finansowa jest związana z gorszym podejmowaniem decyzji finansowych.

Jakub Idzik, Rafał Klepka

A.A. Abeyta, C. Routledge, M. Kersten, C.R. Cox, *The Existential Cost of Economic Insecurity: Threatened Financial Security Undercuts Meaning*, „The Journal of Social Psychology" 2017, vol. 157, iss. 6; P. Dec, *Rola systemu wczesnego ostrzegania w realizacji strategii*, „Ekonomika i Organizacja Przedsiębiorstwa" 2006, nr 10; M. de Goede, *Financial Security*, [w:] *The Routledge Handbook of New Security Studies*, J.P. Burgess (ed.), Routledge, New York–London 2010; S. Griffith-Jones, *International Financial Stability and Market Efficiency as a Global Public Good*, [w:] *Providing Global Public Goods*, I. Kaul, P. Conceicao, K. Le Goulven, R. Mendoza (eds.), Oxford University Press, New York 2003; R.Y. Han, *Financial Internationalization and Financial Security Issues*, „Open Access Library Journal" 2018, vol. 5 (9); R. Klepka, *Kryzys w przedsiębiorstwie, jego symptomy i przyczyny*, „Studia i Materiały. Miscellanea Oeconomicae" 2013, nr 2; tenże, *Specyfika kryzysu finansowego w przedsiębiorstwie*, „Studia i Prace Wydziału Nauk Ekonomicznych i Zarządzania" 2013, nr 32, t. 2; J.M. Lee, K.T. Kim, *Assessing Financial Security of Low-Income Households in the United States*, „Journal of Poverty" 2016, vol. 20, iss. 3; K. Raczkowski, *Bezpieczeństwo finansowe*, [w:] *Ekonomika bezpieczeństwa państwa w zarysie*, J. Płaczek (red.), Wydawnictwo Difin, Warszawa 2014.

BEZPIECZEŃSTWO IDEOLOGICZNE (ang. *ideological security*) – jeden z rodzajów → b e z p i e c z e ń s t w a , wyłoniony na podstawie kryterium przedmiotowego, traktowany również jako dziedzina (subkategoria) → b e z p i e c z e ń s t w a n a r o d o w e g o . Specyficzny charakter bezpieczeństwa ideologicznego, warstwa semantyczna tego pojęcia oraz jego stosunkowo wąski zakres przedmiotowy powodują, że termin ten rzadko pojawia się w literaturze przedmiotu na oznaczenie osobnej kategorii, rodzaju bądź typu bezpieczeństwa. Biorąc pod uwagę fakt, iż ideologia – będąca wyznacznikiem tego rodzaju bezpieczeństwa – jest terminem używanym do określenia zespołu poglądów, ocen, opinii, celów i wartości politycznych danej grupy społecznej, które stanowią o poczuciu jej grupowej tożsamości, bezpieczeństwo ideologiczne jawi się jako element → b e z p i e c z e ń s t w a p o l i t y c z n e g o , ekonomicznego, a nawet kulturowego i religijnego. Często – w pejoratywnym znaczeniu ideologii – wynika to z wyideologizowanego, partykularnego, stronniczego i zafałszowanego obrazu rzeczywistości kształtowanej przez konkretne interesy konkretnych grup społecznych w sferze polityki, ekonomii i preferowanego światopoglądu. Bezpieczeństwo ideologiczne można zatem rozpatrywać z punktu widzenia jego pozytywnego charakteru (dążenie do wypracowania w społeczeństwie wspólnego światopoglądu mającego służyć realizacji → i n t e r e s ó w n a r o d o w y c h [t. 2]) oraz negatywnego (ograniczanie wpływów ideologii obcych i skrajnych).

W. Kitler bezpieczeństwem ideologicznym nazywa właśnie proces obejmujący różnorodne działania i środki z zakresu bezpieczeństwa narodowego (bądź bezpieczeństwa w sensie generalnym, a więc → b e z p i e c z e ń s t w a p o l i t y c z n e g o , → b e z p i e c z e ń s t w a m i l i t a r n e g o , → b e z p i e c z e ń s t w a

ekonomicznego, → bezpieczeństwa społecznego, → bezpieczeństwa kulturowego, → bezpieczeństwa energetycznego, →bezpieczeństwa ekologicznegoi → bezpieczeństwa informacyjnego), których głównym celem jest utrwalenie i kształtowanie wspólnoty światopoglądowej w dążeniu do realizacji poszczególnych interesów narodowych, przeciwdziałanie wszelkim ideologiom o skrajnym zabarwieniu oraz ochrona przed różnymi teoriami postulującymi bądź uzasadniającymi działania o negatywnych konsekwencjach dla narodowego interesu. Bezpieczeństwo ideologiczne, poza wspomnianą ochroną państwa i społeczeństwa przed działaniami destrukcyjnymi dla wewnętrznego ładu i porządku konstytucyjnego, charakteryzuje się też działaniami zmierzającymi do zapewnienia przetrwania, rozwoju i wolności wyznawania innych niż uznawana powszechnie ideologii (zarówno świeckich, jak i religijnych) pod warunkiem, że nie niosą one za sobą szkodliwych dla państwa i narodu rozwiązań ideowych (ideologia, obok → strategii [t. 4] i religii w XX w., na co zwraca się uwagę również współcześnie, była uznawana za jeden z niematerialnych elementów/czynników globalnego → środowiska bezpieczeństwa [t. 4] państwa). Oczywiście należy dokonać tu rozróżnienia na bezpieczeństwo ideologiczne w sensie generalnym (odnoszące się do ideologii preferowanej przez społeczeństwo, znaczną jego część lub określoną grupę społeczną) oraz w sensie partykularnym (odnoszące się do ideologii „wyznawanej" przez wąską grupę sprawującą władzę w państwie albo o nią zabiegającą).

Bezpieczeństwo ideologiczne, biorąc pod uwagę jego podmiotowy charakter i zakres oddziaływania, można rozpatrywać, uwzględniając podział na perspektywę wewnętrzną i zewnętrzną. W pierwszym przypadku działalność instytucji i podmiotów odpowiedzialnych za zapewnienie bezpieczeństwa ideologicznego skupiać się będzie na ograniczeniu działalności (wpływu na społeczeństwo) partii politycznych, grup społecznych, grup nacisku politycznego oraz grup religijnych, które realizując swoje partykularne interesy, propagują i rozpowszechniają ideologie niezgodne z podstawowymi zasadami ustrojowymi państwa. Natomiast w drugim przypadku zapewnienie bezpieczeństwa ideologicznego polegać będzie na ograniczeniu działania państw lub innych podmiotów stosunków międzynarodowych, które szerzą skrajne ideologie oraz podejmują starania o dokonanie zmian ustrojowych w rejonie swojego bezpośredniego oddziaływania. Zarówno pierwsze, jak i drugie ujęcie bezpieczeństwa ideologicznego kładzie nacisk na czynnik ochrony porządku ustrojowego (konstytucyjnego) państwa oraz szeroko pojętego porządku aksjologicznego przed bezprawnym i sprzecznym z przyjętym systemem wartości oddziaływaniem innych (skrajnych) ideologii. Silne zakorzenienie w realistycznym paradygmacie stosunków międzypaństwowych pozwala na stwierdzenie, że istotą bezpieczeństwa jest zapewnienie istnienia, przetrwania i ciągłości państwowej, a więc realizacja interesów narodowych (ochrona głównie przed czynnikami zewnętrznymi) niezależnie od zideologizowanej rywalizacji

i nieuchronnego konfliktu interesów w sferze bezpieczeństwa. To właśnie wiek XX upłynął pod znakiem dominacji takich radykalnych ideologii jak → f a s z y z m [t. 2] czy → k o m u n i z m [t. 2], a fakt stopniowego zastępowania ideologii innymi, pokrewnymi → z a g r o ż e n i a m i [t. 4] dla narodowego i międzynarodowego ładu w XXI w., np. fundamentalizmami, nie umniejsza znaczenia ideologii jako czynnika decydującego o stanie bezpieczeństwa w wymiarze wewnętrznym i zewnętrznym. Jak bowiem podaje W. Pokruszyński, należy uwypuklić:

> problem ideologiczno-polityczny jako jedno z podstawowych uwarunkowań bezpieczeństwa narodowego w systemie sojuszniczym (UE), w którym państwa członkowskie mają różne ideologie, a także swoje polityki i strategie bezpieczeństwa.

Podkreślenia wymaga również fakt, że związki ideologii i polityki na płaszczyźnie zapewniania (czy też realizacji) bezpieczeństwa poszczególnych państw są na tyle trwałe, iż bezpieczeństwo ideologiczne nierzadko traktowane jest w literaturze przedmiotu jako aksjologiczna (odwołująca się do konkretnych wartości) subkategoria bezpieczeństwa politycznego (czyli pewności przetrwania, rozwoju państwa i wewnętrznej stabilności rządów). Bezpieczeństwo ideologiczne w tym kontekście jawi się zatem jako pojęcie odnoszące się do pewności przetrwania i rozwoju ideologii, która stanowi fundament panującego w państwie systemu rządów.

Praktyczny wymiar bezpieczeństwa ideologicznego pozwala na wyodrębnienie jego podtypów, które z jednej strony konkretyzują fazy (etapy) zapewniania tego rodzaju bezpieczeństwa, rozumianego jako pewien ustrukturyzowany proces, a z drugiej strony – dookreślają jego przedmiotowy charakter. E. Maj wymienia następujące podtypy bezpieczeństwa ideologicznego:

- prawno-polityczny – odpowiada za identyfikowanie zagrożeń i kształtowanie podstaw ochrony interesów narodowych na płaszczyźnie ustawodawczej (legislacyjnej);
- organizacyjny – decyduje o ustaleniu zasad powoływania instytucji (struktur) państwowych (politycznych) na podstawie konstytutywnych dla państwa wartości (idee);
- personalny – pozwala na dobór ludzi odpowiednich do piastowania funkcji związanych z wykonywaniem zawodów zaufania publicznego, a więc cieszących się społeczną aprobatą i autorytetem;
- środowiskowy – decyduje o ograniczeniu negatywnego wpływu określonych jednostek bądź grup społecznych na najbliższe otoczenie w celu wzmocnienia bezpieczeństwa narodu i państwa.

Ideologia jako termin będący podstawą do wyodrębnienia bezpieczeństwa ideologicznego spośród innych typów bezpieczeństwa wg J. Filipkowskiego stanowi teorię służącą do opisu rzeczywistości społecznej, zawierającą pewien zasób przeświadczeń dotyczących modelu dobrego („idealnego") społeczeństwa i określającą

metody i sposoby przeprowadzenia przemian społecznych w kierunku tego, „jak być powinno", a także środki potrzebne do tego. Odpowiedź na to pytanie uzależniona jest (w sensie subiektywnym) od założeń konkretnej ideologii. Różne ideologie we właściwy sobie sposób definiują wspomniany stan. Niezależnie od uznania konserwatyzmu, liberalizmu, anarchizmu, socjalizmu, komunizmu czy → n a c j o n a l i z m u [t. 3] za ideologię wiodącą w procesie konceptualizacji wizji społeczeństwa, państwa i jego ustroju, bezpieczeństwem ideologicznym można nazwać proces tworzenia i ochrony zestawu wartości i idei istotnych z punktu widzenia prawidłowego funkcjonowania państwa. Sprawa jest tym bardziej skomplikowana, że każde ideologicznie usposobione środowisko społeczno-polityczne uznaje własny światopogląd za uprawniony do formułowania podstaw bezpieczeństwa – w tym także ideologicznego – państwa.

Posiłkując się bardzo uproszczonym schematem idei będących konstytutywnymi dla poszczególnych ideologii, należy zaznaczyć, że np. dla konserwatystów podstawy bezpieczeństwa ideologicznego państwa stanowią: religia (jako ostoja porządku i stabilności społecznej), własność (jako dobro dziedziczone, strzeżone przez państwo), rodzina (jako naturalna i trwała wspólnota), wolność (jako odzwierciedlenie tradycyjnego i zwyczajowego porządku prawnego) i prawo (jako historycznie kształtowane normy zasługujące na bezwzględny szacunek). Do wyznaczników tych w ideologii liberalizmu zalicza się: jednostkę (jako podmiot → p r a w c z ł o w i e k a [t. 3] i obywatela), własność (jako wyznacznik niezbywalnego prawa do posiadania prywatnego mienia), wolność (jako bezsprzeczny element myśli liberalnej w aspekcie ekonomicznym, politycznym, społecznym i światopoglądowym – w kontekście wolnego rynku, pluralizmu politycznego, wolności słowa, wyznania, pochodzenia, orientacji seksualnej itp.). Dla anarchistów naczelnymi ideami są: wolność (jako swobodny wybór celu i sposobu jego realizacji przez jednostkę) oraz społeczeństwo (jako wspólnota, w której jednostka osiąga stan wolności i autonomii). W socjalizmie kluczowymi ideami są zaś: własność państwowa (jako ograniczenie dla własności prywatnej), równość i sprawiedliwość społeczna (jako eliminacja klasowych barier społecznych), wolność (jako wolność od wyzysku i ograniczeń startu życiowego) i praca (jako podstawa godności człowieka i wyznacznik wartości w społeczeństwie). W komunizmie natomiast główne idee to: brak własności prywatnej (jako warunek równości społecznej), egalitaryzm (jako przeciwieństwo elitaryzmu), sprawiedliwość (jako realizacja hasła „każdemu według potrzeb"), wolność (jako wyzwolenie spod dominacji systemu kapitalistycznego) i bezpaństwowe społeczeństwo (jako eliminacja bodźca skłaniającego do wyzysku, czyli państwa). Podstawami bezpieczeństwa ideologicznego dla nacjonalistów są zaś: idea państwa narodowego (jako suwerenny, nienaruszalny byt kulturowy), naród (jako najwyższe dobro i wartość), solidarność narodowa (jako rezultat współdziałania wszystkich członków danego narodu), tożsamość narodowa (jako najważniejszy składnik tożsamości jednostki) oraz interes narodowy (jako cel, którego realizacja jest nadrzędna w stosunku do interesów poszczególnych jednostek).

Podczas określania istoty bezpieczeństwa ideologicznego ważne jest wskazanie na pewien zakres wewnętrznej spoistości danej grupy czy też większej społeczności, która znajduje odzwierciedlenie w pojęciu tożsamości ideowej (ideologicznej). Tożsamość ta, charakteryzująca się odczuwaniem swoistej więzi wspólnotowej opartej na konkretnych ideach i wartościach decydujących o poczuciu bezpieczeństwa, winna odznaczać się: po pierwsze – wewnętrzną spójnością (spoistością), przesądzającą o sposobie funkcjonowania jednostki w środowisku określonej wspólnoty; po drugie – poczuciem odrębności od otoczenia, pozwalającym na identyfikację cech wyróżniających podmiot spośród innych funkcjonujących w otoczeniu oraz ułatwiającym integrację z innymi podmiotami charakteryzującymi się zbieżnymi lub podobnymi cechami ideowymi; po trzecie – poczuciem ciągłości lub niezmienności, opartym na doświadczeniach indywidualnych i zbiorowych; oraz po czwarte – poczuciem posiadania wewnętrznej treści, decydującym o motywach działań, uczuciach i postawach w stosunku do innych. W ten sposób rozumiana tożsamość ideowa jest istotnym odnośnikiem do procesu zapewniania bezpieczeństwa ideologicznego, ponieważ w całym tym procesie pełni wiele funkcji społecznych. Z jednej strony daje poczucie bezpieczeństwa i świadomość niezagrożenia własnych przekonań i światopoglądu, a z drugiej podkreślanie grupowej odrębności może być bodźcem do narzucania innym własnej ideologii, co skutkować może rozwojem fundamentalizmu, brakiem tolerancji i bezpodstawną → a g r e s j ą . Bezpieczeństwo ideologiczne jest więc w znacznej mierze dookreślane jego zagrożeniami.

Bezpieczeństwo ideologiczne oraz jego zagrożenia można rozpatrywać z obiektywnego lub subiektywnego punktu widzenia. Choć istniejące w teorii nauk społecznych pojęcie uśrednionej ideologii publicznej synergicznie łączy w sobie zarówno obiektywne, jak i subiektywne aspekty ideologicznego dyskursu, to wspomniany podział wydaje się jednak uzasadniony. M. Kowalski pisze o prawdopodobieństwie istnienia uśrednionej ideologii publicznej, która jest „złożona ze stanowisk na rozmaite tematy społeczne, co do których istnieje jawna bądź tylko milcząca zgoda większości społeczeństwa". Zatem bezpieczeństwo ideologiczne w sensie obiektywnym dotyczyć będzie ochrony przed zagrożeniem spowodowanym wszelkim działaniem lub zaniechaniem działania skutkującym ograniczeniami w zakresie wolności słowa, swobody sumienia i wyznania. W tym sensie bezpieczeństwo ideologiczne to ochrona przed negatywnym oddziaływaniem zasad innych ideologii, sprzecznych z interesem społeczeństwa, interesem narodowym, interesem państwa i jego racją stanu. Obiektywny charakter → z a g r o ż e ń b e z p i e c z e ń s t w a [t. 4] ideologicznego świadczy z jednej strony o tym, że ich występowanie i oddziaływanie mogą być niezależne od świadomości człowieka, ale z drugiej strony człowiek ma realny wpływ na kształtowanie systemu ochrony przed tego typu zagrożeniami. Bezpieczeństwo ideologiczne (wraz z jego zagrożeniami) może mieć także bardzo subiektywny charakter i może zależeć od rodzaju „wyznawanej" przez społeczeństwo lub konkretną grupę ideologii.

Subiektywny stan bezpieczeństwa ideologicznego uwarunkowany jest przeżyciami, poglądami i ocenami konkretnego podmiotu. W takim przypadku zagrożeniem dla bezpieczeństwa ideologicznego będzie działanie albo zaniechanie działania sprzeczne z przyjętą (np. przez partię rządzącą) ideologią.

Istotne w tym miejscu będzie przytoczenie ujęcia teoretycznego D. Freia, który obiektywne i subiektywne aspekty zagrożeń bezpieczeństwa państwa sklasyfikował w 4 stanach postrzegania bezpieczeństwa przez społeczeństwo i władzę oraz jego dostosowanie do wymogów charakterystycznych dla ideologicznego wymiaru bezpieczeństwa:

- stan braku bezpieczeństwa – będzie występował w sytuacji, kiedy zagrożenie dla ładu ideologicznego danego systemu (w sensie aksjologicznym lub formalnym) będzie duże, a jego postrzeganie adekwatnie prawidłowe;
- stan obsesji – będzie następował wtedy, gdy nieznaczne zagrożenie wspomnianego porządku określane będzie jako duże (czyli nieadekwatnie do stanu faktycznego);
- stan fałszywego bezpieczeństwa – określa sytuację poważnego zagrożenia, nieadekwatnie postrzeganego jako niewielkie;
- stan bezpieczeństwa – bagatelizowanie zagrożenia (w przypadku uświadomienia sobie jego znaczenia) wydaje się najpoważniejszym zaniechaniem w kontekście zapewnienia stanu bezpieczeństwa – czwartego stanu, występującego kiedy nieznaczne zagrożenie jest postrzegane prawidłowo.

Biorąc pod uwagę 2 stany, skrajnie się od siebie różniące, a więc stan braku bezpieczeństwa i stan bezpieczeństwa, w kontekście występowania konkretnego rodzaju zagrożenia ideologicznego, np. komunizmu czy fundamentalizmu islamskiego (→ f u n d a m e n t a l i z m r e l i g i j n y [t. 2]), można dojść do następujących konstatacji. W przypadku działalności w państwie grup prokomunistycznych stan braku bezpieczeństwa będzie oznaczał, że faktyczne zagrożenie (związane m.in. z rozprzestrzenianiem się w społeczeństwie ideologii komunistycznej, działalnością odśrodkowych ugrupowań i formacji sprzeciwiających się demokratycznym standardom państwa prawa, postulowaniem zniesienia własności prywatnej, ideą robotniczej rewolucji i dominującą rolą totalitarnie usposobionej partii, wszechobecną → c e n z u r ą i tworzeniem nowomowy czy walką z jakimkolwiek przejawem religijności) postrzegane jest przez państwo prawidłowo, a więc jako wymagające rychłej interwencji → s p o ł e c z e ń s t w a o b y w a t e l s k i e g o [t. 4], instytucji i służb państwa w celu jego wyeliminowania. Natomiast w przypadku zagrożenia takiego jak fundamentalizm islamski stan bezpieczeństwa będzie osiągnięty wtedy, gdy owo zagrożenie dla danego państwa będzie nieznaczne lub w ogóle nie zaistnieje, a państwo trafnie zidentyfikuje jego poziom jako niewielki. Niski poziom zagrożenia fundamentalizmem islamskim będzie korzystny nie tylko z punktu widzenia bezpieczeństwa ideologicznego (rozumianego jako przeciwdziałanie wszelkim ideologiom o skrajnym zabarwieniu oraz ochrona przed różnymi teoriami postulującymi bądź uzasadniającymi działania

o negatywnych konsekwencjach dla narodowego interesu), ale także bezpieczeństwa narodowego. Wynika to w znacznej mierze z tego, że fundamentalizm (nawet o sprecyzowanym religijnym wydźwięku) występuje w roli ideologii politycznej. Ideologizacja polityki i polityzacja ideologii to procesy, które wydatnie wpływają na respektowanie w państwie i społeczeństwie obowiązujących zasad i wartości. Fundamentalizm islamski jawnie sprzeciwia się świeckim zasadom organizacji struktury państwowej, pluralizmowi politycznemu i religijnemu, a także liberalnej tolerancji, wolności słowa i wyznania, zachodniemu ateizmowi i postawie materialistycznej, stąd też istnieje – postrzegane jako znaczne – zagrożenie dla bezpieczeństwa ideologicznego współczesnego państwa o demokratycznym systemie rządów.

Ideologiczno-polityczne uwarunkowania bezpieczeństwa państwa są niezwykle istotne w procesie konstruowania strategii bezpieczeństwa narodowego, ponieważ występowanie wielu ideologii w jednym państwie lub ich skrajność mogą powodować wzrost liczby sytuacji konfliktogennych, które państwo powinno uwzględnić w ramach prowadzonej polityki. Według W. Sójki zagrożenia państwa o politycznym charakterze przyjmować mogą formę m.in.:

> podważenia suwerenności i integralności terytorialnej przez inny podmiot, słabości rządów prawa i struktur społeczeństwa obywatelskiego, sporów na tle etnicznym i ideologicznym lub religijnym, dążeń do utworzenia nowego państwa, tworzenia strefy wpływów, regionalnej lub lokalnej dominacji, korupcji struktur władzy i aparatu administracji, aktów terrorystycznych przeciwko instytucji państwa, organizacji międzynarodowej, koalicji lub sojuszowi militarnemu.

Problem występowania wielu różnych ideologii oraz fakt, iż bezpieczeństwo ideologiczne polega na zapewnieniu możliwości funkcjonowania tychże ideologii w jednej przestrzeni społecznej, kulturowej i politycznej (czego konsekwencją mogą być spory na tle ideologicznym), sprawiają, że proces zapewnienia bezpieczeństwa ideologicznego może napotkać na wiele trudności. Wynikać one mogą m.in. z subiektywnego charakteru poszczególnych ideologii występujących w państwie, antypaństwowego charakteru niektórych ideologii, wzajemnie wykluczających się zasad poszczególnych ideologii, upraszczania rzeczywistości i spłaszczania jej do wymiaru dwubiegunowego, absolutyzacji twierdzeń będących fundamentem danej ideologii, utopijnego wymiaru ideologii lub wywyższania tzw. myślenia życzeniowego ponad rzetelną analizę realnej (faktycznej) rzeczywistości. Wspomniane trudności wynikać mogą także z nieskuteczności polityki i ideologii w sytuacji nieznalezienia zwolenników angażujących się we wcielanie określonych wytycznych w życie. Istnieje też uzasadniona obawa, że założenia ideologii oficjalnie panującej w kraju wykluczać będą możliwość funkcjonowania grup o innej ideologii, co podaje w wątpliwość sens bezpieczeństwa ideologicznego – tym bardziej że zasada pluralizmu ideologicznego (a także politycznego, społecznego i ekonomicznego) jest jedną z 3 konstytutywnych zasad (obok zasady suwerenności narodu oraz zasady podziału władzy), na podstawie których funkcjonuje państwo prawa.

Podsumowując, trzeba jednoznacznie stwierdzić, że niezależnie od przyjętej teorii, klasyfikacji, typologii czy konceptualizacji pojęciowej termin bezpieczeństwa ideologicznego, pomimo starań o jego precyzyjne ujęcie naukowe, pozostaje kategorią niezwykle pojemną, którą można traktować jako część, dyscyplinę czy subkategorię bezpieczeństwa narodowego (państwa), a nawet bezpieczeństwa politycznego czy w pewnym sensie również kulturowego. O doniosłości owego stwierdzenia niech świadczy fakt, iż w polskiej przestrzeni naukowo-badawczej, w polskich warunkach uniwersyteckich analizowane pojęcie nie doczekało się dotychczas zwartego monograficznie opracowania, co spowodowane jest zapewne szeregiem wymienionych w powyższym wywodzie czynników związanych z trudnością jego dookreślenia oraz dosyć otwartym katalogiem kategorii klasyfikacyjnych, na podstawie których bezpieczeństwo ideologiczne określane bywa jako konstytutywny element bezpieczeństwa narodowego lub jako osobna kategoria semantyczna. Co ciekawe, oba ujęcia teoretyczne są równie uprawnione. Pozostaje mieć nadzieję, że kwestia bezpieczeństwa ideologicznego jako kategorii badawczej w → n a u k a c h o b e z p i e c z e ń s t w i e [t. 3] doczeka się w nieodległym horyzoncie czasowym szerokiego, komplementarnego i naukowego opracowania monograficznego, na które z pewnością zasługuje.

Paweł Łubiński

Ł. Czekaj, A. Czop, M. Pietrzyk, *Międzynarodowe, regionalne i lokalne aspekty bezpieczeństwa*, Drukarnia Styl Anna Dura, Kraków 2018; K. Dziubka, B. Szlachta, M.L. Nijakowski, *Idee i ideologie we współczesnym świecie*, Wydawnictwo Naukowe PWN, Warszawa 2008; J. Falecki, *Bezpieczeństwo*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; S. Hrebenda, *Mityczne aspekty ideologii*, [w:] *Między realizmem a utopią. Świadomościowo-ideologiczne i polityczne przesłanki pokoju i demokracji na przełomie XX i XXI wieku oraz ich historyczne uwarunkowania*, J. Świeca (red.), Wydawnictwo Uniwersytetu Śląskiego, Katowice 1998; W. Kitler, *Bezpieczeństwo narodowe RP. Podstawowe kategorie, uwarunkowania, system*, AON, Warszawa 2011; A. Heywood, *Ideologie polityczne. Wprowadzenie*, tłum. D. Stasiak, N. Orłowska, M. Habura, Wydawnictwo Naukowe PWN, Warszawa 2008; L.F. Korzeniowski, *Podstawy nauk o bezpieczeństwie*, Wydawnictwo Difin, Warszawa 2017; M. Kowalski, D. Falcman, *Ideologie nauk społecznych – warianty interpretacyjne*, Oficyna Wydawnicza Impuls, Kraków 2012; P. Łubiński, *Bezpieczeństwo ideologiczne*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; tenże, *Naród, nacjonalizm i ruch narodowy z perspektywy politologicznej*, Akademia Wychowania Fizycznego im. Jerzego Kukuczki, Katowice 2018; E. Maj, *Bezpieczeństwo ideologiczne w dyskursie politycznym Narodowej Demokracji*, [w:] *Bezpieczeństwo Europy. Bezpieczeństwo Polski*, t. 1, E. Maj i in. (red.), Wydawnictwo UMCS, Lublin 2016; K. Malak, *Typologia bezpieczeństwa. Nowe wyzwania*, Stosunki-Miedzynarodowe.pl (dostęp 11.01.2019); I. Pawlikowska, *Bezpieczeństwo jako cel polityki zagranicznej państwa*, [w:] *Wstęp do teorii polityki zagranicznej państwa*, R. Zięba (red.),Wydawnictwo Adam Marszałek, Toruń 2004; J. Pawłowski, J. Marczak, K. Gąsiorek, *Definiowanie i uwarunkowania bezpieczeństwa narodowego (państwa)*, [w:] *Podstawy bezpieczeństwa narodowego (państwa)*, J. Pawłowski (red.), Akademia Sztuki Wojennej, Warszawa 2017; J. Schwarzmantel, *Ideology and Politics*, Sage, London 2008; W. Sójka, *Ewolucja środowiska bezpieczeństwa Polski i generowanie nowych kategorii zagrożeń w aspekcie bezpieczeństwa państwa*, [w:] *Metodologia badań bezpieczeństwa narodowego*, t. VIII, P. Sienkiewicz, P. Dela (red.), AON, Warszawa

2016; J. Stańczyk, *Współczesne pojmowanie bezpieczeństwa*, Instytut Studiów Politycznych PAN, Warszawa 1996; R. Tokarczyk, *Współczesne doktryny polityczne*, Wolters Kluwer, Warszawa 2010; G. Ulicka, *Determinanty polityki*, [w:] *Wprowadzenie do nauki o państwie i polityce*, B. Szmulik, M. Żmigrodzki (red.), Wydawnictwo UMCS, Lublin 2007; A. Urbanek, *Bezpieczeństwo kulturowe*, [w:] *Wybrane problemy bezpieczeństwa. Dziedziny bezpieczeństwa*, A. Urbanek (red.), Wydawnictwo Społeczno-Prawne, Słupsk 2013; tenże, *Państwo jako podmiot bezpieczeństwa narodowego – ujęcie dziedzinowe*, [w:] *Wybrane problemy bezpieczeństwa. Dziedziny bezpieczeństwa*, A. Urbanek (red.), Wydawnictwo Społeczno-Prawne, Słupsk 2013; R. Zięba, *Instytucjonalizacja bezpieczeństwa europejskiego. Koncepcje – struktury – funkcjonowanie*, Wydawnictwo Scholar, Warszawa 2004; tenże, *Teoria bezpieczeństwa państwa w ujęciu neorealistycznym*, „Studia Politologiczne" 2018, vol. 49.

BEZPIECZEŃSTWO I HIGIENA PRACY (BHP) – dziedzina wiedzy zajmująca się kształtowaniem właściwych warunków pracy i dotycząca zagadnień z zakresu ergonomii, ekonomiki pracy, medycyny pracy, psychologii pracy i technicznego bezpieczeństwa. Obejmuje zbiór zasad opracowanych w celu zapewnienia bezpiecznego świadczenia pracyw higienicznych warunkach, w tym wyposażenia w odpowiednie środki ochrony. Te zasady dotyczą m.in. kwestii związanych z wymogami techniczno-budowlanymi, jakie muszą spełniać budynki i inne obiekty budowlane, w których znajdują się pomieszczenia pracy. Regulują ponadto normy w zakresie: dróg i przejść (minimalne wymiary, oznaczenia), pomieszczeń pracy (powierzchnie i wysokość, wyposażenie, oświetlenie, temperatura, wilgotność, klimatyzacja / wentylacja, czystość), obsługi maszyn i urządzeń (oznakowanie wyłącznika, zabezpieczenie elementów mogących stwarzać zagrożenie, sprawność, czystość, nadzór), transportu i magazynowania (uprawnienia, rozwiązania techniczne odciążające ręczne przenoszenie ciężarów, określenie miejsc, sposobów i dopuszczalnej wysokości składowania poszczególnych rodzajów materiałów) i innych.

Tworzenie bezpiecznych warunków pracy i motywowanie pracowników do przejawiania bezpiecznych zachowań są warunkowane obowiązkiem nałożonym przez prawo na pracodawcę. Ta odpowiedzialność wynikaz Ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy oraz z wydanych na jej podstawie przepisów wykonawczych. Są wśród nich m.in.: Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 26 września 1997 r. w sprawie ogólnych przepisów bezpieczeństwa i higieny pracy oraz przepisy BHP określające wykonywanie prac w różnych profesjach. Główny ciężar odpowiedzialności za stan bezpieczeństwa i higieny pracy w miejscu pracy w myśl art. 207 § 1 Kodeksu pracy ponosi pracodawca. Jest on zobowiązany chronić zdrowie i życie swoich pracowników przez: właściwą organizację pracy i zapewnienie odpowiednich warunków; egzekwowanie przestrzegania przepisów oraz zasad dotyczących BHP, a w razie stwierdzenia nieprawidłowości wdrożenie działań mających na celu niezwłoczne ich usunięcie i skontrolowanie realizacji wydanych poleceń; reagowanie na zgłaszane potrzeby w zakresie zapewnienia bezpiecznych i higienicznych warunków

pracy oraz dostosowywanie stanowisk pracy zgodnie ze zmieniającymi się standardami; planowanie i rozwój spójnej polityki uwzględniającej zagadnienia techniczne, organizację i warunki pracy, stosunki społeczne oraz wpływ czynników środowiska pracy w celu zapobiegania wypadkom podczas pracy i chorobom zawodowym; zapewnianie szczególnej → o c h r o n y z d r o w i a [t. 3] młodocianym pracownikom, kobietom ciężarnym lub karmiącym piersią oraz osobom niepełnosprawnym; zapewnienie wykonywania nakazów, decyzji i zarządzeń sformułowanych w wyniku przeprowadzonej przez organ nadzoru kontroli; zapewnienie wykonywania zaleceń społecznego inspektora pracy. Każdy pracodawca jest zobligowany posiadać stosowną wiedzę w zakresie nałożonych na niego obowiązków, przepisów i zasad BHP. Powinien on poinformować swoich pracowników o możliwych → z a g r o ż e n i a c h [t. 4] dla życia i zdrowia w miejscu pracy na poszczególnych stanowiskach i w zakresie wykonywanych prac. Oprócz tego pracodawca ma również obowiązek powiadamiać o podejmowanych działaniach ochronnych, zapobiegawczych i eliminujących powstałe zagrożenie (np. awaria), jak również udostępnić → i n f o r m a c j e [t. 2] na temat osób wyznaczonych w miejscu pracy do udzielania → p i e r w s z e j p o m o c y [t. 3] i wykonywania działań na wypadek wystąpienia zagrożenia pożarowego i konieczności przeprowadzenia ewakuacji. W tym celu powinien on zapewnić środki niezbędne do udzielania pomocy przedmedycznej i łączność ze służbami zewnętrznymi.

Oprócz zadań nałożonych na pracodawcę w zakresie bezpieczeństwa i higieny pracy Kodeks pracy określa również obowiązki pracownika w tym zakresie. W myśl zapisów art. 211 powyższej ustawy każdy pracownik jest zobligowany do przestrzegania przepisów i zasad BHP, w tym: zaznajomienia się z odpowiednimi dokumentami, uczestniczenia w szkoleniach z tego zakresu i podchodzenia do egzaminów weryfikujących wiedzę; wykonywania zadań zgodnie z obowiązującymi przepisami i stosowania się do poleceń pracodawcy; dbania o stan i porządek w miejscu pracy oraz stan dostępnego sprzętu i innych urządzeń; stosowania środków ochrony zbiorowej i indywidualnej; wykonywania badań wstępnych, okresowych i kontrolnych oraz stosowania się do wskazań lekarskich; poinformowania o dostrzeżonym zagrożeniu w miejscu pracy; współdziałania z pracodawcą i innymi pracownikami w zakresie obowiązków wynikających z BHP. W sytuacji gdy warunki pracy nie są zgodne z przepisami BHP i stwarzają ryzyko uszczerbku na zdrowiu, a nawet stan zagrożenia życia, pracownik ma prawo powstrzymać się od wykonywania swoich obowiązków, o czym niezwłocznie powinien poinformować swojego przełożonego lub / i pracodawcę.

Niewątpliwie świadome i odpowiedzialne inwestowanie w BHP w miejscu pracy pozwala zapobiegać wielu negatywnym zdarzeniom, takim jak wypadki czy choroby. W dużych zakładach pracy (zatrudniających powyżej 100 pracowników) powoływana jest tzw. służba bezpieczeństwa i higieny pracy – pozwala ona zachować komfortowe warunki świadczenia pracy przez profilaktykę, zapobieganie zagrożeniom i kontrolowanie zasad BHP. Funkcję kontrolną i doradczą w zakresie zasad

→ b e z p i e c z e ń s t w a [t. 1] pełni m.in. przez: sprawdzanie stanu BHP i przestrzegania przepisów; wnioskowanie do pracodawcy o ukaranie pracowników, którzy nie stosują się do przepisów BHP; wstrzymywanie prac urządzeń, które mogą stanowić zagrożenie dla obsługujących je pracowników; odsunięcie pracownika od wykonywania obowiązków w razie przejawiania przez niego zachowania stwarzającego zagrożenie dla siebie i innych; przekazywanie pracodawcy informacji o wykrytych zagrożeniach czy awariach wraz z propozycją ich wyeliminowania; świadczenie pomocy w zakresie opracowywania zasad, zarządzeń, regulaminów, instrukcji postępowań i obowiązków pracowników zarządzających przestrzeganiem zasad BHP i ich opiniowanie; pomoc w identyfikowaniu przyczyn zajść wypadków przy pracy oraz formułowanie rekomendacji i wniosków zaradczych. W służbie BHP można wyodrębnić kilka stanowisk: inspektor ds. bezpieczeństwa i higieny pracy, starszy inspektor ds. bezpieczeństwa i higieny pracy, specjalista ds. BHP, starszy specjalista ds. BHP oraz główny specjalista ds. BHP.

Jeśli pracodawca zatrudnia do 100 pracowników, obowiązki wykonywania zadań służby BHP mogą zostać powierzone pracownikowi zatrudnionemu przy innym zadaniu. Z kolei w zakładach pracy zatrudniających do 10 pracowników (lub 20 w wypadku działalności, dla której ustalono nie wyższą niż trzecia grupa ryzyka w rozumieniu przepisów o ubezpieczeniu społecznym z tytułu chorób zawodowych i wypadków podczas pracy) obowiązki służby bezpieczeństwa i higieny pracy może sprawować sampracodawca po odbyciu odpowiedniego szkolenia.

Szczególnie istotną rolę w zakresie sprawowania nadzoru i kontroli przestrzegania prawa pracy, zwłaszcza w kwestii przepisów BHP czy dotyczących legalności zatrudnienia i wykonywania pracy zarobkowej, odgrywa Państwowa Inspekcja Pracy (PIP). Organ ten działa na podstawie Ustawy z dnia 13 kwietnia 2007 r. o Państwowej Inspekcji Pracy. Jeśli w toku kontroli zostaną obnażone nieprawidłowości związane z nieprzestrzeganiem przepisów lub zasad BHP, to na osobę odpowiedzialną za stan BHP w miejscu pracy może zostać nałożona kara finansowa. Przykładem takich nieprawidłowości są m.in.: brak dotrzymania terminu 30 dni na zawiadomienie właściwego okręgowego i państwowego inspektora pracy o miejscu, rodzaju i zakresie prowadzonej działalności lub wprowadzeniu istotnych zmian technologicznych, mogących powodować zwiększone → r y z y k o zagrożenia dla zdrowia pracowników; brak dopilnowania, aby roboty budowlane czy remontowe dotyczące pomieszczeń pracy były spójne z ich projektem uwzględniającym wymagania BHP; wyposażanie stanowisk pracy w sprzęt, środki ochrony indywidualnej niespełniające wymagań dotyczących oceny zgodności; stosowanie materiałów i procesów technologicznych bez sprawdzenia stopnia ich szkodliwości; niezastosowanie odpowiednich oznaczeń dla substancji chemicznych i mieszanin oraz brak kart charakterystyki produktów; brak zawiadomienia właściwego okręgowego inspektora pracy, prokuratora lub innego właściwego organu o zbiorowym, ciężkim lub śmiertelnym wypadku podczas pracy;

brak zgłoszenia o przypadkach choroby zawodowej czy przedstawianie fałszywych dokumentów na temat okoliczności związanych z wypadkami lub chorobami zawodowymi; brak zastosowania się w określonym terminie do nakazu wydanego przez PIP; utrudnianie organom PIP-u prowadzenia działań w zakresie kontroli miejsca pracy; dopuszczenie do pracy zarobkowej bez zezwolenia właściwego inspektora pracy osoby, która nie ukończyła 16. roku życia.

Gdy naruszenie przepisów BHP przez osobę odpowiedzialną za stan BHP w miejscu pracy nosi znamiona przestępstwa, istnieje konieczność zawiadomienia prokuratora lub innych właściwych organów nadzoru. Oprócz PIP-u funkcję sprawowania nadzoru w tej kwestii pełnią, w zależności od specyfiki danego miejsca pracy, m.in: Wyższy Urząd Górniczy, Urząd Dozoru Technicznego, Inspekcja Transportu Drogowego oraz urzędy nadzoru budowlanego. Przestępstwa dokonane przeciw prawom pracowników określają przepisy Kodeksu karnego. Zgodnie z art. 220 § 1: „Kto, będąc odpowiedzialny za bezpieczeństwo i higienę pracy, nie dopełnia wynikającego stąd obowiązku i przez to naraża pracownika na bezpośrednie niebezpieczeństwo utraty życia albo ciężkiego uszczerbku na zdrowiu, podlega karze pozbawienia wolności do lat 3". W sytuacji jednak nieumyślnego działania § 2 tego artykułu przewiduje grzywnę bądź karę ograniczenia lub pozbawienia wolności do 1 roku.

Bezpieczeństwa i higieny pracy nie należy kojarzyć wyłącznie z koniecznością przestrzegania przepisów. Jest to bowiem nie tylko obowiązek administracyjny, lecz również podstawowy element dobrego zarządzania. Zapewnienie właściwych warunków BHP w miejscu pracy minimalizuje ryzyko wypadków, chorób zawodowych i przyczynia się do usprawnienia codziennej działalności przedsiębiorstwa oraz kreuje jego wizerunek zewnętrzny. Jednym z kluczowych obowiązków prawnych w zakresie BHP nałożonych na pracodawców jest ocena ryzyka zawodowego – jest to fundament właściwego podejścia do spraw związanych z zarządzeniem i konieczny element do stworzenia bezpiecznych i higienicznych warunków pracy. Dzięki właściwie oszacowanym zagrożeniom zdrowotnym w miejscu zatrudnienia łatwiej jest określić, jakie środki, regulaminy czy instrukcje pozwolą zminimalizować ryzyko narażenia pracowników na dane zagrożenie, pozwolą także zapewnić pracownikom dostęp do odpowiednich informacji i szkoleń. Mimo że przepisy nie precyzują dokładnie sposobu, w jaki należy przeprowadzić ocenę ryzyka zawodowego, proces ten obejmuje kilka etapów: gromadzenie informacji i identyfikację zagrożeń, oszacowanie prawdopodobieństwa ich wystąpienia wraz z oceną powagi tych sytuacji, planowanie działań ukierunkowanych na eliminację bądź zminimalizowanie ryzyka oraz dokumentowanie oceny ryzyka. Podczas opracowywania oceny ryzyka warto uwzględnić analizy zdarzeń występujących w przeszłości, statystyki dotyczące chorób zawodowych, porady świadczone przez krajowe organy ds. BHP i związki branżowe, jak również opinie samych pracowników. Co istotne, ocena ryzyka i wynikające z niej działania profilaktyczne i ochronne wymagają bieżącego monitorowania i dostosowywania planów na wypadek pojawienia się nowych czynników

zagrażających zdrowiu. Odpowiednie planowanie w tym zakresie i przewidywanie potencjalnego ryzyka to kluczowa kwestia i najistotniejszy cel BHP.

W ramach środków zapobiegawczych stosowanych w celu zmniejszenia prawdopodobieństwa wystąpienia wypadku podczas pracy lub pojawienia się choroby zawodowej wyodrębnia się: środki ochrony zbiorowej lub środki techniczne (działają bezpośrednio na źródło ryzyka, eliminując lub ograniczając je) oraz środki organizacyjne lub administracyjne (kształtują pozytywną → k u l t u r ę b e z p i e c z e ń s t w a [t. 2] przez bazowanie na zmianie zachowań). W celu optymalizacji działań ukierunkowanych na ochronę zdrowia i życia pracowników należy wymienione środki zapobiegawcze uzupełniać: środkami ochrony (zbiorowe – polegają m.in. na odizolowaniu czynnika ryzyka, np. przez zastosowanie barier fizycznych, rusztowań, siatek chroniących przed upadkiem z wysokości, zainstalowanie wentylacji ogólnej i miejscowej, kabin dźwiękoszczelnych czy ograniczenie czasu narażenia; indywidualne – np. ochraniacze stóp, obuwie ochronne, hełmy, okulary ochronne, środki chroniące przed upadkiem z wysokości) oraz środkami zmniejszającymi ryzyko (m.in. plany ewakuacyjne, plany operacyjno-ratownicze, systemy ostrzegania).

Inwestycje w bezpieczeństwo i higienę pracy są zawsze opłacalne, dlatego ważne jest zapewnienie pracownikom rzetelnych informacji dotyczących BHP w takich sytuacjach jak: przyjęcie do pracy, przeniesienie lub zmiana stanowiska, wprowadzenie zmian technologicznych, zmiana rodzaju lub charakteru zagrożeń w miejscu pracy. Jednym z najistotniejszych czynników decydujących o skuteczności całego systemu bezpieczeństwa jest kultura bezpieczeństwa i higieny w miejscu pracy, przejawiająca się w codziennych działaniach i decyzjach oraz postrzeganiu polityki, celów i zasad dotyczących BHP jako kluczowych wartości dla sprawnego funkcjonowania przedsiębiorstwa.

Żaneta Mrożek, Magdalena Szumiec

Bezpieczeństwo i higiena pracy dotyczą każdego. Praktyczny przewodnik dla pracodawców, Urząd Publikacji Unii Europejskiej, Luksemburg 2016; J. Chojnicki, G. Jarosiewicz, *ABC BHP. Informator dla pracodawców*, Państwowa Inspekcja Pracy, Główny Inspektorat Pracy, Warszawa 2011; *Ogólne zasady BHP*, https://www.biznes. gov.pl/en/publikacje/3257-ogolne-zasady-bhp (dostęp 29.04.2023); *Prawa i obowiązki pracownika w zakresie bhp*, Państwowa Inspekcja Pracy, https://www.pip.gov.pl/ (dostęp 29.04.2023); Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 26 września 1997 r. w sprawie ogólnych przepisów bezpieczeństwa i higieny pracy, tekst jedn. Dz.U. 2003, nr 169, poz. 1650 z późn. zm.; Ustawa z dnia 13 kwietnia 2007 r. o Państwowej Inspekcji Pracy, Dz.U. 2007, nr 89, poz. 589 z późn. zm.; Ustawa z dnia 14 marca 1985 r. o Państwowej Inspekcji Sanitarnej, Dz.U. 2023, poz. 338; Ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy, Dz.U. 1998, nr 21, poz. 94 z późn. zm.

BEZPIECZEŃSTWO INFORMACJI NIEJAWNYCH – w ogólnym rozumieniu dotyczy całokształtu przedsięwzięć technicznych i organizacyjnych ukierunkowanych na zabezpieczenie → i n f o r m a c j i [t. 2] istotnych z punktu widzenia → b e z p i e c z e ń s t w a i podstawowych interesów państwa, w tym również procesów ich przetwarzania.

→ I n f o r m a c j e n i e j a w n e [t. 2] dotyczą najważniejszych obszarów funkcjonowania państwa m.in. w sferze obronności, przemysłu zbrojeniowego, funkcjonowania organów władzy oraz organów i służb systemu bezpieczeństwa państwa, administracji publicznej, jak również pozostałych elementów → i n f r a s t r u k t u r y k r y t y c z n e j [t. 2] państwa, a także jego kluczowych interesów ekonomicznych. Mają też podstawowe znaczenie w procesie wymiany informacji sojuszniczej w ramach międzynarodowych struktur bezpieczeństwa i współpracy. W związku z tym mogą być w zasięgu zainteresowań służb wywiadowczych obcych państw oraz podmiotów pozapaństwowych (organizacji terrorystycznych i grup przestępczych, podmiotów gospodarczych, a nawet organizacji pozarządowych). Przetwarzane mogą być zarówno przez podmioty publiczne (na wszystkich poziomach i w wielu obszarach administracji publicznej), jak i prywatne. Historia tajemnic państwowych sięga początków tej formy organizacji politycznej społeczeństw. Wszystkie organizacje o charakterze politycznym posiadały swoje najpilniej strzeżone tajemnice, które były obiektem zainteresowań przeciwników. Powstawały również różne systemy ich ochrony. W Polsce o budowie systemów ochrony najważniejszych tajemnic dotyczących funkcjonowania państwa we współczesnym rozumieniu tego pojęcia możemy mówić przede wszystkim po odzyskaniu niepodległości w 1918 r. W 20-leciu międzywojennym rozróżniano pojęcia tajemnic państwowych i wojskowych. W okresie Polskiej Rzeczypospolitej Ludowej zasadniczo rozróżniano 2 kategorie najważniejszych tajemnic – państwową i służbową. W 1982 r. została uchwalona ustawa o tajemnicy państwowej i służbowej, która obowiązywała jeszcze prawie 10 lat w okresie III Rzeczypospolitej Polskiej. Wyróżniane były wtedy 2 kategorie tajemnicy państwowej (o klauzulach „tajne" oraz „tajne specjalnego znaczenia"), a także tajemnica służbowa (o klauzuli „poufne").

Wraz ze staraniami Polski o członkostwo w euroatlantyckich strukturach bezpieczeństwa i współpracy – przede wszystkim w → N A T O [t. 3] – oraz związanymi z tym procesem wymogami odnośnie do zapewnienia odpowiedniego poziomu bezpieczeństwa informacji prowadzono prace nad organizacją nowego systemu w tym przedmiocie zgodnie ze standardami tej organizacji, których efektem finalnym była Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych. Ustawa spełniała wymagane kryteria sojusznicze i wprowadzała stosowne rozwiązania, tworząc spójny system ochrony informacji niejawnych. Wprowadzone zostały 2 klauzule tajności w odniesieniu do informacji stanowiących tajemnicę państwową („tajne" i „ściśle tajne") oraz 2 klauzule dotyczące tajemnicy służbowej („zastrzeżone" i „poufne"). Informacje stanowiące tajemnicę państwową podlegały ochronie przez okres 50 lat od daty ich wytworzenia, natomiast w wypadku tajemnicy służbowej okres ten wynosił odpowiednio 2 i 5 lat dla informacji oznaczonych klauzulą „zastrzeżone" i „poufne". Co istotne, zgodnie z ustawą pewne kategorie informacji miały pozostawać chronione bez względu na upływ czasu, mianowicie te uznane przez ustawodawcę za najbardziej wrażliwe (dane identyfikujące funkcjonariuszy służb specjalnych wykonujących

→ c z y n n o ś c i o p e r a c y j n o - r o z p o z n a w c z e , dane identyfikujące tajnych współpracowników służb, czyli osobowych źródeł informacji, oraz informacje niejawne pozyskane od innych państw lub organizacji międzynarodowych, jeżeli taki był warunek ich udostępnienia). Mimo nowoczesnych jak na owe czasy rozwiązań szybkie zmiany cywilizacyjne związane z postępem technologicznym i rozwojem naukowym, nowymi wyzwaniami i → z a g r o ż e n i a m i [t. 4] spowodowały konieczność usprawnienia niektórych elementów funkcjonującego systemu. 5 sierpnia 2010 r. uchwalona została kolejna ustawa o ochronie informacji niejawnych, której zasadniczym celem było uelastycznienie systemu w sposób pozwalający adekwatnie reagować i dostosowywać rozwiązania do szybkich i dynamicznych procesów i zmian współczesnego świata. Zgodnie z zapisami nowej ustawy informacje niejawne to informacje, „których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne". Natomiast ich przetwarzanie stanowią:

> operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie.

Zniesiono obowiązujący przez długi okres podział informacji na tajemnicę państwową i służbową, a informacje niejawne są obecnie klasyfikowane w ramach 4 kategorii, w zależności od stopnia potencjalnej szkody dla państwa, którą mogłoby spowodować ich ujawnienie podmiotom nieuprawnionym. Wyróżnione zostały następujące klauzule:

- „ściśle tajne" – dla informacji, których nieuprawnione ujawnienie spowoduje wyjątkowo poważną szkodę dla Rzeczypospolitej Polskiej (RP) przez to, że:
  - zagrozi niepodległości, → s u w e r e n n o ś c i [t. 4] lub integralności terytorialnej RP;
  - zagrozi bezpieczeństwu wewnętrznemu lub porządkowi konstytucyjnemu RP;
  - zagrozi sojuszom lub pozycji międzynarodowej RP;
  - osłabi gotowość obronną RP;
  - doprowadzi albo może doprowadzić do identyfikacji funkcjonariuszy, → ż o ł n i e r z y [t. 4] lub pracowników służb odpowiedzialnych za realizację zadań → w y w i a d u [t. 4] bądź → k o n t r w y w i a d u [t. 2], którzy wykonują czynności operacyjno-rozpoznawcze;
  - zagrozi albo może zagrozić życiu lub zdrowiu funkcjonariuszy, żołnierzy czy pracowników, którzy wykonują czynności operacyjno-rozpoznawcze, bądź osób udzielających im pomocy w tym zakresie;
  - zagrozi albo może zagrozić życiu lub zdrowiu świadków koronnych bądź osób dla nich najbliższych, osób, którym udzielono środków ochrony i pomocy na podstawie stosownych przepisów;

- „tajne" – dla informacji, których nieuprawnione ujawnienie spowoduje poważną szkodę dla Rzeczypospolitej Polskiej przez to, że:
  - uniemożliwi realizację zadań związanych z ochroną suwerenności lub porządku konstytucyjnego RP;
  - pogorszy stosunki RP innymi państwami lub organizacjami międzynarodowymi;
  - zakłóci przygotowania obronne państwa lub funkcjonowanie → S i ł Z b r o j n y c h R P [t. 4];
  - utrudni wykonywanie czynności operacyjno-rozpoznawczych prowadzonych w celu zapewnienia bezpieczeństwa państwa lub ścigania sprawców zbrodni przez służby albo instytucje do tego uprawnione;
  - w istotny sposób zakłóci funkcjonowanie organów ścigania i wymiaru sprawiedliwości;
  - przyniesie znaczną stratę w interesach ekonomicznych RP;
- „poufne" – w przypadku informacji, których nieuprawnione ujawnienie spowoduje szkodę dla Rzeczypospolitej Polskiej przez to, że:
  - utrudni prowadzenie bieżącej polityki zagranicznej RP;
  - utrudni realizację przedsięwzięć obronnych lub negatywnie wpłynie na zdolność bojową Sił Zbrojnych RP;
  - zakłóci porządek publiczny lub zagrozi bezpieczeństwu obywateli;
  - utrudni wykonywanie zadań służbom albo instytucjom odpowiedzialnym za ochronę bezpieczeństwa lub podstawowych interesów RP;
  - utrudni wykonywanie zadań służbom albo instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwa obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych oraz organom wymiaru sprawiedliwości;
  - zagrozi stabilności systemu finansowego RP;
  - wpłynie niekorzystnie na funkcjonowanie gospodarki narodowej;
- „zastrzeżone" – obejmuje informacje, którym nie nadano wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie → o b r o n y n a r o d o w e j [t. 3], polityki zagranicznej, → b e z p i e c z e ń s t w a p u b l i c z n e g o , przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej.

Zachowano również kategorie informacji podlegających ochronie bez względu na upływ czasu, przy czym nieco rozszerzono ich zakres. Dotyczy to następujących informacji:

- dane mogące doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb i instytucji uprawnionych do wykonywania na podstawie ustawy czynności operacyjno-rozpoznawczych jako funkcjonariuszy, żołnierzy lub pracowników wykonujących te czynności;

- dane mogące doprowadzić do identyfikacji osób, które udzieliły pomocy w zakresie czynności operacyjno-rozpoznawczych służbom i instytucjom uprawnionym do ich wykonywania na podstawie ustawy;
- informacje niejawne uzyskane od organów innych państw lub organizacji międzynarodowych, jeżeli taki był warunek ich udostępnienia.

Zrezygnowano natomiast ze sztywnych i z góry narzuconych okresów ochrony informacji niejawnych w zależności od poszczególnych klauzul. Nadawane są one teraz przez osobę, która jest uprawniona do podpisania dokumentu lub oznaczenia materiału, i podlegają ochronie w ramach danej klauzuli do czasu jej zniesienia bądź zmiany na inną, co z kolei jest możliwe jedynie w przypadku wyrażenia pisemnej zgody przez osobę nadającą albo jej przełożonego po zaistnieniu określonych przesłanek. Osoba, która nadaje klauzule tajności, może jednocześnie określić datę lub wydarzenie, po którym nastąpi jej zniesienie czy zmiana.

Wśród zasad organizacji systemu bezpieczeństwa informacji niejawnych oraz podstawowych środków technicznych i organizacyjnych służących ich ochronie można wskazać m.in. następujące:

- Informacje niejawne mogą być udostępniane wyłącznie osobom uprawnionym zgodnie z obowiązującymi przepisami. Osoba taka musi dawać tzw. rękojmię zachowania tajemnicy, czyli spełniać ustawowe wymogi w zakresie zapewnienia ochrony informacji niejawnych, co stwierdzane jest w ramach stosownych postępowań sprawdzających prowadzonych przez odpowiednie podmioty. Ponadto zgodnie z zasadą wiedzy niezbędnej (z ang. *need-to-know*) informacje mogą być udostępniane osobie uprawnionej do określonego poziomu tajności jedynie w zakresie niezbędnym do pełnienia obowiązków służbowych na zajmowanym stanowisku albo do wykonywania określonych czynności zleconych. Dopuszczenie do pełnienia służby lub wykonywania pracy związanych z dostępem do informacji niejawnych może nastąpić dopiero po odbyciu stosownego szkolenia (nie rzadziej niż raz na 5 lat).
- Przetwarzanie informacji niejawnych musi odbywać się jedynie w określonych warunkach zapewniających ich poufność (zgodnie ze stosownymi wymogami dla poszczególnych klauzul tajności, dotyczącymi m.in. bezpieczeństwa systemów i sieci teleinformatycznych, obiegu dokumentów i innych materiałów, wprowadzenia odpowiednich środków bezpieczeństwa, adekwatnych do stopnia ryzyka związanego z możliwością nieuprawnionego zniszczenia lub ujawnienia informacji niejawnych, w tym tworzenia kancelarii tajnych – obligatoryjnych dla podmiotów przetwarzających informacje o klauzulach „tajne" bądź „ściśle tajne").

Ze względu na rodzaj podmiotów oraz charakter procesów związanych z przetwarzaniem informacji, a także związanymi z nimi określonymi procedurami czy wymogami formalnymi w ramach systemu ochrony informacji niejawnych w Polsce można wyróżnić 3 zasadnicze podsystemy (kategorie):

- Bezpieczeństwa osobowego, które obejmuje w szczególności działalność kontrolną (w tym sprawdzeniową) oraz szkoleniową w odniesieniu do osób, które mają dostęp do informacji niejawnych lub którym się go udziela. W ramach tych czynności prowadzone są postępowania sprawdzające zwykłe, poszerzone i kontrolne (w zależności od pełnionych funkcji, zajmowanych stanowisk czy wykonywanych czynności zleconych oraz odpowiednich klauzul tajności), które mają na celu ustalenie, czy dana osoba daje rękojmię zachowania tajemnicy, i które mogą zakończyć się wydaniem poświadczenia bezpieczeństwa, odmową wydania poświadczenia bezpieczeństwa albo umorzeniem postępowania. Poświadczenie bezpieczeństwa uprawniające do dostępu do informacji o klauzuli „poufne" wydaje się na okres 10 lat, o klauzuli „tajne" na okres 7 lat, a w przypadku klauzuli „ściśle tajne" na okres 5 lat.
- → Bezpieczeństwa teleinformatycznego, dotyczącego całokształtu przedsięwzięć związanych z przetwarzaniem informacji niejawnych z wykorzystaniem systemów i sieci teleinformatycznych. W tym zakresie odpowiednie systemy poddawane są odpowiednim akredytacjom bezpieczeństwa teleinformatycznego, które dla systemów wykorzystywanych do przetwarzania informacji o klauzuli „poufne" i wyższej udzielane są na okres nie dłuższy niż 5 lat. Potwierdzeniem udzielenia akredytacji jest świadectwo akredytacji bezpieczeństwa systemu teleinformatycznego.
- Bezpieczeństwa przemysłowego, które z kolei obejmuje obszar dostępu przedsiębiorców do informacji niejawnych w związku z wykonywaniem umów lub zadań określonych przepisami prawa. Zdolność dostępu w tym przedmiocie stwierdzana jest na podstawie prowadzonych przez odpowiednie służby postępowań bezpieczeństwa przemysłowego. Dokumentem potwierdzającym zdolność dostępu dla informacji o klauzuli „poufne" lub wyższej jest świadectwo bezpieczeństwa przemysłowego, które może określać pełną zdolność (świadectwa pierwszego stopnia), zdolność z wyłączeniem własnych systemów teleinformatycznych danego podmiotu (świadectwa drugiego stopnia) lub zdolność z wyłączeniem przetwarzania w użytkowanych przez podmiot obiektach (świadectwa trzeciego stopnia). Świadectwo bezpieczeństwa przemysłowego o klauzuli „ściśle tajne" potwierdza zdolność do ochrony informacji niejawnych o tej klauzuli przez okres 5 lat, o klauzuli „tajne" przez okres 7 lat i o klauzuli „poufne" przez okres 10 lat od daty jego wystawienia. Natomiast świadectwo bezpieczeństwa przemysłowego o klauzuli „tajne" obejmuje zdolność do ochrony informacji o klauzuli „tajne" i „poufne" odpowiednio przez 7 i 10 lat od daty wystawienia. Świadectwo o klauzuli „poufne" pozwala przetwarzać informacje oznaczone taką klauzulą przez 10 lat od daty wystawienia.

Funkcjonowanie systemu ochrony informacji niejawnych w Polsce jest nadzorowane przez → Agencję Bezpieczeństwa Wewnętrznego (ABW)

i → Służbę Kontrwywiadu Wojskowego [t. 4] (SKW), odpowiednio dla sfery cywilnej i wojskowej. Służby te realizują następujące zadania określone w ustawie o ochronie informacji niejawnych:

- prowadzenie kontroli informacji niejawnych i przestrzegania przepisów obowiązujących w tym zakresie;
- zadania w zakresie bezpieczeństwa systemów teleinformatycznych;
- prowadzenie postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego;
- zapewnianie ochrony informacji niejawnych wymienianych między Rzecząpospolitą Polską a innymi państwami lub organizacjami międzynarodowymi;
- prowadzenie doradztwa i szkoleń w zakresie ochrony informacji niejawnych.

Szef ABW pełni ponadto funkcję krajowej władzy bezpieczeństwa (również w odniesieniu do podmiotów nadzorowanych przez SKW za pośrednictwem szefa tej służby), nadzorując system ochrony informacji niejawnych w odniesieniu do stosunków z innymi państwami lub organizacjami międzynarodowymi (informacji niejawnych międzynarodowych). Odpowiedzialność za ochronę informacji niejawnych – w szczególności za właściwą organizację i funkcjonowanie stosownych systemów w podległych jednostkach organizacyjnych, m.in. organów władzy publicznej różnego szczebla, jednostek podległych tym organom, państwowych osób prawnych, przedsiębiorców ubiegających się o dostęp do informacji niejawnych lub wykonujących zadania albo umowy z nimi związane – spoczywa na ich kierownikach. Są oni również ustawowo zobowiązani do współpracy ze służbami i instytucjami uprawnionymi do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego. Kluczowym podmiotem systemu ochrony informacji niejawnych na poziomie jednostek organizacyjnych jest podlegający bezpośrednio kierownikowi danej jednostki pełnomocnik ochrony informacji niejawnych (POIN), który ma za zadanie zapewniać przestrzeganie przepisów o ochronie informacji niejawnych. Może być wyznaczony również jego zastępca lub zastępcy. W jednostkach większych, gdy istnieje taka potrzeba, mogą być tworzone wyznaczone komórki organizacyjne podległe pełnomocnikom (piony ochrony). Stanowiska pełnomocnika i jego zastępców, a także pracowników pionu ochrony mogą zajmować jedynie osoby, które spełniają określone ustawowo wymagania. Jeżeli w danej jednostce organizacyjnej do przetwarzania informacji niejawnych wykorzystywany jest system teleinformatyczny, w ramach pionu ochrony wyznaczany jest dodatkowo pracownik lub pracownicy pełniący funkcję inspektora bezpieczeństwa teleinformatycznego (odpowiedzialni za weryfikację i kontrolę funkcjonowania tego systemu), a także osoba lub grupa osób niebędące inspektorami bezpieczeństwa teleinformatycznego, które są z kolei odpowiedzialne za prawidłowe funkcjonowanie tego systemu (administratorzy systemu).

Przed pełnomocnikiem ochrony informacji niejawnych postawione zostały następujące ustawowe zadania:

- zapewnienie ochrony informacji niejawnych, w tym stosowanie środków bezpieczeństwa fizycznego;
- zapewnienie ochrony systemów teleinformatycznych, w których są przetwarzane informacje niejawne;
- zarządzanie → r y z y k i e m b e z p i e c z e ń s t w a [t. 3] informacji niejawnych, w szczególności szacowanie ryzyka;
- kontrola ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji, w szczególności okresowa (co najmniej raz na 3 lata) kontrola ewidencji, materiałów i obiegu dokumentów;
- opracowywanie i aktualizowanie wymagającego akceptacji kierownika jednostki organizacyjnej planu ochrony informacji niejawnych w jednostce organizacyjnej, w tym w razie wprowadzenia → s t a n u n a d z w y c z a j n e g o [t. 4], i nadzorowanie jego realizacji;
- prowadzenie szkoleń w zakresie ochrony informacji niejawnych;
- prowadzenie zwykłych postępowań sprawdzających oraz kontrolnych postępowań sprawdzających;
- prowadzenie aktualnego wykazu osób zatrudnionych lub pełniących służbę w jednostce organizacyjnej albo wykonujących czynności zlecone, które mają uprawnienia do dostępu do informacji niejawnych, oraz osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub je cofnięto;
- współpraca z ABW i SKW w określonym zakresie, w szczególności obejmującym przekazywanie danych oraz ewidencję osób związanych z dostępem do informacji niejawnych.

Piotr Swoboda

G. Goryński, *Prawne podstawy ochrony informacji niejawnych w Polsce*, „Colloquium Wydziału Nauk Humanistycznych i Społecznych" 2013, nr 1; B. Jakubus, M. Ryszkowski, *Ochrona informacji niejawnych*, Wydawnictwo Projekt, Warszawa 2001; *Ochrona danych osobowych i informacji niejawnych z uwzględnieniem ogólnego rozporządzenia unijnego*, D. Wociór (red.), C.H.Beck, Warszawa 2016; *Ochrona informacji niejawnych, biznesowych i danych osobowych. Materiały VII Kongresu*, M. Gajos (red.), Krajowe Stowarzyszenie Ochrony Informacji Niejawnych, Uniwersytet Śląski w Katowicach, Katowice 2011; P. Swoboda, *Bezpieczeństwo informacji niejawnych*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, t.j. Dz. U. 2019, poz. 742; S. Zalewski, *Dylematy ochrony informacji niejawnych*, Krajowe Stowarzyszenie Ochrony Informacji Niejawnych, Katowice 2009.

BEZPIECZEŃSTWO INFORMACJI WOJSKOWEJ (ang. *security of military information*) – sięga swymi początkami imperiów starożytnych. Już wówczas kierujący armiami zwracali uwagę na osiąganie i utrzymywanie poufności → i n f o r m a c j i [t. 2] wojskowych; niezawodności ich przesyłania; użyteczności, autentyczności i integralności otrzymywanych informacji; ich dostępności dla osób,

dla których są one przeznaczone, oraz rozliczalności (m.in. jednoznacznego określenia jej nadawcy).

Od wielu stuleci władze państwowe zwracały uwagę na unormowania prawne pozwalające na zabezpieczenie określonych danych przed nieuprawnionymi odbiorcami. Kładziono m.in. bardzo duży nacisk na kary. Miały one odstraszać nieuprawnione osoby pragnące wejść w posiadanie informacji wojskowych.

Obecnie na potencjalnych sprawców przestępstw zagrażających → b e z p i e c z e ń s t w u i n f o r m a c j i wojskowej wpływa dodatkowo aktywność służb specjalnych. Mają one m.in. rozpoznawać wrogą działalność innych państw (i podmiotów pozapaństwowych) wobec potencjału obronnego państwa, a także jej zapobiegać i przeciwdziałać. Chodzi m.in. o ochronę informacji o strukturach i obiektach (np. gospodarczych) o dużym znaczeniu wojskowym oraz zapobieganie wykorzystaniu przez zewnętrznych wrogów państwa informacji wojskowych państwa i związanych z nimi systemów łączności utajnionej do działań zmierzających do obniżenia zdolności obronnych państwa. Stąd wynika ważna rola służb specjalnych w wielu państwach przy organizacji, kontroli bezpieczeństwa informacji wojskowych i nadzorze nad nim.

Obecnie, nie negując wyżej wymienionych działań, najwięcej uwagi badacze skupiają na ochronie informacji wojskowej przed dostępem osób nieuprawnionych. Chodzi nie tylko o utratę informacji, wrogie wykorzystanie i uszkodzenie zasobów informacji wojskowej, którą dysponuje państwo. W związku z rozwojem techniki w XXI w. wzrosło znaczenie ochrony przed zafałszowaniem i zmanipulowaniem informacji wojskowej; uniemożliwieniem dalszego jej przetwarzania; uzyskaniem dostępu przez siły wrogie państwu do poufnych kanałów łączności i wojskowych systemów dowodzenia i wykorzystywaniem ich do rozsyłania nieprawdziwych treści. To ostatnie grozi państwu utratą zdolności dystrybucji informacji wojskowej i/lub jej ograniczoną wiarygodnością dla odbiorców.

Bezpieczeństwo informacji wojskowej definiuje się jako stan i proces. Ten ostatni obejmuje ogół działań podejmowanych przez uprawnione do tego podmioty, w tym stosowane metody i procedury, w celu zabezpieczenia informacji wojskowych przed ich utratą, dostępem osób nieuprawnionych, nieplanowaną modyfikacją oraz dystrybucją informacji uzyskanej drogą nielegalną. Dotyczy on zapewnienia integralności tworzonych, gromadzonych, przetwarzanych, przesyłanych, odbieranych, przechowywanych, kopiowanych oraz niszczonych informacji o charakterze wojskowym związanych np. z poszczególnymi strukturami Sił Zbrojnych czy → i n f r a s t r u k t u r ą k r y t y c z n ą [t. 2].

Działania te podejmowane są zasadniczo wewnątrz kraju. Częściowo dotyczy to też stosunków międzynarodowych. Przykładem może być kontrolowanie zbliżonego stopnia zabezpieczenia informacji wojskowej w państwach tworzących niektóre sojusze wojskowe (np. → N A T O [t. 3]). Jak wiadomo, w XXI w. elementy o charakterze

informacyjnym, a szczególnie informatycznym, mają ogromne znaczenie we wszystkich systemach operacyjnych i systemach wsparcia związanych z obronnością kraju. Powoduje to wzrost znaczenia bezpieczeństwa informacji wojskowej. Mimo znacznego zróżnicowania poziomu ochrony informacji wojskowej między różnymi krajami współcześnie zasoby informacyjne są przechowywane w zdecydowanej większości na innego rodzaju nośnikach niż np. 50 lat temu. Niemniej bezpieczeństwo informacji wojskowej obejmuje nadal również informacje umieszczone np. na papierze.

W XXI w. elementy kluczowe dla bezpieczeństwa informacji wojskowej można podzielić na 4 grupy:

- zasoby informacyjne;
- systemy informacyjne;
- wybrane elementy krytycznej infrastruktury państwa;
- urządzenia techniczne oraz systemy informatyczne, które są wykorzystywane przez osoby pełniące ważne funkcje w sferze militarnej.

Wraz z rozwojem sił zbrojnych, postępem technologicznym i zróżnicowaniem → z a g r o ż e ń m i l i t a r n y c h [t. 4] rośnie ilość informacji wojskowych, które podlegają ochronie. Wzrasta w związku z tym znaczenie stosowania przy ochronie informacji wojskowych określonych procedur. W XX w. w wielu państwach procedury obejmowały nadawanie, przyjmowanie, wydawanie, przewożenie, przechowywanie, użytkowanie, dystrybucję, oznakowanie i niszczenie informacji wojskowej. Nie tylko w krajach demokratycznych zwracano coraz większą uwagę na to, by procedury były precyzyjne, jednoznaczne i oparte na trafnie skonstruowanych, przejrzystych aktach prawnych wyższego rzędu. Troszczono się o jasne dla upoważnionych użytkowników informacji wojskowych zasady ich klasyfikowania. Dbano o spójność i szczelność powstającego stopniowo w wielu krajach systemu zabezpieczeń informacji wojskowych. Doprecyzowano zasady postępowania określające sposób zamiany informacji jawnej w zaszyfrowaną.

Opracowano procedury regulujące dostęp do miejsc, w których są przechowywane, tworzone i przetwarzane informacje wojskowe. Równocześnie zadbano oczywiście o bezpieczne miejsce przechowywania kluczy do pomieszczeń, gdzie są przechowywane informacje wojskowe oraz klucze do szyfrów. Wiele spośród utworzonych wówczas regulacji obowiązuje do dziś.

W XXI w. ze względu na powszechne stosowanie komputerów duże znaczenie ma określenie szczegółowych wymogów odnośnie do wielopoziomowej ochrony systemów teleinformatycznych przetwarzających informacje wojskowe, a także doprecyzowanie trybu i sposobów ich eksploatacji. Podstawą dopuszczenia danego systemu informacyjnego do stosowania przy informacjach o znaczeniu wojskowym jest wdrożenie określonych procedur bezpieczeństwa i osiągnięcie dzięki nim odpowiedniego poziomu ochrony informacji. Procedury zabraniają oczywiście stosowania pożyczonego oprogramowania i regulują sposób zabezpieczania dominujących obecnie nośników

informacji wojskowej, dotyczą również oprogramowania antywirusowego i tworzenia kopii zapasowych. Odpowiednie niszczenie niepotrzebnych informacji (np. zbędnych kopii tajnych dokumentów) ma zapobiec dostaniu się ich w niepowołane ręce. Wbrew pozorom nie jest to sprawa banalna. Już na początku XXI w. dane usunięte z dysku można było odtworzyć, nawet jeśli na miejscu usuniętych danych 2 razy wpisano już inne informacje.

Same dobrze napisane procedury nie powodują oczywiście wzrostu poziomu bezpieczeństwa informacji wojskowej. Muszą być one jeszcze konsekwentnie stosowane, z czym w szeregu krajów nie jest najlepiej.

W związku z postępem technologicznym i rosnącą ilością informacji wojskowych w XXI w. duży nacisk kładzie się na normalizację i standaryzację wymagań wobec służb zajmujących się wytwarzaniem i wykorzystywaniem informacji wojskowej. Ważne jest dostosowanie środków ochrony informacji wojskowej do wagi chronionych informacji i ich ilości. By efektywnie przekazywać informacje wojskowe sojusznikom, omawiane procedury muszą być zgodne ze standardami obowiązującymi w strukturach państw sojuszniczych.

Często do informacji wojskowych niepożądany odbiorca docierał (i dociera), włamując się do miejsc, gdzie są one przechowywane, albo dzięki przechwyceniu ich w trakcie przesyłania. To ostatnie wynika z tego, że dane wojskowe podczas wpisywania lub przetwarzania z reguły nie są zaszyfrowane.

Dlatego też powołano kancelarie tajne. W wielu krajach są one zlokalizowane w osobnych pomieszczeniach. Najczęściej są to odrębne komórki organizacyjne odpowiadające za właściwe zarejestrowanie dokumentów wojskowych, ich przechowywanie, obieg i wydawanie osobom uprawnionym. W wypadku szczególnie ważnych danych niektóre państwa mają możliwość zastosowania m.in. kosztownej osłony elektromagnetycznej. Promieniowanie komputerów z danymi wojskowymi staje się wtedy dla przeciwnika niewidoczne.

Zwraca się uwagę na fizyczne zabezpieczenie pomieszczeń i pracowników w czasie, gdy mają oni bezpośredni dostęp do wojskowych → i n f o r m a c j i n i e j a w n y c h [t. 2]. Wykorzystuje się do tego celu m.in. służby wewnętrzne czy warty. Tworzone są wydzielone strefy bezpieczeństwa wokół miejsc, w których są przechowywane i wytwarzane dane wojskowe. Wstęp do nich jest uregulowany za pomocą przepustek lub ich odpowiedników. Określają one uprawnienia osób do wejścia do strefy bezpieczeństwa, pobytu w niej i jej opuszczenia. Stosowana jest kontrola dostępu przy pomocy ludzi (np. strażnik sprawdzający przepustki) i/lub urządzeń sterowanych przez program (np. na podstawie danych biometrycznych). Równocześnie wykorzystywane są programy pośredniczące, pozwalające na monitorowanie wymiany informacji między wewnętrzną siecią wojskową a światem zewnętrznym.

Poza działaniami wrogich państwu struktur bezpieczeństwu informacji wojskowej zagrażają także inne nieplanowane przez wojskowych zdarzenia. One też mogą m.in.

doprowadzić do utraty informacji lub ich modyfikacji; zmienić techniczne parametry działania nośników informacji i urządzeń ich przetwarzania. Można je podzielić na 4 grupy:

- uchybienia organizacyjne;
- błędy ludzkie;
- błędy techniczne;
- nieprzewidziane zjawiska przyrody i siły natury.

Często o końcowym efekcie skuteczności systemów zabezpieczeń informacji wojskowej decyduje najsłabsze ogniwo. Badacze wielokrotnie zwracali uwagę, że są nim ludzie mający styczność z informacją wojskową i ich → k u l t u r a b e z p i e c z e ń s t w a [t. 2]. Na tę ostatnią składają się poziom etyczny i kompetencje personelu oraz odbiorców informacji wojskowej z użytkownikami systemów teleinformatycznych na czele. Jak wskazuje R. Szandrocho, jeszcze w XXI w. można było spotkać w Europie wojskowych przechowujących „małe kancelarie tajne" na niezarejestrowanych nośnikach poza budynkami do tego przeznaczonymi.

Według unormowań prawnych w Polsce najczęściej za ochronę informacji wojskowej odpowiadają zwierzchnicy jednostek, w których są wytwarzane i przetwarzane materiały tego typu. Nie dziwi więc znaczenie właściwego kierowania przez nich bezpieczeństwem informacji wojskowej w podległych strukturach: odpowiednie monitorowanie; systematyczne, okresowe kontrole stanu zabezpieczenia; regularne sprawdzanie poziomu sprawności systemów monitorujących poziom bezpieczeństwa; w miarę potrzeb wykorzystanie zewnętrznej pomocy i przeznaczenie na tę sferę niemałych środków finansowych.

Sytuacja w tym zakresie w poszczególnych państwach wygląda bardzo różnie. Jeśli pominąć nieliczne, najlepiej rozwinięte gospodarczo kraje, to do najważniejszych uchybień organizacyjnych dotyczących bezpieczeństwa informacji wojskowej należą:

- niejasny podział odpowiedzialności;
- brak należytej troski zwierzchników w odniesieniu do komórek organizacyjnych zajmujących się przetwarzaniem i magazynowaniem informacji;
- niestosowanie obowiązujących procedur;
- wadliwie zorganizowane administrowanie systemami (szczególnie teleinformatycznymi) i ich zasobami;
- niewystarczające monitorowanie;
- niezapewnienie pracownikom odpowiednich kwalifikacji i brak dopilnowania właściwego i starannego wypełniania przez nich obowiązków;
- niedopasowanie środków ochrony informacji wojskowej do rzeczywistego poziomu → z a g r o ż e ń [t. 4];
- wadliwe lub niedostateczne działania w zakresie profilaktyki, diagnostyki oraz prognozowania technicznego prowadzące do zwiększenia ilości uszkodzeń urządzeń oraz złe zarządzanie kluczami szyfrującymi.

Zwierzchnicy muszą nie tylko na bieżąco czuwać nad ochroną informacji wojskowej, ale także uwzględniać to, że przyszłość w tej dziedzinie z pewnością przyniesie nowe wyzwania. Przy planach wprowadzania rzeczywistych zmian w zakresie bezpieczeństwa informacji wojskowych zwierzchnicy muszą brać pod uwagę m.in. ograniczenia kadrowe i dotychczasowe przyzwyczajenia podległych pracowników w omawianej sferze. By ustalić, czy cechy charakteru osoby mającej mieć dostęp do informacji wojskowej, jej stosunek do wykonywanej pracy, przeszłość i kontakty zapewniają bezpieczeństwo, stosowane są postępowania sprawdzające. Ich rodzaj zależy od tego, do jak ważnych dokumentów z punktu widzenia obronności państwa zostanie dopuszczony przyszły pracownik.

W tej sytuacji w XXI w. wzrosło znaczenie odpowiedniego przeszkolenia pracowników mających dostęp do omawianych danych. Podnoszenie kwalifikacji obejmuje pogłębienie wiedzy z zakresu m.in. zarządzania informacją wojskową w instytucji; zasad i sposobów ochrony informacji wojskowej; rzeczywistego poziomu bezpieczeństwa omawianych systemów; obsługi systemów przesyłania informacji wojskowej i jej właściwego odbioru; zachowania tajności danych dotyczących funkcjonowania systemów informacyjnych; przepisów prawnych; odpowiedzialności karnej i służbowej za zaniedbania w tej sferze.

Jeśli szkolenia i kontrole są odpowiednio przeprowadzone, obniżają nie tylko ryzyko zagrożeń wynikających z celowej wrogiej działalności lub sił natury. Redukują równocześnie prawdopodobieństwo wystąpienia zagrożeń będących następstwem zaniedbań wewnątrz struktur wojskowych, które mają styczność z informacją wojskową. Nie chodzi tu jedynie o jej nieumyślną nieautoryzowaną zmianę. Przykładowo kontrola okresowa urządzeń kryptograficznych zmniejszy ilość przypadków słabej jakości uwierzytelnienia, a to z kolei podniesie skuteczność komputerowych systemów kontroli dostępu.

Regularne sprawdzanie stanu oprogramowania i aplikacji pozwala np. zmniejszyć liczbę ukrytych błędów w aplikacjach. Należy brać pod uwagę to, że stosowanie oprogramowania odpowiedniego do poziomu zabezpieczeń i specyfiki informacji wojskowej zwiększy poziom poufności i sprawności systemów służących do przesyłania, odbioru i przechowywania informacji, pod warunkiem jednak, że nowy sprzęt jest kompatybilny z dotychczas używanymi w systemie.

Dostęp do zasobów informacji wojskowej powinni mieć tylko użytkownicy uwierzytelnieni i autoryzowani. W programach kontrolujących dostęp do komputera lub programu niekiedy wykorzystywane są biometryczne metody zapewnienia dostępu do samego systemu (rozpoznawanie np. dłoni, głosu, twarzy).

Potwierdzeniem wiarygodności, rzetelności i autentyczności informacji wojskowej jest jej uwierzytelnienie. Występują różne sposoby uwierzytelnienia: od tradycyjnych podpisów i pieczęci, po wykorzystywanie certyfikatów kluczy publicznych, podpisów cyfrowych, podpisów lokalizacyjnych czy znaków wodnych (dołączanych np. do

obrazu wideo lub nagrania). Pracownicy mają przypisane uprawnienia umożliwiające przegląd, odczytanie, modyfikację, zapis i usuwanie zasobów informacji wojskowej opatrzonych klauzulą tajności tylko na takim poziomie, jaki przypisano kategorii dokumentów, które są im potrzebne. W wielu krajach klauzule przyznaje i zmienia osoba, która jest wytwórcą dokumentu (lub jej zwierzchnik). Zdarza się, że poszczególne części dokumentu mają różne klauzule tajności. Utajnianie informacji wojskowej polega jednak nie tylko na nadawaniu klauzul tajności, ale przede wszystkim na praktycznym wyegzekwowaniu stopnia dostępności informacji.

Od starożytności do zapewniania bezpieczeństwa informacji wojskowej stosowano szyfrowanie i → s t e g a n o g r a f i ę [t. 4]. Ta ostatnia pozwala ukryć istnienie wiadomości w danym nośniku. Do jej użycia odbiorca musi znać metodę szyfrowania oraz tajny klucz otwierający.

Od stuleci wykorzystywana jest także innego rodzaju ochrona informacji wojskowej – poprzez jej preparowanie tak, aby zmieniona treść wprowadzała przeciwnika w błąd. Zdaniem V. Volkoffa jeszcze na początku XXI w. był to najlepszy sposób ochrony tajemnicy wojskowej przed przeciwnikiem.

Wobec tego, że nie da się zapobiec wszystkim wrogim ingerencjom, ważne jest ich szybkie wykrywanie. Może ono pozwolić na ograniczenie skali szkód i wskazać słabe punkty systemów bezpieczeństwa informacji wojskowej. Przykładowo integralność danych można sprawdzić, stosując sumę kontrolną integralności, która jest obliczana na podstawie chronionych danych. Ważną rolę odgrywają systemy zautomatyzowanego wykrywania nieuprawnionych ingerencji w systemach. Ich słabą stroną jest konieczność ciągłej aktualizacji. Pojawiają się bowiem stale nowe metody ataku. Zbyt często systemy nie są w stanie rozpoznać zagrożeń – nieznanych tym, którzy aktualizowali te systemy.

Należy także zabezpieczyć informację wojskową przed konsekwencjami nieprzewidzianych zjawisk przyrody i sił natury. Przykładem może być fizyczne uszkodzenie lub zniszczenie urządzeń oraz systemów służących do przetwarzania informacji przez: → k a t a s t r o f y t e c h n i c z n e [t. 2], zakłócenia w dostawach z sieci energetycznej, wyładowania atmosferyczne (groźne szczególnie dla elementów systemów teleinformatycznych), pożary (np. temperatura), zalanie wodą, wystąpienie silnego pola magnetycznego ziemi oraz w przypadku niektórych systemów także burz radiacyjnych, burz magnetycznych i rozbłysków słonecznych. Istotne jest również zabezpieczenie przed wilgocią. Obniża ona poziom niezawodności urządzeń i systemów teleinformatycznych.

Poza ochroną do zakresu bezpieczeństwa informacji wojskowej trzeba zaliczyć konieczność równoczesnej dbałości o dostępność tego rodzaju informacji dla określonych kategorii odbiorców. Najważniejszym jej aspektem jest zapewnienie strukturom państwa wysokiej jakości informacji dotyczących wojska. Chodzi o aktualność, wiarygodność, użyteczność, kompletność i rzetelność informacji przekazywanych

właściwym organom państwa (wojskowym i cywilnym). Jeśli ci odbiorcy informacji wojskowych są przekonani o tym, że informacje są wiarygodne, to mają one duże znaczenie przy kierowaniu losami wojska oraz podejmowaniu decyzji odnośnie do jego przyszłości; rozpoznawaniu i przeciwdziałaniu w odpowiednim czasie zagrożeniom zewnętrznym godzącym np. w potencjał obronny kraju. Taka ocena informacji o znaczeniu wojskowym pozwala równocześnie na utrzymanie zaufania naczelnych władz państwa (oraz ponadpaństwowych struktur wojskowych) do otrzymywanych informacji wojskowych.

W XXI w. fundamentem dobrego przepływu informacji wojskowej jest nowoczesna oraz sprawnie działająca infrastruktura. Stosowanie wiekowych nośników i urządzeń do przetwarzania informacji oraz przestarzałych technologicznie zabezpieczeń z reguły zwiększa wrażliwość wojskowych systemów informacyjnych nie tylko na wrogi atak, ale także na zniszczenie czy zakłócenie przesyłania informacji wojskowej. Wynika to z utraty przez elementy tych urządzeń dotychczasowych parametrów fizycznych i elektrycznych.

By sprawnie przesyłać informacje wewnątrz sieci, komputery w danej sieci wewnętrznej są często skonfigurowane w taki sposób, by „ufały" sobie nawzajem. Ma to też negatywne konsekwencje. Skuteczne włamanie do jednego z nich pozwala często na dostęp – na określonym poziomie uprawnień – do wszystkich w danym systemie.

Podmioty właściwe w sferze bezpieczeństwa państwa oczekują ogólnych informacji przydatnych do uzyskania ogólnego obrazu państwa, jego sił zbrojnych, infrastruktury krytycznej itp. Przygotowujący je muszą więc dokonać selekcji posiadanych informacji i opracować je w formie ułatwiającej bieżące i perspektywiczne wykorzystanie np. przy wzmacnianiu obronności danego państwa.

Nadmiar przesyłanych do władz informacji powoduje, jak wskazuje słusznie A. Żebrowski, tzw. chaos informacyjny. Większość informacji jest nieużyteczna lub mało przydatna decydentom. Selekcja informacji jest tak czasochłonna, że ich odbiorca nie jest w stanie w optymalnym czasie podjąć odpowiedniej decyzji.

Warto tu przypomnieć, że dezinformowanie to także nieświadome wprowadzanie przełożonych w błąd lub brak podania potrzebnej informacji (np. wojskowej) w odpowiednim czasie (traktowanym nieprzypadkowo jako czwarty wymiar pola walki). Może ono wystąpić wskutek mylnej interpretacji np. rozkazów i zarządzeń zwierzchników albo przeoczenia ważnych wykonawczych wytycznych.

W wielu państwach wyzwaniem dla bezpieczeństwa informacji wojskowych bywa także nadmierna uznaniowość i restrykcyjność ochrony tajemnic wojskowych. Jak wskazał w 2010 r. Żebrowski na przykładzie służb specjalnych, problemy w omawianej sferze czasem wynikają z trudności w przekazywaniu informacji między poszczególnymi komórkami organizacyjnymi oraz między organizacjami. Zbyt często wynikają one z niechęci do dzielenia się posiadaną wiedzą. Nadmierna uznaniowość i restrykcyjność ochrony tajemnic wojskowych może znacznie utrudnić przepływ

informacji i w efekcie istotnie ograniczyć efektywne zarządzanie strategiczne w siłach zbrojnych. Grozi bowiem np. obniżeniem poziomu wyszkolenia na szczeblu plutonu lub kompanii. Nieprzypadkowo Szandrocho zwraca uwagę na wprowadzanie w życie zakazu zawyżania poziomu utajnienia informacji wojskowych.

Inne problemy w zakresie bezpieczeństwa informacji wojskowej stwarza złożoność dostępu. Z jednej strony, dzięki wykorzystaniu różnorodnych środków, podnoszony jest poziom ochrony informacji wojskowych. Upoważniony użytkownik ma jednak mieć do nich szybki dostęp, gdy jest mu to potrzebne w celach służbowych. Nadmierna koncentracja na utajnieniu danych powoduje problemy z dostępem do informacji. Równocześnie dezorganizuje działania pracowników przetwarzających dane wojskowe, powoduje opóźnienia w przesyłaniu danych, spóźnione decyzje władz wojskowych i państwowych oraz frustrację części spośród pracowników zmagających się codziennie np. ze zbyt skomplikowanym dostępem do systemu.

By bezpieczeństwo informacji wojskowej było zachowane, wspomniane wyżej środki muszą być stosowane efektywnie, konsekwentnie i całościowo przez doświadczony, odpowiednio przeszkolony zespół lojalnych pracowników, który został wcześniej właściwie sprawdzony i odpowiednio przeszkolony.

Poziom bezpieczeństwa informacji wojskowej w poszczególnych krajach jest dla badacza z reguły bardzo trudny do oceny. Z powodów oczywistych przytłaczająca większość naruszeń bezpieczeństwa informacyjnego w omawianej sferze to tzw. ciche katastrofy, które nigdy nie będą przez władze podane do wiadomości publicznej.

Jak wynika z przedstawionych rozważań, pojęcie bezpieczeństwa informacji wojskowej jest ściśle związane z polityką bezpieczeństwa informacji. Nie jest jednak tożsame z szerszym znaczeniowo bezpieczeństwem informacyjnym wojskowym.

Tomasz Skrzyński

P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2006; D.E. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, tłum. J. Bloch, Wydawnictwa Naukowo-Techniczne, Warszawa 2002; W. Fehler, *O pojęciu bezpieczeństwa informacyjnego*, [w:] *Bezpieczeństwo informacyjne w XXI wieku*, M. Kubiak, S. Topolewski (red.), Pracownia Wydawnicza Wydziału Humanistycznego Uniwersytetu Przyrodniczo-Humanistycznego, Siedlce–Warszawa 2016; W. Kitler, *Pojęcie i zakres bezpieczeństwa informacyjnego państwa, ustalenia systemowe i definicyjne*, [w:] *Bezpieczeństwo informacyjne. Aspekty prawno-administracyjne*, W. Kitler, J. Taczkowska-Olszewska (red.), Towarzystwo Wiedzy Obronnej, Warszawa 2017; J. Kowalewski, M. Kowalewski, *Polityka bezpieczeństwa informacji w praktyce*, Presscom, Wrocław 2014; A. Leśniak, *Wpływ pogody kosmicznej na bezpieczeństwo przesyłania i przechowywania informacji elektronicznych*, [w:] *Bezpieczeństwo informacyjne w dyskursie naukowym*, H. Batorowska, E. Musiał (red.), Uniwersytet Pedagogiczny im. KEN w Krakowie, Kraków 2017; T. Skrzyński, *Bezpieczeństwo informacji wojskowej*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; R. Szandrocho, *Wybrane problemy gotowości obronnej państwa*, Wydawnictwo Wyższej Szkoły Oficerskiej Wojsk Lądowych, Wrocław 2013; P. Żarkowski, *Wpływ działań informacyjnych na bezpieczeństwo państwa,* [w:] *Informacyjne uwarunkowania współczesnego bezpieczeństwa*, M. Kubiak, R. Białoskórski

(red.), Pracownia Wydawnicza Wydziału Humanistycznego Uniwersytetu Przyrodniczo-Humanistycznego, Siedlce–Warszawa 2016; A. Żebrowski, *Walka informacyjna w asymetrycznym środowisku bezpieczeństwa międzynarodowego. Wybrane problemy*, Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2016; A. Żebrowski, *Wywiad i kontrwywiad XXI wieku*, Wyższa Szkoła Ekonomii i Innowacji w Lublinie, Lublin 2010.

BEZPIECZEŃSTWO INFORMACYJNE – najczęściej definiowane jest jako pożądany poziom ochrony niezbędnych zasobów informacyjnych, technologii ich tworzenia i wykorzystywania, a także praw podmiotów działalności informatycznej oraz zapewnienie im stabilnego funkcjonowania w każdych warunkach międzynarodowych i społecznych. Rzadziej traktuje się bezpieczeństwo informacyjne jako czynnik rozwijający i wzbogacający osobowość człowieka i stanowiący podstawę jego rozwoju intelektualnego, a jej brak jako czasową lub względnie trwałą utratę przez jednostkę zdolności do szeroko rozumianego rozwoju w środowisku → t e c h n o l o g i i i n f o r m a c y j n o - k o m u n i k a c y j n y c h [t. 4], w którym → i n f o r m a c j ę [t. 2] traktuje się jako dobro chronione. K. Liedel bezpieczeństwo informacyjne łączy z uprawianiem polityki gwarantującej państwu i podmiotom, które chroni, istnienie, przetrwanie i swobodę rozwoju → s p o ł e c z e ń s t w a i n f o r m a c y j n e g o [t. 4]. W tym szerszym, pozytywnym rozumieniu kategoria securitologii, jaką jest bezpieczeństwo informacyjne, obejmuje wszystkie procesy technologiczne – od pozyskiwania, poprzez transmisję, przetwarzanie, do przechowywania informacji, czyli odnoszące się do wszystkich etapów (faz) → p r o c e s u i n f o r m a c y j n e g o [t. 3].

J. Janczak i A. Nowak w jej strukturze wyodrębniają 3 elementy: ludzi, technologie i procesy, które składają się na → ś r o d o w i s k o i n f o r m a c y j n e [t. 4]. Definiują oni bezpieczeństwo informacyjne jako kompleks przedsięwzięć zapewniający → b e z p i e c z e ń s t w o tego środowiska oraz działań związanych z jego formowaniem, wykorzystywaniem i rozwojem w interesie obywateli, organizacji i państwa. Przeciwstawiają się poglądowi, że jest to domena wyłącznie informatyków, wskazując na problemy dotyczące kwestii organizacyjnych oraz obszaru świadomości pracowników mających dostęp do informacji. Bezpieczeństwo informacyjne zapewniają nie tylko systemy teleinformatyczne, ale w dużej mierze przeszkolony i świadomy → z a g r o ż e ń [t. 4] personel oraz kierownictwo. Świadomość odpowiedzialności za informacje i jej skutki społeczne stanowi więc ważny obszar dociekań badaczy bezpieczeństwa informacyjnego odnotowujących wzrost zachowań ryzykownych w społeczeństwie wynikających z konsumpcji zmanipulowanych i celowo zniekształconych informacji.

W literaturze przedmiotu termin bezpieczeństwa informacyjnego utożsamiany jest z terminami bezpieczeństwa informatycznego lub bezpieczeństwa informatyzacji i jest często z nimi mylony. Wynika to z przyjęcia przedmiotowego kryterium klasyfikacji pojęcia bezpieczeństwa, w którym bezpieczeństwo informacji odnosi się do informacji krążącej między węzłami sieci i w bazach danych dostępnych za ich

pośrednictwem. Bezpieczeństwo informatyczne określa się zatem jako → b e z p i e c z e ń s t w o w s i e c i , bezpieczeństwo telekomunikacyjne, bezpieczeństwo komputerowe, bezpieczeństwo danych, bezpieczeństwo sieciowe. Rozpatrując bezpieczeństwo informacyjne w kontekście przestrzeni lub obszaru, nie można zawężać jego pola rozważań do → c y b e r p r z e s t r z e n i (bezpieczeństwa danych w sieciach teleinformatycznych), pomijając bezpieczeństwo informacji w instytucjach (bezpieczeństwo zbiorów bibliotecznych, archiwalnych, muzealnych, urzędowych, organizacyjnych itp.) lub bezpieczeństwo prywatnych zbiorów i kolekcji. Ponieważ informacja staje się przedmiotem walki o jej zdobycie, a pozyskiwać ją można różnymi sposobami, nie tylko związanymi z → c y b e r p r z e s t ę p c z o ś c i ą, należy dużą wagę przywiązywać do potencjalnych źródeł zakłóceń jej bezpieczeństwa, np. związanych z kulturą organizacyjną firmy, działalnością mass mediów, → p o l i t y k ą i n f o r m a c y j n ą [t. 3], prawem do wolności słowa. Z tego względu bezpieczeństwo informacyjne można postrzegać jako dobro chronione, stanowiące strategiczną wartość dla organizacji, narodu lub jednostki, jako proces tworzenia pożądanego stanu bezpieczeństwa informacyjnego lub jako stan spokoju, stabilności i braku zagrożenia informacyjnego.

E. Ura i S. Pieprzny wskazują, że zasięg pojęcia bezpieczeństwa informacyjnego może być zmienny, gdyż uzależniony jest od kontekstu związanego ze źródłem zagrożeń, celem ochrony lub rodzajem dóbr chronionych bądź równocześnie od tych 3 elementów i nie można postrzegać go tylko jako kategorii bezpieczeństwa państwa. Przychylają się do definicji, w której łączy się je z ochroną informacji w każdej dostępnej formie, i to zarówno informacji publicznej, jak i prywatnej, chronionej przez państwo, ze szczególnym uwzględnieniem → i n f o r m a c j i n i e j a w n y c h [t. 2], biorąc pod uwagę także zapewnienie pożądanego poziomu ochrony zasobów informacyjnych, technologie informacyjne i prawo podmiotów działalności informacyjnej w celu zapewnienia stabilnego funkcjonowania w każdych warunkach międzynarodowych oraz społecznych.

Wskazując, że rozwój → n a u k o b e z p i e c z e ń s t w i e [t. 3] łączy się z przejmowaniem dorobku różnych dyscyplin i dziedzin, których przedmiotem są wielostronne aspekty bezpieczeństwa człowieka, K. Liderman dostrzega potrzebę utworzenia odrębnej specjalności naukowej – bezpieczeństwa informacyjnego. Argumentuje ją nie tylko konsekwencją przyjęcia kryterium przedmiotu, jakim jest informacja, ale głównie zwróceniem uwagi na jej charakter interdyscyplinarny. Bezpieczeństwo informacyjne rozumiane w szerszym zakresie obejmuje bowiem wszystkie formy, także werbalne, wymiany, przechowywania i przetwarzania informacji. Dotyczy podmiotu (człowieka, organizacji), który może być zagrożony utratą zasobów informacyjnych lub otrzymaniem informacji o złej jakości, niejednokrotnie nie będąc tego świadomym. Oznacza uzasadnione zaufanie podmiotu do jakości i dostępności pozyskiwanej oraz wykorzystywanej informacji. Bezpieczeństwo informacyjne donosi się zatem do:

- samej informacji;

- systemów, w których podlega ona procesowi informacyjnemu;
- środowiska, w którym systemy działają;
- personelu, który korzysta z tych informacji i systemów;
- otoczenia prawnego;
- ochrony człowieka przed zagrożeniami wynikającymi z konieczności funkcjonowania w społeczeństwie informacyjnym.

Bezpieczeństwo informacyjne nie ogranicza się więc tylko do ochrony informacji przed nieuprawnionymi działaniami ludzi, przed awariami sprzętu i wadami oprogramowania, przed skutkami katastrof i działań terrorystycznych oraz przed błędami ludzkimi i organizacyjnymi. Według L.F. Korzeniowskiego w tym szerszym kontekście bezpieczeństwo informacyjne doskonale mieści się w obszarze nauk społecznych jako dziedzina nauk społecznych obejmująca dyscyplinę określaną naukami o bezpieczeństwie.

→ Ś r o d o w i s k o b e z p i e c z e ń s t w a [t. 4] informacyjnego (odnoszące się do sfery kultury mentalnej, organizacyjnej i materialnej) wpływa na sprawne funkcjonowanie systemu bezpieczeństwa informacyjnego kraju. System ten obejmuje sektor publiczny, prywatny oraz obywatelski. Zadaniem tego systemu jest nie tylko przeciwdziałanie zagrożeniom, ale także podejmowanie wyzwań poprzez redukowanie ryzyka i wykorzystywanie szans. Wymaga to od grup i indywidualnych obywateli → k u l t u r y b e z p i e c z e ń s t w a i n f o r m a c y j n e g o [t. 2]. W środowisku cyfrowym za ważny komponent → k u l t u r y b e z p i e c z e ń s t w a [t. 2] należy uznać → k u l t u r ę i n f o r m a c y j n ą [t. 2] społeczeństwa. Włączenie społeczeństwa do budowania środowiska bezpieczeństwa informacyjnego powinno dokonywać się poprzez zapobieganie zjawisku wykluczenia informacyjnego, zaangażowanie społeczeństwa w proces weryfikowania odbieranych przekazów informacyjnych; współpracę z organizacjami służącymi zapewnieniu tożsamości narodowej i dziedzictwa kulturowego; podejmowanie inicjatyw kulturalnych wchodzących w skład przedsięwzięć wspierających politykę informacyjną państwa; podwyższanie własnej odporności na ataki informacyjne i świadomości na temat współczesnej → w o j n y i n f o r m a c y j n e j [t. 4]. Nie bez przyczyny do zadań preparacyjnych systemu bezpieczeństwa informacyjnego włącza się działania tzw. ogniw wsparcia, czyli naukę, edukację i społeczeństwo.

Bezpieczeństwo informacyjne ze względu na liczność interakcji wg P. Sienkiewicza powinno być analizowane na kilku płaszczyznach bezpieczeństwa, tj.: państwa (w zakresie prawa, reguł i procedur dotyczących bezpieczeństwa informacji, współpracy międzynarodowej w ramach polityki bezpieczeństwa, koordynacji działań w przypadku zaistnienia zagrożenia), bezpieczeństwa organizacji i instytucji (w zakresie standardów bezpieczeństwa, norm, odpowiedniej polityki kadrowej) oraz obywateli (w zakresie świadomości zagrożeń, prawa do informacji, ochrony danych osobowych).

Oznacza to, że przedmiotem zainteresowania badaczy problemów bezpieczeństwa informacyjnego jest nie tylko sama informacja i dane mające wartość strategiczną dla podmiotu, ale też człowiek z nich korzystający w dobrych i złych celach oraz środowisko informacyjne, które generuje różne zagrożenia dla człowieka i informacji i które samo ulega degradacji z przyczyn wywołanych przez człowieka. W tym kontekście badacze bezpieczeństwa informacyjnego obejmują refleksją także zjawisko tzw. → c h o r ó b i n f o r m a c y j n y c h . Stanowią one rodzaj niedomagań człowieka (odstępstw od → z r ó w n o w a ż o n e g o r o z w o j u [t. 4] społeczeństwa informacji i wiedzy), wynikających ze stresu generowanego przez współczesne środowisko informacyjne i procesy globalizacyjne. Należą do specyficznych chorób cywilizacji informacyjno-medialnej, atakujących nie tylko pojedyncze osoby, ale również całe społeczności, głównie w krajach wysoko rozwiniętych. Przyczyną większości tych chorób jest stres informacyjny powstały w wyniku nieradzenia sobie z nadmiarem informacji w obszarze zarządzania przepływem informacji oraz → p r z e c i ą ż e n i e i n f o r m a c y j n e [t. 3] zmuszające do powierzchowności i skrótowości w myśleniu i uniemożliwiające głębszą refleksję. Funkcjonując w permanentnym chaosie i szumie informacyjnym, jednostka jest atakowana przez zniekształconą informację, a tzw. infotoksyny (→ i n f o t o k s y k a c j a [t. 2]) powodują u niej zmęczenie informacyjne i infoparaliż, którego konsekwencją może być depresja informacyjna prowadząca do niesprawności i niezdolności do pracy w środowisku informacyjnym, a dalej do całkowitego braku odporności na zagrożenia występujące w → i n f o s f e r z e [t. 2]. Patologie te najczęściej odnoszą się do informacji jako produktu. Pod uwagę należy wziąć także schorzenia informacyjne, które odnoszą się do informacji jako procesu prowadzącego do uzyskania produktu, jakim jest informacja, np. związane z zaleganiem informacji, czyli brakiem drożności w przepływie informacji. Szacuje się, że w przedsiębiorstwach stanowczo więcej czasu trwania procesu informacyjnego przypada na zaleganie informacji niż jej przetwarzanie i wykorzystanie. Wynika to z przeciążenia informacyjnego, które dotyczy także tzw. dystorsji informacji (dwuznaczności informacji) rozumianej jako świadoma lub nieświadoma deformacja (modyfikacja znaczenia) informacji w trakcie jej przepływu z jednego puntu obiegowego do kolejnego. Przeciążenie informacyjne jest w organizacji niejednokrotnie przyczyną zawału informacyjnego (zatkania kanału informacyjnego), gdy informacje, nawet dobrej jakości, nie są przesyłane w odpowiednich momentach do kolejnych punktów obiegowych. Związane jest to nie tyle ze złą organizacją, ile z niedocenianiem znaczenia kultury organizacyjnej w zapewnieniu sprawności realizacji procesu informacyjnego.

Choroby informacyjne bywają niejednoznaczne i niezrozumiałe, nikt nimi nie zarządza i dlatego wg W. Babika są tak niebezpieczne. Wyszczególnia on grupy chorób, na które zapadają nadawcy lub odbiorcy informacji. Nadawców najczęściej dotyka niefrasobliwość informacyjna (brak poczucia odpowiedzialności za komunikat i troski o jego prawdziwość), zakłamanie informacyjne (celowe zniekształcanie treści komunikatu),

urojenia informacyjne (generowanie informacji na podstawie własnych domysłów niepopartych faktami), obłuda informacyjna (infekowanie informacji w celu manipulowania zachowaniami odbiorców). Natomiast odbiorcy informacji chorują najczęściej na bulimię i anoreksję informacyjną (potrzeba pozyskiwania informacji w nadmiarze lub całkowity brak zapotrzebowania na nią), infoholizm, stres informacyjny, pośpiech informacyjny, „informacyjny AIDS", a także na informacyjną samotność, frustrację, głupotę (bezkrytyczny odbiór informacji) itd. Wśród „niedomagań informacji", które w środowisku lokalnym stanowią poważne zagrożenie dla bezpieczeństwa informacji, Babik wymienia przeciążenie informacyjne, wieloznaczność informacji, anemię informacyjną, przekłamanie informacyjne i zawał informacyjny. Zestaw niewłaściwych reakcji człowieka w trakcie korzystania z informacji obejmuje najczęściej działania związane z brakiem odpowiedzialności za tworzone i rozpowszechniane informacje, z bezkrytycznym i tendencyjnym odbiorem informacji, z niewłaściwym rozumieniem komunikatów czy z fragmentarycznym przekazywaniem wiadomości.

Wiele schorzeń wynika także z niekontrolowanej aktywności w cyberprzestrzeni, do których T.W. Grabowski zalicza cyberuzależnienia, → c y b e r p r z e m o c, cyberstres, lęk przed odłączeniem od sieci (cyberlęk), lęk przed pominięciem istotnych dla użytkownika komunikatów (z ang. *fear of missing out*, FoMO), nomofobię, syndrom fantomowych wibracji własnego telefonu komórkowego, cyberchondrię, cyfrową bezsenność, cyberseks, ale też portalozę, czyli chorobliwe korzystanie z portali społecznościowych.

Przeciwdziałanie chorobom informacyjnym związane jest z kształtowaniem kultury informacyjnej społeczeństwa oraz rozwijaniem jego postaw proinfoekologicznych. Podnoszenie poziomu → ś w i a d o m o ś c i i n f o r m a c y j n e j [t. 4] nie tylko redukuje zagrożenia, na które narażony jest każdy człowiek funkcjonujący we współczesnym środowisku informacyjnym, lecz także ukazuje szanse, które stwarza to środowisko dla rozwoju podmiotu. Dążenie do zrównoważenia rozwoju człowieka w świecie informacji polega wg Babika na ochronie infosfery, co wymaga „pełnej akceptacji hybrydowego środowiska informacyjnego, w którym nie dopuszcza się do dominacji ani środowiska naturalnego, ani sztucznego środowiska elektronicznego".

Prowadzenie odpowiedniej polityki informacyjnej oraz polityki bezpieczeństwa informacyjnego definiującej sposoby właściwego i niewłaściwego korzystania z zasobów informacji stanowi gwarancję kształtowania społecznego ładu informacyjnego. Budowanie tego ładu w „dobie → p o s t p r a w d y [t. 3]", gdy możliwość weryfikacji prawdziwości informacji jest coraz trudniejsza, a osobiste emocje uczestników komunikacji odgrywają większą rolę od obiektywnych faktów, powinno wg J. Oleńskiego zagwarantować stworzenie spójnego systemu norm, procesów, systemów i zasobów informacyjnych zaspokajających potrzeby informacyjne ludzi, podmiotów gospodarki narodowej i instytucji sfery publicznej.

Hanna Batorowska

H. Batorowska, *Bezpieczeństwo informacyjne*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; taż, *Bezpieczeństwo informacyjne w dyskursie naukowym – kierunki badań*, [w:] *Bezpieczeństwo informacyjne w dyskursie naukowym*, H. Batorowska, E. Musiał (red.), Uniwersytet Pedagogiczny im. KEN w Krakowie, Kraków 2017; taż, *Świadomość informacyjna warunkiem bezpieczeństwa użytkowników informacji*, [w:] *Bezpieczeństwo – wielorakie perspektywy. Bezpieczeństwo z perspektywy środowisk i obszarów*, N.A. Fechner, A. Zduniak (red.), Wyższa Szkoła Bezpieczeństwa, Poznań 2015; taż, *Wybrane aspekty kultury bezpieczeństwa w społeczeństwie informacji i wiedzy*, „Studia Politologica Ucraino-Polona" 2016, nr 6; W. Babik, *Bezpieczeństwo informacji wyzwaniem dla bezpieczeństwa lokalnego*, [w:] *Elementy teorii i praktyki transdyscyplinarnych badań problemów bezpieczeństwa. Teoretyczne i formalne aspekty bezpieczeństwa w wymiarze lokalnym*, A. Filipek, D. Krzewniak (red.), Wydawnictwo Naukowe UPH, Siedlce 2018; tenże, *Ekologia informacji*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2014; *Bezpieczeństwo informacyjne w dobie postprawdy*, T.W. Grabowski, M. Lakomy, K. Oświecimski (red.), Wydawnictwo Naukowe Akademii Ignatianum, Kraków 2018; P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2006; Z. Bauman, D. Lyon, *Płynna inwigilacja. Rozmowy*, Wydawnictwo Literackie, Kraków 2013; A. Gałach, R. Wójcik, *Zarządzanie bezpieczeństwem informacji w sektorze publicznym*, Wydawnictwo C.H.Beck, Warszawa 2009; J. Janczak, A. Nowak, *Bezpieczeństwo informacyjne. Wybrane problemy*, AON, Warszawa 2013; L.F. Korzeniowski, *Podstawy nauk o bezpieczeństwie*, Wydawnictwo Difin, Warszawa 2012; K. Liderman, *Bezpieczeństwo informacyjne: nowe wyzwania*, Wydawnictwo Naukowe PWN, Warszawa 2017; M. Spitzer, *Cyfrowa demencja. W jaki sposób pozbawiamy rozumu siebie i swoje dzieci*, Wydawnictwo Dobra Literatura, Słupsk 2013; J. Oleński, *Społeczne bezpieczeństwo informacyjne podstawą demokratycznego państwa*, „Rocznik Kolegium Analiz Ekonomicznych" 2015, nr 36; P. Sienkiewicz, *Wyzwania i zagrożenia w sieci: inwigilacja, dezinformacja, cyberterroryzm*, [w:] *Współczesne zagrożenia cyberterrorystyczne i bioterrorystyczne a bezpieczeństwo narodowe Polski*, P. Bogdalski i in. (red.), Wydawnictwo Wyższej Szkoły Policji w Szczytnie, Warszawa–Dęblin 2015; E. Ura, S. Pieprzny, *Bezpieczeństwo informacyjne – kategoria bezpieczeństwa publicznego czy bezpieczeństwa państwa*, [w:] *Bezpieczeństwo informacji państwa i biznesu*, M. Sitek, I. Niedziółka, A. Ukleja (red.), Wyższa Szkoła Gospodarki Euroregionalnej, Józefów 2014; J. Żywiołek, *Bezpieczeństwo informacyjne. Teoria i praktyka*, Oficyna Wydawnicza SMJP, Częstochowa 2017.

BEZPIECZEŃSTWO KLIMATYCZNE – opisuje poważne → z a g r o ż e n i a [t. 4] dla → b e z p i e c z e ń s t w a ludzi, ekosystemów i rozwoju krajów w wyniku globalnego ocieplenia klimatu oraz działań dostosowawczych i łagodzących zmiany klimatu; odnosi się do → z a g r o ż e ń b e z p i e c z e ń s t w a [t. 4], które są bezpośrednio lub pośrednio spowodowane zmianami klimatu. Zagrożenia bezpieczeństwa związane z klimatem mają daleko idące konsekwencje dla sposobu, w jaki podmioty lokalne, a także społeczność światowa traktują pokój i bezpieczeństwo.

W środowisku akademickim bezpieczeństwo klimatyczne jest częścią bezpieczeństwa środowiskowego i zostało po raz pierwszy wspomniane w raporcie Komisji Brundtland w 1987 r. Uczeni analizujący konflikty międzynarodowe od dawna twierdzili, że zmiany klimatu mogą negatywnie wpłynąć na bezpieczeństwo i stabilność międzynarodową.

W latach 70. i 80. grupa doradcza Jason Security Group, zajmująca się bezpieczeństwem, przeprowadziła badania nad zmianami klimatu, które zostały zidentyfikowane jako multiplikator zagrożeń mogący zaostrzyć istniejące zagrożenia.

W 2003 r. P. Schwartz i D. Randall sporządzili raport dotyczący potencjalnych konsekwencji różnych scenariuszy związanych z klimatem dla → b e z p i e c z e ń s t w a n a r o d o w e g o USA.

W badaniu National Research Council z 2013 r. oceniono konsekwencje nagłych zmian klimatu, w tym skutki dla środowiska i społeczeństwa. Autorzy zauważyli: „Kluczową cechą tych zmian jest to, że zmiany mogą przyjść szybciej, niż oczekiwano, zaplanowano lub obliczono, co powoduje reakcje bardziej reaktywne niż proaktywne". Badania wykazały, że ekstremalne fale upałów prowadzą do wyższej śmiertelności. Ekstremalne warunki temperaturowe mogą niekorzystnie wpływać na termoregulację ludzi. W przyszłości rosnące emisje gazów cieplarnianych mogą narazić ok. 74% ludności świata przez co najmniej 20 dni w roku na śmiertelne zagrożenia cieplne. „Zmiana klimatu zwiększa utratę zasobów naturalnych w sposób, który może zwiększyć prawdopodobieństwo dewastacji źródeł utrzymania, niestabilności państwa, przesiedleń ludzi i masowych zgonów", jak pisał A. De Juan.

W 2015 r. Biały Dom opublikował raport pokazujący, że zmiany klimatu zagrażają niektórym obszarom przybrzeżnym i że zmieniająca się Arktyka stanowi zagrożenie dla innych części USA, infrastruktury i zwiększa zapotrzebowanie na zasoby wojskowe. Raport Pentagonu z 2015 r. wskazał, że zmiany klimatu są znaczącym zagrożeniem dla bezpieczeństwa narodowego. Na podstawie sprawozdania rocznego → N A T O [t. 3] za 2015 r. Sojusz planuje inwestować w energię odnawialną i efektywność energetyczną, aby zmniejszyć ryzyko dla → ż o ł n i e r z y [t. 4] w związku ze skutkami zmian klimatu.

W 2017 r. administracja Trumpa usunęła zmiany klimatu ze → s t r a t e g i i b e z p i e c z e ń s t w a n a r o d o w e g o [t. 4]. W styczniu 2019 r. Pentagon opublikował jednak raport stwierdzający, że zmiana klimatu stanowi zagrożenie dla bezpieczeństwa narodowego USA. W czerwcu 2019 r., w trakcie przesłuchań komisji specjalnej ds. wywiadu w sprawie wpływu zmian klimatu na bezpieczeństwo narodowe, zaproponowano utworzyć prezydencką komisję ds. bezpieczeństwa klimatycznego. Kongres USA zwrócił się do Departamentu Obrony z prośbą o przygotowanie raportu na temat wpływu klimatu na bezpieczeństwo. Raport został opublikowany w 2019 r., podkreślono w nim, że skutki zmieniającego się klimatu są kwestią bezpieczeństwa narodowego i mogą oddziaływać na misje i plany operacyjne Departamentu Obrony.

Zagrożenia bezpieczeństwa związane z klimatem mają daleko idące konsekwencje dla sposobu, w jaki świat zarządza pokojem i bezpieczeństwem. Bezpieczeństwo klimatyczne to koncepcja przywołująca pogląd, że zmiany klimatyczne wzmacniają istniejące → z a g r o ż e n i a s p o ł e c z n e [t. 4] wpływające na bezpieczeństwo ludzi, ekosystemów, gospodarki, infrastruktury i społeczeństw.

W raporcie Global Catastrophic Risks z 2017 r., wydanym przez Global Challenges Foundation, podkreślono szeroki zakres zagadnień związanych z bezpieczeństwem, w tym zmiany klimatu. Stwierdzono, że globalne ocieplenie może doprowadzić do zagłady cywilizacji. Zainteresowanie zagrożeniami bezpieczeństwa klimatycznego gwałtownie wzrosło i wpływa na program polityczny w odniesieniu m.in. do bezpieczeństwa żywnościowego i energetycznego, polityki migracyjnej i wysiłków dyplomatycznych. Wpływ zmian klimatu rozkłada się nierównomiernie w różnych regionach, pozostaje jednak jasne, że jest to globalne wyzwanie, które będzie oddziaływać na wszystkie kraje w perspektywie długoterminowej.

Światowy raport oceny zagrożeń z 2018 r. stwierdza, że ostatnie 115 lat było najcieplejszym okresem w historii współczesnej cywilizacji, a ostatnie kilka lat było najcieplejszymi w historii. Ekstremalne zjawiska pogodowe zwiększają ryzyko katastrof humanitarnych, konfliktów, niedoborów wody i żywności, migracji ludności, braku siły roboczej itp. Według badań dotyczących bezpieczeństwa klimatycznego często trudno jest ustalić, czy na zagrożenie bezpieczeństwa i konflikty w różnych krajach i regionach mają wpływ zmiany klimatyczne i problemy związane z klimatem.

Przed spotkaniem przywódców ds. bezpieczeństwa UE 22 czerwca 2018 r., które przypadło na 10. rocznicę przełomowego raportu UE w sprawie zmian klimatu i bezpieczeństwa, 2 wiodące ośrodki analityczne opublikowały raport przedstawiający nowe ramy dla UE dotyczące reakcji na zagrożenia bezpieczeństwa związane ze zmianami klimatu pt. *Odpowiedzialność Europy za zarządzanie zagrożeniami dla bezpieczeństwa klimatu w zmieniającym się świecie*. Centrum ds. Klimatu i Bezpieczeństwa (z siedzibą w Waszyngtonie) i Clingendael Institute (z siedzibą w Hadze) argumentują, że instytucje UE powinny zintegrować zagrożenia powiązane ze zmianą klimatu z takimi zagrożeniami jak → t e r r o r y z m [t. 4] i zagrożenia nuklearne. Raport zawiera szczegółowe zalecenia dotyczące tego, jak mogłaby wyglądać reakcja na zagrożenie spowodowane zmianami klimatu w organach UE:

- europejska społeczność ma „obowiązek przygotować się" na zagrożenia związane z klimatem;
- UE musi bardziej aktywnie podejmować interwencje dyplomatyczne i rozwojowe w regionach kryzysowych dotkniętych zmianami klimatu i zagrożeniami bezpieczeństwa;
- muszą istnieć systemy wczesnego ostrzegania i szybkiego reagowania na zmiany klimatu i ich wpływu na bezpieczeństwo.

W Global Risks Report 2019 Światowego Forum Ekonomicznego wymieniono zmiany klimatu jako jedną z najbardziej niepokojących kwestii. W raporcie jako 3 główne problemy wskazano ekstremalną pogodę, brak działań klimatycznych i klęski żywiołowe. Globalny system polityczny doświadcza rosnących napięć geopolitycznych. Tymczasem nauka dostarcza coraz więcej dowodów na obecne i prawdopodobne

przyszłe skutki zmian klimatu. Istnieje wyraźniejsza i większa potrzeba ściślejszej współpracy w dziedzinie klimatu.

W ciągu ostatniej dekady → R a d a B e z p i e c z e ń s t w a O N Z [t. 3] stopniowo włączała zmiany klimatu do swojego programu pomimo sceptycyzmu ze strony niektórych państw członkowskich. Zmiany klimatu najlepiej postrzegać jako czynnik zwielokrotniający zagrożenia, który zaostrza istniejące tendencje, napięcia i sytuacje niestabilności. Głównym problemem jest to, że zmiany klimatu dodatkowo obciążają państwa i regiony, w których sytuacja już jest delikatna i w których łatwo wybuchają konflikty. Ważne jest, by zdawać sobie sprawę, że zagrożenia te nie mają charakteru wyłącznie humanitarnego, lecz dotyczą również polityki i bezpieczeństwa, które mają bezpośredni wpływ na interesy Europy. Ponadto zgodnie z koncepcją bezpieczeństwa ludzi oczywiste jest, że wiele kwestii związanych z wpływem zmian klimatu na bezpieczeństwo międzynarodowe łączy się ze sobą, a więc wymaga kompleksowych rozwiązań politycznych. Na przykład zaniechanie łagodzenia zmian klimatycznych może całkowicie przekreślić lata działań na rzecz rozwoju w ramach realizacji milenijnych celów.

W kompleksowym raporcie opublikowanym przez amerykańskie Center for Climate and Security 24 lutego 2020 r. eksperci ostrzegają przed katastrofalnymi zagrożeniami dla bezpieczeństwa w związku z trajektorią zmian klimatu. Nawet w scenariuszach zakładających niewielkie ocieplenie każdy region świata będzie narażony na poważne zagrożenia dla bezpieczeństwa narodowego i globalnego w ciągu najbliższych 3 dekad. Znaczne ocieplenie spowoduje katastrofalne i prawdopodobnie nieodwracalne zagrożenie globalnego bezpieczeństwa w XXI w.

Według kluczowych wniosków raportu nawet jeżeli temperatura na Ziemi wzrośnie o 1–2°C, będzie to stanowić poważne i ewoluujące zagrożenia dla globalnego → ś r o d o w i s k a b e z p i e c z e ń s t w a [t. 4], infrastruktury i instytucji we wszystkich rejonach świata. Rosnące temperatury na całym świecie prowadzą do niedoboru zasobów naturalnych, szczególnie w politycznie wrażliwych regionach świata. Konflikty związane z klimatem można zaobserwować np. w północnej Kenii. Duża część ludności żyje tam z koczowniczej hodowli bydła. Konsekwencjami zmian klimatycznych są susze i niestabilne opady atmosferyczne. Zasoby naturalne, które i tak są tam już niewielkie, stają się coraz bardziej ograniczone, a spory z zasiedlonymi rolnikami o pastwiska i zasoby wodne nasilają się. W razie potrzeby wzrasta gotowość ludzi do obrony swojego bytu przy użyciu siły zbrojnej. Napięcia mogą również wzrosnąć na transgranicznych odcinkach rzek, takich jak Nil czy Niger, w regionach, które już są naznaczone konfliktami. W związku z tym, że zmniejsza się ilość słodkiej wody w wyżej wymienionych rzekach, starannie wynegocjowane pogodzenie interesów państw sąsiadujących może zostać wystawione na próbę.

W lutym 2020 r. grupa ekspertów Międzynarodowej Wojskowej Rady ds. Klimatu i Bezpieczeństwa (International Military Council on Climate and Security, IMCCS)

zaprezentowała raport dotyczący klimatu i bezpieczeństwa. Zawiera on globalne i regionalne oceny zagrożeń dla bezpieczeństwa związanych ze zmieniającym się klimatem, a także możliwości przeciwdziałania im. Jest to pierwszy tego rodzaju raport, który ma na celu informowanie o przyszłej polityce oraz przedstawienie analiz odnoszących się do klimatu i bezpieczeństwa. Porusza on szeroki zakres tematów związanych z zagrożeniami bezpieczeństwa wynikającymi ze zmian klimatu, w tym:

- poważne klęski żywiołowe powodujące reakcje wojskowe i humanitarne, masowe przesiedlenia ludzi oraz zagrożenia dla zasobów krytycznych i infrastruktury;
- geopolityczne skutki zmian klimatu, w tym napięcia i konflikty regionalne i międzypaństwowe;
- wpływ zmian klimatu na wojsko i obronę, w tym → i n f r a s t r u k t u r ę w o j s k o w ą [t. 2], gotowość sił, operacje wojskowe i → s t r a t e g i ę [t. 4] wojskową.

Raport został przygotowany z punktu widzenia międzynarodowych ekspertów wojskowych i bezpieczeństwa i stanowi globalny przegląd zagrożeń bezpieczeństwa spowodowanych zmieniającym się klimatem oraz możliwości przeciwdziałania im. Zaleca „międzynarodowe dostosowanie do warunków klimatycznych", w tym infrastruktury, instytucji i polityki, a także znaczne ograniczenie emisji gazów cieplarnianych. Raport przypomina, że łagodzenie zmian klimatu i przystosowanie się do nich muszą być traktowane priorytetowo.

Według S. Goodman, obejmującej stanowisko starszego stratega w IMCCS, byłej zastępczyni podsekretarza obrony USA:

> Zmiana klimatu stanowi zwielokrotnienie zagrożenia, pogarszając istniejące zagrożenia dla bezpieczeństwa, a to oznacza, że wojsko będzie na pierwszej linii walki z zagrożeniami klimatycznymi i budowania odporności. Wielu ekspertów ds. bezpieczeństwa klimatycznego i wojskowych ocenia, że brak bezpieczeństwa wody spowodowany przez klimat będzie stanowić znaczące ryzyko dla bezpieczeństwa globalnego do 2030 r. Poważne i szybkie globalne redukcje emisji są konieczne, aby uniknąć znacznych lub katastrofalnych konsekwencji globalnego bezpieczeństwa w przyszłości. Musimy także przystosować wszystkie elementy bezpieczeństwa do zmian klimatu w tym infrastrukturę, instytucję i politykę.

Zmiany środowiskowe mogą zagrażać bezpieczeństwu, doprowadzić do niestabilności wielu państw, wzrostu ekstremizmu wśród sfrustrowanego społeczeństwa i przymusowej migracji w poszukiwaniu nowych zasobów. W efekcie mogą zaognić się w przyszłości konflikty wewnętrzne i międzypaństwowe. Wpływ tych zmian klimatu, które już obserwujemy, jest jedynie początkiem bardziej poważnych, które dopiero nadejdą. Rosnąca – ale nadal stosunkowo niewielka – część opinii publicznej zaczyna to dostrzegać i wzywa rządy do podejmowania znacznie bardziej zdecydowanych działań.

Zmiany klimatu są powszechnie uznawane za jedną z głównych sił kształtujących przyszłość. Pokazują one wyraźnie, w jaki sposób ludzkie działania wpływają na

podstawowe procesy fizyczne planety z ogromnymi, a w najgorszych przypadkach, katastrofalnymi konsekwencjami dla społeczności na całym świecie. Biorąc to pod uwagę, zmiany klimatu są coraz częściej traktowane jako zagrożenie dla bezpieczeństwa. Ponieważ zmieniający się klimat powoduje i będzie nadal wywoływał różnorodne skutki na całym świecie, związane z nim wyzwania w zakresie bezpieczeństwa są różnorodne. Obejmują one zagrożenia dla bezpieczeństwa ludzi, społeczności oraz będą wymagały reakcji na wszystkich poziomach procesu decyzyjnego, od lokalnego do międzynarodowego.

Olga Wasiuta, Sergiusz Wasiuta

J. Barnett, *Global Environmental Change I: Climate Resilient Peace*?, „Progress in Human Geography" 2019, vol. 43, iss. 5; K. Conca, *Is There a Role for the UN Security Council on Climate Change?*, „Environment: Science and Policy for Sustainable Development" 2019, vol. 61, iss. 1; P.H. Gleick*, Water, Drought, Climate Change, and Conflict in Syria*, „Weather, Climate, and Society" 2014, vol. 6, no. 3; T.F. Homer-Dixon, *Environmental Scarcities and Violent Conflict: Evidence from Cases*, „International Security" 1994, vol. 19, no. 1; T. Ide, J. Scheffran, *On Climate, Conflict and Cumulation: Suggestions for Integrative Cumulation of Knowledge in the Research on Climate Change and Violent Conflict*, „Global Change, Peace & Security" 2014, vol. 26, iss. 3; IMCCS, *The World Climate and Security Report 2020*, 15.02.2020, IMCCS.org (dostęp 10.03.2020); V. Koubi, *Climate Change and Conflict*, „Annual Review of Political Science" 2019, vol. 22; K.J. Mach i in., *Climate as a Risk Factor for Armed Conflict*, „Nature" 2019, no. 571; M. Mobjörk i in., *Climate-Related Security Risks: Towards an Integrated Approach*, Stockholm International Peace Research Institute (SIPRI), Stockholm 2016; NSMIP*, A Security Threat Assessment of Global Climate Change: How Likely Warming Scenarios Indicate a Catastrophic Security Future*, 24.02.2020, ClimateAndSecurity.org (dostęp 10.03.2020); *Report on Effects of a Changing Climate to the Department of Defense*, Office of the Under Secretary of Defense for Acquisition and Sustainment, 2019; I. Salehyan, *Climate Change and Conflict: Making Sense of Disparate Findings*, „Political Geography" 2014, vol. 43; J. Scheffran, P.M. Link, J. Schilling, *Climate and Conflict in Africa*, [w:] *Oxford Research Encyclopedia of Climate Science*, Oxford University Press, 2019; *The International Military Council on Climate and Security (IMCCS)*, ClimateAndSecurity.org (dostęp 10.03.2020); C. Werrell, F. Femia, *Release: International Military Council Issues „World Climate and Security Report 2020" at Munich Security Conference*, 13.02.2020, ClimateAndSecurity.org (dostęp 10.03.2020).

BEZPIECZEŃSTWO KULTUROWE – zdolność społeczeństwa do zachowania swoich podstawowych cech w zmiennych warunkach, a także w stosunku do istniejących lub ewentualnych → z a g r o ż e ń [t. 4] (O. Wæver); proces integracji kultur, który jest konsekwencją współpracy międzynarodowej, związany jednak także z zachowaniem tradycji i przejawów kultury (E. Nemeth); zdolność państwa do ochrony tożsamości kulturowej, dóbr kultury i dziedzictwa narodowego w warunkach otwarcia na świat, umożliwiających rozwój kultury w drodze internalizacji wartości niesprzecznych z własną tożsamością (J. Czaja); konieczność zapewnienia ochrony tożsamości narodowej, przeciwdziałania zagrożeniom dla kultury – w związku z napływem obcych wartości kulturowych – w tym zagrożeniom dla religii i języka (A. Dawidczyk,

J. Czaputowicz); zdolność państwa do pomnażania dotychczasowego dorobku kulturowego oraz jego obrona przed niepożądanym wpływem innych kultur (T. Jemioło); celowe działanie państwa lub społeczeństwa, które ma zapobiegać negatywnym zmianom kultury i tożsamości, np. takie, którego celem jest ochrona dóbr kultury, ale i wykorzystanie dorobku kulturowego danego narodu, aby kształtować pożądane stany w środowisku międzynarodowym, a także umacniać siłę narodową zgodnie z jej celami (W. Kitler).

Do elementów bezpieczeństwa kulturowego możemy zaliczyć:

- ochronę istotnych wartości kultury symbolicznej (języka, religii, zwyczajów, tradycji, filozofii, ideologii itd.);
- ochronę materialnych dóbr kultury i dziedzictwa kulturowego (zabytki, pomniki, całe kompleksy miejskie o starej zabudowie, dzieła sztuki i rzemiosła artystycznego);
- zapewnienie poczucia bezpieczeństwa kulturowego w wymiarze narodu (tożsamość narodowa), jednostkowym (wolność tworzenia) i grup etnicznych (ochrona przed → a s y m i l a c j ą, zapewnienie warunków do rozwoju);
- pojęcie otwartości kultury, polegające przede wszystkim na zachowaniu stanu równowagi między jej wewnętrznym rozwojem a ochroną przed niepożądanymi wpływami zewnętrznymi i jednoczesną internalizacją elementów niesprzecznych z kulturą własną, natomiast rozwijających ją;
- prowadzenie zagranicznej polityki kulturowej mającej na celu popularyzację własnej kultury oraz oddziaływanie na inne kultury i państwa (→ *s o f t p o w e r* [t. 4], polityka historyczna).

Bezpieczeństwo kulturowe determinuje wiele czynników, m.in.: ustrój państwa (demokratyczny lub nie); wolności i → p r a w a c z ł o w i e k a [t. 3]; uwarunkowania historyczne; regulacje i relacje międzynarodowe (w tym stosunek do inicjatyw i postanowień organizacji międzynarodowych); dysproporcje rozwojowe (w ramach relacji na linii: centra – półperyferie – peryferie).

Zagrożeniami dla bezpieczeństwa kulturowego państwa mogą być m.in.: globalizacja (uniwersalizacja kultury); amerykanizacja kultury, imperializm kulturowy (również rusyfikacja / → *r u s s k i j m i r* [t. 3] w obszarze poradzieckim); → k r y z y s y [t. 2] tożsamości kulturowej i narodowej związane z powyższymi zjawiskami; rozwój technologii komunikowania; konflikty zbrojne (wiąże się z tym ochrona dóbr kultury w czasie pokoju i → w o j n y [t. 4]); migracja oraz związana z nią dyfuzja kultur.

Według U. Hannerza kultura światowa może ulec dalszym modyfikacjom w wyniku globalizacji i imperializmu kulturowego. Możliwe ich skutki to realizacja 4 scenariuszy:

- globalna ekumena, czyli globalna homogenizacja – dominacja kultury zachodniej (a zwłaszcza amerykańskiej) będzie całkowita, a wszystkie społeczności staną się mniej lub bardziej udaną repliką zachodniego stylu życia;

- długie historyczne trwanie przez nasycenia kulturowe – kraje peryferyjne powoli, z oporami, w toku kilku generacji zastąpią lokalne idee kulturowe, sensy i wartości zuniformizowanymi treściami płynącymi z dominujących centrów;
- deformacja kulturowa – uproszczenie, zubożenie, a nawet degradacja kultury zachodniej w toku jej adaptacji przez kraje peryferyjne;
- amalgamacja/kreolizacja kultur – hybrydyzacja, wzajemne uzupełnianie się i mieszanie.

Jednym ze zjawisk uważanych za potencjalne zagrożenie dla bezpieczeństwa kulturowego jest polityka wielokulturowości. Termin ten został po raz pierwszy użyty w Australii w 1973 r. i opierał się na założeniu, że różnorodne grupy kulturowe powinny być w stanie wyrażać i celebrować swoją tożsamość kulturową, a społeczeństwo i państwo uznają i szanują odmienność kultur, religii, ras, grup etnicznych, postaw i opinii w środowisku.

Ochrona kultury, zwłaszcza tej o wymiarze materialnym, była podejmowana na arenie międzynarodowej. Pierwszym takim przykładem był pakt Roericha (1935). Po doświadczeniach I wojny światowej podjęto działania w celu ochrony zabytków przed zniszczeniami wojennymi – polegało to choćby na katalogowaniu szczególnie cennych obiektów i ich oznaczaniu. Kolejnym etapem było powołanie w listopadzie 1945 r. Organizacji Narodów Zjednoczonych ds. Oświaty, Nauki i Kultury (United Nations Educational, Scientific and Cultural Organization, → U N E S C O [t. 4]). Problem niszczenia dóbr kultury podjęło też tzw. prawo norymberskie (1946 r.). Kluczowa jest jednak konwencja haska (14 maja 1954 r.). Inne ważne regulacje to m.in.:

- Zalecenie UNESCO z 19 listopada 1964 r.;
- Zalecenie UNESCO w sprawie środków zakazu i zapobiegania nielegalnemu wywozowi, przywozowi i przenoszeniu dóbr kultur z 14 listopada 1970 r.;
- Konwencja dotycząca środków zmierzających do zakazu i zapobiegania nielegalnemu przywozowi, wywozowi i przenoszeniu własności dóbr kultury (tzw. konwencja paryska) z 16 listopada 1972 r.;
- Konwencja w sprawie ochrony światowego dziedzictwa kulturalnego i naturalnego UNESCO z 25 czerwca 1995 r.;
- Konwencja rzymska o zwrocie dzieł skradzionych lub bezprawnie wywiezionych z 25 czerwca 1995 r.

Konwencję haską podpisało 88 państw. Uznano, że dobra kultury (→ d o b r a k u l t u r y – o c h r o n a w w a r u n k a c h k o n f l i k t u z b r o j n e g o [t. 2]) doznały poważnych szkód w toku poprzedzających ją konfliktów i że w następstwie rozwoju techniki wojennej coraz bardziej grozi im zniszczenie; szkody wyrządzone dobrom kultury, do jakiegokolwiek należałyby one narodu, stanowią uszczerbek w dziedzictwie kulturowym całej ludzkości. W celu zachowania i promowania światowego dziedzictwa kulturowego powołano Komitet Światowego Dziedzictwa. W jego skład wchodzą przedstawiciele 21 państw. Komitetowi doradzają następujące organizacje:

Międzynarodowa Rada Ochrony Zabytków i Miejsc Historycznych (International Council on Monuments and Sites, ICOMOS), Międzynarodowa Unia Ochrony Przyrody (International Union for Conservation of Nature, IUCN), Międzynarodowy Ośrodek Studiów nad Ochroną i Konserwacją Dziedzictwa Kulturowego (International Centre for the Study of the Preservation and Restoration of Cultural Property, ICCROM). Jednym z efektów ich pracy jest Lista światowego dziedzictwa UNESCO.

Bezpieczeństwo kulturowe w Polsce jest chronione też na poziomie prawa krajowego. Już preambuła do Konstytucji RP podkreśla wagę zachowania kultury: „zakorzenionej w chrześcijańskim dziedzictwie Narodu i ogólnoludzkich wartościach". Ponadto art. 5 wprowadza nakaz strzeżenia dziedzictwa narodowego. Artykuł 6 pkt 1 nakłada obowiązek stworzenia warunków upowszechniania i równego dostępu do dóbr kultury, będącej źródłem tożsamości narodu polskiego, jego trwania i rozwoju. Innymi źródłami prawa, które sankcjonują bezpieczeństwo kulturowe, są m.in.: Ustawa z dnia 7 października 1999 r. o języku polskim (Dz. U. 1999, nr 90, poz. 999), Ustawa z dnia 15 lutego 1962 r. o ochronie dóbr kultury (Dz. U. 1962, nr 10, poz. 48), Ustawa z dnia 6 stycznia 2005 r. o mniejszościach narodowych i etnicznych oraz o języku regionalnym (Dz. U. 2005, nr 17, poz. 141), Ustawa z 21 listopada 1996 r. o muzeach (Dz. U. 1996, nr 5, poz. 24), Rozporządzenie Rady Ministrów z 23 kwietnia 1963 r. w sprawie prowadzenia rejestru zabytków i centralnej ewidencji zabytków (Dz. U. 1963, nr 19, poz. 101; zm. Dz. U. 1986, nr 42, poz. 204). Organami szczególnie odpowiedzialnymi w tym zakresie są m.in. minister kultury i dziedzictwa narodowego, Generalny Konserwator Zabytków, działający w imieniu ministra kultury, wojewoda przy pomocy wojewódzkiego konserwatora zabytków jako kierownika jednostek organizacyjnych (wojewódzkiego oddziału Państwowej Służby Ochrony Zabytków), dyrektorzy (kierownicy) muzeów.

Jednym z ważniejszych problemów bezpieczeństwa kulturowego w Polsce jest współcześnie zabezpieczenie przed kradzieżami dzieł sztuki, a także odzyskiwanie utraconych w trakcie wojen, szczególnie podczas II wojny światowej, obiektów kultury (zob. → g r a b i e ż e d ó b r k u l t u r y [t. 2]). Nadal istnieją braki w skatalogowaniu skradzionych i zrabowanych dzieł.

Przemysław Mazur, Katarzyna Pabis-Cisowska

W. Bednarczyk, M. Kopczewski, *Bezpieczeństwo kulturowe w systemie bezpieczeństwa RP*, „Przedsiębiorczość i Zarządzanie" 2017, t. 18, z. 5, cz. 3; *Bezpieczeństwo państwa: wybrane problemy*, K.A. Wojtaszczyk, A. Materska-Sosnowska (red.), ASPRA-JR, Warszawa 2009; J. Czaja, *Bezpieczeństwo kulturowe Rzeczypospolitej Polskiej*, Krakowskie Towarzystwo Edukacyjne, Kraków 2004; tenże, *Kulturowe czynniki bezpieczeństwa*, Krakowskie Towarzystwo Edukacyjne, Oficyna Wydawnicza AFM, Kraków 2008; U. Hannerz, *Powiązania transnarodowe: kultura, ludzie, miejsca*, tłum. K. Franek, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2006; M. Marcinko, P. Łubiński, *Wybrane zagadnienia z zakresu międzynarodowego prawa humanitarnego*, Centrum Szkolenia Ochrony Ludności i Dóbr Kultury, Kraków 2009; P. Mazur, *Bezpieczeństwo kulturowe*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka,

R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; A. Włodkowska, *Bezpieczeństwo kulturowe*, [w:] *Bezpieczeństwo państwa*, K.A. Wojtaszczyk, A. Materska-Sosnowska (red.), ASPRA JR, Warszawa 2009; A.W. Ziętek, *Bezpieczeństwo kulturowe w Europie*, Wydawnictwo UMCS, Lublin 2013.

BEZPIECZEŃSTWO LOKALNE – stanowi ważny obszar w → n a u k a c h o b e z p i e c z e ń s t w i e [t. 3]. Upowszechniające się zjawisko desensytyzacji życia społecznego prowadzi do zwiększenia realnego poczucia → z a g r o ż e n i a [t. 4] w wyniku powszechnej znieczulicy, wycofania się lub izolowania społecznego. Przy omawianiu pojęcia bezpieczeństwa lokalnego należy szczególnie podkreślić rolę, jaką odgrywa w życiu człowieka jego własne poczucie → b e z p i e c z e ń s t w a. Na drodze socjalizacji jednostki uznają za własne narzucane im wartości i cele, dzięki którym wzrasta poziom ich bezpieczeństwa, gdyż warunkują one sprawne funkcjonowanie grupy społecznej, a tym samym zezwalają na jej przetrwanie. Wartością nazywane jest to, czemu można przypisać konkretne znaczenie. Nie tylko poprzez zbudowanie i zrozumienie pojęciowe, ale przede wszystkim poprzez działanie zgodne z definicją. Społeczność lokalna traktowana jest jako system społeczny zdeterminowany układem przestrzennym danego terytorium, przy czym bierze się pod uwagę wiele czynników determinujących funkcjonowanie społeczności lokalnej w ujęciu funkcjonalnym, natomiast przestrzeń społeczna ujmowana jest jako twór społeczny, w mniejszym stopniu zależny od warunków przyrodniczych czy typologicznych. Podkreślić należy, że gminy, miasta i powiaty różnią się pod wieloma względami, m.in.: powierzchnią, zaludnieniem, uprzemysłowieniem, zasobami, infrastrukturą, zatrudnieniem, poziomem zasobności mieszkańców czy rodzajem zagrożeń, obszarem i intensywnością ich występowania. Realizując zadania na rzecz osiągania pożądanego poziomu bezpieczeństwa lokalnego, samorządy muszą uwzględniać uwarunkowania, które właśnie na poziomie lokalnym różnicują zakres i skalę działań, jakie można i należy podejmować. Do grupy zasadniczych uwarunkowań bezpieczeństwa lokalnego możemy zaliczyć uwarunkowania: geograficzne, ekonomiczne, społeczne, polityczne i kulturowe. W Polsce podmioty działające na rzecz bezpieczeństwa lokalnego to: służby, inspekcje, straże, służby komunalne, opieka społeczna oraz organizacje pozarządowe.

Łukasz Czekaj

Bezpieczeństwo w środowisku lokalnym, W. Fehler (red.), Wydawnictwo Arte, Warszawa 2009; *Bezpieczeństwo w wymiarze lokalnym*, M. Leszczyński (red.), Warszawa 2013; Ł. Czekaj, *Bezpieczeństwo lokalne*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; A. Kłoskowska, *Socjologia kultury*, Wydawnictwo Naukowe PWN, Warszawa 1983; E. Moczuk, *Postrzeganie bezpieczeństwa publicznego w środowisku lokalnym*, Wydawnictwo Uniwersytetu Rzeszowskiego, Rzeszów 2003; H. Podedworna, *Analiza struktur społecznych. Wybrane przykłady*, [w:] *Socjologia ogólna: wybrane problemy*, J. Polakowska-Kujawa (red.), Oficyna Wydawnicza SGH, Warszawa 2007; A. Sosnowski, *Rozwój społeczności lokalnych u schyłku XX wieku*, [w:] *Społeczności lokalne w perspektywie integracji europejskiej. Studia i materiały*, R.B. Woźniak (red.), Bałtycka Wyższa Szkoła

Humanistyczna, Koszalin 2000; A. Urban, *Bezpieczeństwo społeczności lokalnych*, Editions Spotkania, Warszawa 2009.

BEZPIECZEŃSTWO LUDZKIE (ang. *human security*) – inaczej bezpieczeństwo jednostki, bezpieczeństwo człowieka, bezpieczeństwo personalne lub bezpieczeństwo humanitarne – koncepcja → b e z p i e c z e ń s t w a, która oznacza stan braku → z a g r o ż e n i a [t. 4] życia lub zdrowia, a także innych istotnych dla jednostki ludzkiej wartości i potrzeb np. wolności, pracy, posiadanych dóbr materialnych. Zasadniczą jej istotą jest ochrona i zapewnienie warunków realizacji żywotnych i ważnych interesów jednostki społecznej oraz ochrona przed zagrożeniami. Bezpieczeństwo ludzkie stanowi najwyższą wartość człowieka i wynika z jego indywidualnych cech osobowości, doświadczeń własnych i osób jemu najbliższych. Koncentruje się na zapewnieniu jednostce jako zasadniczemu podmiotowi bezpieczeństwa godnego życia, pewności przetrwania oraz możliwości rozwoju. Dąży do ograniczenia do minimum przeżyć negatywnych wynikających z uczestnictwa jednostki w życiu społecznym, które przejawiają się w postaci lęku lub strachu. Są to stany emocjonalne, które człowiek przeżywa na co dzień i których nie sposób uniknąć. Lęk dotyczy → z a g r o ż e ń s p o ł e c z n y c h [t. 4], np. utraty pracy, strach natomiast jest właściwy dla sytuacji zagrożenia fizycznego, np. doznanie uszczerbku na zdrowiu w wyniku napaści lub wypadku.

Koncepcja ta najczęściej jest łączona z działalnością ONZ. W najogólniejszym rozumieniu podmiotem bezpieczeństwa w koncepcji *human security* jest człowiek, jednostka ludzka. Celem bezpieczeństwa natomiast jest godne przetrwanie i rozwój w demokratycznym państwie prawa, źródłem zagrożeń są zaś: państwo (*sic!)*, procesy globalizacyjne, → k a t a s t r o f y n a t u r a l n e [t. 2] oraz zmiany klimatyczne.

Koncepcja *human security* stała się kolejnym etapem ewolucji poszerzonego ujmowania bezpieczeństwa. Rozszerzone podejście w definiowaniu bezpieczeństwa rozpoczęło się w 2. poł. XX w., kiedy to w przypadku państwa jako podmiotu bezpieczeństwa wyraźna stała się tendencja do integrowania bezpieczeństwa wewnętrznego i zewnętrznego. Państwo jawi się tu już nie tylko jako → b e z p i e c z e ń s t w o m i l i t a r n e, ale także jako bezpieczeństwo społeczne. M. Cieślarczyk zwrócił uwagę, że „przedmiot bezpieczeństwa mieści się z jednej strony w sferze wartości podmiotu, z drugiej zaś – w sferze aktywności podmiotu", dlatego należy wymienić → b e z p i e c z e ń s t w o e k o l o g i c z n e, bezpieczeństwo zdrowotne, → b e z p i e c z e ń s t w o e k o n o m i c z n e, → b e z p i e c z e ń s t w o p o l i t y c z n e i →b e z p i e c z e ń s t w o s p o ł e c z n e. Kompleksowe podejście uwzględniające zarówno militarne, jak i pozamilitarne ujęcie bezpieczeństwa – znane jako szkoła kopenhaska – rozwinął B. Buzan wraz z O. Wæverem i J. de Wildem w pracy *Security. A New Framework for Analysis*. Otworzyli oni nowe pola eksploracji, zwracając

uwagę, że zagrożenia państwa mają nie tylko charakter zewnętrzny militarny, ale także wewnętrzny. Według badaczy można wyróżnić 5 sektorów bezpieczeństwa:

- wojskowy – implikujący przymus siłowy;
- polityczny – skupiający się na relacjach władzy, instytucji zarządzania oraz identyfikowania;
- ekonomiczny – opierający się na relacjach w handlu;
- społeczny – dotyczący wspólnej tożsamości;
- ekologiczny – opierający się na relacjach, jakie zachodzą pomiędzy działalnością człowieka oraz środowiskiem naturalnym.

Tym sektorom bezpieczeństwa odpowiada 5 typów bezpieczeństwa: militarne, polityczne, ekonomiczne, społeczne oraz ekologiczne. Koncepcja szkoły kopenhaskiej Buzana dała początek pogłębianiu badań nad naturą bezpieczeństwa, a konsekwencją tego postępowania stało się właśnie opracowanie koncepcji *human security*.

Kluczowym elementem koncepcji *human security* jest spojrzenie na kwestię bezpieczeństwa nie przez pryzmat państwa i jego globalnych zagrożeń, ale z punktu widzenia jednostki, zainteresowanie się jej życiem, problemami oraz przysługującymi jej prawami i wolnościami. Koncepcja stawia człowieka i ludzkie zbiorowości w centrum zainteresowania, debaty i polityki. To człowiek jest tu najważniejszy, jego potrzeby i oczekiwania, a rola państwa ma charakter instrumentalny i służy zapewnieniu dobrobytu. Pogląd ten opiera się na tradycji → p r a w c z ł o w i e k a [t. 3], które mają chronić jednostkę przed nadużyciami ze strony własnego państwa, a także na koncepcji rozwoju, zgodnie z którą państwo jest instrumentem koniecznym dla promowania bezpieczeństwa ludzkiego. Z perspektywy człowieka istotne jest zapewnienie bezpieczeństwa w różnych dziedzinach życia: ekonomicznej, żywnościowej, zdrowotnej, ekologicznej, fizycznej, społecznej i politycznej. Przekłada się to bezpośrednio na zagadnienia, które powinny być rozpatrywane w ramach bezpieczeństwa ludzkiego, są to: ubóstwo, → p r z e m o c [t. 3] na tle seksualnym i płciowym, handel narkotykami, degradacja środowiska naturalnego, choroby zakaźne, zwłaszcza AIDS, katastrofy naturalne, ochrona cywilów podczas konfliktów zbrojnych, uchodźcy i przesiedlenia wewnętrzne, → i n t e r w e n c j a h u m a n i t a r n a [t. 2], dzieci-ofiary konfliktów zbrojnych, → p r z e s t ę p c z o ś ć z o r g a n i z o w a n a [t. 3] transnarodowa, → t e r r o r y z m [t. 4], karanie zbrodni międzynarodowych, społeczna odpowiedzialność korporacji transnarodowych i rola aktorów pozapaństwowych.

Wybitny kanadyjski badacz bezpieczeństwa – F.O. Hampson – analizując zakres zagadnienia bezpieczeństwa jednostki, wskazał 3 odmienne rozumienia tego pojęcia. Pierwsze z nich określa bezpieczeństwo jednostki w kategoriach praw naturalnych i rządów prawa. Koncepcja ta opiera się na centralnym dla liberalizmu uznaniu podstawowych praw człowieka (do życia, wolności i dążenia do szczęścia), które społeczność międzynarodowa obowiązana jest chronić i wspierać. Druga interpretacja pojęcia bazuje na humanitaryzmie. W ten nurt wpisują się m.in. działania na rzecz pogłębiania

i wzmacniania prawa międzynarodowego w kwestii → ludobójstwa [t. 3] i → zbrodni wojennych [t. 4] czy eliminacji broni szczególnie niebezpiecznej dla → ludności cywilnej [t. 3]. Z tej koncepcji wywodzi się również idea interwencji humanitarnych, mających na celu poprawę podstawowych warunków życia uchodźców i innych grup ludzi oderwanych od własnych domów i społeczności z powodu konfliktów zbrojnych. Trzecia koncepcja, w dużym stopniu ukształtowana przez idee sprawiedliwości społecznej, ujmuje bezpieczeństwo jednostki w sposób bardzo szeroki. Swoim zakresem obejmuje różne formy zagrożeń (np. gospodarcze, ekologiczne, społeczne) dla podstaw utrzymania jednostek oraz ich dobrostanu i szeroko rozumie zagrożenia (realne lub potencjalne) dla przetrwania i zdrowia jednostek.

Początków współczesnej koncepcji bezpieczeństwa ludzkiego należy szukać po II wojnie światowej, kiedy nastąpił wzrost zainteresowania społeczności międzynarodowej prawami człowieka i koncentracją na prawach jednostek. Źródeł koncepcji trzeba jednak upatrywać w oświeceniowych poglądach J.-J. Rousseau, T. Hobbesa oraz J. Locke'a. Ci wielcy humaniści stali się prekursorami myślenia o konieczności uznania praw podstawowych przynależnych każdemu człowiekowi. Państwo postrzegali jako gwaranta tych praw i instytucję, która na mocy umowy społecznej winna jest zapewnić bezpieczeństwo i ochronę jednostce ludzkiej. W pokoju dostrzegali szanse człowieka na godne i bezpieczne życie. Idee te, wówczas pionierskie, stały się po II wojnie światowej źródłem poglądów nobilitujących godność i wartość człowieka jako istoty ludzkiej, a także wskazywały potrzebę włączenia podmiotów innych niż państwo – takich jak choćby organizacje międzynarodowe – do odpowiedzialności za bezpieczeństwo ludzi. W ten sposób postrzegania człowieka wpisywała się również mowa prezydenta USA F.D. Roosevelta wygłoszona w 1941 r., w której wspomniał o 4 wolnościach ludzkich: słowa (*freedom of speech*), wyznania (*freedom of worship*), wolności od niedostatku, nędzy i ubóstwa (*freedom from want*) oraz wolności od strachu (*freedom from fear*). Kontynuacją tego sposobu myślenia było stwierdzenie sekretarza stanu USA E. Stettiniusa na konferencji założycielskiej ONZ w 1945 r.:

> Walka o pokój musi być toczona na dwóch frontach. Pierwszy to front bezpieczeństwa, gdzie zwycięstwo oznacza wolność od strachu, drugi to front ekonomiczny i społeczny, gdzie zwycięstwo oznacza wolność od niedostatku. Tylko zwycięstwo na tych dwóch frontach może zagwarantować światu trwały pokój.

Samo pojęcie *human security* zostało najprawdopodobniej użyte po raz pierwszy w 1966 r. przez psychologa rozwoju i autora teorii bezpieczeństwa – W. Blatza z Uniwersytetu w Toronto.

Okres wygaszania → zimnej wojny [t. 4] i sukcesywnego zmniejszania się poziomu zagrożenia poważniejszym → konfliktem międzynarodowym [t. 2] sprzyjał szerszemu spojrzeniu na kwestię bezpieczeństwa, innemu niż tylko w wymiarze militarnym. Wówczas zaczęto dostrzegać nowe wyzwania – pochodne

procesów globalizacji, nierównomiernego rozwoju, wzmożonych ruchów migracyjnych oraz narastania → p r z e s t ę p c z o ś c i [t. 3]. Zaobserwowano, że zagrożenia te godzą najbardziej w poczucie bezpieczeństwa indywidualnego jednostki ludzkiej. Dało to asumpt do powstania i rozwoju idei *human security*. Formalnym początkiem nowej koncepcji, wskazującej człowieka jako podstawowy podmiot bezpieczeństwa, stała się podjęta w 1991 r. w Sztokholmie inicjatywa 30 wybitnych polityków na rzecz globalnego bezpieczeństwa i zarządzania. Wzywała ona społeczność międzynarodową do stworzenia szerszej koncepcji bezpieczeństwa obejmującej także zagrożenia wynikające z niepowodzeń rozwoju, degradacji środowiska, nadmiernego wzrostu liczby ludności i jej migracji oraz braku postępów w rozwoju demokracji. Konkretyzacja tego pomysłu nastąpiła w publikowanym corocznie Raporcie o rozwoju społecznym (Human Development Report) Programu Narodów Zjednoczonych ds. Rozwoju (United Nations Development Programme, UNDP) z 1994 r., który do dziś stanowi kluczowy dokument w zakresie studiów nad bezpieczeństwem ludzkim. Zwrócono w nim uwagę na to, że rozpatrywanie bezpieczeństwa ludzkiego musi ujmować podstawowe własności bezpieczeństwa człowieka we współczesnym świecie. Wskazano:

- uniwersalizm pojęcia i jego powszechność – obejmuje wszystkich ludzi na całym świecie, niezależnie od miejsca zamieszkania;
- współzależność wszystkich wymiarów bezpieczeństwa i ich wzajemne powiązanie ze sobą;
- łatwość jego zapewnienia poprzez uznanie za priorytetowe działań profilaktycznych i zapobiegawczych (w porównaniu z trudniejszą późniejszą interwencją i niwelowaniem skutków naruszenia bezpieczeństwa ludzkiego);
- zogniskowanie na człowieku – uczynienie człowieka (a nie państwa) centralnym obiektem zainteresowania.

Przedmiotem zainteresowania stała się jednostka, a nie państwo i jego środowisko. Stwierdzono, że współczesne zagrożenia są wywołane głównie przez człowieka i wskazano na konieczność rozumienia związku między → z r ó w n o w a ż o n y m r o z w o j e m [t. 4] ludzkości a bezpieczeństwem. Zauważono, że dla większości społeczeństwa brak poczucia bezpieczeństwa wynika z obawy o codzienny byt (pożywienie, praca, zdrowie), a nie ze strachu przed globalną katastrofą. W dokumencie przedstawiono 2 główne nurty koncepcji *human security*: pierwszy dotyczył bezpieczeństwa wolnego od przewlekłych problemów, takich jak głód, choroby i prześladowania, drugi oznaczał ochronę przed nagłymi i bolesnymi wypadkami w życiu codziennym. W raporcie sformułowano także 6 kategorii → z a g r o ż e ń g l o b a l n y c h [t. 4] dla bezpieczeństwa ludzkości: niekontrolowany przyrost demograficzny, nierówny poziom rozwoju gospodarczego, nadmierne migracje, degradację środowiska naturalnego, produkcję narkotyków i handel nimi oraz międzynarodowy terroryzm i proliferację broni jądrowej. Bezpieczeństwo ludzkie obejmuje więc 2 kluczowe kwestie – wolność od strachu i wolność od głodu.

W dokumencie UNDP do 5 sektorów bezpieczeństwa Buzana dodano jeszcze 3: bezpieczeństwo żywnościowe, zdrowotne i osobiste. Bezpieczeństwo jednostki można określić jako ograniczenie do minimum negatywnych doznań jednostki w związku z jej uczestnictwem w życiu publicznym.

W raporcie stwierdzono ponadto, że źródłem współczesnych → z a g r o ż e ń b e z p i e c z e ń s t w a [t. 4] ludzkiego mogą być – obok samego człowieka i państwa – także procesy globalizacyjne, katastrofy naturalne, zmiany klimatyczne, a nawet procesy ekonomiczne. Zagrożenia dla bezpieczeństwa ludzkiego zatraciły swój indywidualny, lokalny lub narodowy charakter i nabrały bardziej globalnego charakteru, obejmując takie problemy jak m.in.: narkotyki, AIDS czy terroryzm. Pojęcie bezpieczeństwa ludzkiego obejmuje także bezpieczeństwo godności, miejsca zamieszkania, tajemnice życia osobistego, nieingerencję w życie osobiste i rodzinne, wolność myśli i słowa, światopoglądu, działalność gospodarczą, bezpieczeństwo własności itp. Bezpieczeństwo ludzkie jest bodźcem dla wszystkich krajów, zarówno rozwiniętych, jak i rozwijających się, do przeglądu istniejących polityk bezpieczeństwa, ekonomicznych, rozwojowych i społecznych. Nadrzędnym celem tych polityk powinno być tworzenie rzeczywistych możliwości zapewniania ludziom bezpieczeństwa, środków do życia i godności.

Koncepcja *human security* pierwotnie zrodziła się na gruncie ONZ i tam też była wykorzystywana jako narzędzie analizy służące lepszemu rozpoznaniu środowiska międzynarodowego, jego potrzeb oraz wypracowaniu metod ich realizacji. Została następnie zaimplementowana przez różne państwa i podmioty międzynarodowe. Początkiem instytucjonalnego podejścia do bezpieczeństwa ludzkiego było utworzenie w 1999 r. przez rząd Japonii i ONZ Funduszu Powierniczego ds. Bezpieczeństwa Ludzkiego (United Nations Trust Fund for Human Security, UNTFHS) z wkładem początkowym w wysokości 90 mln USD. Fundusz ten wspierał rozmaite programy służące m.in.: ochronie osób narażonych na przemoc fizyczną, dyskryminację i wykluczenie, ochronie uchodźców i migrantów ekonomicznych oraz osób w sytuacjach konfliktów zbrojnych, zapewnieniu minimalnych standardów życia ludziom żyjącym w skrajnym ubóstwie, wzmocnieniu opieki zdrowotnej i usług medycznych w miejscach, gdzie nie interweniowały inne instytucje, a także projektów służących poprawie szans edukacyjnych, głównie dla dziewcząt. Następnie w 2001 r. powstała Komisja Bezpieczeństwa Ludzkiego (Commission on Human Security, CHS), której głównymi inicjatorami byli S. Ogata, była komisarz ds. uchodźców, i A. Sen – laureat Nagrody Nobla w dziedzinie ekonomii. Celem działania komisji było opracowanie koncepcji bezpieczeństwa ludzkiego jako narzędzia służącego formułowaniu i wdrażaniu konkretnych programów działań w tym zakresie. Komisja zakończyła działalność w 2003 r. sprawozdaniem zatytułowanym *Human Security Now.* Zdefiniowano w nim bezpieczeństwo ludzkie jako ochronę podstawowych wolności będących istotą życia, a także konieczność zabezpieczenia ludzi przed krytycznymi i powszechnymi zagrożeniami. Za niezbędny

do eliminacji owych zagrożeń uznano system krajowych i międzynarodowych norm, procesów i instytucji, zdolnych do elastycznego działania.

Koncepcja *human security* dzieli się na 2 szkoły: japońską (tzw. szeroki zakres *human security*) oraz kanadyjską (wąski zakres *human security*). Przedstawiciele szkoły japońskiej, rozwijanej głównie przez Japonię oraz inne państwa azjatyckie, koncentrowali się na kwestiach rozwoju i poszanowania praw człowieka, które odpowiadały nurtowi *freedom from want* (wolność od ubóstwa w sensie materialnym). Podejście to odnosi się nie tylko do wolności od zewnętrznych konfliktów międzynarodowych stanowiących zagrożenie dla państwa, ale także od konfliktów wewnętrznych, zagrożenia przestępczością, chorób, głodu, degradacji środowiska, terroryzmu, naruszania praw człowieka zarówno w skali indywidualnej, jak i zbiorowej. Zgodnie z tymi poglądami bezpieczeństwo nie może ograniczać się jedynie do bezpośredniej pomocy militarnej, lecz powinno obejmować także zagrożenia fizyczne, dobrobytu ekonomicznego, godności i wartości człowieka jako istoty ludzkiej. Specyfika Japonii jako jednego z najbardziej zaawansowanych pod względem stopnia rozwoju państw świata, ale jednocześnie doświadczonego tragedią nuklearnego holokaustu, w następstwie gospodarczego → k r y z y s u [t. 2] azjatyckiego, który dotknął państwa regionu w 1997 r., spowodowała, że w tym państwie oficjalnie wdrożono założenia koncepcji *human security* do polityki zagranicznej, koncentrując się głównie na aspektach społecznych i gospodarczych. Kryzys gospodarczy, który w latach 90. XX w. spowodował destabilizację sytuacji w Japonii, wygenerował konieczność podjęcia aktywnych działań w kierunku złagodzenia jego efektów, a nawet całkowitego zażegnania. Ówczesny minister spraw zagranicznych – H. Fukuda – w 1994 r. wskazał konieczność działania na rzecz osiągnięcia dostatku i dobrobytu ludzi, ochrony praw człowieka i świadczenia pomocy humanitarnej. Ponadto na forum ONZ zapowiedział walkę z zagrożeniami o charakterze społecznym, gospodarczym i ekologicznym.

Japońska szkoła *human security* podkreśla godność człowieka. W tym czasie również inne państwa azjatyckie zaczęły przychylniej podchodzić do założeń *human security*. A. Fukushima i W.T. Tow wskazali – oprócz kryzysu azjatyckiego – inne przyczyny włączania koncepcji do polityk zagranicznych państw, były to m.in.: epidemia SARS w 1999 r., epidemia ptasiej grypy, tsunami na Oceanie Indyjskim w 2004 r., trzęsienia ziemi w Pakistanie w 2005 r. i w Chinach w 2008 r., jak również awaria elektrowni atomowej w Fukushimie w Japonii w 2011 r. Wszystkie te zagrożenia godziły w życie i przetrwanie rzesz ludzi, a ponadto miały charakter masowy, przenikały granice, będąc niemożliwymi do zwalczenia przez lokalne i krajowe władze. Jako że w konstytucji Japonii z 1946 r. znajduje się zapis, że państwo to wyrzeka się → w o j n y [t. 4] oraz użycia bądź groźby użycia siły, naturalna była droga Japonii w kierunku raczej „wolności od ubóstwa" niż „wolności od strachu". Jej śladem podążały kolejne państwa i organizacje azjatyckie, zwłaszcza regionu Azji Południowo-Wschodniej, które mocniej zaczęły akcentować problematykę zagrożeń społeczno-gospodarczych.

Władze Japonii w polityce zagranicznej dużą wagę przywiązywały do kwestii dostarczania pomocy humanitarnej i rozwojowej dla państw jej potrzebujących. W ramach ONZ to z inicjatywy rządu Japonii powołano UNTFHS, z którego finansowano projekty związane bezpośrednio z promocją bezpieczeństwa jednostki. Ponadto sfinansowano utworzenie międzynarodowej Komisji ds. Bezpieczeństwa Jednostki. W Japonii w pierwszej kolejności koncentrowano się na zaspokajaniu potrzeb ludzkich, głównie poprzez zapewnienie bezpiecznego środowiska i pomocy humanitarnej, dopiero w następnej zaś zwrócono uwagę na prawa człowieka oraz wolności polityczne.

Terminem *human security* posłużył się po raz pierwszy premier Japonii K. Obuchi w 1998 r., w swoich przemowach stwierdzając, że bezpieczeństwo jednostki ludzkiej „jest koncepcją, która przyjęła wszechstronny punkt widzenia na wszystkie zagrożenia dla ludzkiego przeżycia, życia i godności oraz podkreśla potrzebę odpowiedzi na takie zagrożenia". Jego pogląd ukształtował podejście Japonii do koncepcji bezpieczeństwa ludzkiego. Została ona wdrożona do założeń polityki zagranicznej. W raportach nazywanych Niebieskimi Księgami Dyplomacji (Diplomatic Bluebooks), przyjmowanych po 1990 r., widoczne jest to, jak dużą wagę przywiązywano do kwestii dostarczania pomocy humanitarnej i rozwojowej dla państw potrzebujących. W kolejnych niebieskich księgach wyjaśniono, w jaki sposób Japonia rozumie i chce wdrażać koncepcję *human security*. W 2000 r. podkreślono np. potrzebę skoncentrowania się na człowieku i jego potrzebach oraz zaspokajaniu tych potrzeb drogą współpracy międzynarodowej na poziomie rządów, organizacji międzynarodowych i → s p o ł e c z e ń s t w a o b y w a t e l s k i e g o [t. 4]. Koncepcję bezpieczeństwa ludzkiego zdefiniowano ostatecznie w Niebieskiej Księdze z 2002 r., uznając, że jest to program, który skupia się na wzmocnieniu skoncentrowanych na człowieku działań z perspektywy ochrony życia, środków do życia i godności indywidualnej jednostki ludzkiej oraz realizacji możliwości tkwiących w każdej jednostce. Uzupełniono zatem dotychczasowe rozumienie koncepcji opartej na kwestiach społecznych i ekonomicznych o elementy rozwoju, czyli sposobności wykorzystania własnych możliwości, kładąc jednocześnie spory nacisk na poszanowanie godności osobistej każdego człowieka. W pierwszej kolejności skoncentrowano się zatem na zaspokojeniu potrzeb ludzkich w zakresie zapewnienia bezpieczeństwa i zdrowego środowiska oraz dostępu do pomocy humanitarnej, a w następnej kolejności rozszerzono to pojęcie na prawa człowieka oraz wolności politycznych.

Szkoła kanadyjska (norweska) wypracowała odrębne, wąskie podejście, które łączy bezpieczeństwo ludzkie z wolnością od strachu (*freedom from fear*), uwydatniając znaczenie przestrzegania praw człowieka i związaną z tym niekiedy konieczność prowadzenia operacji zagranicznych w celu → o c h r o n y l u d n o ś c i [t. 3] cywilnej. Podłożem do zainteresowania kanadyjskich władz kwestiami bezpieczeństwa jednostki była działalność ministra spraw zagranicznych Kanady L. Axworthy'ego, nominowanego do Pokojowej Nagrody Nobla. Liczne inicjatywy tego męża stanu zaowocowały

zmianą w kanadyjskiej polityce zagranicznej w kierunku *human security.* Zauważono wówczas, że bezpieczeństwo ludzkie to coś więcej niż brak militarnego zagrożenia. To zabezpieczenie przed niedostatkiem gospodarczym, zagwarantowanie akceptowalnej jakości życia oraz fundamentalnych praw człowieka. To koncentracja na ochronie istnień ludzkich przed szeroko rozumianą przemocą, w tym również o podłożu politycznym, a także na ludzkich kosztach konfliktów zbrojnych, masowych śmierci, represji i wysiedleń. To wywieranie dużego nacisku na wojskowe interwencje humanitarne prowadzone w celu ochrony życia i praw jednostek w sensie funkcjonowania w demokratycznym państwie prawa i w warunkach społeczeństwa obywatelskiego.

W 1997 r. Kanada wdrożyła koncepcję *human security* do swojej polityki. Naczelnym celem polityki zagranicznej Kanady stała się ochrona jednostki w pokojowych operacjach zagranicznych. W dokumencie *Wolność od strachu. Polityka zagraniczna Kanady dla bezpieczeństwa ludzkiego* (*Freedom from Fear: Canada's Foreign Policy for Human Security*) wyznaczono 5 głównych wytycznych: ochronę ludności cywilnej, udział w operacjach pokojowych, zapobieganie konfliktom, zarządzanie i odpowiedzialność za stabilizowane tereny oraz → b e z p i e c z e ń s t w o p u b l i c z n e . Ponadto w dokumencie wskazano, że państwo może stanowić źródło zagrożeń dla ludzi, oraz stwierdzono, że *human security* nie jest przeciwstawne do → b e z p i e c z e ń s t w a n a r o d o w e g o , ale powinno być względem niego komplementarne. Szkoła kanadyjska była popierana przez Norwegię, a także Holandię.

Efektem działań szkoły kanadyjskiej było powstanie w 1999 r. Sieci Bezpieczeństwa Jednostki (Human Security Network, HSN), której członkami stało się 12 państw – są to: Austria, Chile, Kostaryka, Grecja, Irlandia, Jordania, Mali, Norwegia, Panama, Słowenia, Szwajcaria i Tajlandia; Republika Południowej Afryki ma obecnie status obserwatora – reprezentujących podobne poglądy na bezpieczeństwo ludzkie. Sieć ta stanowiła swoistą platformę dyskusyjną oraz konsultacyjną dla ministrów spraw zagranicznych, członków społeczeństwa obywatelskiego oraz środowiska naukowego. Efekt owych działań miał na celu podnoszenie świadomości w społeczeństwie w zakresie bezpieczeństwa ludzkiego, pobudzanie procesów politycznych oraz koncentrację uwagi międzynarodowej na kwestiach dotyczących tej kategorii bezpieczeństwa.

Kanadyjski punkt widzenia podzielany jest zwłaszcza przez Norwegię, a także Holandię i inne państwa europejskie. Efektem zacieśnienia współpracy kanadyjsko-norweskiej było podpisanie w 1998 r. deklaracji z Lysøen, w której wskazano 9 podstawowych zagadnień z obszaru bezpieczeństwa ludzkiego, w ramach których miała zostać podjęta współpraca. Były to: kampania na rzecz zaprzestania stosowania min lądowych; działalność → M i ę d z y n a r o d o w e g o T r y b u n a ł u S p r a w i e d l i w o ś c i [t. 3]; prawa człowieka; → m i ę d z y n a r o d o w e p r a w o h u m a n i t a r n e [t. 3]; rola kobiet w procesie budowania pokoju; proliferacja broni; udział dzieci w konfliktach zbrojnych; wykorzystanie dzieci do pracy; współpraca z państwami Północy i Arktyki. Obszary te wyznaczają więc zakres przedmiotowy

human security w wąskim ujęciu, które w przeciwieństwie do podejścia ONZ oraz Japonii nie akcentuje wymiaru społeczno-gospodarczego, skupiając się raczej na sferze politycznej i militarnej. W ujęciu kanadyjskim wyróżnia się 5 priorytetów bezpieczeństwa jednostki. Jest to ochrona ludności cywilnej podczas konfliktów zbrojnych, udział w operacjach pokojowych, zapobieganie konfliktom, właściwe administrowanie oraz bezpieczeństwo publiczne.

Koncepcja bezpieczeństwa ludzkiego w 2004 r. została przyjęta także przez UE. Opublikowano wówczas dokument pod nazwą *A Human Security Doctrine for Europe*, w którym wskazano, że polityka bezpieczeństwa UE powinna opierać się na bezpieczeństwie człowieka, a nie bezpieczeństwie państwa. Następnie wskazano 7 zasad, na których będzie zakotwiczona europejska doktryna bezpieczeństwa. Należy do nich: prymat praw człowieka, legitymizowana władza oparta na zasadach demokratycznych, zasada multilateralizmu, preferencje dla oddolnych inicjatyw, wzmocnienie współpracy regionalnej, wykorzystanie w działaniach narzędzi zgodnych z prawem oraz stosowne do zagrożenia użycie siły. Także inne organizacje europejskie, m.in. Organizacja Bezpieczeństwa i Współpracy w Europie (OBWE), uznały koncepcję *human security*, wskazując, że zapewnienie bezpieczeństwa ludzkiego jest obowiązkiem indywidualnym i zbiorowym wszystkich państw, a prawa człowieka i bezpieczeństwo są nierozdzielne. Od tego momentu poszanowanie praw człowieka uznane zostało za jeden z fundamentów porządku międzynarodowego.

Od lat 90. koncepcja ewoluowała i współcześnie wpisuje się w doktrynę prowadzenia pokojowych operacji zagranicznych. Początkowo koncentrowała się głównie na fizycznej ochronie życia jednostki, z czasem w jej zakres włączono wszelkie militarne i niemilitarne zagrożenia nie tylko wobec pojedynczego człowieka, lecz także dla całego społeczeństwa. Istotne jest to, że koncepcja staje się coraz bardziej rozpowszechniona i rozwija się szczególnie prężnie w demokratycznych systemach politycznych. W znacznie większym stopniu niż w ustrojach autorytarnych czy totalitarnych podejmuje się w nich starania w kierunku realizacji interesów własnych obywateli. Co ważne, bezpieczeństwa ludzkiego nie należy traktować jako alternatywnego i kolizyjnego z bezpieczeństwem państwa, ale jako je uzupełniające, poszerzone rozumienie bezpieczeństwa, które w hierarchii potrzeb Maslowa sytuuje się zaraz za potrzebami fizjologicznymi.

Koncepcja *human security* – mimo że zdobywa coraz więcej zwolenników wśród państw i organizacji międzynarodowych, m.in. USA i UE – rodzi jednak spore kontrowersje i sprzeczne oceny. Główne zarzuty dotyczyły jej zbyt szerokiego zakresu, obejmującego prawie wszystkie dziedziny życia, co w konsekwencji może stanowić zbyt obszerny zakres prowadzonych badań, brak uniwersalnej definicji, a także brak jednoznacznego rozróżnienia bezpieczeństwa ludzkiego i praw człowieka. Powoduje to, że jest ona mało przydatna dla decydentów politycznych. Poszczególni obserwatorzy i analitycy koncepcji zaliczają do tej kategorii rozmaite negatywne zjawiska,

w związku z czym trudno jest określić definitywnie, co bezpieczeństwem ludzkim nie jest, a co jest. W podejściu do bezpieczeństwa ludzkiego nie sprecyzowano dokładnie hierarchii jego zagrożeń, nie wskazano też, które podmioty konkretnie są odpowiedzialne za jego zapewnienie. Istotnym problemem jest ponadto określenie uniwersalnego progu bezpieczeństwa ludzkiego, determinowanego przez uwarunkowania społeczne i kulturowe. Nie istnieją bowiem standardy uniwersalne w tym względzie. To, co dla ludności krajów rozwiniętych godzi w sposób nieakceptowalny w ludzką godność, może być dla pewnych środowisk codziennością. Pomimo instytucjonalizacji oraz szerokiej promocji koncepcji bezpieczeństwa ludzkiego idea ta pozostaje nadal w fazie formowania i stanowi rodzaj wyzwania dla świata.

Amerykańscy badacze poszerzają koncepcję 7 obszarów *human security* wskazanych w raporcie UNDP z 1994 r. dodatkowo o bezpieczeństwo psychologiczne oraz o bezpieczeństwo płci. W UE kluczowym dokumentem w zakresie *human security* jest raport barceloński z 2004 r. – *A Human Security Doctrine for Europe* – który również przyjął założenia szkoły kopenhaskiej.

Praktyczne aspekty koncepcji przedstawia G. Michałowska, zwracając uwagę, że bezpieczeństwo państwa nie jest jednoznaczne z bezpieczeństwem obywateli konkretnego państwa. Przykładem takich państw są Korea Północna czy Sudan. Powołując się na dokument UNDP, badaczka określa bezpieczeństwo ludzkie jako zabezpieczenie przed stałymi zagrożeniami (takimi jak głód, choroby, ucisk), a także zapewnienie ochrony przed gwałtownymi i szkodliwymi wstrząsami w życiu codziennym. Przedstawia również genezę utworzonego w 1999 r. UNTFHS. Z budżetu funduszu udało się zrealizować liczne projekty w wielu krajach. Wspierane programy dotyczyły m.in.: ochrony uchodźców wewnętrznych oraz migrantów ekonomicznych, ochrony osób w sytuacjach konfliktów zbrojnych, zapewnienie minimalnych standardów życia dla osób narażonych na ubóstwo, wzmocnienia → o c h r o n y z d r o w i a [t. 3] w miejscach wcześniej niewspieranych przez inne instytucje oraz poprawy szans edukacyjnych. Według badaczki koncepcja bezpieczeństwa ludzkiego jest w fazie ciągłego formowania się.

We współczesnym rozumieniu koncepcji *human security* ustalono, że dla bezpieczeństwa ludzkiego istotne jest stworzenie takich warunków, aby jednostka będąca podmiotem nie była oraz nie czuła się zagrożona w jakikolwiek sposób w otaczającym ją świecie. Koncepcja bezpieczeństwa ludzkiego ma wymiar uniwersalny, co oznacza, że bezpieczeństwo ludzkie jest istotne dla wszystkich ludzi na całym świecie. Wiele problemów, takich jak bezrobocie, przestępczość czy zanieczyszczenia środowiska, jest wspólnych dla wszystkich. Ponadto elementy składowe bezpieczeństwa ludzkiego są współzależne, pojawiające się w jednym miejscu na świecie problemy nie dają się współcześnie odizolować – jest duże prawdopodobieństwo, że dany problem dotknie też inne narody, by wspomnieć np. epidemie, terroryzm czy konflikty etniczne. Bezpieczeństwo ludzkie zorientowane jest na człowieku jako jednostce, na tym, czy w miejscu, w którym żyje, ma możliwość dokonywania wyborów oraz czy żyje w warunkach

pokoju. Z uwagi na pojawiające się coraz to nowsze zagrożenia na świecie problemy takie jak zanieczyszczenia środowiska, epidemie, choroby, przestępczość, ubóstwo, handel narkotykami, terroryzm czy migracje powinno się rozpatrywać w ramach bezpieczeństwa ludzkiego.

Sabina Olszyk, Żaneta Mrożek

A Decade of Human Security. Global Governance and New Multilateralisms, D.R. Black, T.M. Shaw, S.J. MacLean (eds.), Routledge, London 2016; B. Buzan, O. Wæver, J. de Wilde, *Security. A New Framework for Analysis*, Lynne Rienner Publishers, Boulder–London 1998; M. Cieślarczyk, *Teoretyczne i metodologiczne podstawy badania problemów bezpieczeństwa i obronności państwa*, Wydawnictwo Akademii Podlaskiej, Siedlce 2009; Commission on Human Security, *Human Security Now: Protecting and Empowering People*, Commission on Human Security, New York 2003; A. Fukushima, W.T. Tow, *Human Security and Global Governance*, [w:] *Security Politics in the Asia-Pacific: A Regional-Global Nexus?*, W.T. Tow (ed.), Cambridge University Press, New York 2009; P. Grzywna, *Bezpieczeństwo zdrowotne w nauce o polityce społecznej. Wprowadzenie do dyskusji*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2017; F.O. Hampson, *Bezpieczeństwo jednostki*, [w:] *Studia bezpieczeństwa*, P.D. Williams (red.), tłum. W. Nowicki, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2012; K.P. Marczuk, *Bezpieczeństwo wewnętrzne w poszerzonej agendzie studiów nad bezpieczeństwem*, [w:] *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia*, S. Sulowski, M. Brzeziński (red.), Dom Wydawniczy Elipsa, Warszawa 2009; taż, *Pojęcie i zakresy human security*, [w:] *Trzy wymiary współczesnego bezpieczeństwa*, S. Sulowski, M. Brzeziński (red.), Dom Wydawniczy Elipsa, Warszawa 2014; taż, *Trzecia opcja. Gwardie narodowe w wybranych państwach basenu Morza Śródziemnego*, Europejskie Centrum Edukacyjne, Toruń 2009; G. Michałowska, *Bezpieczeństwo ludzkie*, [w:] *Świat wobec współczesnych wyzwań i zagrożeń*, J. Symonides (red.), Wydawnictwo Naukowe Scholar, Warszawa 2010; E. Newman, *New Forms of Security and the Challenge for Human Security*, [w:] *Issues in 21st Century World Politics*, M. Beeson, N. Bisley (eds.), Macmillan International Higher Education, New York 2013; R. Picciotto, F. Olonisakin, M.Clarke, *Global Development and Human Security*, Routledge, London 2017; *Routledge Handbook of Human Security*, M. Martin, T. Owen (eds.), Routledge, London–New York 2014; M. Skarżyński, *Homo securitas*, [w:] *Jednostka wobec wyzwań zmieniającego się środowiska bezpieczeństwa*, I. Andruszkiewicz, M. Skarżyński (red.), Wydawnictwo WNPiD, Poznań 2015; A. Szpak, *Bezpieczeństwo ludzkie ludów tubylczych w Arktyce na przykładzie Samów. Wybrane zagadnienia*, Wydawnictwo Naukowe UMK, Toruń 2018; E. Szweda, *Podmiot bezpieczeństwa człowieka a koncepcja human security*, „Przedsiębiorczość i Zarządzanie" 2016, vol. 17, z. 5, cz. 2; F. Tereszkiewicz, *Human security jako paradygmat polityki bezpieczeństwa Unii Europejskiej w kryzysowych czasach*, „Roczniki Nauk Społecznych" 2018, vol. 46, no. 1; R. Thakur, *The United Nations, Peace and Security. From Collective Security to the Responsibility to Protect*, Cambridge 2006; UNDP, *Human Development Report 1994: New Dimensions of Human Security*, HDR. UNDP.org (dostęp 10.01.2020); A. Urbanek, *Współczesny człowiek w przestrzeni bezpieczeństwa: w poszukiwaniu teoretyczności bezpieczeństwa personalnego*, Wydawnictwo Naukowe Akademii Pomorskiej, Słupsk 2015.

BEZPIECZEŃSTWO MEDIALNE – oznacza istnienie stanu niezakłóconego funkcjonowania systemu medialnego w danym państwie oraz dążenie do jego utrzymania. Na ów stan składa się szereg czynników, począwszy od edukacji medialnej społeczeństwa i jego przygotowania do odbioru treści medialnych, poprzez techniczne i technologiczne uwarunkowania dostępności mediów, prawne gwarancje wolności

→ i n f o r m a c j i [t. 2], wypowiedzi i formułowania opinii, po istnienie ładu medialnego, gwarantującego istnienie pluralistycznego systemu mediów, zapewniającego swobodną możliwość niezależnej ekspresji poglądów oraz brak koncentracji własności mediów w rękach ograniczonej liczby podmiotów. Pojęcie bezpieczeństwa medialnego dotyka także rozlicznych, nierozpoznanych jeszcze w pełni uwarunkowań funkcjonowania → m e d i ó w s p o ł e c z n o ś c i o w y c h [t. 3].

Troska o bezpieczeństwo medialne wynika z faktu, że współcześnie obywatele, niezależnie od tego, jak bardzo byliby zaangażowani w aktywne zdobywanie informacji o najważniejszych procesach społecznych i politycznych, jakie zachodzą w otaczającym ich świecie, w znacznym stopniu skazani są na wiedzę płynącą z mediów. Badania dotyczące źródeł, z jakich ludzie czerpią informacje o polityce przeprowadzone w USA oraz w państwach UE, dowodzą, że telewizja stanowi najpopularniejsze źródło informacji, odpowiednio dla 69% mieszkańców USA i 77% Europejczyków, drugie miejsce zajmuje internet (50% i 40%), na trzecim miejscu znajduje się prasa (32% i 39%), zaś na czwartym miejscu radio (odpowiednio 23% i 38%). Inne, niemedialne źródła pochodzenia informacji o otaczającym świecie wskazało odpowiednio 2% badanych w USA oraz 5% w Europie.

Media pełnią istotne funkcje i usługi dla systemu politycznego w demokracji, przy czym za najważniejsze uznać należy monitorowanie władzy mające na celu informowanie obywateli o działaniach państwa, w szczególności odnosi się to do rozpowszechniania i szerokiego prezentowania nieprawidłowości, jakie mają miejsce w państwie, samorządzie lub partiach politycznych. Monitorowanie władzy dotyczy w szczególnym stopniu polityków zajmujących kluczowe stanowiska w instytucjach międzynarodowych, państwowych oraz lokalnych, przy czym największą uwagę skupia się zwykle na monitorowaniu nieprawidłowości finansowych, skandali obyczajowych oraz zakresie realizacji obietnic wyborczych.

B. McNair wskazuje 5 zadań, jakie można postawić przed mediami w idealnym, demokratycznym społeczeństwie. Mają one:

- informować obywateli o tym, co dzieje się wokół nich – realizacja funkcji „nadzoru" lub „monitorowania" przez media;
- edukować co do rozumienia i oceny znaczenia „faktów", dlatego istotny jest profesjonalizm dziennikarzy, ich obiektywizm, który zakłada umiejętność zdystansowania się od analizowanych zagadnień;
- stanowić platformę publicznego dyskursu politycznego, ułatwiającego formowanie → o p i n i i p u b l i c z n e j [t. 3] oraz prezentowanie tej opinii społeczeństwu, które ją wyraziło;
- służyć jako kanał wyrażania poglądów politycznych, dzięki któremu wszyscy aktorzy polityczni – tacy jak partie polityczne czy stowarzyszenia – mogą proponować i przedstawiać swoje idee, bronić swoich punktów widzenia, przekonywać co do ich słuszności;

- upubliczniać skandale i zjawiska łamania prawa przez aktorów politycznych.

Zgodnie z tradycyjną teorią liberalną główną demokratyczną rolą mediów jest działanie na rzecz kontroli państwa. Media powinny monitorować pełen zakres jego działalności i bez obaw ujawniać nadużycia władzy publicznej. Rola ta jest określana jako *watchdog* (z ang. „pies stróżniczy") i stanowi najistotniejszą spośród wszystkich innych funkcji mediów. Określa ona i wyznacza przede wszystkim formę, w jakiej system medialny powinien być zorganizowany. Tendencja ta w USA prowadzi do wniosku, że media powinny być elementem wolnego rynku, gdyż tylko w ten sposób można zapewnić całkowitą niezależność mediów od rządzących i ich wpływów. Gdyby media stały się przedmiotem regulacji państwa, mogłyby utracić swoją rolę strażniczą, a wręcz mogłyby zostać przekształcone w działające na rzecz państwa.

Znaczącym wydarzeniem, które nie tylko w USA przyczyniło się do podkreślania roli mediów w zakresie monitorowania władzy, była afera Watergate. Doniesienia B. Woodwarda i C. Bernsteina z „Washington Post" doprowadziły do ujawnienia nielegalnych działań prezydenta R. Nixona na rzecz własnej reelekcji, łącznie z próbą zainstalowania → p o d s ł u c h u [t. 3] w siedzibie sztabu wyborczego konkurenta. Wydarzenie to dowiodło ogromnej roli mediów i tego, że czwarta władza ma realną siłę w zakresie działań na rzecz etyki w polityce i przestrzegania zasad przez → f u n k c j o n a r i u s z y p u b l i c z n y c h [t. 2].

Bezpieczeństwo medialne uzależnione jest od przygotowania odbiorców mediów do konsumpcji treści medialnych, w szczególności dotyczących najważniejszych procesów społecznych i politycznych. Na kształtowanie się wiedzy o tych procesach wpływ mają informacje medialne, jednak nie są one jedynym czynnikiem, a odbiór treści przekazu medialnego nie następuje u wszystkich jednostek w ten sam sposób. Ten sam przekaz medialny może zostać inaczej odebrany przez różnych odbiorców. Poza użytkowaniem mediów na proces przyswajania wiedzy wpływają także czynniki demograficzne oraz psychologiczne procesy poznawcze. Badania empiryczne prowadzone w różnych państwach dowodzą, że na sposób odbioru informacji medialnych największy wpływ ma poziom formalnej edukacji danej osoby oraz miejsce w strukturze społecznej, w mniejszym zaś zakresie wiek oraz płeć.

Ogromną rolę dla bezpieczeństwa medialnego odgrywa istnienie wielu różnych źródeł informacji, gwarantujących pluralizm mediów. Zarówno teoretycy demokracji, jak i badacze mediów uznają, że muszą istnieć zróżnicowane źródła informacji, które nie znajdują się pod kontrolą rządu ani żadnej pojedynczej grupy politycznej usiłującej wywrzeć wpływ na polityczne przekonania i postawy, i że takie źródła informacji powinny być skutecznie chronione przez prawo. Ważny pozostaje także wysoki poziom profesjonalizmu dziennikarskiego oraz rozwiązania systemowe, personalne i prawne, w których wyniku media mogą pełnić funkcję niezależnych źródeł informacji. Realizacja takich założeń wymaga świadomego społeczeństwa, w którym prawo do wolności mediów jest respektowane przez elitę władzy i opinię publiczną, niezależność

organizacji dziennikarskich zaś i samych dziennikarzy jest silnie chroniona przez obowiązujące prawo. Wyróżnić można 2 modele pluralizmu mediów: pluralizm wewnętrzny – oznaczający, że każde medium dąży do prezentowania wielu racji i punktów widzenia – oraz pluralizm zewnętrzny, oznaczający istnienie wielu stronniczych mediów, z których każde preferuje swój subiektywny punkt widzenia, ale na poziomie systemu medialnego to sama różnorodność gwarantuje, że każde zdanie i opinia mogą zostać wyartykułowane w którymś z istniejących środków masowego przekazu.

Dążenie do bezpieczeństwa medialnego wymaga także właściwego postawienia zadań przed mediami publicznymi, rozważenia, czy media publiczne – biorąc pod uwagę choćby sposób ich finansowania i zależności od innych instytucji – mają prezentować polityczny punkt widzenia aktualnie rządzących, stanowić swoistego rodzaju państwowy biuletyn informacyjny, czy też powinny w szczególnym stopniu wpisywać się w model mediów bezstronnych. W Polsce rozwiązania w tym zakresie precyzuje ustawa o radiofonii i telewizji, która wskazuje, że nadawcy publiczni mają realizować obowiązki i powinności tworzenia programów cechujących się pluralizmem, bezstronnością, wyważeniem i niezależnością oraz innowacyjnością, wysoką jakością i integralnością przekazu.

Obecnie najsilniejszym motorem transformacji i wyzwań dla bezpieczeństwa medialnego pozostaje rozwój sieci cyfrowej. Technologie cyfrowe znacznie obniżyły koszty produkcji wszystkich formatów medialnych, a internet dał możliwości niemal nieograniczonego udostępniania treści w różnych formatach multimedialnych. W konsekwencji nastąpiła eksplozja dostępnej treści, głównie za sprawą niewielkich ograniczeń przepustowości internetu w porównaniu z ograniczoną liczbą częstotliwości radiowych i telewizyjnych czy dostępną powierzchnią w prasie. Sieci cyfrowe radykalnie zmniejszyły koszty przechowywania i dystrybucji treści, rozszerzając zakres i zasięg rynków, usuwając wiele starych barier wejścia i sprzyjając konwergencji rynku. Wraz z wprowadzeniem nowych urządzeń do uzyskiwania dostępu do treści multimedialnych takich jak urządzenia mobilne znacznie wzrosły możliwości tworzenia, wykorzystywania i uzyskiwania dostępu do treści multimedialnych, co przekształciło zarówno rynek mediów, jak i rynek urządzeń mobilnych oraz zachowania rynkowe, które określają krzywe popytu i podaży na rynkach mediów. Transformacja ta pozwala oddzielić treści od samych mediów. Konsumpcja mediów jest w coraz większym stopniu napędzana aktywnym zainteresowaniem określoną treścią za pomocą środków dystrybucji umożliwiających dostosowanie treści do zainteresowań odbiorcy. Jest to radykalna zmiana, która pod wpływem zachowań odbiorców napędzających popyt i określających sposób wykorzystania mediów, silnie wpływa na działania podażowe na rynku mediów, co potencjalnie rodzić może liczne → z a g r o ż e n i a [t. 4] dla odbiorców treści medialnych.

Szybki rozwój technologii komunikacyjnych radykalnie zmienił środowisko medialne w ciągu ostatnich lat. W centrum tej zmiany znajduje się zdolność coraz

większej części społeczeństwa do korzystania z łatwo dostępnych urządzeń mobilnych i sieciowych, aby jej głos i punkt widzenia były słyszalne i zauważalne. Rozwój ten przyniósł szansę zdemokratyzowania społeczeństw, które mogą podważyć monopol informacyjny → m e d i ó w t r a d y c y j n y c h [t. 3]. Owe zmiany dają nowe możliwości, ale też kreują nowe zagrożenia dla bezpieczeństwa medialnego, nadając jednak nowy kontekst także bezpieczeństwu globalnemu. Nowe media oraz media społecznościowe stały się nie tylko narzędziem demokratyzacji, lecz również połączeni z siecią użytkownicy wykreowali model „obywatela stale monitorowanego", co umożliwia licznym podmiotom wywiadowczym bezprecedensową rutynową inwigilację. Część rządów chętnie wykorzystuje nowe źródła informacji wywiadowczych, ale rodzi to także niepokój wobec faktu, że nowa przestrzeń komunikacyjna okazała się łatwym terytorium do rozpowszechniania ekstremistycznych poglądów, zagrożeń terrorystycznych i nieograniczonej, niezweryfikowanej i często nieweryfikowalnej informacji. Powoduje to nieuniknione obawy dotyczące niebezpieczeństw w nowym środowisku komunikacyjnym. Wywołują je spekulacje na temat znaczenia spersonalizowanych komunikatów, jakie za pośrednictwem portali społecznościowych – takich jak Facebook czy Twitter – kierowane były do wybranych użytkowników w czasie kampanii wyborczej w USA w 2016 r. czy w okresie kampanii poprzedzającej głosowanie nad opuszczeniem UE przez Wielką Brytanię. Uwagę zwraca niemal całkowity brak kontroli nad treścią i zakresem oddziaływania postów i wiadomości przesyłanych w czasie → w o j n y h y b r y d o w e j [t. 4] Rosji przeciwko Ukrainie, służących realizacji interesów agresora. Podobny niepokój w kontekście bezpieczeństwa medialnego budzi zakres i sposób wykorzystywania przez przedsiębiorców będących właścicielami portali społecznościowych dobrowolnie przekazywanych im przez użytkowników danych o samych sobie i szerokiej gamy informacji towarzyszących tym danym.

Jakub Idzik, Rafał Klepka

F. Al-Rfouh, *Mass Communication and National Security*, „Democracy and Security" 2005, vol. 1, iss. 1; M. Bereźnicka, R. Klepka, *Przestrzeń medialna*; *Rynek medialny*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 2: *N–Z*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; J.G. Blumler, M. Gurevitch, *The Crisis of Public Communication*, Routledge, London–New York 1995; P. Busch, *The Changing Media*, [w:] *The Palgrave Handbook of Security, Risk and Intelligence*, R. Dover, H. Dylan, M. Goodman (eds.), Palgrave Macmillan, London 2017; J. Idzik, *Man in the World of Old and New Media – Selected Concepts of Media Influence and their Contemporary Interpretations*, „Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate" 2019, nr 9 (3); J. Idzik, R. Klepka, *Monitorowanie władzy*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; R. Klepka, *Bezpieczeństwo medialne*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; tenże, *Obrazy polityki w mediach: podstawowe uwarunkowania*, [w:] *Medialne obrazy świata*, R. Klepka (red.), Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2018; R. Klepka, E. Musiał, *Bezpieczeństwo medialne*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka

(red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; B. McNair, *An Introduction to Political Communication*, Routledge, London–New York 2011; R.M. Perloff, *The Dynamics of Political Communication: Media and Politics in a Digital Age*, Routledge, New York–London 2014; J. Prier, *Commanding the Trend Social Media as Information Warfare*, „Strategic Studies Quarterly" 2017, vol. 11, no. 4; D. Shapley, *The Media and National Security*, „Daedalus" 1982, vol. 111, no. 4; *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; O. Wasiuta, S. Wasiuta, *Medialna manipulacja informacją w wojnie hybrydowej Rosji przeciwko Ukrainie*, [w:] *Medialne obrazy świata*, R. Klepka (red.), Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2018.

BEZPIECZEŃSTWO MIĘDZYNARODOWE – związane w strukturach międzynarodowych i zabezpieczone traktatami i umowami na podstawie prawa międzynarodowego suwerenne państwa (zob. → s u w e r e n n o ś ć p a ń s t w a [t. 4]) poprzez łączenie się w organizacje międzynarodowe wprowadzają w życie przyjmowaną przez nie politykę utrzymania bezpieczeństwa międzynarodowego i → b e z p i e c z e ń s t w a n a r o d o w e g o oraz stabilnego pokoju. Organizacje międzynarodowe są podmiotami prawa międzynarodowego, choć wtórnego i pochodnego, ponieważ tworzone są przez państwa, główne podmioty prawa międzynarodowego.

Prymarnym celem systemu bezpieczeństwa międzynarodowego jest wzmocnienie bezpieczeństwa zewnętrznego, co wzmacnia jednocześnie bezpieczeństwo wewnętrzne każdego z państw. Nowoczesny system bezpieczeństwa międzynarodowego musi chronić swoich uczestników nie tylko przed → z a g r o ż e n i a m i [t. 4] zewnętrznymi, ale także od wewnątrz. Musi być stabilny i silny w swojej strukturze, aby realizować ów cel.

System bezpieczeństwa międzynarodowego można analizować jako:

- politykę promującą tworzenie skutecznych gwarancji pokoju zarówno dla poszczególnych krajów, jak i całej społeczności światowej;
- stan stosunków gospodarczych, politycznych, społecznych, wojskowych, międzynarodowych, gwarantujący ochronę przed zagrożeniami zewnętrznymi, uniemożliwiający prowadzenie → w o j e n [t. 4], konfliktów i starć;
- warunki konieczne do istnienia i funkcjonowania państw, zapewniające ich pełną suwerenność i równorzędne relacje z innymi krajami;
- metodę ochrony bezpieczeństwa obywateli, społeczeństwa i narodowych interesów państw.

Skuteczność systemu bezpieczeństwa międzynarodowego zależy od systemu zobowiązań, gwarancji i możliwości podmiotów oraz jego struktury, w szczególności od:

- koncepcji i polityki zapewnienia bezpieczeństwa międzynarodowego;
- międzynarodowych, państwowych i publicznych instytucji i organizacji zapewniających bezpieczeństwo jednostki i społeczeństwa;
- środków, sposobów i metod zapewnienia bezpieczeństwa międzynarodowego.

Bezpieczeństwo międzynarodowe zależy od:

- skali – globalnej, regionalnej, subregionalnej, lokalnej, umów dwustronnych;

- charakteru przedmiotów – osobowych, społecznych, państwowych;
- sfery życia publicznego – politycznej, ekonomicznej, społecznej, humanitarnej, psychologicznej, wojskowej, kulturowej.

Uwzględnienie tych wszystkich elementów powoduje, że bezpieczeństwo międzynarodowe staje się bardziej zróżnicowane oraz integralne i może odnosić się do różnych obszarów geograficznych, a także różnych podmiotów działających w różnych sferach. Zapewnienie bezpieczeństwa obejmuje kompleksowe podejście, integralność bezpieczeństwa i → z r ó w n o w a ż o n e g o r o z w o j u [t. 4]; ciągłość działań, w tym organizację stałego monitorowania i kontroli stanu środowiska społecznego i przyrodniczego oraz potencjalnie niebezpiecznych obiektów itp.

Przedmiotami bezpieczeństwa międzynarodowego są narody i państwa, obywatele różnych krajów, odpowiednie instytucje, stowarzyszenia, organizacje, ludzkość jako całość. Podmiotami bezpieczeństwa międzynarodowego są zaś państwa i wszyscy pozostali uczestnicy stosunków międzynarodowych (ruchy publiczne i międzynarodowe, organizacje międzyrządowe i pozarządowe). Podmioty te uczestniczą w opracowywaniu norm i zasad prawa międzynarodowego regulujących działania w tym obszarze.

Kształtowanie się systemu bezpieczeństwa międzynarodowego formuje się w zależności od charakteru rzeczywistych zagrożeń i niebezpieczeństw oraz z uwzględnieniem środków ich przezwyciężenia. Niezbędnym warunkiem niezawodności bezpieczeństwa międzynarodowego jest system odstraszający, w szczególności dostępność niezbędnych zdolności obronnych.

Ogólnie rzecz biorąc, skuteczność każdego międzynarodowego systemu bezpieczeństwa zależy od kilku kluczowych czynników:

- stanu i tendencji obecnej sytuacji geostrategicznej (→ g e o s t r a t e g i a [t. 2]),
- realiów międzynarodowych na poziomie regionalnym i subregionalnym;
- wewnętrznej sytuacji państw i ich rzeczywistych możliwości w perspektywie długoterminowej;
- charakteru współczesnych zagrożeń, które mają najbardziej znaczący wpływ na stabilność państw na poziomie regionalnym i subregionalnym;
- skuteczności już istniejących systemów bezpieczeństwa i ich zdolności do zmiany w kontekście nowych zadań;
- rzeczywistych możliwości tworzenia nowych systemów bezpieczeństwa i charakteru ich interakcji z już istniejącymi.

Współczesny system bezpieczeństwa międzynarodowego jest regulowany przez zasady:

- ogólnego charakteru i jednakowego poziomu bezpieczeństwa dla wszystkich krajów;
- międzynarodowej współpracy w rozwiązywaniu problemów bezpieczeństwa;
- zbiorowych działań mających na celu wyeliminowanie → a g r e s j i i uniemożliwienie jej spowodowania;

- wykorzystania szerokiego arsenału narzędzi do utrzymywania pokoju;
- zaufania do stosunków międzynarodowych i przejrzystości polityki światowej oraz systemu bezpieczeństwa.

Zbiorowe bezpieczeństwo to system współpracy międzynarodowej, w którym bezpieczeństwo międzynarodowe jest zabezpieczone poprzez wspólne wysiłki państw zgadzających się wspierać każde państwo uczestnika systemu bezpieczeństwa zbiorowego, które stanie się ofiarą agresji. System zbiorowego bezpieczeństwa ma na celu odrzucenie użycia siły do rozwiązywania sporów między uczestnikami systemu i pokojowe rozstrzyganie sporów na podstawie prawa międzynarodowego.

W praktyce światowej system zbiorowego bezpieczeństwa stał się powszechny jako zbiór wspólnych środków państw dla utrzymania pokoju, zapobiegania wojnie, zaprzestania aktów agresji i zapewnienia zbiorowej pomocy. Bezpieczeństwo zbiorowe opiera się na integralności – każdy członek systemu bezpieczeństwa zbiorowego musi przyjść z pomocą innym poprzez środki dyplomatyczne, działania gospodarcze, a w skrajnych przypadkach środki wojskowe. Zbiorowe działania w zakresie bezpieczeństwa mogą odbywać się w ramach ONZ i innych organizacji międzynarodowych lub na szczeblu regionalnym. Stworzenie systemu zbiorowego bezpieczeństwa wymaga użycia zestawu środków o charakterze politycznym, gospodarczym, prawnym, a także wojskowo-organizacyjnym.

Zbiorowe bezpieczeństwo opiera się na następujących podstawowych zasadach:

- integralności bezpieczeństwa – agresja wobec jednego państwa uczestnika jest uważana za agresję w stosunku do reszty państw uczestników;
- równej odpowiedzialności – wszystkie państwa strony są w równym stopniu odpowiedzialne za utrzymanie bezpieczeństwa;
- nieingerowaniu w sprawy wewnętrzne i uwzględnianiu interesów wszystkich uczestników systemu bezpieczeństwa zbiorowego;
- zbiorowej obrony;
- konsens – decyzje w kluczowych kwestiach wspólnego bezpieczeństwa podejmowane są na zasadzie konsensusu.

System zbiorowej obrony jest skierowany na zewnątrz i ma na celu ochronę członków przed zewnętrzną agresją. W ramach zbiorowej obrony wszystkie państwa strony odpowiedniej umowy biorą na siebie zobowiązanie bronić jakiegokolwiek innego państwa członkowskiego, które jest przedmiotem napaści zbrojnej państwa lub grupy państw spoza sojuszu.

Pierwszy system → b e z p i e c z e ń s t w a e u r o p e j s k i e g o został ustanowiony w XVII w., po zawarciu pokoju westfalskiego kończącego wojnę trzydziestoletnią (1618–1648), był to system zwany układem równowagi sił. Jego zasady przewidywały szacunek do terytorialnej równowagi sił i wzajemnych konsultacji w razie ewentualnego konfliktu. Owa równowaga została zbudowana na legitymizacji dominującej pozycji wielkich mocarstw i imperiów. Należy zauważyć, że mniej lub

bardziej skutecznie system ten działał aż do czasu rozpoczęcia I wojny światowej. Co więcej, wielkie mocarstwa ściśle kontrolowały i determinowały losy oraz zachowanie średnich i małych państw. Jedną z cech tego systemu było istnienie hierarchii państw, a zatem ich nierówność.

Każde państwo realizowało swoje interesy, ciągle zmieniając sojuszników bez naruszenia ogólnej struktury sojuszy i stosunków między państwami. Wszelkie roszczenia do hegemonii na arenie międzynarodowej jednego z wielkich mocarstw powodowały natychmiastową reakcję innych dużych państw wraz z ich sojusznikami, które łączyły się w koalicję przeciwko sprawcy podważenia status quo.

System równowagi sił doprowadził do pierwszych prób rozwiązywania międzynarodowych sporów i konfliktów poprzez wprowadzenie stałych norm oraz powszechnie uznawanych traktatów i umów międzynarodowych. Stał się on podstawą do utworzenia systemu zbiorowego bezpieczeństwa. Pierwszą organizacją bezpieczeństwa zbiorowego we współczesnej historii była Liga Narodów, która powstała po I wojnie światowej. Jej członkowie zobowiązali się chronić siebie nawzajem w przypadku ataku jakiegokolwiek innego państwa. Na zasadach zbiorowego bezpieczeństwa działa obecnie ONZ. Do systemu środków zbiorowych należą:

- zakaz stosowania groźby lub użycia siły wobec innych państw;
- pokojowe rozstrzyganie sporów międzynarodowych;
- narzędzia rozbrojenia;
- ustalenia dotyczące bezpieczeństwa w okresie przejściowym;
- wykorzystanie regionalnych organizacji bezpieczeństwa;
- tymczasowe środki przeznaczone do utrzymania pokoju;
- obowiązkowe środki do utrzymania pokoju bez użycia sił zbrojnych i obowiązkowe środki z użyciem sił zbrojnych.

Trzeba podkreślić, że system bezpieczeństwa zbiorowego ONZ w warunkach 2-biegunowego świata mierzył się z pewnymi komplikacjami na poziomie regionalnym.

Na kontynencie europejskim są 4 międzynarodowe organizacje, które działają dla zabezpieczenia bezpieczeństwa międzynarodowego: Organizacja Bezpieczeństwa i Współpracy w Europie (OBWE), UE, → N A T O [t. 3], Organizacja Układu o Bezpieczeństwie Zbiorowym (OUBZ), które określają architekturę europejskiego bezpieczeństwa.

R. Zięba wyodrębnił 5 typów międzynarodowych systemów bezpieczeństwa:

- Jednostronne – realizowane poprzez indywidualne wysiłki jednego państwa. Państwo realizuje swoje własne bezpieczeństwo we własnym zakresie, przy użyciu pewnego rodzaju polityki zagranicznej, która może być skierowana na hegemonię, izolację, → n e u t r a l n o ś ć [t. 3], pozablokowość lub nawet samowystarczalność.
- Równowaga sił – oparta na braku znaczącej przewagi jednego państwa nad innymi w systemie międzynarodowym i zasadzie wzajemności zagrożenia. Każde państwo w takim systemie dzięki posiadanym siłom jest zagrożeniem dla innych państw,

a stabilność w relacjach między nimi wynika z równowagi zagrożeń. Klasyczny „koncert mocarstw" lub 2-biegunowy system lat 50. i 90. XX w. są wariantami takiego systemu, który R. Aron nazwał „równowagą strachu".

- System bezpieczeństwa blokowego – jest szerszą wersją systemu równowagi sił, ponieważ równowaga i stabilność w nim zależą od mocy bloków. Każde z państw stara się zagwarantować swoje bezpieczeństwo, uczestnicząc w działaniach jednego z bloków militarno-politycznych. W związku z tym otrzymują one gwarancje pomocy w razie wojny, ale muszą również brać pod uwagę ryzyko zaangażowania w konflikt zbrojny zgodnie z *casus foederis*. Naruszenie ustalonej równowagi sił między blokami – potencjalnymi przeciwnikami – przeważnie prowadzi do wielkiej wojny (klasycznym przykładem jest I wojna światowa). W takim systemie rządy poszczególnych państw są zmuszone rozwiązać dylemat, czy podjąć niezależne działania w dziedzinie bezpieczeństwa wraz z wszelkim ryzykiem wynikającym z tego czy przystąpić do jednego z wojskowo-politycznych bloków, z czym wiąże się ryzyko ewentualnego udziału państwa w konflikcie zbrojnym zgodnie z podjętymi zobowiązaniami.
- System bezpieczeństwa zbiorowego związany z wielostronnymi gwarancjami wzajemnego bezpieczeństwa państw, podpisaniem odpowiednich umów i konwencji międzynarodowych, obowiązkowym przestrzeganiem przez rządy państw podjętych zobowiązań. Próba stworzenia uniwersalnego systemu bezpieczeństwa zbiorowego została zainicjowana w Pakcie Ligi Narodów podpisanym w dniu 28 czerwca 1919 r., w którym wyróżniano 3 podstawowe elementy bezpieczeństwa zbiorowego:
  - przyjęcie przez wszystkie państwa istniejącego w chwili podpisywania status quo i ich odmowę jakichkolwiek jego zmian w przyszłości;
  - zbiorowe starania państw o zachowanie status quo jako gwarancji pokoju i stabilności na świecie;
  - uznanie za kluczowe terminów „agresor" i „agresja", ponieważ ich jednoznaczne zrozumienie miało określić odpowiednie środki społeczności międzynarodowej dla tego typu państw i ich działań.

Po II wojnie światowej w ramach ONZ niektóre elementy zbiorowego bezpieczeństwa zostały skodyfikowane w Karcie Narodów Zjednoczonych. Jednak → k r y z y s [t. 2] w Kosowie i wojna w Iraku (2003) wyraźnie zakwestionowały nie tylko system prawa międzynarodowego, ale także ustalone normy stosunków międzypaństwowych. Ogólnie rzecz biorąc, zbiorowy międzynarodowy system bezpieczeństwa nigdy nie miał precedensu w historii pomimo dość ambitnych prób jego utworzenia.

- Spółdzielczy system bezpieczeństwa polega na dążeniu większości państw świata do współpracy, którą rządzące elity polityczne uważają za bardziej pożądaną niż konfrontację. Chodzi o sposób interakcji między państwami, jego *modus vivendi* ustala się na podstawie indywidualnych umów, które – choć nie określają zasady

wzajemnych stosunków – wprowadzają klimat zaufania i czynią możliwą współpracę w różnych sprawach będących przedmiotem wspólnego zainteresowania.

Sergiusz Wasiuta

J. Czaputowicz, *Bezpieczeństwo w teoriach stosunków międzynarodowych*, [w:] K. Żurkowska, *Bezpieczeństwo międzynarodowe – przegląd aktualnego stanu*, IusAtTax, Warszawa 2011; S. Koziej, *Między piekłem a rajem. Szare bezpieczeństwo na progu XXI wieku*, Toruń 2006; E. Nowak, M. Nowak, *Zarys teorii bezpieczeństwa narodowego*, Difin, Warszawa 2011; G. Sen, *International Relations and International Security in the 21st Century: The World in Transition*, „Manekshaw Paper" 2014, no. 49; *Słownik terminów z zakresu bezpieczeństwa narodowego*, B. Balcerowicz, J. Pawłowski, A. Ciupiński, W. Łepkowski (red.), AON, Warszawa 2002–2009; R. Stańczyk, *Współczesne postrzeganie bezpieczeństwa*, PAN, Warszawa 1996; R. Thakur, *Nuclear Weapons and International Security: Collected Essays*, Routledge, New York 2015; S. Wasiuta, *System bezpieczeństwa międzynarodowego*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; R. Zięba, *Bezpieczeństwo międzynarodowe po zimnej wojnie*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2008; K. Żukrowska, M. Grącik, *Bezpieczeństwo międzynarodowe. Teoria i praktyka*, Szkoła Główna Handlowa, Warszawa 2006.

BEZPIECZEŃSTWO MILITARNE – zdolność państwa narodowego do obrony i/lub powstrzymania → a g r e s j i militarnej; określa również stan ochrony → i n t e r e s ó w n a r o d o w y c h [t. 2], → s u w e r enn oś ci [t. 4], integralności terytorialnej i nienaruszalności państwa przed ingerencją z użyciem siły militarnej. Termin bezpieczeństwa militarnego jest często używany jako synonim → b e z p i e c z e ń s t w a . Jest to tradycyjnie najwcześniej uznana forma → b e z p i e c z e ń s t w a n a r o d o w e g o . Zakres bezpieczeństwa militarnego rozszerzył się z konwencjonalnych form konfliktu między państwami narodowymi na → w o j n ę c z w a r t e j g e n e r a c j i [t. 4] między państwem a podmiotami niepaństwowymi. Głównym celem zapewnienia bezpieczeństwa militarnego jest eliminacja zewnętrznych i wewnętrznych → z a g r o ż e ń [t. 4] dla bezpieczeństwa narodowego państwa w sferze militarnej oraz stworzenie sprzyjających warunków dla zagwarantowanej ochrony jego interesów narodowych. W praktyce międzynarodowej bezpieczeństwo militarne zapewnia prawo suwerennego państwa do samoobrony i/lub → o d s t r a s z a n i a [t. 3] przed agresją wojskową, pozwala na użycie siły militarnej przez państwo w celu ochrony jego suwerenności i integralności terytorialnej.

Bezpieczeństwo militarne odnosi się do zagrożeń, które w znaczący sposób mogą wpłynąć na przetrwanie państwa. Polegają one głównie na obronie terytorium przed → a g r e s j ą zewnętrzną o charakterze militarnym. Bezpieczeństwo militarne wiąże się z kategoriami takimi jak:

- potencjał obronny,
- potencjał ofensywny,

które dotyczą poszczególnych państw i są powiązane z intencjami i ich postrzeganiem w stosunkach międzynarodowych.

Bezpieczeństwo militarne w ujęciu tradycyjnym jest jednym z członków przedmiotowych bezpieczeństwa państwa. Utożsamia się je zazwyczaj z brakiem ataku ze strony innego państwa (podmiotu stosunków międzynarodowych). Na tej podstawie fundamentalnymi wartościami chronionymi przed zagrożeniami zewnętrznymi były:

- integralność terytorialna;
- niezależność polityczna;
- przetrwanie narodu i państwa (w skrajnych przypadkach). Szybki rozwój technologii doprowadził do przesunięcia punktu ciężkości z klasycznych niebezpieczeństw militarnych, występujących głównie pod postacią agresji zbrojnej, w kierunku zagrożeń pozamilitarnych. Nowe, pozamilitarne zagrożenia przeniknęły do wszelkich sfer i dziedzin aktywności państwa, odsuwając tym samym wymiar bezpieczeństwa militarnego na dalszy plan.

Tradycyjne podejście do bezpieczeństwa militarnego zakłada również, iż to siła wojskowa i oddziaływania polityczno-dyplomatyczne są głównymi środkami zapewnienia bezpieczeństwa państwa w stosunkach międzynarodowych.

Sposób ujmowania bezpieczeństwa militarnego ewoluował i na przestrzeni dziejów uległ zmianie. Dowodem może być książka J. Świniarskiego *O naturze bezpieczeństwa*, w której autor uwypukla nietrafność użycia siły militarnej jako wyznacznika służącego zapewnieniu bezpieczeństwa militarnego – „nieracjonalne jest jej użycie i zastosowanie", pisze badacz. Można stwierdzić, że armia nie zawsze i nie w każdych warunkach zapewnia istnienie państwa i imperium. Jako przykłady mogą służyć fakty z dziejów różnych państw i imperiów, które, jak twierdzi Świniarski:

> z jednej strony – rozpadły się, mimo że nie poniosły klęski militarnej, nie przegrały konfliktu zbrojnego, wojny bądź batalii – z drugiej zaś – powstały bądź odradzały się, mimo że nie prowadziły zwycięskich działań zbrojnych, nie wygrały militarnie wojny.

Rewolucja naukowo-techniczna miała duży wpływ na bezpieczeństwo militarne i na rolę sił zbrojnych w tym zakresie. W wyniku przemian znaczenie sił zbrojnych oraz nowej technologii wojennej – siły nuklearnej – zmalało. Pomimo stawianego nierzadko pytania o sens utrzymywania i wykorzystywania sił zbrojnych w bezpieczeństwie militarnym i poszukiwania innych środków oraz sposobów zapewniania bezpieczeństwa, z uwzględnieniem m.in. wielości aspektów bezpieczeństwa, w tym np. bezpieczeństwa militarnego, należy zdecydowanie podkreślić, iż w rzeczywistości rola sił zbrojnych w dalszym ciągu pozostanie nie do przecenienia w ochronie i obronie narodowej kraju.

Współczesne pojmowanie bezpieczeństwa militarnego państwa w istocie stanowi relację, jaka zachodzi między państwem a środowiskiem międzynarodowym, w której bierze udział czynnik militarny. To relacja, w której ze strony czynnika militarnego może dojść lub dochodzi do zagrożenia interesów państwa związanych z:

- istnieniem,
- rozwojem,
- funkcjonowaniem państwa.

Na tej podstawie uznaje się, że bezpieczeństwo militarne jest stanem uzyskanym w rezultacie utrzymywania odpowiednio zorganizowanych i wyposażonych sił zbrojnych oraz zawartych sojuszy wojskowych, a także opracowania koncepcji wykorzystania będących w dyspozycji sił, stosownie do zaistniałej sytuacji. Do zasadniczych elementów wchodzących w skład bezpieczeństwa militarnego zalicza się:

- siły zbrojne – ich organizację i wyposażenie,
- zawarte sojusze militarne i inne organizacje,
- koncepcje strategiczne wykorzystania wszelkich sił.

Wśród autorów rozpatrujących problematykę bezpieczeństwa militarnego można napotkać definicje bezpieczeństwa jako stanu uzyskanego w rezultacie:

- utrzymywania potencjału militarnego na wymaganym poziomie,
- zawartych sojuszy wojskowych,
- podpisanych umów polityczno-militarnych,
- posiadania koncepcji strategicznej, operacyjnej i taktycznej,
- wykorzystywania tego potencjału stosownie do zaistniałej sytuacji i ocenianych zagrożeń wymagających użycia siły militarnej.

W obszarze zainteresowań bezpieczeństwa militarnego znajdują się natomiast:

- podstawy normatywne i teoretyczne,
- → zagrożenia militarne [t. 4],
- aspekt naukowy bezpieczeństwa militarnego,
- potencjał militarny i koncepcje strategiczne wykorzystania posiadanego potencjału,
- sojusze militarne,
- operacje militarne,
- operacje reagowania kryzysowego i wsparcia pokoju,
- prognostyczne kierunki zmian w bezpieczeństwie militarnym. Przez całe wieki bezpieczeństwo państw (czy też grupy państw) opierało się na sile militarnej. Siła i suwerenność stały się swoistymi kamieniami węgielnymi systemu obrony państw.

W budowie siły wojskowej wykorzystywano inne elementy, takie jak:

- położenie geograficzne,
- zasoby naturalne,
- stan zaawansowania technicznego. Jak pisze D. Kompała:

> wraz z rozwojem cywilizacji stan ten ulegał zmianie. Po II wojnie światowej powstały dwa bloki państw skupione wokół mocarstw dysponujących potężną siłą wojskową. Narastanie potencjałów militarnych po obu stronach nie powodowało konieczności ich użycia. Potencjały te były doskonałym środkiem odstraszania i politycznego oddziaływania na przeciwników. Zapewnienie bezpieczeństwa militarnego wymagało współpracy i równowagi pomiędzy elementami wojskowymi

> i pozawojskowymi. […] Pomimo rozwoju cywilizacyjnego i wielu zmian, jakie zachodzą we współczesnym świecie, priorytet bezpieczeństwa militarnego jest niezachwiany. Choć ryzyko wykorzystania siły militarnej zmniejsza się, to jednak ona jest traktowana jako podstawowy środek zapewnienia zasadniczych interesów państwa. Powszechnie uznaje się, że posiadanie siły militarnej jest niezbędne dla zapewnienia bezpieczeństwa terytorialnego i narodowej niezależności.

Wskazuje się, że do zasadniczych źródeł braku poczucia bezpieczeństwa militarnego państwa należą:

- rywalizacja polityczna między państwami,
- postęp techniki i technologii zbrojeniowej.

Przyjmuje się, że bezpieczeństwo militarne państwa to:

- relacje między państwem a środowiskiem międzynarodowym będące wynikiem istnienia siły militarnej i mające bezpośredni wpływ na bezpieczeństwo państwa;
- stan związany z istnieniem potencjałów militarnych w państwach oraz doktryn i → s t r a t e g i i [t. 4] związanych z ich wykorzystywaniem;
- rozległa i złożona, wielopłaszczyznowa praktyka, będąca trwałym zjawiskiem środowiska międzynarodowego;
- zjawisko, system lub proces, który jest specyficznym, wyraźnie wyodrębnionym obszarem poznania naukowego.

Rezultatem analizy problemów dotyczących siły militarnej państwa jest wyspecyfikowanie jej 3 zasadniczych determinantów powiązanych z bezpieczeństwem militarnym, takich jak:

- potencjał militarny, tzn. wielkość środków, jakie państwo może przeznaczyć na siły zbrojne;
- znaczenie przywiązywane do siły wojskowej przez państwo, wyrażające się w wielkości środków, jakie jest ono gotowe przeznaczyć na utrzymanie sił zbrojnych i uzbrojenia;
- efektywność wykorzystania powyższych środków, umiejętności polityczne i wojskowe dysponowania tymi siłami.

Jak wskazuje Kompała, za zasadne uznaje się, że:

> państwo postrzega swoje bezpieczeństwo militarne przez pryzmat zagrożeń wojskowych. Wiąże je przede wszystkim z niebezpieczeństwem agresji przeprowadzonej przez inne państwo. Może być nim kraj sąsiedni lub państwo niegraniczące z terytorium kraju podbitego. […] Bezpieczeństwo militarne państwa ma również wymiar narodowy i międzynarodowy. Aspekt narodowy bezpieczeństwa militarnego jest związany z oceną własnych zagrożeń, jakiej dokonuje każde państwo. […] Międzynarodowy wymiar bezpieczeństwa militarnego traktuje tę problematykę szerzej i wszechstronniej. Źródło tego stanu rzeczy tkwi w pełniejszym traktowaniu bezpieczeństwa militarnego niż wyznaczać to mogą dwustronne porozumienia państw. Wszechstronność proponowanych i realizowanych w ramach zinstytucjonalizowanych struktur koncepcji bezpieczeństwa militarnego sprawia,

> że współcześnie użycie sił zbrojnych daleko wykracza poza ramy suwerennej decyzji państwa.

Jak zauważa badacz nieco dalej:

> pomimo szerokiego postrzegania bezpieczeństwa, siła militarna wciąż pozostaje jednym z głównych instrumentów międzynarodowej polityki państw. Dlatego też niezmiernie ważne jest posiadanie aktualnej wiedzy o sytuacji militarnej w otoczeniu państwa i umiejętne kształtowanie tej sytuacji. Istotnym elementem w opisywaniu bezpieczeństwa militarnego jest nadążanie za cywilizacyjnym rozwojem i wynikającymi z niego zmianami sfery militarnej. Odnosi się to do ewolucji broni – jednej z najważniejszych kategorii sfery bezpieczeństwa militarnego.

Każde państwo, chcąc zapewnić sobie bezpieczeństwo militarne na jak najwyższym poziomie, powinno przestrzegać kilku prostych zasad, którymi są:

- zasada wiarygodności bezpieczeństwa militarnego polegająca na dążeniu do utrzymania takiego potencjału militarnego, który zapewni wykonanie zobowiązań sojuszniczych, a także będzie stanowił właściwą siłę do odstraszania potencjalnego agresora i zagwarantuje oczekiwaną wiarygodność w gronie państw sojuszniczych;
- zasada partnerstwa w bezpieczeństwie militarnym polegająca na utrzymywaniu relacji sojuszniczych i z państwami sąsiednimi;
- zasada współdziałania w bezpieczeństwie militarnym polegająca na dokładnym określeniu zadań dla wykonawców, przypuszczalnego czasu i miejsca działania.

Na tej podstawie można stwierdzić, że współcześnie bezpieczeństwo militarne nie może być utożsamiane tylko z potencjałem militarnym stanowiącym siły i środki sił zbrojnych. Znaczący wpływ na bezpieczeństwo militarne ma bardzo wiele czynników, a wśród nich m.in.:

- sytuacja geopolityczna,
- uwarunkowania sojusznicze,
- nowe technologie.

Głównymi cechami i warunkami wstępnymi powstania i istnienia zagrożenia militarnego dla państwa ze strony potencjalnego agresora są:

- ukryte interesy potencjalnego agresora (roszczenia terytorialne, gospodarcze i inne), które mogą wymagać użycia siły wojskowej w celu jego zaspokojenia;
- orientacja i gotowość wojskowo-politycznego kierownictwa agresora do użycia siły wojskowej do osiągnięcia swoich celów;
- gotowość bojowa sił zbrojnych agresora, które dają mu możliwość prowadzenia ofensywnych działań wojennych przeciwko wybranemu państwu.

Zagrożenia militarne niekoniecznie są związane z rozpoczęciem militarnego przygotowania potencjalnego przeciwnika. Ich źródła mają zazwyczaj charakter ukryty. Źródłami zagrożeń militarnych mogą być różnorodne zjawiska i procesy życia społecznego, w szczególności:

- przecięcie się interesów politycznych ludzi, grup społecznych, państw lub ich koalicji;
- gospodarcze, społeczne, etniczne lub religijne konflikty;
- nagromadzenie jądrowej lub konwencjonalnej broni;
- obecność i rozmieszczenie armii, zwiększona aktywność sił zbrojnych w pobliżu granic innego państwa itp.

Eksperci zachodni i polscy wyróżniają 2 główne wymiary spektrum zagrożeń militarnych:

- wojskowo-polityczny – związany ze zmianami geopolitycznego rozmieszczenia sił;
- czysto wojskowy („technologiczny") – związany ze zmianą charakteru konfliktów zbrojnych.

Ostatnio eksperci zauważyli pojawienie się nowych rodzajów wyzwań i zagrożeń, w szczególności zagrożenia międzynarodowym → t e r r o r y z m e m [t. 4], niekontrolowanego rozprzestrzeniania materiałów i technologii jądrowych oraz zagrożenia → c y b e r p r z e s t r z e n i , które wymagają opracowania nowych podejść w dziedzinie bezpieczeństwa militarnego.

Jak celnie zauważał Kompała:

> obecnie prawidłowo interpretowane bezpieczeństwo militarne powinno skupiać się nie tylko na sile militarnej danego kraju, lecz także na relacjach międzynarodowych – w tym przede wszystkim na uwarunkowaniach sojuszniczych. Dlatego też należy stwierdzić, iż zapewnienie bezpieczeństwa militarnego powinno polegać na odpowiednim zbalansowaniu czynnika militarnego – sił zbrojnych – z uwarunkowaniami sojuszniczymi.
>
> *Marek Pietrzyk*

B. Balcerowicz, *Bezpieczeństwo militarne*, NP.UW.edu.pl (dostęp 1.01.2020); tenże, *O pokoju. O wojnie*, Wydawnictwo Rambler, Warszawa 2013; tenże, *Strategia obronna państwa*, AON, Warszawa 1994; BBN, *Aspekty bezpieczeństwa militarnego w ujęciu Strategicznego Przeglądu Bezpieczeństwa Narodowego* „Bezpieczeństwo Narodowe" 2012, nr III–IV (23–24); S. Dworecki, *Zagrożenia bezpieczeństwa państwa*, AON, Warszawa 1994; W. Kitler, *Bezpieczeństwo narodowe RP. Podstawowe kategorie, uwarunkowania, system*, AON, Warszawa 2011; D. Kompała, *Pojmowanie bezpieczeństwa militarnego*, „Obronność. Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej" 2015, nr 3 (15); A. Madejski, *Wystarczalność obronna – kontrowersje i realia*, [w:] *Wystarczalność obronna*, P. Sienkiewicz (red.), Bellona, Warszawa 1996; R. Szpyra, *Bezpieczeństwo militarne*, AON, Warszawa 2012.

BEZPIECZEŃSTWO MORSKIE – jest terminem wieloznacznym i jednocześnie bardzo pojemnym. W ogólnym ujęciu oznaczać może bowiem wszelkie aspekty szeroko rozumianego → b e z p i e c z e ń s t w a na morzu – od zapewnienia wolnej od → z a g r o ż e ń [t. 4] żeglugi w znaczeniu nawigacyjnym (drożność szlaku żeglugowego, system latarni morskich i innych oznaczeń) po bezpieczeństwo wynikające z uwarunkowań geograficzno-klimatycznych. Jednak najważniejszym aspektem

bezpieczeństwa morskiego jest aspekt militarny w znaczeniu wolności nie tylko od zagrożeń *stricte* militarnych rozumianych jako groźba otwartych działań zbrojnych, ale także od → p i r a c t w a [t. 3], → t e r r o r y z m u [t. 4] oraz działań nieregularnych (zob. → m i l i t a r n e d z i a ł a n i a n i e r e g u l a r n e [t. 3]) mieszczących się w ramach pojęcia tzw. → w o j n y h y b r y d o w e j [t. 4]. Kwestie te od stuleci absorbowały uwagę społeczeństw, szczególnie tych, których egzystencja uzależniona była od bezpieczeństwa handlu morskiego.

Ta konstatacja nakazuje cofnąć się aż do czasów starożytnej Grecji. Przyczyną wojny trojańskiej było nie uprowadzenie małżonki spartańskiego króla, ale raczej wysokie myto nakładane na statki achajskie podążające przez Dardanele ku Morzu Czarnemu. Po wojnach perskich i wyprawach Dariusza oraz Kserksesa (490 p.n.e. i 480–479 p.n.e.) hegemonem morskim wśród greckich polis stały się Ateny. Utworzony pod ich przywództwem Związek Morski utrzymywał bezpieczeństwo żeglugi między ateńską metropolią a miastami sojuszniczymi (niektóre z nich wyrzekły się posiadania własnej floty wojennej) oraz koloniami w basenie Morza Śródziemnego. Fakt ten w połączeniu z agresywnie prowadzoną polityką narzucania hegemonii mniejszym polis wzbudził podejrzliwość Sparty, co ostatecznie doprowadziło do wybuchu wojny peloponeskiej (431–404 p.n.e.). Z kolei starożytny Rzym po wygraniu wojen punickich (264–146 p.n.e.) do sprawy bezpieczeństwa własnych linii komunikacyjnych na Morzu Śródziemnym podchodził z dużą dezynwolturą. Sytuacja ta doprowadziła do rozkwitu piractwa u progu I w. p.n.e. Dopiero energiczne działania Pompejusza Wielkiego 67–66 r. p.n.e. położyły kres tej pladze.

W średniowiecznej Europie plaga piractwa (także na niewielkich akwenach jak np. Bałtyk) była na tyle duża, że wymagała kolektywnego przeciwdziałania państw zagrożonych tą patologią, np. Związku Hanzeatyckiego.

Warunki żeglugi, głównie przybrzeżnej, były trudne ze względu na niemal całkowity brak oznaczeń nawigacyjnych. Jedynym stałym ich rodzajem były dość prymitywne latarnie morskie. Sytuację diametralnie zmieniły wielkie odkrycia geograficzne przełomu XV i XVI w. Od tej pory handel europejski nabrał wymiaru oceanicznego, a olbrzymie akweny wodne stały się areną walk mocarstw o dominację w wymiarze morskim. Istotnym elementem, który od owych czasów wpływał negatywnie na poziom bezpieczeństwa morskiego, było korsarstwo wspierane przez wszystkie ówczesne mocarstwa morskie – uciekające się do niego nie tylko w czasie konfliktów zbrojnych, ale również podczas pokoju, by wspomnieć najsłynniejszego w ich gronie korsarza doby XVI w. F. Drake'a. Korsarstwa formalnie zabronił dopiero układ pokojowy z Paryża (1856) kończący wojnę krymską. Data ta wyznaczała też inną rewolucję w dziedzinie bezpieczeństwa morskiego i żeglugi. Era żagla przechodziła ostatecznie do historii. Drewniane statki i okręty napędzane wiatrem szybko ustępowały miejsca stalowym konstrukcjom napędzanym silnikami parowymi. Dawało to nowe możliwości, uniezależniało od kaprysów natury, zwiększając jednocześnie prędkość poruszania

się statków i okrętów. Przewrót technologiczny, jaki miał miejsce u schyłku XIX w., szedł w parze z lawinowo narastającą ekspansją kolonialną mocarstw europejskich. Fakt ten wymuszał nie tylko utrzymywanie coraz większej floty przez te państwa, lecz także skłaniał do refleksji teoretycznej dotyczącej tego, czym jest bezpieczeństwo morskie, ujmowane wszakże w owej epoce najczęściej jako „potęga morska" (ang. *sea power*). Trudno bowiem oprzeć się wrażeniu, że aż do epoki admirała H. Nelsona → m a r y n a r k i w o j e n n e [t. 3] potęg nawet takich jak brytyjska były rozbudowywane – albo demobilizowane (→ d e m o b i l i z a c j a [t. 2]) – w zależności od bieżących potrzeb, nie istniały długofalowe plany dotyczące ich miejsca i funkcji w systemie bezpieczeństwa państwa. Nie bez znaczenia był fakt olbrzymich kosztów utrzymania floty, również w przeszłości zdecydowanie przewyższały one sumy potrzebne do funkcjonowania stałej armii lądowej. Ta prawidłowość utrzymuje się też współcześnie. Oba światowe konflikty XX w. udowodniły dobitnie, jak ważną rolę odgrywa bezpieczeństwo na morzu nie tylko dla imperiów morskich takich jak Wielka Brytania, USA czy Japonia, lecz także dla potęg lądowych jak Rzesza Niemiecka czy ZSRR. W przypadku kaiserowskich i nazistowskich Niemiec → b l o k a d a m o r s k a ostatecznie pogrążyła ich gospodarkę, a zwłaszcza przemysł zbrojeniowy. Jeśli chodzi o ZSRR, ciągłość dostaw sprzętu oraz żywności dla Armii Radzieckiej w dużej mierze przyczyniła się do jej zwycięstwa w II wojnie światowej. Konflikt ten udowodnił olbrzymie znaczenie zaplecza logistycznego (w tym przemysłu stoczniowego) w zapewnieniu bezpieczeństwa morskiego. Po raz pierwszy w dziejach czynnik ten okazał się bardzo istotny, a jego rola po 1945 r. zaczęła rosnąć. Jednocześnie bezpieczeństwo morskie zaczęto postrzegać nie tylko w wymiarze militarnym (tj. potencjału marynarki wojennej danego państwa), ale znacznie szerzej, w kontekście wielkości i charakteru jego floty handlowej, rybackiej (zwłaszcza dalekomorskiej) oraz infrastruktury towarzyszącej, takiej jak stocznie budujące nowe jednostki, stocznie remontowe oraz warsztaty naprawcze, porty i bazy przeładunkowe, przede wszystkim kontenerowe itd.

Ujmując problem współcześnie, należy wskazać, że bezpieczeństwo morskie jest zarówno wypadkową polityki zewnętrznej państwa, jego rzeczywistych potrzeb w tym zakresie, jak i możliwości ekonomicznych. One z kolei pozostają we współzależności z ogólną doktryną → b e z p i e c z e ń s t w a n a r o d o w e g o danego kraju. Według T. Szubrychta bezpieczeństwo morskie wyprowadza się wprost z szeroko rozumianej polityki morskiej państwa, będącej:

> całokształtem zamierzonych działań władzy ustawodawczej i wykonawczej, podmiotów gospodarczych oraz społecznych zapewniających szeroko pojęte bezpieczeństwo morskie państwa. Musi ona stworzyć warunki umożliwiające zarówno zasobów morza, jak i nadmorskiego położenia zgodnie z interesami politycznymi, gospodarczymi, militarnymi i społecznymi państwa, przy jednoczesnym zapewnieniu zrównoważonej ochrony środowiska naturalnego.

Z kolei wg autora z młodszego pokolenia badaczy tej problematyki – Ł. Wyszyńskiego – bezpieczeństwo morskie to „działalność podmiotów gospodarczych oraz społecznych, w celu zapewnienia bezpieczeństwa morskiego". Zauważa on przy tym ścisłą korelację → s t r a t e g i i [t. 4] tego segmentu bezpieczeństwa narodowego oraz prowadzonej przez państwo polityki zewnętrznej i wewnętrznej.

W nauce zachodniej (głównie amerykańskiej) problem ten jest nieco zawężony, tzn. aspekt bezpieczeństwa morskiego sprowadzany jest przede wszystkim do zapewniania sobie przewagi w rozumieniu militarnym za pomocą własnych sił morskich korzystających ze wsparcia pozostałych rodzajów sił zbrojnych, zwłaszcza lotnictwa. W bardzo niewielkim stopniu zwraca się uwagę na pozamilitarne aspekty bezpieczeństwa morskiego, zarówno gdy chodzi o rolę własnej marynarki handlowej, jak i bezpieczeństwo żeglugi pod względem nawigacyjnym. W podobnym tonie utrzymane jest rosyjskie ujęcie tematu. Stanowi to pewną redefinicję poglądów admirała Gorszkowa, które wszak były do końca istnienia ZSRR obowiązującą w tym zakresie doktryną. Jak się wydaje – i strona rosyjska tego nie kryje – taki stan rzeczy wynika z nie najlepszej aktualnie kondycji finansów publicznych Rosji. Obecnie utrzymywanie silnej marynarki wojennej i jednocześnie dużej floty handlowej przerasta ekonomiczne możliwości Federacji Rosyjskiej.

Należy jednak zwrócić uwagę, że także państwa znacznie zamożniejsze od Rosji redukują własną marynarkę handlową i wolą korzystać z usług tzw. tanich bander. Interesująco przedstawia się natomiast ewolucja chińskiej doktryny bezpieczeństwa morskiego. Do początków bieżącego stulecia Chińska Republika Ludowa i jej siły zbrojne koncentrowały się na zapewnieniu bezpieczeństwa morskiego w pasie wód terytorialnych i – w najlepszym wypadku – akwenów do nich przylegających. W ostatnich latach znacznie się to zmieniło. Ambicje Pekinu w tym względzie sięgają całego zachodniego Pacyfiku, a Morze Południowochińskie wręcz jest traktowane jako strefa wewnętrzna Chin, co oczywiście prowadzi do zaognienia stosunków Pekinu z ich najbliższymi sąsiadami, a także z USA. Ambicje chińskiej elity przywódczej są jednak większe. Marynarka wojenna Chińskiej Armii Ludowo-Wyzwoleńczej zaczyna przejawiać aspiracje na skalę światową. Jej okręty eskortują chińskie statki handlowe w odległych i niebezpiecznych rejonach takich jak Róg Afryki czy cieśnina Ormuz. Bezpieczeństwo morskie ma zatem dla Pekinu zakres globalny, czemu zresztą przywódcy chińscy nie zaprzeczają; deklarują budowę baz morskich swej floty w dalekich od rodzimych brzegów rejonach, m.in. u wybrzeży kontynentu afrykańskiego. Nie da się jednak zaprzeczyć, że obecność okrętów ChRL na zagrożonych piractwem i terroryzmem akwenach zwiększa bezpieczeństwo morskie wszystkich uczestników światowej żeglugi.

Bezpieczeństwo morskie jest terminem, który zwraca uwagę na nowe wyzwania, jednak nie osiągnięto międzynarodowego konsensusu w sprawie jego definicji. Odnosi się on do zagrożeń takich jak spory morskie między państwami, terroryzm morski,

piractwo, handel narkotykami, ludźmi i nielegalnymi towarami, rozprzestrzenianie broni, nielegalne połowy, przestępstwa przeciwko środowisku lub wypadki i katastrofy morskie. Bezpieczeństwo morskie należałoby zatem definiować jako brak tych zagrożeń, podejście to zostało jednak słusznie skrytykowane jako niewystarczające, ponieważ nie nadaje priorytetów konkretnym kwestiom ani nie zapewnia wskazówek, w jaki sposób te problemy są ze sobą powiązane oraz nie opisuje, jak można zaradzić tym zagrożeniom.

W 2014 r. Wielka Brytania, UE, a także Unia Afrykańska (UA) rozpoczęły ambitne strategie bezpieczeństwa morskiego. → N A T O [t. 3] uwzględniło bezpieczeństwo morskie jako jeden ze swoich celów w strategii morskiej Sojuszu z 2011 r. USA były pionierami tego rozwoju, wprowadzając krajową politykę bezpieczeństwa morskiego w 2004 r. Ponadto Komitet Bezpieczeństwa Morskiego (Martime Safety Committee, MSC) Międzynarodowej Organizacji Morskiej (International Maritime Organisation, IMO) umieścił bezpieczeństwo morskie na swojej liście zadań. Jak odzwierciedlono w polityce USA, koncepcja bezpieczeństwa morskiego zyskała na znaczeniu po atakach terrorystycznych z 11 września i związanych z nimi obawach wywołanych rozprzestrzenianiem się terroryzmu morskiego. Jeśli terroryzm morski przez dłuższy czas pozostawał w dużej mierze wirtualnym zagrożeniem, to przełom w dziedzinie bezpieczeństwa morskiego nastąpił wraz ze wzrostem piractwa u wybrzeży Somalii w latach 2008–2011. Zagrożenia związane z piractwem wprowadziły morski wymiar bezpieczeństwa do globalnej świadomości. Co więcej, napięcia międzypaństwowe w regionach takich jak Arktyka, Morze Południowochińskie i Morze Wschodniochińskie oraz znaczne inwestycje w marynarki wojenne wschodzących mocarstw, takich jak Indie i Chiny, zwróciły większą uwagę na oceany i przestrzeń bezpieczeństwa.

Dyskusje na temat reakcji na bezpieczeństwo morskie przedstawiają dość szeroką i niespójną kombinację różnorodnych propozycji politycznych, które zwykle obejmują wezwania do większej koordynacji, wymiany → i n f o r m a c j i [t. 2], regulacji, egzekwowania prawa i budowania zdolności. Otwartą kwestią pozostaje to, co powinno być koordynowane lub regulowane oraz kto powinien być koordynowany albo regulowany, a także kto powinien budować jaki rodzaj zdolności.

Zapewnienie bezpieczeństwa morskiego jest poważnym wyzwaniem międzyagencyjnym, nawet na poziomie krajowym. Im szersze rozumienie bezpieczeństwa morskiego, tym szerszy zakres zaangażowanych podmiotów. Podczas gdy dokładna forma koordynacji krajowej, wspólnych polityk i operacji oraz wymiany informacji zależy od projektu działań rządowych, różne agencje funkcjonalne wymagają koordynacji. Obejmuje to koordynację cywilno-wojskową, ponieważ nie ma wyraźnego rozdziału między działaniami cywilnymi a operacjami morskimi, a także kilka agencji regulacyjnych, takich jak ministerstwa transportu, rybołówstwa, rolnictwa i handlu, oraz agencje prawne, od straży przybrzeżnej, po władze portowe, straż graniczną, → p o l i c j ę [t. 3] lub służby wywiadowcze. Dotyczy to również koordynacji między państwem

a przedsiębiorstwami żeglugowymi i rybackimi, przemysłem zasobów oraz prywatnymi podmiotami zapewniającymi bezpieczeństwo morskie.

Bezpieczeństwo morskie jest szeroko rozumiane jako zadanie ponadnarodowe. Raport sekretarza generalnego ONZ z 2008 r. podkreśla znaczenie współpracy międzynarodowej i skoordynowanych reakcji oraz zwraca uwagę na to, że bezpieczeństwo morskie jest wspólną odpowiedzialnością i wymaga nowej wizji bezpieczeństwa zbiorowego. Inne strategie morskie, w tym strategie USA, NATO, UE lub Wielkiej Brytanii, również podkreślają znaczenie multilateralizmu i wspólnych skoordynowanych reakcji. Biorąc pod uwagę to, że → z a g r o ż e n i a b e z p i e c z e ń s t w a [t. 4] morskiego mają charakter ponadnarodowy, a ich sprawcy działają ponad granicami, a także ze względu na płynny charakter morskich granic terytorialnych oraz złożony międzynarodowy charakter globalnej żeglugi i handlu, w którym każda pojedyncza operacja obejmuje różne narodowości i jurysdykcje, brak bezpieczeństwa morskiego ma konsekwencje również ponadnarodowe.

Roman Kochnowski

H. Bo, G. Till, *Chinese Maritime Power in the 21th Century. Strategic Plannig, Policy and Predictions*, Routledge, London–New York 2020; *Deutsche Marinen im Wandel. Vom Symbol nationaler Einheit zum Instrument internationaler Sicherheit*, W. Rahn (hrsg.), De Gruyter, München 2005; J.R. Holmes, T. Yoshihara, *Red Star over the Pacific. China's Rise and Chellenge to U.S. Maritime Strategy*, Naval Institute Press, Annapolis 2018; *Leksykon bezpieczeństwa morskiego. 100 najważniejszych pojęć*, T. Szubrycht (red.), C.H.Beck, Warszawa 2016; Ch. Parry, *Super Highway: Sea Power in the 21st Century*, Elliott & Thompson, London 2014; T. Sommer, *China First. Die Welt auf dem Weg ins Chinesische Jahrhundert*, C.H.Beck, München 2019; J. Stavridis, *Sea Power. The Geopolitics of the World's Ocean*, Penguin Press, New York 2017; T. Szubrycht, *Bezpieczeństwo morskie państwa. Zarys problemu*, AMW, Gdynia 2011; Ł. Wyszyński, *Marynarka Wojenna RP w systemie bezpieczeństwa narodowego w latach 2007–2012* [rozprawa doktorska], Poznań 2019.

BEZPIECZEŃSTWO NARODOWE (ang. *national security*) – jeden z rodzajów → b e z p i e c z e ń s t w a wyłoniony ze względu na kryterium podmiotowe. W → n a u k a c h o b e z p i e c z e ń s t w i e [t. 3] rozpatrywane bywa jako stan, proces, wartość i/lub potrzeba odnoszące się do stabilnej egzystencji, niezakłóconego funkcjonowania państwa i jego rozwoju zarówno w aspekcie wewnętrznym, jak i zewnętrznym, a więc do ochrony przed istniejącymi lub potencjalnymi → z a g r o ż e n i a m i [t. 4] dla państwa, jego instytucji i organów, narodu, społeczeństwa, grup społecznych i poszczególnych jednostek. Termin ten – biorąc pod uwagę wielość ujęć teoretyczno-koncepcyjnych, ewolucję bezpieczeństwa narodowego w ciągu ostatnich kilkudziesięciu lat oraz wieloaspektowość bezpieczeństwa jako samoistnej kategorii badawczej w naukach społecznych – jest niezwykle trudny do jednoznacznego określenia i objęcia zwartą definicją wszystkich uwarunkowań i płaszczyzn obronno-ochronnych państwa. O wspomnianej trudności świadczy choćby fakt, że dotychczas nie powstała spójna i powszechnie akceptowalna definicja bezpieczeństwa narodowego.

Potrzeba usystematyzowania problematyki bezpieczeństwa narodowego w dalszym ciągu jest więc wyzwaniem dla teoretyków i specjalistów z zakresu bezpieczeństwa państwa.

Pragnienie istnienia, przetrwania, tożsamości, rozwoju czy stabilizacji było odczuwane i artykułowane przez ludzkość od zawsze, mimo że nie zawsze określano ją mianem bezpieczeństwa. W okresie starożytności, kiedy rozpoczął się proces formowania „narodów" z grup etnicznych, które tworzyły własne organizmy państwowe, dostrzegano konieczność rozciągnięcia nad nimi pieczy w znaczeniu politycznym i militarnym. Bezpieczeństwo narodowe w ciągu ostatnich kilkudziesięciu lat ewoluowało wraz z dostrzeżeniem szerszej niż tylko wojskowa płaszczyzny ochrony społeczeństwa, jego dóbr i środowiska oraz państwa jako instytucji politycznej, co znalazło swój wyraz na przełomie XX i XXI w. Wynika to z wzięcia pod uwagę wielu różnorodnych (nie tylko wojskowych) przyczyn → z a g r o ż e ń b e z p i e c z e ń s t w a [t. 4] narodowego, a także z tego, że obecnie nie tylko siły zbrojne mogą stanowić narzędzie oddziaływania na innych uczestników stosunków międzynarodowych oraz pozostałe źródła zagrożeń. Zagadnienia bezpieczeństwa rozszerzyły się więc stopniowo o problemy gospodarcze, ekologiczne, demograficzne, kulturowe, ideologiczne, społeczne, technologiczne oraz inne. Do najważniejszych czynników, które miały wpływ na zmiany w zakresie bezpieczeństwa narodowego, R. Zięba zalicza: rewolucję naukowo-techniczną, delegalizację wojny napastniczej i międzynarodową kontrolę zbrojeń, wzrost roli i znaczenia podmiotów pozarządowych oraz wzrost współzależności międzynarodowych.

Funkcjonujące w literaturze przedmiotu ujęcia definicyjne bezpieczeństwa narodowego zawierają wiele wspólnych elementów, choć rozkład akcentów na poszczególne czynniki bywa zróżnicowany. Biorąc pod uwagę wielość definicji bezpieczeństwa narodowego, warto przybliżyć istotę kilku z nich, bardzo popularnych w naukach o bezpieczeństwie. Tak np. przez

W. Kitlera bezpieczeństwem narodowym została określona:

> najważniejsza wartość, potrzeba narodowa i priorytetowy cel działalności państwa, jednostek i grup społecznych, a jednocześnie proces obejmujący różnorodne środki, gwarantujące trwały, wolny od zakłóceń byt i rozwój narodowy (państwa), w tym ochronę i obronę państwa jako instytucji politycznej oraz ochronę jednostek i całego społeczeństwa, ich dóbr i środowiska naturalnego przed zagrożeniami, które w znaczący sposób ograniczają jego funkcjonowanie lub godzą w dobra podlegające szczególnej ochronie.

Bezpieczeństwo narodowe zawiera się więc w wyartykułowanej potrzebie i faktycznej dążności podmiotów różnego szczebla (państwo, społeczeństwo, grupy społeczne i jednostki) do kształtowania materialnego i niematerialnego bytu państwa oraz jego rozwoju poprzez ochronę przed zagrożeniami dla żywotnych interesów państwa i narodu, za pomocą różnorodnych środków. Powyższa definicja charakteryzuje się

dualistycznym podejściem do kwestii bezpieczeństwa narodowego, ponieważ odnosi się zarówno do jego warstwy pozytywnej (aspekt prorozwojowy), jak i negatywnej (aspekt ochrony przed zagrożeniami), która w innych koncepcjach zdecydowanie dominuje. W.J. Taylor jr. określa bezpieczeństwo narodowe jako:

> nie tylko ochronę narodu i terytorium przed fizyczną napaścią, lecz również ochronę – za pomocą różnych środków – żywotnych interesów ekonomicznych i politycznych, których utrata zagroziłaby żywotności i podstawowym wartościom państwa.

W. Stankiewicz z kolei określa je jako „stan równowagi między zagrożeniem wywołanym możliwością zaistnienia konfliktu a potencjałem obronnym". S. Dworecki bezpieczeństwem narodowym nazywa:

> rzeczywisty stan stabilności wewnętrznej i suwerenności, który odzwierciedla brak lub występowanie jakichkolwiek zagrożeń (w sensie zaspokajania podstawowych potrzeb egzystencjalnych i behawioralnych społeczeństwa oraz traktowania państwa jako suwerennego podmiotu w stosunkach międzynarodowych).

Wydaje się, że kompleksową koncepcję teoretyczną w zakresie definiowania bezpieczeństwa narodowego przedstawił J. Stańczyk. Można z niej wyodrębnić następujące elementy (tezy):

- bezpieczeństwo narodowe dotyczy pewności przetrwania i swobody rozwoju;
- żywotne wartości, potrzeba, cel, interes narodowy i racja stanu to czynniki wzmagające proces zapewniania bezpieczeństwa narodowego;
- bezpieczeństwo narodowe jest stanem obiektywnym, niezależnym od subiektywnych partykularyzmów;
- bezpieczeństwo narodowe realizuje się w sferze wewnętrznej i zewnętrznej;
- czas modyfikuje priorytety w zakresie bezpieczeństwa narodowego.

Nierzadko w literaturze przedmiotu pojęcie bezpieczeństwa narodowego utożsamia się z pojęciem bezpieczeństwa państwa i stosuje zamiennie z nim, wskutek tego, że oba te pojęcia są zakorzenione w terminologii nauk o bezpieczeństwie i powszechnie używane. O ile jednak bezpieczeństwo państwa sugeruje koncentrowanie się przede wszystkim na bezpieczeństwie państwa jako instytucji, o tyle bezpieczeństwo narodowe mocniej akcentuje ochronę interesów nie tylko państwa jako całości, ale również społeczeństwa i jego składowych. Używanie terminu bezpieczeństwa państwa jest najbardziej adekwatne w odniesieniu do państw demokratycznych, z gospodarką wolnorynkową, w których prawa jednostki i grup społecznych mają kluczowe znaczenie. Jednocześnie, jak słusznie zauważa Z. Sabak, najważniejszym zadaniem państwa i narodu polskiego w kwestii bezpieczeństwa jest zapewnienie bezpiecznego bytu i rozwoju, suwerennego traktowania w stosunkach międzynarodowych, zagwarantowanie nienaruszalności granic oraz integralności terytorialnej. Tym samym bezpieczeństwo narodowe jest procesem, tzn. celową i zorganizowaną działalnością upoważnionych organów państwa, opierającym się na określonej

koncepcji – doktrynie – bezpieczeństwa oraz jest realizowane sposobami i środkami polityki zagranicznej.

Każde państwo w trosce o własne bezpieczeństwo narodowe ustala zbiór wartości narodowych, które jego zdaniem powinny być chronione przed zagrożeniami, i przyjmuje odpowiedni zespół środków zabezpieczających te wartości przed wszelkiego rodzaju zagrożeniami. Środki narodowej polityki bezpieczeństwa są zróżnicowane, zależą od charakteru, rozmiarów i siły zagrożeń względem wartości uznanych za ważne dla przetrwania oraz rozwoju państwa. Mogą to być przedsięwzięcia w ramach wewnętrznej funkcji państwa, takie jak wzmacnianie jego siły militarnej, gospodarczej, optymalizacja systemu społeczno-politycznego i stabilności politycznej, oraz działania realizowane w ramach funkcji zewnętrznej (międzynarodowej). Środki służące ochronie i umacnianiu bezpieczeństwa narodowego można dzielić wg kryterium przedmiotowego na polityczne, wojskowe, gospodarcze, naukowo-techniczne, kulturowe, ideologiczne, ekonomiczne itp. Ich zakres i dobór zależą nie tylko od potrzeb stwarzanych przez powstające zagrożenia (czy wyzwania), ale przede wszystkim od percepcji tych zagrożeń przez organy kierownicze państwa i pozostających w jego dyspozycji zasobów materialnych oraz intelektualnych, a także od umiejętności ich efektywnego wykorzystywania. Według Zięby na pojęcie bezpieczeństwa narodowego składają się wartości takie jak:

- przetrwanie państwa jako suwerennej jednostki politycznej (zob. → s u w e r e n n o ś ć p a ń s t w a [t. 4]), narodu jako wyróżnionej grupy etnicznej, biologiczne przeżycie ludności – naczelna wartość, dla której każde państwo gotowe jest poświęcić inne wartości, gdyż nie mogą być one zachowane w sytuacji zagrożenia istnienia samego podmiotu;
- integralność terytorialna – uważana za główny korelat bezpieczeństwa;
- niezależność polityczna – w sensie ustrojowym, samowładności i swobody;
- jakość życia, na którą składają się wartości szczegółowe, takie jak standard życia, szczebel rozwoju społeczno-gospodarczego, system kulturalny, możliwości perspektywy dalszego rozwoju.

Z wartościami narodowymi związane są potrzeby w zakresie bezpieczeństwa narodowego. Oznaczają one dążenia do przygotowania państwa na wszystkich szczeblach i we wszystkich dziedzinach do ciągłej i skutecznej ochrony i obrony interesów oraz wartości narodowych przed → z a g r o ż e n i a m i m i l i t a r n y m i [t. 4] i niemilitarnymi w warunkach niepewności i postępu, zapewniające przetrwanie narodu i jego wartości, pomyślność i dobrobyt oraz tworzenie korzystnych warunków dla obecnych i przyszłych pokoleń. W literaturze przedmiotu potrzeby w zakresie bezpieczeństwa narodowego zazwyczaj dzieli się wg kryterium podmiotowego i przedmiotowego.

Według pierwszego z nich potrzeby te dotyczą:

- każdej jednostki, niezależnie od jej wieku, pozycji społecznej, sytuacji materialnej, rozwoju psychofizycznego i środowiska, w którym żyje (cywilizacyjnego, społecznego i naturalnego);

- grup społecznych, formalnych (rodzin, organizacji społecznych, zawodowych, politycznych) i nieformalnych;
- całej grupy państw – w zakresie wartości wspólnych dla całego społeczeństwa zamieszkującego dane państwo;
- społeczności międzynarodowej – w ramach wspólnych wartości.

Według kryterium przedmiotowego natomiast potrzeby związane z dziedziną bezpieczeństwa narodowego dotyczą m.in.:

- bezpieczeństwa państwa (w tym głównie → bezpieczeństwa militarnego, → bezpieczeństwa politycznego i porządku konstytucyjnego) – m.in. w zakresie ochrony i obrony przed naruszeniem suwerenności państwa, jego integralności terytorialnej, ochrony tożsamości narodowej wobec procesów globalizacyjnych, zachowania suwerennej władzy, ochrony wolności, → praw człowieka [t. 3] i obywatela itp.;
- bezpieczeństwa i porządku publicznego – głównie w zakresie zwiększenia wykrywalności i egzekucji; zwalczania wykroczeń i przestępstw przeciwko życiu, zdrowiu i mieniu, → przemocy [t. 3] w rodzinie, szkole i środowisku społecznym; przeciwdziałania demoralizacji i → przestępczości [t. 3] nieletnich, alkoholizmowi, narkomanii; zapewnienia pomocy ofiarom przestępstw i wykroczeń; poprawy bezpieczeństwa ruchu drogowego; zagwarantowania ochrony dóbr materialnych, w tym → infrastruktury krytycznej [t. 2]; zapobiegania → przestępczości zorganizowanej [t. 3], → korupcji [t. 2]; zwiększenia udziału społeczeństwa w aktywnym przeciwdziałaniu zagrożeniom itd.;
- → bezpieczeństwa powszechnego – w obszarze usprawnienia jakości działania służb ratowniczych; zapewnienia natychmiastowej doraźnej pomocy materialnej i opieki psychologicznej, w tym religijnej; zagwarantowania tymczasowego schronienia, wyżywienia, pomocy medycznej i innych form pomocy społecznej; wspierania tworzenia społecznych (pozarządowych) form → ochrony ludności [t. 3] i ratownictwa; poprawy bezpieczeństwa w miejscach wypoczynku; sprawnej organizacji pomocy humanitarnej itp.;
- → ochrony zdrowia [t. 3] oraz bezpieczeństwa sanitarno-epidemiologicznego – w zakresie stworzenia warunków sprawnej opieki zdrowotnej; zwiększenia dostępności do usług medycznych w miejscu zamieszkania; ograniczenia ryzyka zachorowań ludzi i zwierząt; zapobiegania chorobom odzwierzęcym; zwalczania naruszeń przepisów BHP, norm technologicznych i żywieniowych itd.;
- ochrony środowiska i gospodarki odpadami – w kwestii poprawy jakości wód, gleby, wody i powietrza; chronienia przyrody ożywionej i nieożywionej; egzekwowania przepisów dotyczących gospodarowania odpadami i zwalczania naruszeń w tym względzie; edukacji ekologicznej społeczeństwa;

- ochrony dorobku kulturowego i tożsamości narodowej – kultywowania dziedzictwa narodowego; poszanowania różnic światopoglądowych i etnicznych; ochrony dziedzictwa kulturowego narodu (duchowego i materialnego) itp.;
- → b e z p i e c z e ń s t w a e k o n o m i c z n e g o – stylu i jakości życia, dobrobytu materialnego; dostępu do pomocy społecznej w sytuacjach ekstremalnych; dostępu i możliwości wyboru miejsca pracy; godziwych zarobków itd.;
- oświaty i wychowania – w tym równości szans dzieci i młodzieży, a nawet dorosłych; dostępu do publicznych form edukacji, wychowania (muzea, biblioteki, ośrodku kultury); dostępu do obiektów sportowo-rekreacyjnych; kształtowania wiedzy, umiejętności i nawyków zachowania w sytuacjach trudnych; pomocy psychologiczno-pedagogicznej; integrowania społeczeństwa wokół wspólnych inicjatyw lokalnych.

Wspomniane powyżej wartości i potrzeby decydują o bezpieczeństwie narodowym jako centralnej kategorii społecznej, która wg J. Marczaka:

> stanowi dla jednostek, społeczności lokalnych oraz państwa pierwotną, egzystencjalną, naczelną potrzebę i wartość, a zarazem priorytetowy cel działania we wszystkich dziedzinach i na wszystkich szczeblach organizacji państwowej i społecznej.

Ów autor stwierdza też, że bezpieczeństwo narodowe w znaczeniu funkcjonalnym jest misją społeczeństwa i państwa, której realizacja polega na ochronie i obronie → i n t e r e s ó w n a r o d o w y c h [t. 2] przed zagrożeniami oraz tworzeniu wewnętrznych i zewnętrznych warunków do rozwoju w trudnej do przewidzenia przyszłości. Natomiast w znaczeniu strukturalnym bezpieczeństwo narodowe jawi się jako przygotowanie i organizacja państwa w zakresie prawnych podstaw bezpieczeństwa, polityki i → s t r a t e g i i b e z p i e c z e ń s t w a n a r o d o w e g o [t. 4], cywilno-wojskowej organizacji ochrony i → o b r o n y n a r o d o w e j [t. 3], infrastruktury bezpieczeństwa, → e d u k a c j i d l a b e z p i e c z e ń s t w a [t. 2] oraz współpracy międzynarodowej na rzecz bezpieczeństwa.

Podstawowymi uwarunkowaniami bezpieczeństwa narodowego w układzie sektorowym są uwarunkowania:

- polityczne – aspekt międzynarodowy (stabilność systemu stosunków międzynarodowych, liczba i efektywność organizacji międzynarodowych, sposoby rozstrzygania sporów), aspekt narodowy (efektywność struktur państwa, jakość systemu politycznego itd.);
- militarne – liczebność i jakość sił zbrojnych, uczestnictwo w sojuszach wojskowych, → s t r a t e g i a [t. 4] wykorzystania posiadanych zasobów;
- ekonomiczne – stan gospodarki, ilość środków przeznaczanych na obronność, rozwój gospodarczy i skuteczne przeciwdziałanie zewnętrznym naciskom;
- kulturowe – ochrona wartości kultury symbolicznej, ochrona materialnych dóbr kultury i dziedzictwa narodowego, otwartość kulturowa jednostek i narodów;

- społeczne – ochrona egzystencjalnych podstaw życia ludzi, umożliwienie realizacji aspiracji życiowych, zapewnienie odpowiedniego poziomu życia, niedopuszczenie do marginalizacji i wykluczenia społecznego;
- ekologiczne – ochrona przed zagrożeniami dla środowiska naturalnego;
- informacyjne – zabezpieczenie przed atakami sieciowymi i skutkami ataków fizycznych.

Biorąc pod uwagę, że to państwo w dalszym ciągu jest podstawowym (i głównym zarazem) uczestnikiem stosunków międzynarodowych, a także – w myśl paradygmatu realistycznego – fakt, iż to siła państwa, jego autorytet i rola w kształtowaniu polityki wewnętrznej decydują o poziomie bezpieczeństwa obywateli, ma ono do wypełnienia szereg istotnych funkcji w zakresie bezpieczeństwa narodowego. Należą do nich m.in.:

- troska o wysoką pozycję państwa w stosunkach międzynarodowych;
- ochrona porządku konstytucyjnego;
- zapewnienie obywatelom odpowiednich warunków życia;
- zapewnienie bezpieczeństwa i porządku publicznego (ładu społecznego, ochrona norm i obyczajów, ochrona praw i wolności obywatelskich);
- zapewnienie bezpieczeństwa powszechnego (ochrona przed skutkami klęsk żywiołowych, → k a t a s t r o f t e c h n i c z n y c h [t. 2], → e d u k a c j a d l a b e z p i e c z e ń s t w a [t. 2]);
- zapewnienie → b e z p i e c z e ń s t w a s p o ł e c z n e g o (egzystencja i rozwój osobisty);
- ochrona życia, zdrowia, mienia i środowiska naturalnego;
- kształtowanie → m o r a l e [t. 3] narodowego, postaw proobywatelskich;
- zapewnienie dobrobytu (odpowiednich warunków) i → zrównoważonego rzwoju [t. 4];
- zapewnienie → b e z p i e c z e ń s t w a k u l t u r o w e g o ;
- materialne i duchowe trwanie ludności w stanie pokoju, → k r y z y s u [t. 2] i wojny;
- zapewnienie bezpieczeństwa militarnego (integralność terytorialna, suwerenność, ochrona granicy, niezależność i niepodległość).

Podsumowując, bezpieczeństwo narodowe jest związane ze wszystkimi obszarami funkcjonowania państwa, uwzględnia bezpieczeństwo pojedynczych osób, grup społecznych oraz całego społeczeństwa, obejmuje przeciwdziałanie wszelkim istniejącym i potencjalnym zagrożeniom. Zapewnia poczucie ich braku, stabilność i rozwój państwa, jego ochronę i obronę jako instytucji politycznej oraz ochronę pojedynczych osób i całego społeczeństwa. Bezpieczeństwo narodowe jest również najważniejszą potrzebą, najwyższą wartością, priorytetowym celem działalności państwa – do jego zapewnienia państwo wykorzystuje wszystkie dostępne siły i środki. Jest zjawiskiem niezwykle szerokim i powinno być ujmowane wielowymiarowo, zarówno w aspekcie

celów, zadań, funkcji, identyfikacji podmiotów zajmujących się analizowaną problematyką, jak i obszaru, na który oddziałuje. Dotyczy to różnorodnych działań zewnętrznych w sferze stosunków międzynarodowych oraz działań wewnętrznych mających na celu ochronę wartości narodowych i realizację potrzeb, interesów i celów bezpieczeństwa narodowego. Jednocześnie należy stwierdzić, że autorzy definicji bezpieczeństwa narodowego bardzo często dookreślają to pojęcie, używając terminów takich jak wartości narodowe, potrzeby i interesy narodowe oraz cele bezpieczeństwa narodowego.

Paweł Łubiński, Janusz Falecki

S. Dworecki, *Zagrożenia bezpieczeństwa państwa*, AON, Warszawa 1994; J. Falecki, *Dylematy zarządzania kryzysowego w Rzeczypospolitej Polskiej*, Oficyna Wydawnicza „Humanitas", Sosnowiec 2016; A.A. Jordan, W.J. Taylor, *American National Security: Policy and Process*, Johns Hopkins University Press, Baltimore 1981; W. Kitler, *Bezpieczeństwo narodowe RP. Podstawowe kategorie, uwarunkowania, system*, AON, Warszawa 2011; W. Kitler, J. Gryz, *Misje państwa w zakresie bezpieczeństwa narodowego*, [w:] *System bezpieczeństwa narodowego RP. Wybrane problemy*, W. Kitler, K. Drabik, I. Szostek (red.), AON, Warszawa 2014; M. Kuliczkowski, *Przygotowania obronne w Polsce. Uwarunkowania formalnoprawne, dylematy pojęciowe i próba systematyzacji*, AON, Warszawa 2013; *Leksykon bezpieczeństwa wewnętrznego*, W. Fehler, J.J. Piątek, R. Podgórzańska (red.), Wydawnictwo Naukowe Wydziału Humanistycznego US Minerwa, Szczecin 2017; J. Marczak, *Bezpieczeństwo narodowe*, [w:] *Bezpieczeństwo narodowe Polski w XXI wieku. Wyzwania i strategie*, R. Jakubczak, J. Marczak (red.), Bellona, Warszawa 2011; J. Pawłowski, J. Marczak, K. Gąsiorek, *Definiowanie i uwarunkowania bezpieczeństwa narodowego (państwa)*, [w:] *Podstawy bezpieczeństwa narodowego (państwa). Podręcznik akademicki*, J. Pawłowski (red.), Akademia Sztuki Wojennej, Warszawa 2017; Z. Sabak, J. Królikowski, *Ocena zagrożeń bezpieczeństwa Rzeczypospolitej Polskiej*, AON, Warszawa 2000; W. Stankiewicz, *Bezpieczeństwo narodowe a walki niezbrojne. Studium*, AON, Warszawa 1991; *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; L. Wyszczelski, *Bezpieczeństwo narodowe Polski w XX–XXI wieku na tle wyzwań bezpieczeństwa globalnego*, [w:] *Współczesne bezpieczeństwo militarne*, M. Kubiak, A. Turek (red.), Wydawnictwo Naukowe UPH, Warszawa–Siedlce 2012; *Wyzwania, szanse, zagrożenia i ryzyko dla bezpieczeństwa narodowego RP o charakterze wewnętrznym*, R. Jakubczak, B. Wiśniewski (red.), Wydawnictwo Wyższej Szkoły Policji w Szczytnie, Szczytno 2016; R. Zięba, *Pojęcie i istota bezpieczeństwa w stosunkach międzynarodowych*, „Sprawy Międzynarodowe" 1989, nr 10.

BEZPIECZEŃSTWO PLANETARNE – jest przede wszystkim związane z kwestią ochrony planetarnej poprzez unikanie zanieczyszczeń organicznych i biologicznych podczas eksploracji kosmosu przez ludzi i roboty. Oznacza to, że należy dopilnować, aby organizmy lądowe i składniki organiczne nie spadły celowo lub przypadkowo na inne planety lub inne ciała Układu Słonecznego, należy również monitorować wszystkie statki, które powracają z kosmosu na Ziemię z próbkami wszelkich substancji pozaziemskich.

W lipcu 2018 r. agencja kosmiczna NASA (National Aeronautics and Space Administration) ogłosiła poszukiwanie pracownika na stanowisko funkcjonariusza ds. bezpieczeństwa planetarnego. NASA przestrzega zasady polityki ochrony planet mającej

zastosowanie do wszystkich misji lotów kosmicznych, zgodnie z którą konieczne jest zapobieganie celowemu lub przypadkowemu przenoszeniu mikroorganizmów i wszelkich substancji organicznych z planety Ziemia do innych ciał niebieskich i odwrotnie. Obrońca planetarny NASA będzie musiał monitorować przestrzeganie tych zasad i obserwować misje eksploracji kosmosu organizowane przez NASA, niezależnie od tego, czy są to loty załogowe czy badania robotyczne, które powracają na Ziemię z próbkami.

W związku z tym obowiązki funkcjonariusza ds. bezpieczeństwa planetarnego są następujące:

- planowanie i koordynacja wszystkich działań związanych z misjami NASA wpływającymi na bezpieczeństwo planetarne;
- dokonywanie niezależnej oceny i zapewnienie dodatkowych badań wszystkich misji kosmicznych;
- badanie wszystkich statków powracających na Ziemię z kosmosu;
- szkolenie urzędników państwowych dotyczące ryzyka związanego z bezpieczeństwem planetarnym;
- organizowanie współpracy i koordynacji z naukowcami i komisjami ekspertów w tych kwestiach;
- opracowywanie nowych protokołów, dyrektyw i standardów NASA związanych z bezpieczeństwem planetarnym.

Ludzkość wkroczyła w nową fazę ewolucji – erę ryzyka związaną z rosnącym niebezpieczeństwem samozagłady cywilizacji w wyniku globalnej katastrofy (nuklearnej, ekologicznej, demograficznej). Niebezpieczeństwo dla istnienia cywilizacji wypływa z samej cywilizacji i – sądząc po dynamice procesów globalnych – będzie trwało w najbliższej przyszłości. Polityka bezpieczeństwa planetarnego jest budowana w zależności od poziomu i zakresu działalności, może być ukierunkowana na różne obszary – sferę gospodarczą, ekologiczną, wojskową, informacyjną, społeczno-kulturową. Może przejawiać się na różnych poziomach przestrzennych – globalnym, regionalnym, ogólnopaństwowym i lokalnym.

Bezpieczeństwo planetarne można uznać za złożony problem zapewnienia podstawowych funkcji *homo sapiens* na Ziemi, ale procesy, które trwają na naszej planecie, mogą stanowić ekstremalne → z a g r o ż e n i e [t. 4] dla bezpieczeństwa planetarnego. Mamy do czynienia z poważnymi wyzwaniami dla bezpieczeństwa planetarnego, które są złożone, szybko zachodzące i bardzo destrukcyjne. Zmiany klimatu są podstawowym przykładem takiego wyzwania, ale inne – w większości niezamierzone konsekwencje naszej cywilizacji *high-tech* – są już widoczne horyzoncie. Będą je wyznaczać:

- eskalacja wszelkiego rodzaju → k a t a s t r o f n a t u r a l n y c h [t. 2] (geofizycznych, pogodowych, klimatycznych, społecznych, ekologicznych itp.). Szczególnie niebezpieczne są: wybuchy wulkanów, trzęsienia ziemi i osuwiska; gwałtowne

zmiany pogody i klimatu; tsunami i huragany; ogromne pożary, powodzie, problemy ekologiczne i epidemie; dynamiczne niszczenie infrastruktury; awaryjne odmowy wszechstronnych (lądowych, pływających, powietrznych, kosmicznych itp.) technicznych (w tym energii jądrowej, transportu i wojskowych) środków; wybuchy konfliktów lokalnych (społecznych, politycznych, wojskowych) i groźba ich eskalacji na dużą skalę;

- seria dynamicznych przyspieszeń orbity i osi Ziemi, które będą zagrażać katastrofami o formie i konsekwencjach wykraczających poza granice powszechnego doświadczenia współczesnej cywilizacji;
- lokalizacja wielu miast na obszarach potencjalnie zagrożonych dużymi zniszczeniami, zaniedbanie wpływu anomalii geofizycznych podczas budowy miast;
- ogromna eskalacja niedoboru odporności populacji światowej.

Problemy te zostaną wzmocnione przez:

- znaczący brak równowagi wielu organizmów ludzkich (długoterminowy, destrukcyjny wpływ środków odurzających, alkoholowych, technogennych i informacyjnych, nowoczesnych produktów żywnościowych i leków itp.);
- niezdolność niezrównoważonych układów odpornościowych do zapewnienia wystarczającej odporności organizmów na rosnące zagrożenia wirusowe i inne, w tym ekologiczne;
- brak odpowiedniej wiedzy i technologii z zakresu nauk przyrodniczych;
- zakłócanie na dużą skalę jakości kodu genetycznego społeczeństwa przez trwające destrukcyjne procesy, utratę genetycznych potencjałów emocjonalnych, intelektualnych i immunologicznych w wielu populacjach;
- niemożność pogodzenia rosnących zagrożeń planetarnych z ograniczoną możliwością przewidywania zmian w skali planetarnej.

W raporcie ONZ z grudnia 2019 r. wyraźnie stwierdzono, że konieczne są pilne działania w celu ograniczenia emisji gazów cieplarnianych, które przyczyniają się do globalnego ocieplenia. Cieplejsza planeta będzie coraz częściej prowadzić do wyzwań związanych z bezpieczeństwem planetarnym. Może być potrzebna większa świadomość, lepsze narzędzia prognozowania, a także nowe struktury organizacyjne.

Jedną z najbardziej niepokojących rzeczy w związku z obecnymi wydarzeniami na naszej planecie jest brak świadomości wśród ludzi, w mediach i na szczeblu rządowym – a w konsekwencji powszechne samozadowolenie – w kwestii zmian klimatu. Media koncentrują się na treściach, które przyniosą zyski dzięki wyświetleniom, kliknięciom i like'om, a rządy skupiają się na wygrywaniu kolejnych wyborów, unikając wydatków na przygotowanie się do świata przyszłości, które nie cieszą się popularnością wśród głosujących. Szkody na naszej planecie globalizują się szybciej, niż koordynowane są światowe reakcje na nie. Wpływ zmian klimatu obserwowany obecnie to dopiero początek bardziej znaczących przemian, które nadejdą w przyszłości. Rosnąca, ale wciąż stosunkowo niewielka część społeczeństwa zaczyna zdawać sobie z tego sprawę

i wzywa rządy do podjęcia znacznie bardziej zdecydowanych działań. Strajk szkolny dla klimatu (szw. *Skolstrejk för klimatet*) G. Thunberg zainspirował światowy protest młodzieży przeciwko brakowi działań pokolenia ich rodziców.

Nie ma wątpliwości, że działalność człowieka przyspiesza efekt cieplarniany, co powoduje globalne ocieplenie. Zostało to potwierdzone w Ramowej konwencji Narodów Zjednoczonych w sprawie zmian klimatu (United Nations Framework Convention on Climate Change, UNFCCC), która została przyjęta na Szczycie Ziemi w Rio de Janeiro w 1992 r. i od tego czasu została ratyfikowana przez 197 krajów. Jednak dopiero w porozumieniu paryskim z 2015 r. sygnatariusze UNFCCC wyznaczyli cele, obiecując utrzymać globalne ocieplenie znacznie poniżej wzrostu o 2°C w stosunku do temperatur z okresu przedindustrialnego i spróbować ograniczyć wzrost temperatury do 1,5°C.

Niestety, obecnie jesteśmy zbyt powolni w podejmowaniu działań, aby osiągnąć te cele – emisje gazów cieplarnianych nadal rosną. W raporcie z 2019 r. na temat różnic w poziomie emisji wydanym przez Program Środowiskowy ONZ (United Nations Environment Programme, UNEP) stwierdzono, że istnieje ogromna i rosnąca przepaść między tym, co należy zrobić, aby przeciwdziałać zmianie klimatu, a tym, co faktycznie robimy. Wyzwanie jest ogromne: raport stwierdza, że emisje gazów cieplarnianych muszą być zmniejszane o 7,6% rocznie przez następne 10 lat, jeśli chcemy ograniczyć ocieplenie do 1,5°C.

Nie możemy odkładać skutecznych działań na rzecz klimatu, musimy rozpocząć przygotowania do życia w drastycznie innym świecie, w którym zmiany klimatu i związana z tym globalna degradacja środowiska wpłyną na bezpieczeństwo ludzi i bezpieczeństwo planetarne.

Gwałtowny wzrost wydobycia zasobów, zużycia paliw kopalnych, produkcji, zużycia i odpadów przyczynił się do wzrostu emisji CO_2, znacznego zanieczyszczenia i utraty różnorodności biologicznej, wpływając na wszelkiego rodzaju inne procesy na planecie. Coraz częściej oddziałujące na Ziemię procesy fizyczne, chemiczne i biologiczne przekraczają punkty krytyczne, a pętle sprzężenia zwrotnego będą miały jeszcze większy wpływ na środowisko.

Dlatego bezpieczeństwo planetarne lepiej oddaje nowe → wyzwania bezpieczeństwa [t. 4] naszego stulecia niż wyrażenie → bezpieczeństwo klimatyczne lub nawet szersza koncepcja „środowiska i bezpieczeństwa". Skali tych wyzwań można nie docenić, ale przyszłość może wówczas przynieść znacznie więcej ekstremalnych scenariuszy. Biorąc pod uwagę złożoność współoddziałujących procesów na planecie, trudno jest dokładnie przewidzieć, co stanie się w zakresie różnych średnich temperatur. Jednak im jest cieplej, tym większe zakłócenia będą widoczne we wzorcach pogodowych, ekosystemach i poziomach mórz.

Wilgotność i ciepło mogą sprawić, że duże części stref tropikalnych nie będą nadawać się do zamieszkania przez co najmniej część roku. Wiele lodowców w Himalajach

zapewniających niezawodne źródło wody dla ponad 1 mld ludzi prawdopodobnie zniknie. Wiele nadmorskich miast może zostać pochłoniętych przez wodę. Miliardy ludzi mogą być narażone na niedobór żywności. Już teraz widzimy oznaki tego, co nas czeka: fale upałów, pożary lasów i zwiększone zniszczenia przez huragany, powodzie i inne formy ekstremalnych warunków pogodowych. W nadchodzących dziesięcioleciach, a już na pewno w drugiej połowie tego stulecia, zmiany klimatu staną się największym wyzwaniem, przed jakim kiedykolwiek stanęła ludzkość. Na przykład Mozambik w marcu i kwietniu 2019 r. został uderzony przez 2 gwałtowne cyklony, które spowodowały śmierć ok. 700 osób. Światowa Organizacja Meteorologiczna stwierdziła, że nie było wcześniej żadnych przesłanek pozwalających przewidzieć 2 burze o takiej intensywności, które nawiedziły kraj w tym samym sezonie. To sprawia, że zmiany klimatu stają się nowym wrogiem.

Dwa kluczowe wydarzenia wpłyną na naszą zdolność do przewidywania potencjalnej niestabilności lub konfliktu. Z jednej strony zmiana klimatu i degradacja środowiska jeszcze bardziej skomplikują przewidywanie konfliktów. Z drugiej strony szybki wzrost dużych zbiorów danych i sztucznej inteligencji (AI) może zwiększyć naszą zdolność do prognozowania przyszłych → z a g r o ż e ń b e z p i e c z e ń s t w a [t. 4]. Te nowe narzędzia mogą pomóc nam przygotować się do życia w przemienionym świecie z nowymi wyzwaniami. Trudno też przewidzieć, jakie działania podejmą światowi liderzy w przyszłości, aby zapobiec rozpadowi naszych ekosystemów, zwłaszcza w kontekście zabiegów (lub ich braku) mających na celu ograniczenie emisji gazów cieplarnianych.

Od 2015 r. w Hadze odbywają się coroczne konferencje na temat bezpieczeństwa planetarnego, na których → R a d a B e z p i e c z e ń s t w a O N Z [t. 3], UE i inne organizacje regionalne w coraz większym stopniu zwracają uwagę na wyzwania związane z bezpieczeństwem planetarnym. Wciąż jednak brakuje skutecznej, długoterminowej struktury uwzględniającej wiedzę i role wszystkich zainteresowanych stron.

Olga Wasiuta

IPCC, *Global Warming of 1,5°C. Special Report*, IPCC.ch (dostęp 18.01.2020); UNFCCC, *Cut Global Emissions by 7,6 Percent Every Year for Next Decade to Meet 1,5°C Paris Target – UN Report*, 26.11.2019, UNFCCC.int (dostęp 18.01.2020); USA Jobs, *Planetary Protection Officer*, 13.07.2013, USAJobs.gov (dostęp 18.01.2020); A. Verbeek, *Planetary Security: The Security Implications of Climate Change*, 10.12.2019, NATO.int (dostęp 18.01.2020); В.П. Мельников, Л.В. Константиновская, П.П. Кузнецов, В.А. Поляченко, Г.П. Шибанов, *Планетарная безопасность человечества*, ООО „Буки Веди", Москва 2014.

BEZPIECZEŃSTWO POLITYCZNE (ang. *political security*) – zestaw środków służących identyfikacji i eliminacji czynników, które mogą zaszkodzić interesom politycznym kraju, narodu, społeczeństwa, obywateli, determinować regresję polityczną, a nawet śmierć polityczną państwa; to również zdolność i możliwość narodu oraz jego instytucji państwowych do samodzielnego rozwiązywania dylematów ustrojowych, niezależnego prowadzenia polityki zewnętrznej i wewnętrznej

zgodnie z interesami jednostki i społeczeństwa. Bezpieczeństwo polityczne to ponadto zestaw środków służących zachowaniu konstytucyjnie legitymizowanego systemu politycznego państwa, zapewniającego istnienie państwa i jego konstruktywną politykę. Istotą bezpieczeństwa politycznego jest → s u w e r e n n o ś ć [t. 4] polityczna w stosunkach międzynarodowych i stabilność polityczna społeczeństwa, co osiąga się poprzez tworzenie stabilnego systemu politycznego, który powinien zapewniać równowagę interesów różnych grup społecznych dzięki zasadzie państwa prawa. Brak jednego z tych elementów nieuchronnie niszczy bezpieczeństwo polityczne kraju.

Bezpieczeństwo polityczne nie jest jednoznacznym pojęciem. Raport o rozwoju społecznym (Human Development Report, HDR) z 1994 r. określił definicję i parametry bezpieczeństwa politycznego w mniej niż 400 słowach. Zdefiniowano je jako zapobieganie represjom rządowym, systematycznemu łamaniu → p r a w c z ł o w i e k a [t. 3] i groźbie militaryzacji. Raport omawia bezpieczeństwo polityczne w kontekście 7 głównych kategorii → z a g r o ż e n i a [t. 4] dla bezpieczeństwa ludzi, chociaż zakres → b e z p i e c z e ń s t w a s p o ł e c z n e g o został w nim zawężony głównie do kwestii obserwowania podkategorii praw człowieka i represji wobec obywateli przez → r e ż i m y [t. 3] wojskowe. W dokumencie zwrócono uwagę także na powszechne niepokoje polityczne w krajach, które stosowały represje polityczne. Taka definicja nawet w chwili jego publikacji była bardzo wąska, nie uwzględniono nowych globalnych wyzwań w zakresie bezpieczeństwa, które wyłoniły się już w tym okresie. Jest oczywiste, że demokracja lub wprowadzenie reżimów demokratycznych jest składnikiem bezpieczeństwa politycznego, jeśli bezpieczeństwo definiuje się jako stan rzeczy osiągnięty z korzyścią dla jednostki i grup. Niestety raport nie wskazywał wyraźnie demokracji jako elementu politycznego bezpieczeństwa.

Treści bezpieczeństwa politycznego są zróżnicowane w zależności od kategorii podmiotu i poziomu, na którym on funkcjonuje. Można je podzielić:

- pod względem zakresu i stref wpływów na:
  - międzynarodowe,
  - regionalne,
  - państwowe;
- ze względu na charakter i zawartość zagrożeń na:
  - wojskowe,
  - polityczne,
  - gospodarcze,
  - ekologiczne,
  - informacyjne;
- w odniesieniu do podmiotów zagrożeń na:
  - zewnętrzne,
  - wewnętrzne.

Bezpieczeństwo polityczne jest integralną częścią, głównym ogniwem i podstawą bezpieczeństwa narodowego. Brak bezpieczeństwa politycznego jako kluczowego pojęcia w encyklopediach nauk społecznych sprawia, że (re)konceptualizacja tego terminu nie jest łatwa. Istotę bezpieczeństwa politycznego interpretuje się na różne sposoby. Jedni rozumieją je jako zachowanie istniejącego porządku konstytucyjnego, stabilności politycznej i społecznej, drudzy jako podtrzymywanie demokratycznych wartości, jeszcze inni zaś jako niestosowanie → p r z e m o c y [t. 3] w celach politycznych itp.

Definicje bezpieczeństwa politycznego koncentrują się przede wszystkim na państwie i politycznym wymiarze → b e z p i e c z e ń s t w a n a r o d o w e g o. J. Czaputowicz stwierdza, że bezpieczeństwo polityczne dotyczy „zagrożeń dla stabilności społecznej państw i rządów, czyli suwerenności wewnętrznej, związanej z rzeczywistą kontrolą określonego terytorium przez legalne władze państwa". I. Pawlikowska określa bezpieczeństwo polityczne jako „stan pewności przetrwania i rozwoju systemu politycznego danego państwa bądź grupy państw". Zdaniem B. Balcerowicza wymiar narodowy bezpieczeństwa politycznego obejmuje „kompleks problemów związanych ze stabilnością państwa i jego ustroju, w którym mieszczą się m.in. efektywność struktur państwa, jakość systemu politycznego itd.". Z kolei R. Olszewski, opisując bezpieczeństwo polityczne, wskazuje na szeroki zakres wartości chronionych państwa, wymienia m.in.: suwerenność, integralność terytorialną, zdolność prawnomiędzynarodową państwa, porządek konstytucyjny (prawny), jakość władzy i dyplomacji, legitymizację władzy, prawa człowieka, samorządność społeczną, zgodność interesów jednostek, grup społecznych i państwa. L. Chojnowski uważa, że „bezpieczeństwo polityczne państwa to stan pewności przetrwania, skutecznego i stabilnego funkcjonowania i rozwoju systemu politycznego państwa oraz jego suwerenności".

Głównym celem zapewnienia bezpieczeństwa politycznego jest z jednej strony tworzenie i funkcjonowanie mechanizmu formułowania i wdrażania polityki państwowej, która realizuje → i n t e r e s y n a r o d o w e [t. 2], z drugiej zaś zapobieganie przekształceniu tej polityki pod wpływem wewnętrznych i zewnętrznych czynników destrukcyjnych w niebezpieczny stan, zagrażający rozwojowi demokratycznemu i istnieniu społeczeństwa. Środki bezpieczeństwa nie powinny utrudniać, a wręcz przeciwnie, powinny promować rozwój systemu politycznego, w tym jakościowy. Dlatego bezpieczeństwo polityczne nie tylko musi być oceniane na podstawie nienaruszalności systemu, ale także określać, w jaki sposób przyczynia się do rozwoju i dobrobytu kraju w kategoriach strukturalnych konfliktów, ryzyka i niepewności.

Główne kierunki zapewnienia bezpieczeństwa politycznego:

- stworzenie skutecznych mechanizmów ochrony praw obywateli w kraju i na świecie;
- zapobieganie próbom angażowania się obcych sił w wewnętrzne sprawy państwa i eliminacja takich prób;
- uczestnictwo w istniejących i tworzących się systemach uniwersalnego i regionalnego bezpieczeństwa;

- unikanie politycznego ekstremizmu, wspieranie pojednania obywatelskiego i stabilności społecznej;
- budowanie wiarygodnego systemu zasad konstytucyjnych, zapobieganie naruszeniom prawa i porządku i ich zwalczanie, tworzenie warunków niezbędnych do skutecznej walki z → k o r u p c j ą [t. 2] i → p r z e s t ę p c z o ś c i ą [t. 3], a zwłaszcza jej zorganizowanymi formami;
- zapewnienie prawidłowej realizacji decyzji prawnych organów państwowych i organów samorządu terytorialnego.

Istnienie państw może być zagrożone zarówno przez zagrożenia zewnętrzne, jak i wewnętrzne. Skrajną formą zewnętrznego zagrożenia jest → w o j n a [t. 4]. Ekstremalnymi formami zagrożeń wewnętrznych są: → w o j n a d o m o w a [t. 4], bunt, wahania, niestabilność. Do środków zachowania i utrzymania bezpieczeństwa politycznego należy przede wszystkim tworzenie warunków politycznych, społecznych i ekonomicznych do funkcjonowania instytucji demokratycznych, zrównoważonej i innowacyjnej gospodarki i pełnego zatrudnienia, a także perspektywy społeczne obywateli: równy dostęp do edukacji, medycyny, osiągnięcia w rozwoju wysokich standardów europejskich itp.

Stabilność bezpieczeństwa politycznego zabezpieczają wyspecjalizowane organy – uniemożliwiające rozmaite wewnętrzne lub zewnętrzne działania agresywne wobec istniejącego systemu politycznego – oraz silne, tolerancyjne i pluralistyczne media. Te i inne czynniki bezpieczeństwa politycznego dzieli się na zapobiegawcze, taktyczne i strategiczne. We wszystkich przypadkach podstawą działalności jest zapewnienie stabilności politycznej i społeczno-gospodarczej, etnicznej i społeczno-politycznej harmonii, zaufanie społeczeństwa do rządu, partii politycznych i ich liderów.

Mechanizm bezpieczeństwa politycznego obejmuje wiele elementów i ich celową interakcję, w szczególności:

- obiekty (terytorium, rząd i instytucje społeczno-polityczne, organy władzy, prawa i wolności polityczne, a także realna działalność polityczna obywateli, grup społecznych i stowarzyszeń itp.), które wymagają ochrony;
- poglądy, zasady, koncepcje w tym zakresie;
- system odpowiedniej podstawy prawnej;
- podmioty (specjalne instytucje i organy, inne instytucje państwowe i publiczne, społeczeństwo i obywatele), które powinny chronić sferę polityczną.

Polityka bezpieczeństwa jest definiowana jako funkcja państwa związana z zapewnieniem ochrony żywotnych interesów politycznych społeczeństwa (osób, grup społecznych, społeczności w ogóle) przed zagrożeniami wewnętrznymi i zewnętrznymi.

Priorytety politycznych interesów narodowych:

- zapewnienie społecznej stabilności i harmonii, pokojowych rozwiązań wewnętrznych konfliktów społecznych;
- legislacyjne i organizacyjne zapewnienie efektywnego funkcjonowania mechanizmu władzy państwowej;

- realizacja politycznych interesów jednostek i grup społecznych, w tym opozycji, poprzez tworzenie demokratycznego systemu instytucji politycznych, poprawę kultury politycznej narodu;
- zwiększenie autorytetu wszystkich gałęzi władzy, zapewnienie wysokiego poziomu zaufania publicznego do struktur władzy;
- zapewnienie demokratycznej ciągłości systemu zarządzania i reżimu politycznego, polityki wewnętrznej i zagranicznej;
- rozpowszechnienie w świadomości społecznej idei patriotyzmu, solidarności, wspólnych historycznych celów i historycznego losu;
- wzmacnianie woli politycznej władz, kultywowanie państwowej ideologii.

Warto wyróżnić jeszcze jeden bardzo ważny element w zrozumieniu istoty bezpieczeństwa politycznego. Bezpieczeństwo społeczeństwa zależy w dużej mierze od jego stabilności politycznej, a zagrożenia stabilności politycznej w pewnych warunkach stają się zagrożeniem dla bezpieczeństwa całego społeczeństwa. Rozwiązanie problemu stabilności systemu politycznego jest możliwe jedynie na podstawie wstępnej analizy struktury społecznej, poziomu rozwoju gospodarczego, wartości, cech etnicznych i poszczególnych instytucji politycznych. Stabilność systemu politycznego oznacza zatem jego zdolność do zapewnienia zachowania własnej struktury i podstawowych zasad w kontekście ciągłych zmian w środowisku wewnętrznym i zewnętrznym. Wynika z tego, że instytucje polityczne mają swoją własną wartość i dysponują znacznym potencjałem stabilizacyjnym. Regulują działalność polityczną, odtwarzają i nawiązują pewne stosunki polityczne z poszanowaniem zasady ciągłości.

Główne funkcje systemu bezpieczeństwa politycznego państwa:

- prognostyczna – prognozowanie, przewidywanie, identyfikacja rzeczywistych i potencjalnych zagrożeń politycznych i innych;
- informacyjna – dostarczenie podmiotom bezpieczeństwa → i n f o r m a c j i [t. 2] o stanie obiektów zabezpieczających, charakterze i zakresie działań destrukcyjnych i destabilizujących;
- prewencyjna – ostrzeganie i neutralizacja przyczyn ewentualnych zagrożeń politycznych na najwcześniejszym etapie ich powstawania i rozwoju;
- mobilizująca – zdolność całego systemu do szybkiego reagowania na zagrożenia, terminowego angażowania niezbędnych sił i zasobów;
- eliminacja zagrożeń – klucz do systemu bezpieczeństwa; w razie wystąpienia zagrożeń musi nastąpić adekwatna reakcja z użyciem sił i środków odpowiednich do charakteru zagrożeń;
- ochronna – zarówno ochrona przywództwa politycznego państwa i bezpiecznej działalności wszystkich instytucji politycznych, jak i i powstrzymywanie przyjęcia błędnych decyzji politycznych, zmniejszających bezpieczeństwo polityczne;

- kontrolna – ocena politycznego bezpieczeństwa i podejmowanie adekwatnych działań korygujących w zakresie stosowanych sił i środków, metod, technik i sposobów zapewniania bezpieczeństwa politycznego.

Oczywiste jest, że wskazane funkcje są organicznie połączone, wzajemnie się określają i powinny być wdrażane nie osobno, a kompleksowo.

Międzynarodowy wymiar bezpieczeństwa politycznego związany jest z funkcjonowaniem systemu i podsystemów międzynarodowych, dotyczy przetrwania i rozwoju określonego ładu międzynarodowego i utożsamiany jest z jego stabilizacją oznaczającą trwałość i równowagę procesów zachodzących w systemie międzynarodowym (podsystemach międzynarodowych). Według Balcerowicza wymiar międzynarodowy bezpieczeństwa politycznego obejmuje problemy związane z funkcjonowaniem systemu międzynarodowego, takie jak stan stabilności sytemu (systemów), liczba i efektywność organizacji międzynarodowych, sposoby rozstrzygania sporów, zagrożenia ładu międzynarodowego. Natomiast M. Pietraś uważa, że ujęcie międzynarodowe politycznego wymiaru bezpieczeństwa dotyczy przede wszystkim struktur stabilizujących ład międzynarodowy, do których należą mechanizmy pokojowego rozstrzygania sporów oraz proces instytucjonalizacji współpracy w różnych dziedzinach.

Na początku XXI w. system zagrożeń dla bezpieczeństwa politycznego społeczeństwa i państwa stał się znacznie bardziej zróżnicowany. Obok tradycyjnych wyzwań, niebezpieczeństw i zagrożeń ujawniają się nowe, dotychczas nieuważane za obiektywnie zagrażające stabilności politycznej i bezpieczeństwu. W nowoczesnych warunkach żaden kraj na świecie nie może być uważany za w pełni chroniony. Dlatego przy zapewnieniu bezpieczeństwa politycznego konieczne jest zwiększenie zdolności systemu politycznego do stawiania czoła zagrożeniom, ryzykom i wyzwaniom. Aktywność państwa i społeczeństwa realizowana jest w różnych sferach, a w każdej z tych dziedzin może istnieć ryzyko działania różnych negatywnych czynników, zagrożeń i niebezpieczeństw. Ze względu na kształtowanie i rozwój zagrożeń dla bezpieczeństwa politycznego można warunkowo podzielić je na potencjalne i rzeczywiste. Potencjalne zagrożenie określa się na podstawie pochodzenia i powstawania warunków wstępnych, pojawienia się pewnych niebezpieczeństw, które w przyszłości mogą zaszkodzić państwu. Bezpieczeństwo polityczne zajmuje kluczowe miejsce w całym systemie bezpieczeństwa. Utrata kontroli politycznej przez społeczeństwo lub nieprzestrzeganie szans i interesów państwa nieuchronnie prowadzi do jego degradacji i zniszczenia.

Problem demokracji ma zasadnicze znaczenie dla pojęcia bezpieczeństwa, a także dla podniesienia legalności regulowanego systemu międzynarodowego. Bezpieczeństwo polityczne dotyczy natury rządu, zbioru relacji między jednostką a grupą oraz jednostką a państwem w kontekście wykonywania praw i obowiązków w zakresie podziału władzy. Ponadto należy wskazać, że nowe wyzwania dla państwa niekiedy wykraczają poza politykę, ponieważ postęp technologiczny, który doprowadził do

powstania wirtualnego świata internetu i zmienił wiele kwestii związanych z prywatnością, może zmieniać i kształtować bezpieczeństwo polityczne.

Olga Wasiuta

R. Allison, *The Military and Political Security Landscape in Russia and the South*, [w:] *Russia, the Caucasus, and Central Asia*, R. Menon, Y.E. Fedorov, G. Nodia (eds.), Routledge, London 2016; B. Balcerowicz, *Bezpieczeństwo polityczne Rzeczypospolitej Polskiej*, AON, Warszawa 2004; J. Besant-Jones i in., *World Development Report 1994: Infrastructure for Development*, World Bank, Oxford University Press, New York 1994; *Bezpieczeństwo polityczne i wojskowe*, A. Ciupiński, K. Malak (red.), AON, Warszawa 2004; B. Bowden, *Civilizational Security*, [w:] *The Routledge Handbook of New Security Studies*, J.P. Burgess (ed.), Routledge, London, New York 2013; L. Chojnowski, *Bezpieczeństwo. Zarys teorii*, Wydawnictwo Akademii Pomorskiej w Słupsku, Słupsk 2015; J. Czaputowicz, *Bezpieczeństwo w teoriach stosunków międzynarodowych*, [w:] *Bezpieczeństwo międzynarodowe. Teoria i praktyka*, K. Żukrowska, M. Grącik (red.), Szkoła Główna Handlowa, 2006; M. Dillon, *Politics of Security: Towards a Political Philosophy of Continental Thought*, Routledge, London–New York 2003; R. Foks, *Rola „bezpieczeństwa politycznego" w systemie bezpieczeństwa narodowego Federacji Rosyjskiej a „nowy rosyjski autorytaryzm"*, „Rocznik Bezpieczeństwa Międzynarodowego" 2007, t. 2; S. Korycki, *Bezpieczeństwo polityczne*, [w:] *System bezpieczeństwa Polski*, AON, Warszawa 1993; J.F. McEldowney, *Political Security and Democratic Rights*, „Democratisation" 2005, vol. 12, iss. 5; R. Olszewski, *Bezpieczeństwo współczesnego świata*, Wydawnictwo Adam Marszałek, Toruń 2005; I. Pawlikowska, *Bezpieczeństwo jako cel polityki zagranicznej państwa*, [w:] *Wstęp do polityki zagranicznej państwa*, R. Zięba (red.), Wydawnictwo Adam Marszałek, Toruń 2005; *The Politics of Security in Modern Russia*, M. Galeotti (ed.), Ashgate, Farnham–Burlington 2010; P.F. Walsh, *Securing State Secrets*, [w:] *The Palgrave Handbook of Security, Risk and Intelligence*, R. Dover, H. Dylan, M. Goodman (eds.), Palgrave Macmillan, London 2017; O. Wasiuta, *Bezpieczeństwo polityczne*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; A. White, *Politics, Economics and Security*, [w:] *The Handbook of Security*, R. Dover, M. Gill (eds.), Palgrave Macmillan, London 2014.

BEZPIECZEŃSTWO POWSZECHNE I OCHRONA LUDNOŚCI – „powszechny" to „dotyczący wszystkich, wszystkiego, publiczny, ogólny", publiczny zaś to „dotyczący ogółu ludzi, służący ogółowi przeznaczony, dostępny dla wszystkich". Bezpieczeństwo powszechne dotyczy więc szerokiego spektrum przejawów codzienności człowieka, jego życia, zdrowia oraz poczucia opieki ze strony właściwych podmiotów, tj. służb, inspekcji i straży, które zostały utworzone do tego celu.

Termin ten według większości znawców i ekspertów dotyczy ochrony przed pożarami, powodziami, huraganami, silnymi opadami atmosferycznymi, awariami technicznymi oraz innymi negatywnymi zdarzeniami wynikającymi z działania sił natury lub rozwoju cywilizacyjnego. Co warte podkreślenia, postrzegane zjawiska i/lub zdarzenia są utożsamiane z czynnikami względnie niezależnymi od uwarunkowań ekonomicznych, społecznych, politycznych czy też kulturowych. Są na tyle istotne dla prawidłowej egzystencji i rozwoju społeczności lokalnych, a nawet całych narodów, że doczekały się zainteresowania i regulacji normatywnych o zasięgu międzynarodowym. Pomimo istotności analizowanej problematyki w perspektywie nauk społecznych bezpieczeństwo powszechne nie zyskało takiej rangi jak chociażby kwestie związane z → b e z p i e c z e ń s t w e m

narodowym, → bezpieczeństwem wewnętrznym państwa, → bezpieczeństwem społecznym czyteż → bezpieczeństwem publicznym, z którym jest ono często łączone lub nawet są traktowane synonimicznie. Taką postawę reprezentują chociażby W. Fehler, a także S. Pikulski. To rozumowanie nie do końca prawidłowe. Oczywiście, w jednym i drugim przypadku chodzi o ochronę przed → zagrożeniami [t. 4] obywateli. Jednak w pierwszym z nich dotyczy to ochrony życia i zdrowia oraz ochrony dóbr i środowiska przed zagrożeniami sił natury oraz przed tymi, które są związane z rozwojem cywilizacyjnym (np. awarie techniczne). W bezpieczeństwie publicznym zaś chodzi o zapewnienie ochrony przed działaniami zabronionymi, które naruszają prawnie usankcjonowany porządek społeczny, godzą w życie i zdrowie (zabójstwa, uszkodzenia ciała) lub porządek publiczny (handel ludźmi, nielegalne zgromadzenia itd.).

Funkcjonują również interpretacje bezpieczeństwa powszechnego wykraczające poza ramy bezpieczeństwa wewnętrznego państwa, znajdujemy je najczęściej w literaturze zagranicznej, w której większość zagrożeń naturalnych nie jest lokowana w sferze bezpieczeństwa wewnętrznego państwa, a → bezpieczeństwa ekologicznego. Takie przedstawianie problemu również jest obarczone pewnymi nieścisłościami. Oczywiście kwestie bezpieczeństwa powszechnego i ekologicznego zazębiają się w pewnym stopniu, można dostrzec ich cechy wspólne. Dotyczyć może to choćby nierzadko tych samych czynników wpływających negatywnie na oba rodzaje bezpieczeństwa, jak np. awarie techniczne, klęski żywiołowe itp. Należy jednak podkreślić, że przedmiotem bezpieczeństwa ekologicznego jest środowisko, natomiast przedmiotem bezpieczeństwa powszechnego jest człowiek – ochrona jego życia i zdrowia.

Termin bezpieczeństwa powszechnego pojawia się również w aspekcie czysto prawnym jako dobro, przeciwko któremu występując, narażamy się na szereg sankcji karnych. Owo dobro to przede wszystkim zdrowie, życie oraz mienie. A. Zoll pisze, że „bezpieczeństwo powszechne należy rozumieć po prostu jako stan, w którym wspomnianym wartościom nie zagraża bezprawna ingerencja". Zdaniem A. Spotowskiego natomiast:

> przez pojęcie niebezpieczeństwa (powszechnego) należy rozumieć powstanie sytuacji, która w drodze dalszych dynamicznych przekształceń doprowadzić może do powstania zmian w świecie realnym, które podlegają negatywnej ocenie z punktu widzenia społecznie akceptowanego wzorca.

Historyczny rozwój przepisów chroniących bezpieczeństwo powszechne sięga kodyfikacji prawa karnego u schyłku XVIII w. Na gruncie polskim odzwierciedleniem tego były zapisy, jakie znalazły się w kodeksie karnym z 1932 r. Penalizowano tam:

> sprowadzenie powszechnego zagrożenia dla życia, zdrowia lub mienia w wielkich rozmiarach, które przybierało postać gwałtownego wyzwolenia sił przyrody lub katastrofy budowlanej względnie komunikacyjnej, a także posłużenia się niebezpiecznymi przedmiotami lub substancjami bądź zniszczenia i uszkodzenia istotnych urządzeń użyteczności publicznej.

Kolejny etap niewątpliwie wiąże się z kształtem kodeksu karnego z 1969 r. i pierwszymi regulacjami chroniącymi prawnie bezpieczeństwo ekologiczne. W obecnie obowiązującym kodeksie karnym zakres ochrony bezpieczeństwa powszechnego obejmuje poprzez przewidziane sankcje karne zachowania trojakiego rodzaju:

- polegające na sprowadzeniu skutków w postaci gwałtownego wyzwolenia sił przyrody (zarówno ze źródeł naturalnych, jak i ukształtowanych przez zachowanie się człowieka),
- polegające na sprowadzeniu zagrożenia epidemiologicznego lub innego powszechnego zagrożenia dla zdrowia nie tylko ludzi, ale także roślin i zwierząt,
- polegające na dokonaniu gwałtownego zamachu na elementy szeroko rozumianej infrastruktury.

Bezpieczeństwo powszechne można więc definiować jako obecność zespołu warunków, w których społeczeństwo nie odczuwa presji (lęku) przed zagrożeniami natury technicznej lub związanymi z siłami przyrody. Utrzymanie takiego stanu rzeczy (braku lęku, odczuwania go na akceptowalnym poziomie) wiąże się z podejmowaniem szeregu działań systemowych mających na celu:

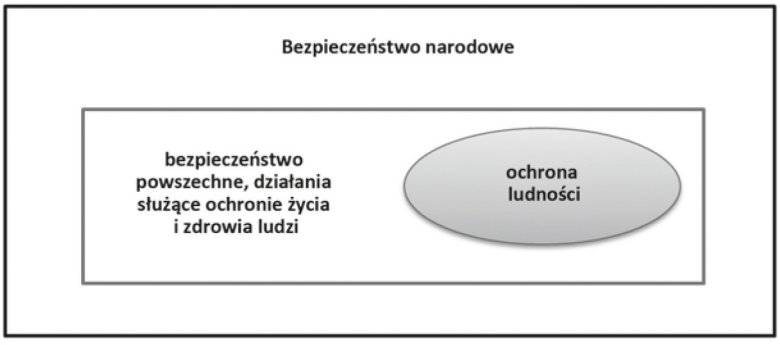
- przewidywanie zagrożeń (natury technicznej, związanych z siłami przyrody) oraz zapobieganie im i ich skutkom,
- minimalizowanie ryzyka takich zagrożeń,
- przygotowanie systemów reagowania,
- skuteczne reagowanie (ratownictwo),
- działania przywracające stan normalny.

Jaka jest zatem geneza wspomnianych zagrożeń właściwych dla obszaru bezpieczeństwa powszechnego? Odpowiedź na to pytanie jest dwoista. Zagrożenia techniczne czy wynikające z rozwoju cywilizacyjnego mają w przeciwieństwie do → k a t a s t r o f n a t u r a l n y c h [t. 2] charakter antropogeniczny. To człowiek, konstruując coraz to szybsze pociągi, samochody, budując coraz to większe i wyższe budynki, tworząc niezwykle zaawansowane technologicznie konstrukcje, wyzwalając olbrzymie pokłady energii i siły (np. elektrownie jądrowe), kreuje w pewien sposób nowe zagrożenia mające znaczny i realny wpływ na życie i zdrowie każdego z nas. Zagrożenia takie cechuje nagłość występowania, a ich skutki mogą być krótkotrwałe (akcja ratownicza po wypadku samochodowym) lub trwać stosunkowo długo (awaria elektrowni jądrowej). Należałoby przypomnieć tu rok 1986 i najtragiczniejszą jak dotąd w skutkach awarię elektrowni jądrowej w Czarnobylu. Wśród bezpośrednich ofiar katastrofy znajdowali się uczestnicy akcji ratunkowej i pracownicy elektrowni, którzy zapadli na chorobę popromienną, będącą przyczyną śmierci części z nich. Konsekwencje zdrowotne, a także społeczne i polityczne skutki katastrofy miały skalę dotychczas niespotykaną. Z rejonu w promieniu 30 km od elektrowni ewakuowano mieszkańców, ogółem przesiedlono ok. 350 tys. osób, 100 tys. ha ziemi rolnej wyłączono z użytkowania. Skażeniu uległo 9% powierzchni dzisiejszej Ukrainy. Nieco odmiennie rzecz się ma z katastrofami naturalnymi. W tym

przypadku skutki są w pewnej mierze przewidywalne, a samo wystąpienie zagrożenia jest możliwe do przewidzenia z pewnym czasowym wyprzedzeniem.

Jako przykład zagrożenia naturalnego o zasięgu globalnym można podać erupcję superwulkanu, która mogłaby wpłynąć na atmosferę całej Ziemi i trudno byłoby przewidzieć jej skutki. Zdaniem wulkanologów największą udokumentowaną erupcją był wybuch wulkanu Tambora w Indonezji, na małej wysepce Sumbawa w kwietniu 1815 r. W powietrze wyleciały wtedy niewyobrażalne ilości pyłów i skał, pozostawiły zaś po sobie zagłębienie o głębokości 700 m i średnicy kilku kilometrów. Chmury popiołu zakryły niebo i przez 3 dni panowały zupełne ciemności. Energia, jaka została uwolniona podczas wybuchu, była porównywalna z siłą wybuchu 200 tys. bomb atomowych. Skutki odczuto na całym świecie, a rok 1816 nazwano „rokiem bez lata" – w Ameryce Północnej nie zebrano plonów z pól, a temperatura w Londynie była niższa od temperatur w poprzednich latach o ok. 3°C. W wielu państwach (nawet leżących tysiące kilometrów od Tambory) ludzie cierpieli wielki głód. Konsekwencją tej tragedii była gigantyczna fala tsunami w zatoce Bima, która zniszczyła wiele budynków i statków stojących na redzie. W wyniku tych tragicznych zdarzeń śmierć poniosło ponad 90 tys. osób.

Kluczowym elementem bezpieczeństwa powszechnego jest → o c h r o n a l u d n o ś c i [t. 3] m.in. poprzez organizację i realizację działań ratowniczych. Ochrona ta powinna obejmować ochronę życia, mienia oraz środowiska – w zakresie niezbędnym do przetrwania, w każdym czasie i w każdej sytuacji. Każda zbiorowość ludzka (społeczeństwo) ma nienaruszalne, niezbywalne i konstytucyjne prawo do ochrony przed skutkami szkodliwej działalności człowieka, sił natury i działań zbrojnych. Można przyjąć, że ochrona ludności stanowi kluczową sferę realizacyjną w dziedzinie bezpieczeństwa narodowego, w tym bezpieczeństwa powszechnego. Podobnie sytuacja przedstawia się w przypadku → o b r o n y c y w i l n e j [t. 3], rozumianej w świetle m.in. misji tożsamej ochronie ludności, aczkolwiek realizowanej w warunkach → w o j n y [t. 4] i okupacji.



Rys. 1. Zależności pomiędzy ochroną ludności a bezpieczeństwem powszechnym i narodowym

Źródło: Oprac. aut. na podstawie: W. Kitler, A. Skrabacz, *Bezpieczeństwo ludności cywilnej*, Towarzystwo Wiedzy Obronnej, Warszawa 2010, s. 65.

Bezpieczeństwo powszechne i ochrona ludności powinna być realizowana we wszystkich stanach i warunkach, które za Kitlerem można określić w sposób następujący:

- w stanie permanentnego czuwania i doraźnego reagowania,
- w → s y t u a c j i k r y z y s o w e j [t. 4],
- w czasie konfliktu zbrojnego.

Wśród wielu zaproponowanych w literaturze przedmiotu definicji bezpieczeństwa powszechnego proponuje się przyjąć, że bezpieczeństwo powszechne to stan otoczenia społecznego i środowiska naturalnego wolny od zagrożeń dla istnienia obywateli, ich interesów życiowych, zdrowia, dóbr materialnych i środowiska, zapewniający ochronę przed zagrożeniami nagłymi. W ujęciu podmiotowym stanowi ono część, rodzaj bezpieczeństwa narodowego, którego zasadniczym celem jest zapewnienie bezpieczeństwa → l u d n o ś c i c y w i l n e j [t. 3], a zarazem jest stanem uzyskanym w wyniku zorganizowanej ochrony życia i zdrowia ludzi, a także dóbr materialnych i kulturalnych oraz środowiska naturalnego. Można rozpatrywać je również jako proces, byłby to wówczas ogół działań na rzecz ochrony życia, zdrowia i środowiska naturalnego realizowany głównie przez służby, inspekcje i straże, a więc przez administrację publiczną. Najprościej rzecz ujmując, bezpieczeństwo powszechne to dziedzina bezpieczeństwa narodowego traktująca o organizacji ochrony życia i zdrowia ludzi, jak również dóbr materialnych i kulturalnych oraz środowiska naturalnego w zakresie niezbędnym do przetrwania ludzi, ochrona przed negatywną działalnością (i jej skutkami) człowieka przeciwko człowiekowi lub siłom natury.

Łukasz Szewczyk

Disaster risk reduction: Resolution adopted by the General Assembly on 19 December 2019, A/RES/74/218; W. Fehler, *Bezpieczeństwo publiczne*, „Społeczeństwo i Polityka" 2009, nr 4 (21); N. Jonina, M. Kubiejew, *Wielkie katastrofy*, tłum. M. Leszczycka, Bellona, Warszawa 2010; W. Kitler, *Bezpieczeństwo narodowe RP. Podstawowe kategorie, uwarunkowania, system*, AON, Warszawa 2011; W. Kitler, A. Skrabacz, *Bezpieczeństwo ludności cywilnej*, Towarzystwo Wiedzy Obronnej, Warszawa 2010; *Kodeks karny. Część szczególna. Komentarz*, t. 2: art. 117–277, E. Zoll (red.), Kraków 1999; S. Pikulski, *Podstawowe zagadnienia bezpieczeństwa publicznego*, [w:] *Bezpieczeństwo to wspólna sprawa. Ochrona bezpieczeństwa publicznego – rozwiązania systemowe w skali kraju i regionu*. *Materiały poseminaryjne*, J. Fiebig, M. Róg, A. Tyburska (red.), Wydawnictwo Wyższej Szkoły Policji w Szczytnie, Szczytno 2002; D. Smith, *Crisis Management – Practice in Search of a Paradigm*, [w:] *Key Readings in Crisis Management Systems and Structures for Prevention and Recovery*, D. Smith, D.Elliott, (eds.), Routledge, London–New York 2006; A. Spotowski, *Funkcja niebezpieczeństwa w prawie karnym*, Warszawa 1990; J. Zboina, *Miejsce i rola ochrony przeciwpożarowej w systemie bezpieczeństwa państwa*, [w:] *Ochrona przeciwpożarowa a bezpieczeństwo państwa*, J. Zboina, F. Wiśniewski (red.), CNBOP – PIB, Józefów 2014.

BEZPIECZEŃSTWO PRACY – zespół warunków prowadzący do wyeliminowania lub też możliwie najszerszego ograniczenia warunków niekorzystnych dla pracownika w miejscu jego pracy. W literaturze przedmiotu, a także w dyskusjach

zarówno na gruncie akademickim, jak i politycznym czy społecznym, bezpieczeństwo pracy w sposób bezpośredni i często nierozłączny wiązane jest z higieną pracy. Rozpatrując pojęcie *sensu largo*, zwraca się uwagę na cały zespół czynników, takich jak środki prawne, naukowo-techniczne, organizacyjne, medyczne, higieniczne czy psychologiczne, które mają w znaczącym stopniu odpowiadać za bezpieczeństwo pracownika w miejscu wykonywania przez niego obowiązków wynikających z umowy o pracę. Ujmując kwestię jeszcze szerzej, niektórzy odwołują się do problematyki techniki, technologii oraz postępu technicznego, a także do kwestii związanych z higieną i występowaniem chorób zawodowych wynikających bezpośrednio z czynników związanych z fizjologią pracy oraz czynnikami w niej występującymi, na które narażony jest pracownik. W zakresie bezpieczeństwa pracy na szczególną uwagę zasługuje bezpieczeństwo pracy kobiet ciężarnych oraz młodocianych. Należy zaznaczyć, że bezpieczeństwo pracy jest wartością konstytucyjną, bezwzględną i powszechną, zapewnioną przez ustawodawcę w art. 66 ust. 1 Konstytucji RP: „każdy ma prawo do bezpiecznych i higienicznych warunków pracy, a sposób realizacji tego prawa oraz obowiązki pracodawcy określa ustawa". Szczegółowe regulacje dotyczące bezpieczeństwa pracy można znaleźć m.in. w:

- Ustawie z dnia 7 lipca 1994 r. – Prawo budowlane,
- Ustawie z dnia 28 marca 2003 r. o transporcie kolejowym,
- Rozporządzeniu Ministra Rolnictwa i Rozwoju Wsi z dnia 26 września 2001 r. w sprawie bezpieczeństwa i higieny pracy przy przetwórstwie ziemniaków,
- Rozporządzeniu Ministra Gospodarki z dnia 27 kwietnia 2000 r. w sprawie bezpieczeństwa i higieny pracy przy pracach spawalniczych,
- Konwencji nr 62 w sprawie przepisów bezpieczeństwa w przemyśle budowlanym, przyjętej w Genewie dnia 23 czerwca 1937 r.,
- Konwencji nr 176 dotyczącej bezpieczeństwa i zdrowia w kopalniach, przyjętej w Genewie dnia 22 czerwca 1995 r.

Bezpieczeństwo pracy jest niepodzielne pojęciowo tak w sensie prawnym, jak i materialnym i przysługuje każdej osobie wykonującej pracę. Współcześnie coraz większą wagę przykłada się do szerszego rozumienia bezpieczeństwa i higieny pracy w organizacjach, zwracając uwagę na motywowanie pracowników do organizowania właściwych warunków pracy. Brytyjski Komitet Wykonawczy podaje do wiadomości, że kultura bezpieczeństwa pracy zależy od składowych wartości pracowników, a także stylu zarządzania na szczeblach kierowniczych. Coraz większego znaczenia w tym wymiarze nabiera efektywna komunikacja na wszystkich szczeblach organizacji dążąca do zapewnienia jak najlepszych warunków. Pojęcie bezpieczeństwa pracy jest wielopłaszczyznowe i składa się z → k u l t u r y b e z p i e c z e ń s t w a [t. 2] społeczeństwa, kultury bezpieczeństwa przedsiębiorstwa / organizacji / pracodawcy oraz kultury bezpieczeństwa jednostki.

F. Jucha podaje wzór algorytmiczny, na podstawie którego można określić kulturę bezpieczeństwa. Składają się na niego następujące czynniki:

- akceptowalny poziom kultury bezpieczeństwa,
- bariera,
- edukacja i jej egzekwowanie,
- ocena ryzyka.

Kontrolą oraz nadzorem nad bezpieczeństwem pracy w zakładach pracy zajmuje się wyspecjalizowany organ w postaci Państwowej Inspekcji Pracy. Kwestiami teoretycznymi oraz gromadzeniem → i n f o r m a c j i [t. 2] związanych z funkcjonowania systemu bezpieczeństwa pracy zajmuje się z kolei Centralny Instytut Ochrony Pracy oraz jednostki badawcze wyższych uczelni. Ich działalność służy realizacji zadań związanych z wprowadzeniem zmian oraz tworzeniem nowych norm prawa pracy.

Barbara Partyńska-Brzegowy, Dorota Koptiew

M. Gersdorf, K. Rączka, M. Raczkowski, *Kodeks pracy*. *Komentarz*, LexisNexis Polska, Warszawa 2014; F. Jucha, *Kultura bezpieczeństwa i higieny pracy w szkole*, „Pedagogika Pracy" 2005, nr 46; F. Małysz, *Klauzule generalne w kodeksie pracy*, „Atest – Ochrona Pracy" 2010, nr 6; M. Milczarek, *Kultura bezpieczeństwa w przedsiębiorstwie – nowe spojrzenie na zagadnienia bezpieczeństwa pracy*, „Bezpieczeństwo Pracy" 2000, nr 10; M. Stankiewicz, M. Sznajder, *Kultura bezpieczeństwa i higieny pracy w organizacji*, [w:] *Kształtowanie kultury bezpieczeństwa i higieny pracy w organizacji*, J. Ejdys (red.), Oficyna Wydawnicza Politechniki Białostockiej, Białystok 2010; A. Wróbel, *Bezpieczeństwo i higiena pracy – pojęcie i odpowiedzialność*, „Przegląd Prawa i Administracji" 2014, t. 96.

BEZPIECZEŃSTWO PRAWNE – pojęcie wieloznaczne, które można definiować na kilku płaszczyznach, w tym filozofii prawa, historii polityki, prawa, a w szczególności prawa konstytucyjnego. Można określać je jako stan, w którym dobra i interesy jednostek są strzeżone przez prawo w sposób całkowity i skuteczny. W literaturze wyróżnia się bezpieczeństwo prawne w znaczeniu obiektywnym i subiektywnym. Pierwsze z wymienionych odnosi się do stanu prawnego, w którym prawo pozytywne zabezpiecza interesy, dobrobyt i bezpieczeństwo jednostek, niezależnie od świadomości, którą mają. W drugim ujęciu dotyczy subiektywnego przekonania podmiotu o zabezpieczeniu, jakie daje mu prawo. Jako zasadne jawi się pytanie o racjonalne podstawy bezpieczeństwa prawnego w ujęciu subiektywnym. Założenie, że jednostka jest w stanie posiąść wiedzę o zasadach działania organów państwa oraz o konsekwencjach prawnych, jakie pociągają za sobą zachowania różnych podmiotów, stanowi idealizację. Rzetelna wiedza na temat prawa i jego wykładni występuje dość rzadko w życiu społecznym. Dlatego należy przyjąć, że poczucie bezpieczeństwa prawnego wynika raczej z indywidualnego nastawiania do państwa i prawa. Poczucie bezpieczeństwa opiera się zatem na zaufaniu do państwa, a tym samym do tworzonego i stosowanego przez nie prawa. Przypomnieć trzeba, że korzenie idei bezpieczeństwa prawnego sięgają epoki oświecenia. Wówczas starano się tworzyć koncepcje, które pomogą ochronić niepewnego i bezbronnego obywatela w konfrontacji z wszechwładnym, absolutystycznym państwem policyjnym. Właśnie w oświeceniu wolność obywatela

utożsamiana była z wolnością od arbitralnych i niczym nielimitowanych rozstrzygnięć władzy państwowej. Koncepcja bezpieczeństwa prawnego miała także istotne miejsce w ramach nurtu pozytywizmu prawnego, zgodnie z którym państwo liberalne powinno gwarantować swoim obywatelom bezpieczną i stabilną pozycję prawną.

G. Radbruch wskazywał bezpieczeństwo prawne jako jeden z celów prawa, akcentując jednocześnie jego trojakie znaczenie, rozumiane po pierwsze jako bezpieczeństwo przez prawo, po drugie jako pewność prawa, po trzecie jako ochrona praw nabytych. Koncepcja utożsamiania bezpieczeństwa prawnego z pewnością prawa nie została zarzucona – posługiwał się nią w orzeczeniach Trybunał Konstytucyjny. Można stwierdzić, że pojęcie bezpieczeństwa prawnego ma zbliżoną treść do zasad ochrony zaufania obywateli do państwa i stanowionego przez nie prawa, ale ujmowane jest z perspektywy jednostki. W związku z tym można wyodrębnić szereg wymagań, takich jak:

- pozytywność prawa – odpowiednia forma przepisów dzięki przestrzeganiu zasad poprawnej legislacji, takich jak dostateczna określoność prawa,
- praktyczność prawa – adresat normy prawnej powinien mieć możliwość ustalenia, czy i jakie jego zachowania będą miały konsekwencje prawne,
- stabilność prawa – prawo powinno być trwałe i niezmienne, a w przypadku zmian należy minimalizować ich skutki dla odbiorców.

W tym ujęciu bezpieczeństwo prawne należy rozumieć jako warunek urzeczywistnienia → p r a w c z ł o w i e k a [t. 3], a nawet jako jedno z praw człowieka.

Pojęcie bezpieczeństwa prawnego pozostaje w bliskim związku z koncepcją demokratycznego państwa prawnego, którą można uznać za ideę szerszą i bardziej ogólną, wiele miejsca poświęcono jej w ramach nauki prawa konstytucyjnego. W literaturze wskazuje się bowiem, że klauzula demokratycznego państwa prawnego jest źródłem wielu zasad bardziej szczegółowych, w tym zasady ochrony zaufania obywateli do państwa, która zapewnia jednostce możliwość działania przy pełnej znajomości przesłanek działania organów państwowych i konsekwencji prawnych, jakie te działania mogą pociągnąć; zakazuje tworzenia uprawnień nieurealnionych istnieniem procedur ich dochodzenia, zakazuje tworzenia iluzorycznych konstrukcji normatywnych, które są niewykonalne. Łatwo więc wskazać, że wymienione elementy są związane z bezpieczeństwem prawnym w ujęciu obiektywnym i subiektywnym. Wniosek ten będzie aktualny także w stosunku do dalszych reguł, składających się na koncepcję demokratycznego państwa prawnego, wśród których L. Garlicki wymienia:

- zakaz domniemywania kompetencji organów państwa,
- zasadę ochrony praw nabytych,
- zasadę określoności prawa,
- zasadę proporcjonalności (pomiędzy podejmowanymi przez państwo środkami a postulowanym do osiągnięcia celem),
- zasadę sprawiedliwości społecznej.

Bezpieczeństwo prawne stało się jednym z podstawowych kryteriów jakości życia jednostek i całego społeczeństwa. Rozwój nowych technologii, gospodarki i zwiększenie mobilności społeczeństw stanowią źródło nowych wyzwań w zakresie budowania bezpieczeństwa prawnego. Jednostka pozostaje bowiem coraz częściej w orbicie oddziaływania systemów prawnych różnych państw. Trzeba też zwrócić uwagę na problem pionowego nakładania się norm prawnych regulujących te same zagadnienia: międzynarodowych, unijnych i wewnętrznych. Stąd też tak istotne są wysiłki podejmowane np. przez UE czy Haską Konferencję Prawa Prywatnego w celu harmonizacji prawa lub tworzenia reguł kolizyjnych.

Anna Pacholska, Jakub Idzik

L. Garlicki, *Polskie prawo konstytucyjne*, Wolters Kluwer Polska, Warszawa 2015; M. Konarski, *Legal Security and Coup D'état – Historical and Modern Perspectives*, „Review of Comparative Law" 2017, vol. 30, no. 3; J. Krukowski, *Bezpieczeństwo państw demokratycznych w procesie integracji europejskiej: tożsamość narodowa a społeczeństwo obywatelskie. Doświadczenia i perspektywy*, [w:] *Bezpieczeństwo prawne państw demokratycznych w procesie integracji europejskiej: Polska – Słowacja – Ukraina*, J. Krukowski, J. Potrzeszcz, M. Sitarz (red.), Wydawnictwo KUL, Lublin 2016; J. Potrzeszcz, *Bezpieczeństwo prawne w orzecznictwie Polskiego Trybunału Konstytucyjnego*, „Roczniki Nauk Prawnych" 2006, t. 16, nr 1; taż, *Bezpieczeństwo prawne z perspektywy filozofii prawa*, Wydawnictwo KUL, Lublin 2013; G. Radbruch, *O celu prawa*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 1937, nr 3; B. Sitek, *Bezpieczeństwo prawne a wertykalna wielowarstwowość systemów prawnych*, „Journal of Modern Science" 2012, no. 1 (12).

BEZPIECZEŃSTWO PRZESYŁU I DYSTRYBUCJI ENERGII – wszystkie procesy technologiczne dowolnej produkcji związane są ze zużyciem energii. Zdecydowana większość zasobów energetycznych konsumowana jest w procesie produkcyjnym. Najważniejszą rolę w każdym przedsiębiorstwie przemysłowym odgrywa energia elektryczna – najbardziej uniwersalny rodzaj energii, który jest głównym źródłem energii mechanicznej. Konwersja surowców różnego rodzaju (węgla, gazu, ropy itp.) na energię elektryczną zachodzi w elektrowniach.

Wyróżnia się 3 etapy dostaw energii elektrycznej: produkcję, przesył i dystrybucję. Każdy z tych etapów obejmuje różne procesy produkcyjne, działania i → z a g r o ż e n i a [t. 4]. Źródłami zagrożeń dla procesu wytwarzania energii elektrycznej są wybuchy i pożary wynikające z nieoczekiwanych awarii urządzeń. Wypadki zdarzają się również wtedy, gdy nie istnieją właściwe procedury blokowania lub wyłączania. Procedury te mają na celu kontrolę źródeł produkujących energię elektryczną.

Po wytworzeniu energia elektryczna jest przesyłana na odległość za pomocą linii przesyłowych. Linie przesyłowe są ulokowane między podstacjami przesyłowymi znajdującymi się w elektrowniach. Linie energetyczne buduje się z przewodów fazowych rozwieszonych na słupach, mogą one znajdować się także pod ziemią. W celu zapewnienia dotarcia do odbiorców energia musi być przesyłana poprzez Krajowy System Elektroenergetyczny, na który składają się:

- sieć najwyższych napięć o napięciu 220 i 400 kV,
- sieć dystrybucyjna wysokiego napięcia o napięciu 110 kV,
- sieci średniego i niskiego napięcia.

Praca elektrowni w systemie krajowym umożliwia – ze względu na dużą liczbę równolegle działających jednostek generujących energię elektryczną – zwiększenie niezawodności dostarczania energii do odbiorców, pełne obciążenie najbardziej ekonomicznych jednostek elektrowni oraz zmniejszenie kosztów wytwarzania energii elektrycznej. Ponadto w takim systemie elektroenergetycznym wydajność jednostki jest zmniejszona, ale zapewniona jest wyższa jakość energii elektrycznej dostarczanej do konsumentów.

Niezawodność systemu jest pojęciem nadrzędnym dla poszczególnych systemów sieciowych w aspekcie technicznym. To zdolność dostarczania odbiorcom wymaganej ilości paliw i energii przy zachowaniu określonych standardów. Dotychczas był to podstawowy czynnik decydujący o → b e z p i e c z e ń s t w i e dostaw energii do odbiorców, ale postęp techniczny pozwala obecnie na stosowanie rozwiązań co najmniej częściowo niezależnych od systemów sieciowych. Wskazać tutaj należy rozwój generacji rozproszonej. W ramach niezawodności systemu wyróżnia się 2 aspekty: wystarczalność i bezpieczeństwo pracy systemu. Pierwszy z nich to zdolność systemu do dostaw paliw lub energii na pokrycie zagregowanego zapotrzebowania odbiorców w każdej chwili, z uwzględnieniem planowanych i racjonalnie oczekiwanych wyłączeń elementów systemu (standardów jakości i niezawodności), pewności jego zasilania w energię pierwotną, zależną od stopnia jej zdywersyfikowania, krajowych zapasów paliw i możliwości interwencyjnych dostaw z zagranicy.

W procesie zagwarantowania bezpieczeństwa przesyłu energii elektrycznej bardzo ważną rolę odgrywa dywersyfikacja dostaw, czyli korzystanie z szerokiego wachlarza źródeł energii, a także dywersyfikacja dostawców oraz szlaków i mechanizmów transportu. System oparty na kilkunastu dużych elektrowniach jest bardziej wrażliwy na sabotaż niż system oparty na kilkunastu tysiącach źródeł rozproszonych o małej i średniej mocy. Ryzyko związane z zależnością energetyczną UE można zmniejszyć, budując wiarygodne partnerstwa z dostawcami, krajami tranzytowymi i odbiorcami.

Z powodu niedorozwoju sieci energetycznych wynikającego z braku rozbudowy i modernizacji sieci przesyłowych i dystrybucyjnych oraz z braku dostosowania infrastruktury sieciowej do zmieniającego się lokalizacyjnie i strukturalnie zapotrzebowania na energię elektryczną powstają problemy związane z odbiorem energii elektrycznej z elektrowni wiatrowych, słonecznych lub biogazowych.

Analizując gęstość polskiej sieci elektroenergetycznej, warto odnieść się do stanu sieci w innych krajach europejskich. Zgodnie z danymi z 2009 r. zagęszczenie infrastruktury sieciowej linii przesyłowych najwyższych napięć umiejscawia Polskę prawie na samym końcu – gorzej było tylko na Węgrzech – wynosiło ono ok. 41 km na każde 1 tys. km^2. Stan na początek 2020 r. nie pozwalał sądzić, że sytuacja ta uległa

znaczącej poprawie. Nadal można dostrzec istotną różnicę na niekorzyść Polski, porównując gęstość polskiej sieci elektroenergetycznej ze stanem sieci w innych krajach europejskich.

Na podstawie analizy zapotrzebowania energii elektrycznej, która wskazuje na zwiększenie zapotrzebowania na nią w okresie letnim, zwłaszcza w dużych aglomeracjach, można stwierdzić, że sieci zasilające pracują na granicy swoich możliwości technicznych i wymagają modernizacji oraz rozbudowy. Obrazuje to skalę koniecznych przedsięwzięć inwestycyjnych w kraju.

Dywersyfikacja bazy paliwowo-energetycznej obejmuje zróżnicowanie struktury używanych paliw i energii, stopień ich uzależnienia od importu i zróżnicowanie kierunków ich dostaw. Celem dywersyfikacji jest ograniczenie ryzyka obniżenia → b e z p i e c z e ń s t w a e n e r g e t y c z n e g o kraju wskutek wystąpienia zakłóceń w jednym ze składników bazy paliwowo-energetycznej z różnych powodów (politycznych, awarii technicznych, strajków itp.).

Bezpieczeństwo przesyłu energii elektrycznej można rozpatrywać w różnych aspektach. Inaczej jest ono definiowane na potrzeby analizy krótkoterminowej, dotyczącej np. ryzyka wstrzymania dostaw nośników energii przez głównych producentów, inaczej natomiast przy spojrzeniu długoterminowym, np. w kontekście kwestii wyczerpywania się zapasów surowców energetycznych i wzrostu cen surowców z tego tytułu. Podobnie różnie będzie definiowana kwestia bezpieczeństwa energetycznego – a w szczególności instrumentów mających na celu jego zapewnienie – z punktu widzenia biznesu oraz z punktu widzenia polityki kraju. Bez względu jednak na różnice w podejściu do kwestii bezpieczeństwa energetycznego jego podstawową cechą jest troska o zabezpieczenie dostaw energii pod różną postacią w ilości pokrywającej zgłaszany w danym regionie popyt. Coraz częściej w definicjach wskazuje się konieczność zapewnienia dostaw w wysokości gwarantującej trwały rozwój gospodarczy regionu, potrzebę zapewnienia dostaw do finalnych odbiorców, a biorąc pod uwagę historyczne gwałtowne wzrosty cen nośników energii, w tym głównie ropy naftowej, definicja uzupełniana jest także o czynnik cenowy. Dodatkowo definicja często wskazuje też na konieczność utrzymania infrastruktury kluczowej dla zaopatrzenia odbiorców w energię, jak również zagwarantowania bezpieczeństwa najważniejszych elementów infrastruktury. Niejednokrotnie jako cele działań zmierzających do zapewnienia bezpieczeństwa energetycznego określa się zmniejszenie wrażliwości gospodarek poszczególnych krajów na groźby i presje wywierane przez głównych producentów surowców energetycznych, przeciwdziałanie występowaniu → s y t u a c j i k r y z y s o w y c h [t. 4] oraz minimalizowanie negatywnego wpływu potencjalnych → k r y z y s ó w [t. 2] na rozwój gospodarczy oraz → b e z p i e c z e ń s t w o m i l i t a r n e kraju. Warto zauważyć że za długookresowe bezpieczeństwo funkcjonowania systemu odpowiada też jego operator, zarówno w odniesieniu do sieci przesyłowej, jak i sieci dystrybucyjnych. Prawo energetyczne mówi wprost:

> Operator systemu przesyłowego elektroenergetycznego lub systemu połączonego elektroenergetycznego w zakresie systemu przesyłowego, stosując obiektywne i przejrzyste zasady zapewniające równe traktowanie użytkowników tych systemów oraz uwzględniając wymogi ochrony środowiska, jest odpowiedzialny za bezpieczeństwo dostarczania energii elektrycznej poprzez zapewnienie bezpieczeństwa funkcjonowania systemu elektroenergetycznego i odpowiedniej zdolności przesyłowej w sieci przesyłowej elektroenergetycznej.

Odnawialne źródła energii mogą stanowić istotny udział w bilansie energetycznym poszczególnych gmin czy nawet regionów Polski. Mogą przyczynić się do zwiększenia bezpieczeństwa energetycznego w regionach, a zwłaszcza do poprawy zaopatrzenia w energię na terenach o słabo rozwiniętej infrastrukturze energetycznej. Potencjalnie największym odbiorcą energii ze źródeł odnawialnych może być rolnictwo, a także mieszkalnictwo i komunikacja.

Innym ważnym aspektem związanym z bezpieczeństwem przesyłu energii jest kogeneracja – wytwarzanie energii elektrycznej i cieplnej w najbardziej efektywny sposób, czyli w jednym procesie technologicznym, tzw. skojarzeniu. Polega ona na wytwarzaniu energii elektrycznej oraz cieplnej na potrzeby procesów przemysłowych, do ogrzewania budynków i wytwarzania ciepłej wody użytkowej. Taki proces prowadzi do oszczędzania zasobów energetycznych i redukcji emisji CO_2. Kogeneracja, a w szczególności kogeneracja rozproszona, ma ogromne znaczenie dla bezpieczeństwa przesyłowego oraz energetycznego ze względu na to, że układy kogeneracyjne, również te wykorzystujące źródła energii odnawialnej, położone są w bezpośrednim sąsiedztwie odbiorców energii. Zaletą takiego układu jest brak potrzeby rozbudowy systemu przesyłowego, jak również obniżenie kosztów związanych z eksploatacją. Warto zwrócić uwagę na to, że kogeneracja wpływa nie tylko na bezpieczeństwo przesyłu i efektywność energetyczną, ale również umożliwia ograniczenie emisji dwutlenku węgla oraz innych szkodliwych substancji chemicznych.

Aleksander Wasiuta

M.H. Brown, C. Rewey, T. Gagliano, *Energy Security,* National Conference of State Legislatures, Denver–Washington 2003; Dyrektywa 2004/8/WE Parlamentu Europejskiego i Rady z dnia 11 lutego 2004 r. w sprawie wspierania kogeneracji w oparciu o zapotrzebowanie na ciepło użytkowe na rynku wewnętrznym energii oraz zmieniająca dyrektywę 92/42/EWG, Dz. Urz. UE L 052 z 21.02.2004 r.; *Materiały Konferencyjne Konferencji „Wykorzystanie odnawialnych źródeł energii w Euroregionie Nysa"*, SIPH, Świdnica 2007; *Polski system przesyłu na tle Europy*, LiniaPilaPlewiska.pl (dostęp 23.01.2020); PSE, *Plan sieci elektroenergetycznej najwyższych napięć*, PSE.pl (dostęp 23.01.2020); R. Samuels, *Securing Asian Energy Investments*, „The MIT Japan Program Science, Technology and Management Report" 1997, vol. 4, no. 2; A. Stankowska, *Realizacja elektroenergetycznych inwestycji liniowych*, „Elektroenergetyka" 2009, nr 1; T. Suzuki i in., *A Framework for Energy Security Analysis and Application to a Case Study Japan*, Nautilus Institute for Security and Sustainable Development, Berkley 1998; W. Szymczak, *Sposoby monitoringu stanu bieżącego systemu dystrybucji energii elektrycznej*, [w:] *Konferencja Bezpieczeństwo Energetyczne Dolnego Śląska. Stan obecny i perspektywy*, Karpacz 2007; Ustawa z dnia 10 kwietnia 1997 r. – Prawo energetyczne, Dz. U.

1997, nr 54, poz. 348; A. Wasiuta, *Zwiększenie dywersyfikacji dostaw oraz źródeł pochodzenia energii jako podstawowy czynnik bezpieczeństwa energetycznego w kontekście polityki energetycznej Polski*, [w:] *Globalizacja a problematyka ochrony środowiska*, T. Noch, A. Wesołowska (red.), Wydawnictwo GSW, Gdańsk 2010; A. Wasiuta, J. Rokitowska, *Ekonomiczne i społeczne aspekty bezpieczeństwa sektora energetycznego w kontekście zrównoważonego rozwoju*, Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2019.

BEZPIECZEŃSTWO PUBLICZNE – ogół warunków i instytucji chroniących życie, zdrowie i mienie obywateli oraz majątek narodowy, ustrój i → s u w e r e n n o ś ć p a ń s t w a [t. 4] przed zjawiskami groźnymi dla jego ładu społecznego.

Zdaniem Z. Ścibiorka to stan, w którym obywatele mogą swobodnie, zgodnie z obowiązującymi normami, korzystać z praw i swobód obywatelskich. Według J. Zaborowskiego to:

> taki stan faktyczny wewnątrz państwa, który umożliwia bez narażenia na szkody (wywołane zarówno zachowaniem ludzi, jak i działaniem sił natury, techniki itp.) normalne funkcjonowanie organizacji państwowej i realizację jej interesów, zachowanie życia, zdrowia i mienia jednostek żyjących w tej organizacji oraz korzystanie przez te jednostki z praw i swobód zagwarantowanych Konstytucją i innymi przepisami prawa.

Z kolei wg W. Kitlera bezpieczeństwo publiczne jest procesem obejmującym różnorodne działania (środki), których zasadniczym celem jest ochrona porządku prawnego w państwie przed działaniami zabronionymi i takimi, które godzą w instytucje i urządzenia publiczne, życie i zdrowie ludzi lub porządek publiczny, a także w normy i obyczaje społeczne i w interesy państwa chronione przez ustawę. S. Kowalkowski definiuje bezpieczeństwo publiczne jako stan wewnętrzny państwa, który niezależnie od grożących niebezpieczeństw zapewnia normalne funkcjonowanie całokształtu organizacji państwowej, w tym szczególnie ochronę życia i zdrowia jednostek żyjących w państwie oraz mienia osób fizycznych i prawnych. Bezpieczeństwo publiczne za K. Grosicką, L. Grosickim i P. Grosickim można określić także jako pożądany stan wewnątrz państwa, gwarantujący jego istnienie i rozwój. A. Misiuk określa bezpieczeństwo publiczne jako stan przejawiający się ochroną porządku prawnego, życia i zdrowia obywateli oraz majątku narodowego przed bezprawnymi działaniami; stan braku → z a g r o ż e n i a [t. 4] dla funkcjonowania organizacji państwowej i realizacji jej interesów, umożliwiający normalny, swobodny jej rozwój, przy czym gwarancją prawną tego stanu są właściwe normy prawne, a gwarancją instytucjonalną kompetencje organów państwa.

Zakres przedmiotowo-podmiotowy bezpieczeństwa publicznego obejmuje państwo ze swoim ustrojem i innymi urządzeniami, człowieka (jego życie, zdrowie, mienie, realizację jego praw podmiotowych) oraz formy życia zbiorowego.

A. Osierda przyjmuje za S. Pieprznym, że bezpieczeństwo publiczne to stan istniejący w państwie, w którym człowiekowi i ogółowi społeczeństwa nie grozi żadne

niebezpieczeństwo, niezależnie od źródeł, z którego miałoby pochodzić. Granice bezpieczeństwa zakreślone są przepisami prawa i wszystko to, co zakłóca te granice, stanowi niebezpieczeństwo. Bezpieczeństwo jest nie określonym stanem rzeczy, a raczej ciągłym procesem społecznym, w ramach którego podmioty starają się doskonalić mechanizmy zapewniające im poczucie bezpieczeństwa.

Podobnie jak bezpieczeństwo publiczne także porządek publiczny określa się jako pewien stan wewnętrzny państwa. Porządek jest stanem pozytywnym, publiczny oznacza to samo co państwowy, powszechny, dotyczący ogółu, jawny, społeczny, związany z urzędem czy instytucją. Porządek publiczny zatem, jak twierdzi Misiuk, to faktycznie istniejący układ stosunków społecznych, uzupełniony przez zespół norm prawnych i innych norm społecznie akceptowanych, gwarantujący niezakłócone i bezkonfliktowe funkcjonowanie jednostek w społeczeństwie. Obejmuje wszystkie stosunki społeczne uregulowane przez prawo i normy innych systemów, które kształtują się w miejscach publicznych. Dotyczy to norm gwarantowanych prawem, a także tych akceptowanych powszechnie w danej społeczności, np. norm moralnych, religijnych, obyczajowych, zasad współżycia społecznego. W podobnym tonie wypowiada się J. Filaber, wg którego porządek publiczny to przestrzeganie norm prawnych, moralnych, obyczajowych, religijnych i zasad współżycia społecznego, którego skutkiem jest harmonizacja poszczególnych jednostek i społeczności ludzkich.

Zakres przedmiotowy porządku publicznego określa kodeks wykroczeń, w którym uregulowano odpowiedzialność za wykroczenia przeciwko: porządkowi i spokojowi publicznemu; instytucjom państwowym, samorządowym i społecznym; bezpieczeństwu osób i mienia; bezpieczeństwu i porządkowi w komunikacji; osobie i zdrowiu; mieniu i interesom konsumenta; obyczajności publicznej; obowiązkowi ewidencji; szkodnictwu leśnemu, polnemu i ogrodowemu.

Jak wskazują R. Jakubczak i J. Flis, dziedzina bezpieczeństwa i porządku publicznego to wewnętrznie uporządkowany zbiór elementów kierowania i elementów wykonawczych przeznaczony do zwalczania → p r z e s t ę p c z o ś c i [t. 3] oraz zjawisk kryminogennych, zapewnienia ochrony przed bezprawnymi zamachami na życie i zdrowie ludzkie, dorobek materialny i kulturalny społeczeństwa, a także zachowania porządku publicznego.

J. Gierszewski definiuje bezpieczeństwo publiczne jako część systemu → b e z p i e c z e ń s t w a w e w n ę t r z n e g o p a ń s t w a stanowiącą zbiór organów władzy i administracji publicznej, metod oraz sposobów działania związanych z ochroną życia i zdrowia obywateli, majątku narodowego przed bezprawnymi działaniami. Wiodącą częścią podsystemu jest minister właściwy ds. wewnętrznych i komendant główny Policji.

Ochronę bezpieczeństwa i porządku publicznego generalnie przypisuje się organom → p o l i c j i [t. 3] i wymiaru sprawiedliwości, jest to jednak istotne uproszczenie, ponieważ – jak wyjaśniają Jakubczak i Flis – czynniki kształtujące poziom

bezpieczeństwa i porządku publicznego oraz zagrożenia są liczne i różnorodne, w świetle obowiązujących przepisów prawa podmiotami realizującymi zadania w zakresie bezpieczeństwa i porządku publicznego są zarówno policja, → straże gminne [t. 4], straż graniczna, żandarmeria wojskowa, jak i tzw. policje administracyjne – straże, inspekcje, którym z mocy prawa przypisano pewne uprawnienia kontrolne i egzekucyjne.

Zadania Policji w zakresie utrzymania bezpieczeństwa i porządku publicznego regulowane są Ustawą o Policji z dn. 6 kwietnia 1990 r. Zgodnie z jej zapisami Policja jest umundurowaną i uzbrojoną formacją (→ formacje uzbrojone [t. 2]) służącą społeczeństwu, przeznaczoną do ochrony bezpieczeństwa ludzi i utrzymania bezpieczeństwa i porządku publicznego. Do jej podstawowych zadań należą: ochrona życia ludzi oraz mienia przed bezprawnymi zamachami; ochrona bezpieczeństwa i porządku publicznego, w tym zapewnienie pokoju w miejscach publicznych oraz w środkach transportu i komunikacji publicznej w ruchu drogowym i na wodach przeznaczonych do powszechnego korzystania; inicjowanie i organizowanie działań mających na celu zapobieganie popełnianiu przestępstw i wykroczeń oraz zjawiskom kryminogennym i współdziałanie w tym zakresie z organami państwowymi, samorządowymi i organizacjami społecznymi; wykrywanie przestępstw i wykroczeń oraz ściganie ich sprawców; nadzór nad strażami gminnymi oraz nad → specjalistycznymi uzbrojonymi formacjami ochronnymi [t. 4]; kontrola przestrzegania przepisów porządkowych i administracyjnych związanych z działalnością publiczną lub obowiązujących w miejscach publicznych; współdziałanie z policjami innych państw oraz ich organizacjami międzynarodowymi. Z punktu widzenia rodzaju, charakteru i celu oraz sposobów realizacji wymienionych zadań policja spełnia następujące funkcje: operacyjną, interwencyjną, wykrywczą, kontrolno-orzekającą, egzekucyjną, wychowawczą. Funkcja operacyjna polega na pozyskiwaniu za pomocą utajnionych technik → informacji [t. 2] ze środowisk przestępczych, które umożliwiają podejmowanie działań uprzedzających lub szybkie wykrywanie sprawców przestępstw. Ta sfera działania otoczona jest szczególną tajemnicą ze względu na wartość informacji i potrzebę ochrony źródła, które może być wykorzystywane wielokrotnie. Do powszechnie znanych technik operacyjnych należy zakup kontrolowany, → podsłuch [t. 3] i kontrola korespondencji. Należy podkreślić, że prowadzone są one zgodnie z zasadą legalizmu. Funkcja interwencyjna to głównie bezpośrednia interwencja funkcjonariuszy policji i stosowanie przez nich przewidzianych prawem → środków przymusu bezpośredniego [t. 4], a w razie konieczności również broni palnej podczas reagowania na zaistniałe przypadki naruszenia bezpieczeństwa i porządku publicznego.

W razie niepodporządkowania się poleceniom organów Policji i jej funkcjonariuszy policjanci mogą stosować następujące środki przymusu bezpośredniego: fizyczne, techniczne i chemiczne środki służące do obezwładnienia bądź konwojowania osób

oraz zatrzymania pojazdów: pałki służbowe, wodę i środki obezwładniające, psy służbowe, pociski niepenetracyjne miotane z broni palnej. Jeżeli środki przymusu bezpośredniego są niewystarczające lub ze względu na okoliczności ich zastosowanie jest niemożliwe, policjant może użyć broni palnej. Szczegółowe zasady użycia broni palnej zostały doprecyzowane w Rozporządzeniu Rady Ministrów z dnia 17 września 1990 r. w sprawie określenia przypadków oraz warunków i sposobów użycia przez policjantów środków przymusu bezpośredniego. Użycie broni palnej powinno wyrządzać jak najmniejszą szkodę osobie, przeciwko której broń została użyta, i nie może zmierzać do pozbawienia jej życia, a także narażać na niebezpieczeństwo utraty życia lub zdrowia innych osób. Broń palna powinna być wykorzystywana w sytuacjach wyjątkowych, jako środek ostateczny, absolutnie konieczny, jak wskazuje europejska Konwencja o ochronie praw człowieka i podstawowych wolności. Funkcja wykrywania polega na wykonywaniu przez policję zadań jako organu ścigania, a więc służy bezpośrednio wykrywaniu sprawców przestępstw. Wypełnienie tej funkcji jest podstawą do osądzania sprawców przez sądy i wymaga stosowania wielu technik pracy operacyjno-rozpoznawczej, jawnych i niejawnych, za pomocą których możliwe jest uzyskiwanie informacji, ich gromadzenie i przetwarzanie, utrwalanie śladów i dokumentowanie dowodów. Celowi temu mogą służyć rutynowe przesłuchania świadków zdarzeń przestępczych, niejawne osobowe źródła informacji oraz środki techniczne, a także kontrola korespondencji, zakup kontrolowany i niejawne nadzorowanie przesyłek. Z uwagi na możliwość nieuzasadnionego stosowania tych technik w czasie postępowania dochodzeniowego ustawa o Policji określa przypadki, w jakich możliwe jest ich wykorzystanie, oraz konieczne warunki zabezpieczające.

W celu wykrycia przestępstw umyślnych, ściganych z oskarżenia publicznego (przestępstw umyślnych: przeciwko życiu, ciężkiemu uszkodzeniu ciała lub ciężkiemu rozstrojowi zdrowia; pozbawienia człowieka wolności; nielegalnego wytwarzania i posiadania broni, amunicji, materiałów wybuchowych, środków odurzających, materiałów promieniotwórczych oraz obrotu nimi; gospodarczych powodujących znaczną stratę majątku; → k o r u p c j i [t. 2] i fałszerstwa), ustalenia ich sprawców, a także uzyskania i utrwalenia dowodów w sprawie minister spraw wewnętrznych i administracji po uzyskaniu pisemnej zgody prokuratora generalnego może zarządzić na czas określony kontrolę korespondencji i stosowanie środków technicznych. Jednocześnie ustawa zobowiązuje ministra do bieżącego informowania prokuratora generalnego o wynikach prowadzonych czynności. Funkcja kontrolno-orzekająca polega na kontrolowaniu przestrzegania przepisów prawa przez instytucje i obywateli oraz orzekaniu w postępowaniu mandatowym w sprawach o wykroczenia. Policjanci mają prawo: legitymowania osób w celu ustalenia ich tożsamości, zatrzymania osób w trybie i przypadkach określonych w przepisach kodeksu postępowania karnego; zatrzymania osób pozbawionych wolności, które opuściły areszt na podstawie zezwolenia i w wyznaczonym terminie nie powróciły do niego, zatrzymania osób stwarzających

zagrożenie dla życia lub zdrowia ludzkiego i mienia; przeszukiwania osób i pomieszczeń, dokonywania kontroli osobistej, przeglądania zawartości bagaży i sprawdzania ładunku w portach i na dworcach oraz w środkach transportu lądowego, powietrznego i wodnego, w razie uzasadnionego podejrzenia popełnienia → c z y n u z a b r o n i o n e g o pod groźbą kary. W przypadkach naruszenia przepisów prawa kwalifikowanych jako wykroczenia policjanci mogą nakładać mandaty w trybie określonym w kodeksie wykroczeń lub kierować wnioski o ukaranie przez kolegia orzekające w sprawach wykroczenia. Funkcja egzekucyjna obejmuje realizację zadań zleconych przez sądy, → p r o k u r a t u r y [t. 3] lub inne upoważnione organy oraz egzekucję ich decyzji. Organy policji są podległe sądom, prokuratorom oraz organom administracji państwowej i samorządu terytorialnego, lecz tylko w zakresie wykonywania czynności określonych w odrębnych ustawach.

W odniesieniu do sądu i prokuratury będzie to kodeks postępowania karnego, w myśl którego policja może być zobowiązana do: doręczenia wezwań i innych pism adresatowi; doprowadzenia osoby podejrzanej; tymczasowego zajęcia mienia ruchomego osoby podejrzanej, jeżeli zachodzi obawa usunięcia tego mienia. Funkcja wychowawcza przejawia się w realizacji zadań społeczno-organizatorskich – programy bezpieczeństwa i porządku publicznego realizowane wspólnie z organami samorządu terytorialnego i społeczności lokalnych. Szczególną opieką władz samorządowych i policji objęto szkoły i młodzież ze środowisk zagrożonych przestępczością. Przedstawionych funkcji nie należy rozpatrywać oddzielnie, gdyż w codziennej praktyce występują równolegle i przeplatają się. Przepisy prawa określające zakres działań wyszczególnionych podmiotów bezpieczeństwa i porządku publicznego stanowią wielokrotnie o współdziałaniu. Wynika z nich, że współdziałającymi partnerami są partnerzy niezależni od siebie, samodzielni – niepodporządkowani; ustawy nie rozstrzygają form czy też zasad współdziałania, są one określone w przepisach wykonawczych; współdziałanie może dotyczyć spraw ogólnych i indywidualnych; ustawy wskazują, kto z czyjego współdziałania ma korzystać, a więc dają upoważnienie do żądania tej formy współpracy w określonych przepisami dziedzinach. Współdziałanie jest instytucją ustawowo-prawną, co w praktyce oznacza, ze aktywność podmiotu uprawnionego do współdziałania musi wyzwalać aktywność drugiego podmiotu w zakresie ustawowych zadań (dziedzin). Często problem inicjowania współdziałania jest rozwiązany w postaci zapisu uprawniającego do żądania pomocy, wymiany informacji lub nadzoru. Ustawowym instrumentem koordynowania działań są również porozumienia zawierane pomiędzy określonymi organami – w postaci umów wiążących strony – precyzujące zasady, sfery i procedury współdziałania. Oprócz współdziałania wynikającego z przepisów prawa obserwuje się współpracę międzyorganizacyjną podejmowaną samorzutnie przez równorzędne podmioty. Jej źródłem jest rozumienie nadrzędnych racji interesu publicznego. Warunkiem koniecznym współpracy międzyorganizacyjnej jest świadomość członków organizacji misji spełnianych w ramach szeroko rozumianego

systemu ochrony bezpieczeństwa i porządku publicznego.

Zadania realizowane przez organy i instytucje w ramach systemu bezpieczeństwa publicznego obejmują zapewnienie:

- rozwoju socjalnej struktury i stosunków w społeczeństwie, systemów zapewnienia życia i socjalizacji ludzi,
- bezpieczeństwa obywateli, spokoju społecznego czy praworządności,
- stanu społeczeństwa zapewniającego trwanie i przetrwanie.

Strategia Bezpieczeństwa Narodowego RP z 2014 r. wymienia zadania dotyczące różnego rodzaju czynów zabronionych, w tym przestępczości pospolitej, jak i zorganizowanej o charakterze ekonomicznym, narkotykowym i kryminalnym.

Zadania te wynikają z istniejących i pojawiających się zagrożeń, do których należą: wysoki poziom bezrobocia, rozwarstwienie ekonomiczne, wzrost migracji zewnętrznej, osłabienie więzi społecznych, marginalizacja dużych grup społecznych, niedostateczna kontrola dostępu do broni palnej, mało skuteczna polityka fiskalna, niedoskonałość stanowionego prawa, niska efektywność organów ścigania, niska skuteczność i aktualność programów edukacyjnych i profilaktycznych, podatność społeczeństwa na manipulacje.

W literaturze dokonano również podziału zagrożeń. Wyodrębniono kategorię przestępstw mających decydujący wpływ na stan bezpieczeństwa obywateli, dóbr materialnych i niematerialnych oraz porządku publicznego. Są to przestępstwa przeciwko mieniu, życiu i zdrowiu, fałszerstwa, → t e r r o r y z m [t. 4], przestępczość gospodarcza, narkotykowa, korupcja, przestępczość zorganizowana. Osobną kategorię stanowią naruszenia porządku publicznego traktowane jako wykroczenia związane głównie z masowymi imprezami (→ i m p r e z a m a s o w a [t. 2]) sportowymi i kulturalnymi.

Jak zauważa Kitler, bezpieczeństwo publiczne łączone jest często z porządkiem publicznym w postaci jednego terminu bezpieczeństwa i porządku publicznego (ustawa o Policji, art. 1, ust 1). Ta sama ustawa odrębnie wymienia kategorię bezpieczeństwa ludzi, która obejmuje kwestie ochrony życia i zdrowia ludzi oraz mienia przed bezprawnymi zamachami naruszającymi te dobra (art. 2 pkt 1 ustawy o Policji). Kitler podkreśla, że jedynie kodeks karny odrębnie odwołuje się do porządku publicznego, wymieniając przestępstwa przeciwko porządkowi publicznemu, co pozwala stwierdzić, że bezpieczeństwo publiczne oraz porządek publiczny stanowią odrębne kategorie. Przyjmuje się, że bezpieczeństwo publiczne jest nadrzędne dla porządku publicznego. Wynika to z istoty porządku publicznego, który jest związany z przestrzeganiem norm oraz utrzymaniem sprawności instytucji publicznych. W literaturze przedmiotu spotyka się szersze i węższe podejście interpretacyjne do bezpieczeństwa publicznego. Szerokie ujęcie traktuje je jako ochronę przed wszelkimi zagrożeniami, niezależnie od ich źródeł – charakterystyczne dla teoretyków prawa, którzy termin „publiczny" odróżniają od terminu „prywatny". Węższe podejście, jak wskazuje S. Bolesta, odnosi się do stosunków społecznych i uregulowań prawnych zapewniających ochronę

społeczeństwa, jednostki oraz mienia przed niebezpieczeństwami ze strony działań ludzi, jak również sił przyrody. Dla takiego postrzegania niestety nie znaleziono praktycznych rozwiązań organizacyjnych. Inna jest materia przeciwdziałania siłom natury, a inna bezprawnym działaniom ludzi.

Kowalkowski zwraca uwagę na fakt, że porządek publiczny jest nierozłącznym elementem bezpieczeństwa publicznego. Kategorie te są traktowane w przepisach prawnych i administracyjnych jako osobne instytucje, ale przez większość badaczy porządek publiczny ujmowany jest jako element bezpieczeństwa publicznego.

Osierda przyjmuje, że bezpieczeństwo publiczne i porządek publiczny to pojęcia zbliżone, w wielu przypadkach pokrywające się pod względem treści, trudne do precyzyjnego oddzielenia, ale mimo wszystko niejednoznaczne. Łączne używanie tych pojęć wg. Pieprznego jest pewnego rodzaju narzędziem prawnym umożliwiającym wskazanie szerszego przedmiotu ochrony prawnej. Nie należy w pełni przeciwstawiać znaczenia obu tych pojęć, ponieważ w tekstach prawnych w pewnym zakresie pozostają one we wzajemnych, zamierzonych przez normodawcę relacjach.

Przepisy prawa unijnego także nie podają definicji pojęć bezpieczeństwa i porządku publicznego, chociaż klauzula bezpieczeństwa publicznego pojawia się we wszystkich swobodach. Nie sformułował ogólnej definicji tych pojęć także → T r y b u n a ł S p r a w i e d l i w o ś c i U E [t. 4], który w swym orzecznictwie pojęciem bezpieczeństwa publicznego obejmuje też bezpieczeństwo zewnętrzne państwa (np. zagrożeniem może być tranzyt towarów, które mogą być przeznaczone do celów militarnych). W odniesieniu do pojęcia porządku publicznego pewnych wskazówek interpretacyjnych dostarcza Dyrektywa 2004/38/WE Parlamentu Europejskiego i Rady z 29 kwietnia 2004 r. w sprawie prawa obywateli na terytorium państw członkowskich. Przy interpretacji tych pojęć stosowana jest zasada proporcjonalności jako jedna z ogólnych zasad prawa unijnego, jak wskazuje E. Ura. Daje to podstawy, by sądzić, że pojęcia bezpieczeństwa publicznego i porządku publicznego są terminami języka prawnego, występującymi oddzielnie lub łącznie w porządku administracyjnoprawnym. Pojęcia te najczęściej związane są z regulacjami określającymi funkcje, zadania publiczne i prawne formy działania organów, instytucji i innych podmiotów tworzących administrację bezpieczeństwa i porządku publicznego.

Różnorodność interpretacji można uzasadnić wzajemnymi powiązaniami bezpieczeństwa publicznego z innymi dziedzinami bezpieczeństwa.

Danuta Kaźmierczak

J. Gierszewski, *Bezpieczeństwo wewnętrzne. Zarys systemu*, Difin, Warszawa 2013; L. Grosicki, K. Grosicka, P. Grosicki, *Organizacja i kierowanie instytucjami bezpieczeństwa wewnętrznego państwa*, Akademia Humanistyczna im. Aleksandra Gieysztora, Pułtusk 2013; D. Kaźmierczak, *Bezpieczeństwo publiczne*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; W. Kitler, *Organizacja bezpieczeństwa narodowego RP w kontekście ochrony ładu wewnętrznego w państwie*, „Zeszyty Naukowe AON" 2013,

nr 4; S. Kowalkowski, *Niemilitarne zagrożenia bezpieczeństwa publicznego*, AON, Warszawa 2010; *Obronność. Teoria i praktyka*, J. Wołejszo, R. Jakubczak (red.), Bellona, Warszawa 2013; A. Osierda, *Prawne aspekty pojęcia bezpieczeństwa publicznego i porządku publicznego*, „Studia Iuridica Lublinensia" 2014, nr 23; W. Pokruszyński, K. Straszewski, T. Terlikowski, *System bezpieczeństwa publicznego Polski*, AON, Warszawa 1996; Z. Ścibiorek i in., *Bezpieczeństwo wewnętrzne. Podręcznik akademicki*, Wydawnictwo Adam Marszałek, Toruń 2017; Ustawa z dnia 20 maja 1971 r. – Kodeks wykroczeń, Dz. U. 1971, nr 12, poz. 114 z późn. zm.; J. Zaborowski, *Administracyjnoprawne ujęcie pojęć „bezpieczeństwo publiczne" i „porządek publiczny" (niektóre uwagi w świetle unormowań prawnych) 1983–1984*, „Zeszyty Naukowe Akademii Spraw Wewnętrznych" 1985, nr 41; H. Zięba-Załucka, *Konstytucyjne aspekty bezpieczeństwa*, „Studia Iuridica Lublinensia" 2014, nr 22.

BEZPIECZEŃSTWO REGIONALNE – integralna część → b e z p i e c z e ń s t w a m i ę d z y n a r o d o w e g o, ochrona systemu stosunków wzajemnych państw regionu przed → z a g r o ż e n i a m i [t. 4] destabilizacji sytuacji, → k r y z y s a m i [t. 2], konfliktami zbrojnymi i → w o j n a m i [t. 4] o charakterze regionalnym; to również stan stosunków międzynarodowych w tej lub innej części świata, w którym w wyniku kompleksu przyjętych wspólnie przez zainteresowane strony środków i w efekcie podpisania wielostronnych traktatów międzynarodowych lub umów zapewnia się utrzymanie pokoju i współpracy państw i narodów oraz gwarantuje się rozwiązywanie sporów poprzez negocjacje bez użycia siły lub groźby jej użycia. Bezpieczeństwo regionalne to także stan stosunków wewnątrz poszczególnych społeczno-terytorialnych instytucji danego regionu oraz między nimi, w którym wszystkim należącym do niego państwom, narodom, obywatelom, instytucjom publicznym i grupom zapewnia się obronę ich żywotnych interesów, istnienie solidnego i stabilnego rozwoju. Jest realizowane na różnych poziomach: w ramach poszczególnych jednostek administracyjno-terytorialnych kraju, w odniesieniu do kilku sąsiednich obszarów państw oraz w skali grupy krajów należących do określonego obszaru geograficznego. Na każdym poziomie jest ono budowane w połączeniu z → b e z p i e c z e ń s t w e m n a r o d o w y m i międzynarodowym, obejmując ekonomiczne, polityczne, środowiskowe, wojskowe i inne kluczowe elementy → b e z p i e c z e ń s t w a.

Korzenie badań nad bezpieczeństwem regionalnym można odnaleźć w badaniach geopolitycznych z przełomu XIX i XX w., choć z czasem zmieniły się definicje regionów. Podczas → z i m n e j w o j n y [t. 4] bezpieczeństwo regionalne i stabilność były definiowane głównie w kategoriach miejsca, które region zajmował w obliczeniach strategicznych USA lub ZSRR. Współczesna troska o bezpieczeństwo regionalne odzwierciedla zbieżność ciągłego znaczenia tradycyjnego podejścia geostrategicznego (→ g e o s t r a t e g i a [t. 2]) oraz pojawianie się nowych wyzwań w zakresie bezpieczeństwa, które na nowo zdefiniowały treść i zakres porządku we współczesnym systemie międzynarodowym. Rosnące znaczenie bezpieczeństwa regionalnego w każdym wymiarze interakcji spowodowało zaskakująco dużą liczbę formalnych porozumień międzynarodowych, które różnią się zakresem, złożonością i siłą.

Początki współczesnego rozumienia bezpieczeństwa regionalnego można odnajdywać w końcu lat 40. XX w., kiedy badacze szczególnie zainteresowali się koncepcją integracji regionalnej i regionalnych instytucji bezpieczeństwa po II wojnie światowej i kiedy pojawiły się organizacje regionalne i subregionalne zajmujące się budowaniem bezpieczeństwa regionalnego.

W XXI w. pojawiły się nowe koncepcje dotyczące bezpieczeństwa regionalnego, spośród których należy wyróżnić:

- Regionalną kompleksową teorię bezpieczeństwa (ang. *regional security complex theory*, RSCT) – to teoria stosunków międzynarodowych zawierająca model bezpieczeństwa regionalnego oraz pozwalająca analizować i do pewnego stopnia przewidywać i wyjaśniać rozwój sytuacji w dowolnym regionie. Została przedstawiona przez B. Buzana i O. Wævera w 2003 r. w książce *Regions and Powers: The Structure of International Security*. Badacze uważają, że bezpieczeństwo międzynarodowe należy rozpatrywać z perspektywy regionalnej. RSCT zakłada, że działania i motywacje państw w dziedzinie bezpieczeństwa międzynarodowego mają charakter regionalny. Oznacza to, że obawy dotyczące bezpieczeństwa państwa generowane są przede wszystkim w ich bezpośrednim sąsiedztwie. Bezpieczeństwo każdego państwa w regionie współdziała z bezpieczeństwem innych podmiotów, a zagrożenia w najbliższym otoczeniu są najprawdopodobniej najsilniejsze.
- Regionalne kompleksy bezpieczeństwa (ang. *regional security complexes*, RSC) – zdefiniowane jako odrębne i stabilne wzorce interakcji bezpieczeństwa między podmiotami. Różnią się one między sobą stopniem interakcji. Poziom interakcji między członkami tego samego RSC jest wysoki, podczas gdy między członkami różnych RSC jest stosunkowo niski. Jak sama nazwa wskazuje, kompleksy bezpieczeństwa regionalnego są z natury geograficzne, składają się z sąsiadujących podmiotów i są odizolowane od siebie naturalnymi barierami takimi jak oceany, pustynie czy pasma górskie. Ze względu na sposób działania zasady sąsiedztwa często występuje intensywna współzależność w zakresie bezpieczeństwa w obrębie RSC, ale interakcja z państwami z zewnątrz jest znacznie mniej aktywna.

Teorię komplikuje istnienie podmiotów o globalnym interesie bezpieczeństwa i zdolnościach do prognozowania siły. Buzan i Wæver twierdzą jednak, że nawet interesy bezpieczeństwa światowych mocarstw mają zasadniczo charakter regionalny i podkreślają znaczenie przyjęcia perspektywy regionalnej (w przeciwieństwie do dominującej globalnej) i zwrócenia większej uwagi na podmioty bezpieczeństwa inne niż państwa.

RSC mogą być interpretowane jako systemy same w sobie, jako mikrosystemy wbudowane w większy, globalny system polityczny. RSC zawierają własną dynamikę bezpieczeństwa, która w normalnych okolicznościach jest w dużej mierze niezależna od globalnej dynamiki bezpieczeństwa. Umożliwia to stosowanie różnych koncepcji bezpieczeństwa regionalnego – takich jak równowaga sił, biegunowość i współzależność – w skali regionalnej. Regiony takie jak Europa czy Bliski Wschód niekoniecznie

stanowią RSC, jednak pokrywają się z teoretycznie zdefiniowanymi RSC i kulturowymi definicjami regionów.

R. Kelly w 2007 r. umieścił bezpieczeństwo regionalne w ogólnych ramach „nowego regionalizmu", E. Solingen traktuje regionalne bezpieczeństwo jako wspólny produkt koalicji państwowej i międzypaństwowej, podczas gdy D. Lemke uogólnia teorię transformacji władzy, aby uchwycić dynamikę regionalnych systemów bezpieczeństwa. Natomiast R. Fawn reprezentuje główne nurty teorii stosunków międzynarodowych i rosnącego – pomimo intensyfikującej się globalizacji – znaczenia regionalnych systemów bezpieczeństwa.

Bezpieczeństwo regionalne buduje się z reguły w drodze porozumień regionalnych albo na podstawie układu regionalnego, który działa zawsze w obrębie jakiegoś regionu międzynarodowego (Europa, Azja, Ameryka Północna, Ameryka Łacińska, Azja Południowo-Wschodnia). Powstanie regionalnej instytucji bezpieczeństwa w większości wypadków opiera się na geograficznych granicach regionu wytworzonego na płaszczyźnie współpracy funkcjonalnej.

Zakres kompetencji i sposoby zapewnienia bezpieczeństwa regionalnego są określone przez postanowienia 8. rozdziału Karty Narodów Zjednoczonych, „Porozumienia regionalne". Przewidują one pokojowe rozstrzyganie sporów, zapobieganie konfliktom między członkami regionalnego systemu, funkcjonowanie organizacji zbiorowego działania w celu powstrzymania aktów → a g r e s j i i wyeliminowania zagrożenia dla pokoju, stosowanie → d y p l o m a c j i p r e w e n c y j n e j [t. 2], przestrzeganie → p r a w c z ł o w i e k a [t. 3], podtrzymanie, ustanowienie i umocnienie pokoju w okresie po zakończeniu konfliktu, kontrolę zbrojeń oraz zapewnianie → b e z p i e c z e ń s t w a e k o n o m i c z n e g o i ochronę środowiska. Z całości takich porozumień, organizacji i struktur powstaje regionalny system bezpieczeństwa.

Bezpieczeństwo regionalne jest ważnym warunkiem i znaczącym czynnikiem bezpieczeństwa międzynarodowego pod warunkiem, że umowy i porozumienia dotyczące bezpieczeństwa regionalnego są zgodne z celami i zasadami ONZ. Za najbardziej oczywisty przykład zapewnienia bezpieczeństwa regionalnego może służyć Organizacja Bezpieczeństwa i Współpracy w Europie (OBWE, ang. Organization for Security and Cooperation in Europe, OSCE), międzynarodowa, paneuropejska organizacja ds. bezpieczeństwa i współpracy będąca kontynuatorką Konferencji Bezpieczeństwa i Współpracy w Europie (KBWE), do której należy 57 państw członkowskich, wspólnie obejmujących region od Vancouver po Władywostok. Jej członkami są wszystkie kraje europejskie, USA, Kanada, państwa Azji Środkowej i Zakaukazia. Izrael, Jordania, Egipt, Tunezja, Algieria i Maroko mają status partnerów śródziemnomorskiej współpracy, natomiast Japonia, Republika Korei Południowej, Tajlandia, Afganistan i Australia mają status azjatyckich partnerów do współpracy. OBWE jest największą na świecie organizacją bezpieczeństwa, stowarzyszeniem politycznym, które pracuje nad koncepcją wspólnej i kompleksowej ochrony, integrując 3 wymiary: wojskowo-

polityczny, gospodarczy (środowiskowy) i humanitarny, kierując się zasadami równego partnerstwa, solidarności i przejrzystości. Wszystkie państwa uczestnicy mają równy status. Organizacja zajmuje się ustanawianiem norm regulujących stosunki między państwami i między państwem a jego obywatelami oraz nadzorem wykonywania tych norm; prowadzi dialog i negocjacje w sprawach bezpieczeństwa europejskiego; podejmuje działania na rzecz zapobiegania konfliktom, ostrzegania przed nimi oraz rozwiązywania zaistniałych kryzysów; prowadzi rozmowy nad doskonaleniem wojskowych środków budowy zaufania i bezpieczeństwa międzynarodowego.

Innymi organizacjami regionalnymi są np.: Organizacja Jedności Afrykańskiej (OJA, ang. Organization of African Unity, OAU), która zrzesza ponad 50 niezależnych krajów afrykańskich; Organizacja Państw Amerykańskich (OPA, ang. Organization of American States, OAS), zrzeszająca ponad 30 państw; Stowarzyszenie Narodów Azji Południowo-Wschodniej (Association of South-East Asian Nations, ASEAN). W aktach założycielskich szeregu organizacji regionalnych zawarto świadczenie zbiorowej samoobrony w razie zbrojnego ataku na któregokolwiek z członków tych organizacji.

Doświadczenie → N A T O [t. 3] pokazuje, że współpraca regionalna nie jest substytutem innych przedsięwzięć, lecz ich uzupełnieniem. Właśnie dlatego, że potencjał współpracy regionalnej i subregionalnej jest tak wyraźny, Sojusz udzielał coraz większego wsparcia tym wysiłkom, nawet wśród krajów, które nie aspirują do członkostwa w NATO, chociaż żaden zatwierdzony dokument nie określa podstaw współpracy regionalnej ani sposobów jej wspierania przez Sojusz. Zamiast tego podejście to jest przedstawione w wielu dokumentach, z których każdy dotyczy określonego obszaru lub problemu – ujmowane razem tworzą spójną intelektualnie całość. Sojusz działa na rzecz promowania regionalnej współpracy w zakresie bezpieczeństwa przede wszystkim na Bałkanach, na Kaukazie i w krajach bałtyckich w ramach ogólnych wysiłków NATO na rzecz pokoju i bezpieczeństwa w obszarze euroatlantyckim. NATO przyjmuje indywidualne, ukierunkowane podejście do każdego regionu.

Stopień zaangażowania wielkich mocarstw w zapewnienie bezpieczeństwa regionalnego jest szczególnie wysoki na kontynencie europejskim oraz w regionie Azji i Pacyfiku. Aby utrzymać i wzmocnić bezpieczeństwo regionalne, istnieją regionalne porozumienia międzypaństwowe podyktowane potrzebą dostosowania regionalnych struktur bezpieczeństwa do zmieniających się realiów, chęcią ich wzmocnienia. W Europie, gdzie jest najwięcej zapasów broni wszelkiego rodzaju, osiągnięto porozumienie w sprawie znacznej redukcji liczby rakiet nuklearnych średniego i krótkiego zasięgu oraz rakiet i broni konwencjonalnej.

Bezpieczeństwo regionalne jest największą zmienną, a jego poziom zależy od siły i dynamiki wewnętrznych i umiędzynarodowionych konfliktów, w jakie są zaangażowane państwa regionalne, w związku z którymi pożytkowane są przez państwa regionalne łączne zasoby ludzkie i materialne w celu zabezpieczenia bezpieczeństwa, znaczenia i efektywności regionalnych sojuszy wojskowych i instytucji zbiorowego

bezpieczeństwa w regionie. Wspólnie wykorzystując zasoby we właściwy sposób, podobnie myślące kraje mogą skuteczniej zwiększyć swoje bezpieczeństwo.

Od połowy lat 80. XX w. nastąpiła eksplozja różnych form projektów regionalistycznych w skali globalnej. Rozszerzenie i pogłębienie UE jest najbardziej typowym przykładem, ale regionalizm uwidacznia się również poprzez rewitalizację lub ekspansję wielu innych projektów regionalnych na całym świecie, by wspomnieć Unię Afrykańską, ASEAN, Wspólnotę Gospodarczą Państw Afryki Zachodniej (Economic Community of West African States, ECOWAS) czy Północnoamerykański Układ Wolnego Handlu (North American Free Trade Agreement, NAFTA).

W rzeczywistości działania państw są ważnym wskaźnikiem bezpieczeństwa regionalnego. Państwo, które nie odczuwa niebezpieczeństwa lub odczuwa je na stosunkowo niskim poziomie, nie zwraca dużej uwagi na indywidualnie lub wielostronne środki bezpieczeństwa w swojej działalności. Ponieważ większość państw we współczesnym świecie to państwa poziomu regionalnego, zagrożenia, które bezpośrednio zagrażają ich bezpieczeństwu narodowemu, mają także charakter regionalny (pochodzą one albo ze źródeł, które znajdują się w obrębie regionu, albo są korelacją procesów regionalnych z niektórymi globalnymi trendami).

Większość światowych środków wydzielonych do zapewnienia bezpieczeństwa narodowego jest odzwierciedleniem wewnętrznych (w obrębie kraju) i regionalnych zagrożeń. W nowoczesnych warunkach problemy bezpieczeństwa wewnętrznego czy regionalnego mają tendencję do umiędzynarodowienia.

Olga Wasiuta

Afghanistan and Central Asia: NATO's Role in Regional Security Since, O. Tanrisever (ed.), IOS Press, Amsterdam 2013; A.J.K. Bailes, A. Cottey, *Regional Security Cooperation in the Early 21st Century*, [w:] *SIPRI Yearbook 2006: Armaments, Disarmament and International Security*, SIPRI, Stockholm 2006; *Bilateral Perspectives on Regional Security: Australia, Japan and the Asia-Pacific Region*, W. Tow, R. Kersten (eds.), Springer, London 2012; B. Buzan, O. Wæver, *Regions and Powers: The Structure of International Security*, Cambridge University Press, Cambridge 2003; *Central Asia and Regional Security*, P.L. Dash, A. Sengupta, M.M. Bakhadirov (eds.), KW Publishers, New Delhi 2014; R. Fawn, *Globalising the Regional, Regionalising the Global*, Cambridge University Press, Cambridge 2009; M. Gupta, *Indian Ocean Region: Maritime Regimes for Regional Cooperation*, Springer, London 2010; G. Janusz, *Bezpieczeństwo regionalne w kontekście rzekomego naruszania praw ludności rosyjskiej na Ukrainie oraz mechanizmów europejskiego systemu ochrony praw mniejszości*, „Eastern Review" 2016, t. 5; R.E. Kelly, *Security Theory in the 'New Regionalism'*, „International Studies Review" 2007, no. 9; D. Lemke, *Regions of War and Peace*, Cambridge University Press, Cambridge 2002; E. Solingen, *Regional Orders at Century's Dawn: Global and Domestic Influences on Grand Strategy*, Princeton University Press, Princeton 1998; *Teoretyczne i praktyczne aspekty rozwoju regionalnego*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług" 2010, nr 582; O. Wasiuta, *Bezpieczeństwo regionalne*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018.

BEZPIECZEŃSTWO RODZINY – jeden z rodzajów → b e z p i e c z e ń s t w a , stan wolny od → z a g r o ż e ń [t. 4] dla integralności, trwałości i rozwoju

rodziny. Pojęcie to nierozerwalnie wiąże się zarówno z wymiarem jednostkowym, jak i społecznym (rodzina jako grupa czy instytucja społeczna), gdyż zachwianie bezpieczeństwem któregokolwiek spośród jej członków wpływa na całą rodzinę. Co więcej, bezpieczeństwo rodziny stanowi kluczową wartość nie tylko dla niej, ale dla każdego społeczeństwa, w którym stanowi podstawową komórkę. Już Arystoteles dowodził, że w rodzinie jak w soczewce odzwierciedla się całe społeczeństwo, dlatego dbałość o jej kondycję (w tym elementarne bezpieczeństwo) powinna być przedmiotem troski ogółu.

Według F. Adamskiego rodzinę tworzy niewielka grupa osób połączonych wspólnym ogniskiem domowym, aktami wzajemnej pomocy i opieki, wiarą w łączność biologiczną, tradycję rodzinną i społeczną. Spośród innych grup wyróżnia ją współwystępowanie takich cech jak wspólne zamieszkanie członków, wspólne nazwisko, wspólna własność, ciągłość biologiczna oraz wspólna kultura duchowa. W węższym ujęciu rozpatruje się rodzinę jako grupę, w której mają miejsce bezpośrednie, intymne relacje, a jej nieodzowną cechą są więzi przede wszystkim osobowe, ale także rzeczowe. Z kolei w ujęciu szerszym rodzinę określa się jako instytucję społeczną, która zaspokaja potrzeby społeczne. Wyróżnia się następujące funkcje, jakie powinna pełnić rodzina:

- instytucjonalne – prokreacyjna/biologiczna, ekonomiczna, opiekuńcza, socjalizacyjna, stratyfikacyjna, integracyjna;
- osobowe – małżeńska, rodzicielska, braterska.

Jeżeli pojawiają się poważne problemy i nieprawidłowości w realizowaniu tych funkcji, rodzina staje się dysfunkcyjna. Wówczas socjalizacja jest nieprawidłowa, a podstawowe potrzeby członków rodziny nie są zaspokajane w wystarczającym stopniu. Zarówno powodem, jak i skutkiem takiej sytuacji mogą być patologie. Często niezbędna jest fachowa pomoc osób i instytucji, które mogą profesjonalnie wesprzeć rodzinę w → k r y z y s i e [t. 2].

Jak wskazuje J. Izdebska, pomoc rodzinie dysfunkcyjnej może przybierać różne formy. W zasadzie do wszystkich rodzin można odnieść profilaktykę wychowawczą, przejawiającą się pogłębianiem wiedzy rodziców o rozwoju i wychowaniu dziecka, wpływającą na podniesienie poziomu ich kultury pedagogicznej. Inną formę stanowi kompensacja społeczna, czyli wyrównywanie deficytów i neutralizowanie przeszkód w prawidłowym funkcjonowaniu rodziny. W najpoważniejszych przypadkach, głównie w domach dotkniętych patologiami, ma miejsce ratownictwo. Przy czym zgodnie z zasadą pomocniczości nie powinno się wyręczać rodziny tam, gdzie może poradzić sobie samodzielnie. Interwencję należy ograniczyć do wyjątkowo trudnych sytuacji, w których rodzina faktycznie nie jest w stanie sama sobie poradzić w wypełnianiu określonych zadań.

Większość ludzi ma w swoim życiu kilka rodzin, poczynając od rodziny pochodzenia w dzieciństwie, poprzez rodzinę prokreacji, założoną wraz z zawarciem

małżeństwa, aż do ról babci czy dziadka odgrywanych w późniejszym okresie życia. Ponadto pojęcie rodziny funkcjonuje w szerszym sensie i ma związek z różnymi układami, np. w relacji:

- rodzina – rodzina (relacje wewnątrzrodzinne w ramach rodziny nuklearnej, dużej zredukowanej itp.);
- rodzina – mikroukłady społeczne (najbliższe, bezpośrednie kontakty sąsiedzkie, rówieśnicze, towarzyskie);
- rodzina – mezoukłady społeczne (lokalne, okoliczne środowisko wychowawcze, np. osiedle, szkoła, ośrodki kulturalne, sportowe, pomocy społecznej, parafia, spółdzielnia mieszkaniowa);
- rodzina – makrostruktury społeczne (relacje związane z wykonywanym zawodem, wyznaniem, tożsamością etniczną itp.);
- rodzina – społeczeństwo globalne i szersze układy i zjawiska (kontakty pośrednie i jednostronne, a także interaktywne możliwe dzięki rozwojowi nowoczesnych technologii, głównie internetu).

Pojęcie bezpieczeństwa (od wyrażenia przyimkowego *bez pieczy* oznaczającego „bez bojaźni", „bez troskliwości", ang. *security* od łac. *sine*, bez; *cura*, troska, uwaga, niepokój; *securus*, wolność od troski, pewność) rozumie się najczęściej jako stan bez niepokojów lub zagrożeń. Źródłem zagrożeń zewnętrznych mogą być: przyroda, np. w kontekście klęsk żywiołowych, wytwory cywilizacji lub inni ludzie, czynniki ekonomiczne, takie jak bezrobocie, kryzys edukacji, nauki, zdrowia, czynniki społeczne, np. patologie. Źródła zagrożeń wewnętrznych tkwią w jednostkach, które mogą zmagać się z chorobami psychicznymi, uzależnieniami, autoagresją, a nawet samobójstwami.

Bezpieczeństwo rodziny wiąże się zarówno z właściwym i skutecznym realizowaniem wspomnianych wyżej funkcji, jak i odpowiednimi warunkami, w których przebiegają relacje rodziny z wymienionymi układami życia ludzkiego. Na bezpieczeństwo rodziny w wymiarze personalnym i lokalnym wpływa szereg uwarunkowań. Czynniki egzystencjalno-socjalne związane są ze sferą ekonomiczną, w tym pomocą socjalną czy opieką medyczną. Problemy, które mogą tu mieć miejsce i poważnie zachwiać poczuciem bezpieczeństwa członków rodziny, to złe warunki materialne i bytowe, syndrom 3B – bieda, bezrobocie, bezdomność, trudna sytuacja finansowa rodzin wielodzietnych, niepełnych czy popegeerowskich. Poza samą rodziną – rodzicami sprawującymi opiekę nad dziećmi, ale również niejednokrotnie troszczącymi się o najstarszych członków rodziny (babcie, dziadków) – za bezpieczeństwo rodziny odpowiada państwo, zgodnie z jego konstytucyjnym obowiązkiem. Administracja publiczna organizuje instytucje, których rolą jest nie tylko dbanie o aspekty bezpośrednio związane z bezpieczeństwem, ale również kwestie materialne, zdrowotne, edukacyjne, kulturalne, społeczne i socjalne, zadania takie jak zwalczanie → p r z e s t ę p c z o ś c i [t. 3], profilaktyka uzależnień i innych → p a t o l o g i i s p o ł e c z n y c h [t. 3], zapobieganie wykluczeniu społecznemu itd. Aby skutecznie pomóc rodzinie

w spełnianiu jej funkcji, prowadzi się politykę rodzinną, opartą na normach prawnych, działaniach i środkach sprzyjających powstaniu rodziny, jej funkcjonowaniu i rozwojowi w korzystnych warunkach. Powinna również umożliwiać wypełnianie przez nią pożądanych społecznie ról. Polityka rodzinna dotyczy kwestii takich jak: lokum dla życia rodzinnego (mieszkanie, dom), zatrudnienie umożliwiające utrzymanie rodziny, system podatkowy oraz zasiłki społeczne, prawo wspierające rodziny i chroniące nieletnich, programy wychowawcze, edukacyjne, profilaktyczne i prorodzinne, rzetelną diagnozę potrzeb społecznych i analizę oddziaływań na rodzinę, mającą na celu weryfikację i ewentualną zmianę działań podejmowanych na rzecz rodziny.

Ważną grupę uwarunkowań bezpieczeństwa rodziny stanowią także czynniki psychiczno-duchowe, na które składają się: dobre samopoczucie fizyczne i psychiczne, pozytywne cechy osobowościowe, odpowiednie postawy, świadomość własnych możliwości i dobrych perspektyw życiowych, pewność wynikająca ze stabilności dóbr indywidualnych i wspólnych, religijność i rozwój duchowy, więzi międzyludzkie. Nieodzowna jest tu pewnego rodzaju równowaga, balans, szeroko pojęta wiara, ale i wiedza oparta na racjonalnym podejściu do rzeczywistości. Wiele z tych elementów, zwłaszcza odnoszących się do cech charakteru, zachowań, nastawienia, orientacji życiowej, wiąże się w dużym stopniu z 2 kolejno omówionymi poniżej grupami.

Czynniki społeczne to dobre, zdrowe i życzliwe relacje z bliskimi, rodziną, przyjaciółmi, powodzenie w pracy zawodowej i poza nią, przynależność do organizacji społecznej, pomoc innym, poważanie, sprawiedliwość i ład. Niezwykle ważny jest tu, zwłaszcza w początkowym okresie życia, klimat czy atmosfera domu rodzinnego, w którym poza zapewnieniem obiektywnego bezpieczeństwa wpływa się również na budowanie i umacnianie (bądź osłabianie) subiektywnego poczucia bezpieczeństwa każdego z członków. Nie do przecenienia są tu miłość, zaufanie, bliskość z drugim człowiekiem, potencjalna możliwość znalezienia w nim oparcia i zrozumienia. W tym kontekście niepokoi osłabienie więzi w rodzinie, rozpad rodzin wielopokoleniowych, autonomizacja członków rodziny, powodująca koncentrację na interesach indywidualnych, a nie dążeniach grupowych. Można zaobserwować również atomizację społeczną – dezintegrację wspólnot lokalnych i kontaktów interpersonalnych, rozpad więzi sąsiedzkich, zmniejszenie kontroli społecznej, kryzys wartości, osłabienie myślenia wspólnotowego. Negatywny wpływ mogą tu mieć patologie społeczne, np. uzależnienie od alkoholu, narkotyków, hazardu czy internetu, przestępstwa, a także → p r z e m o c [t. 3] fizyczna i psychiczna. Należy podkreślić, że patologia, która dotyka jednego członka rodziny, wpływa na pozostałych, zaburzając funkcjonowanie rodziny i jej wewnętrzne, a niekiedy również zewnętrzne relacje.

Czynniki edukacyjno-kulturowe to przede wszystkim dbałość o wychowanie i wykształcenie, podnoszenie kwalifikacji, aktywność, pobudzanie kreatywności, czerpanie czynne i bierne z kultury, kultywowanie tradycji, rozsądne i umiejętne korzystanie z mass mediów. Badania wskazują, że kultura pedagogiczna rodziców

nie jest na zadowalającym poziomie, mimo że teoretycznie możliwości dokształcania się w kwestiach związanych z wychowaniem, stosowaniem odpowiednich metod, komunikacją interpersonalną, konsekwencjami niepożądanych postaw są praktycznie nieograniczone. Dochodzą do tego zagrożenia wynikające ze stosowania nowych technologii, takie jak mediatyzacja i dezorganizacja życia rodziny poprzez nadmierny udział mediów i multimediów w jej funkcjonowaniu, a niekiedy wręcz zastępowanie rodziców w pełnieniu przez nich funkcji opiekuńczo-wychowawczych. Istnieje duże ryzyko związane z bezpieczeństwem danych i → i n f o r m a c j i [t. 2], ich ujawnianiem, kradzieżą danych lub tożsamości oraz innymi oszustwami związanymi z bankowością elektroniczną, zakupami przez internet itp. Zagrożeniem dla wychowania i rozwoju młodych ludzi, a co za tym idzie – czynnikiem szkodliwym dla funkcjonowania całej rodziny – mogą być niepożądane treści, np. materiały pornograficzne, pedofilskie, strony zawierające drastyczne obrazy lub przemoc, materiały o narkotykach, sektach i innych potencjalnie groźnych zagadnieniach, niebezpieczne porady (np. strony zachęcające do głodzenia się czy popełniania samobójstwa), portale społecznościowe pełne → c y b e r p r z e m o c y, → s e k s t i n g [t. 4], niebezpieczne znajomości nawiązywane w wirtualnym świecie czy wreszcie uzależnienie od komputera, telefonu bądź internetu i wiążące się z nim problemy zdrowotne, jak również wiele innych ryzykownych zjawisk pojawiających się wraz z rozwojem technologii.

Biorąc pod uwagę czynniki egzystencjalno-socjalne oraz edukacyjno-kulturowe, konieczne jest oddziaływanie na aspiracje edukacyjne rodzin. Pomocne w tym może być ograniczanie nierówności i wyrównywanie szans edukacyjnych młodego pokolenia. Uwzględniając przemiany skutkujące podejmowaniem pracy zawodowej przez oboje rodziców, potrzebne są rozwiązania w prawie pracy, formach organizacji czasu pracy i zabezpieczeniach społecznych, które ułatwiłyby im godzenie obowiązków zawodowych z rodzinnymi.

Czynniki przyrodnicze wiążą się z właściwym zagospodarowaniem terenu, estetycznym otoczeniem, walorami przyrodniczymi i brakiem groźnych zanieczyszczeń. To także zapewnienie dziecku warunków sprzyjających rozwojowi, przestrzeni spełniającej wymogi higieniczne i zdrowotne, umożliwienie kontaktu z przyrodą, dbanie o środowisko i kształtowanie postaw proekologicznych.

Zagrożeń dla stabilności, a więc i pełnego bezpieczeństwa rodziny, jest znacznie więcej. Część z nich wiąże się z przemianami tej komórki społecznej determinowanymi przez zmiany cywilizacyjne. Przykładowo dezorganizację struktury rodzinnej może spowodować – poza śmiercią jednego z małżonków – coraz częstsze zjawisko, jakim jest rozwód bądź separacja oraz długotrwała czasowa nieobecność rodzica (wyjazd za granicę, choroba, więzienie). Ponadto pojawia się coraz więcej nowych, alternatywnych form quasi-rodzinnych. Inne problemy to zmniejszająca się dzietność, starzenie się społeczeństwa itd.

Bezpieczeństwo rodziny to taki stan – czy raczej taki niekończący się proces – w którym sama rodzina może bezpiecznie realizować swoje funkcje, a jej członkowie mogą rozwijać się wielostronnie zarówno jako grupa, wspólnota rodzinna, jak i w sposób indywidualny, bez większych barier czy zagrożeń zewnętrznych i wewnętrznych. To również – biorąc pod uwagę fakt, że nie da się całkiem uniknąć ryzyka czy niepowodzenia – właściwa edukacja członków rodziny – dzieci, dorosłych, starszych pokoleń – w kwestiach związanych z bezpieczeństwem. Taka edukacja winna mieć miejsce w domu, w szkole, w instytucjach oświatowych, jak również w mediach.

Małgorzata Bereźnicka

F. Adamski, *Rodzina. Wymiar społeczno-kulturowy*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2002; B. Balcerzak-Paradowska, *Rodzina i polityka rodzinna na przełomie wieków. Przemiany, zagrożenia, potrzeba działań*, Instytut Pracy i Spraw Socjalnych, Warszawa 2004; M. Bereźnicka, *Bezpieczeństwo rodziny*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; taż, *Kultura pedagogiczna rodziców w społeczeństwie informacyjnym*, Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2015; taż, *Wychowanie dziecka we współczesnej rodzinie*, Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2014; K. Drabik, *Bezpieczeństwo personalne i strukturalne*, AON, Warszawa 2013; B. Hołyst, *Zagrożenia ładu społecznego*, Wydawnictwo Naukowe PWN, Warszawa 2013; J. Izdebska, *Dziecko osamotnione w rodzinie*, Wydawnictwo Uniwersyteckie Trans Humana, Białystok 2004; S. Kawula, J. Brągiel, A. Janke, *Pedagogika rodziny. Obszary i panorama problematyki*, Wydawnictwo Adam Marszałek, Toruń 2009; M. Winiarski, *Bezpieczeństwo lokalne – problemem pedagogicznym*, „Edukacja i Dialog" 2000, nr 9 (122).

BEZPIECZEŃSTWO SANITARNO-EPIDEMIOLOGICZNE (z gr. *epi* 'na' lub 'nad', *demos* 'ludność', *logos* 'nauka', w dawnym znaczeniu 'to, co przechodzi na lud') – ogół warunków i instytucji chroniących społeczeństwo przed patogenami chorobotwórczymi stwarzającymi zagrożenie epidemiczne dla → z d r o w i a p u b l i c z n e g o [t. 4]. Można je wyodrębnić z bezpieczeństwa zarówno wewnętrznego, jak i zewnętrznego. Ściśle skorelowane jest również z dyscypliną nauk medycznych.

Bezpieczeństwo sanitarno-epidemiologiczne jest związane ze zdrowiem, z higieną, profilaktyką chorób, a także badaniem czynników wpływających na zbiorowość ludzką oraz jej dobrostan zdrowotny. Pojęcie szczególnie zyskało na znaczeniu w trakcie pandemii → C O V I D - 1 9 [t. 5] w latach 2020–2023, kiedy epidemiologia ponownie ukierunkowała się ku chorobom zakaźnym, by przeciwdziałać ich rozprzestrzenianiu się. Bezpieczeństwo sanitarno-epidemiologiczne jest to zarówno stan, jak i proces, który w ujęciu holistycznym koncentruje się na diagnozowaniu i weryfikowaniu → s y t u a c j i k r y z y s o w y c h [t. 4] wynikających z niekorzystnego wpływu szkodliwych i uciążliwych czynników środowiskowych, przeciwdziałaniu im oraz reagowaniu na nie, a także zapobieganiu chorobom zakaźnym, zwłaszcza tym o wysokim stopniu wirulencji. Dbałość o ten rodzaj → b e z p i e c z e ń s t w a [t. 1] jest szczególnie ważna, ponieważ patogeny chorobotwórcze znajdujące się w miejscach

publicznych mogą stanowić realne zagrożenie dla zdrowia, a nawet życia ludzi, co w konsekwencji może doprowadzić do załamania się innych rodzajów bezpieczeństwa, zwłaszcza zdrowotnego, publicznego oraz narodowego. Przykładem była pandemia COVID-19, której konsekwencje były widoczne i odczuwalne w niemal każdej sferze funkcjonowania państwa.

Do podstawowych rodzajów epidemiologii zalicza się epidemiologię:

- ogólną – zajmuje się ona metodologią badań epidemiologicznych, których celem jest ocena zjawisk zdrowotnych zachodzących w społeczeństwie;
- chorób zakaźnych – obszar badań dotyczy rozpoznawania i zwalczania epidemii lub – szerzej – → p a n d e m i i [t. 5], następnie procesów epidemicznych chorób zakaźnych, opracowywania ognisk epidemicznych, a także innych problemów związanych z rozprzestrzenianiem się chorób zakaźnych;
- kliniczną – zajmuje się zastosowaniem zasad i metod epidemiologicznych w warunkach szpitalnych;
- środowiskową – przedmiotem badań jest wpływ różnych czynników i warunków środowiskowych na częstotliwość i rozpowszechnienie chorób zakaźnych i niezakaźnych (epidemiologia chorób niezakaźnych, np. cukrzyca, choroby układu krążenia, zaburzenia psychiczne, nowotwory) lub różnych stanów fizjologicznych wśród ludności;
- społeczną – obejmuje epidemiotechnikę (opracowywanie metod profilaktyki i zwalczania chorób oraz weryfikowanie ich za pomocą doświadczeń na określonych grupach ludności, np. w formie epidemiologicznych badań kontrolowanych), ocenę sytuacji zdrowotnej ludności (za pomocą epidemiologicznych badań opisowych w formie sondaży epidemiologicznych, badań reprezentatywnych, długofalowych badań monitorowych) i wynikających z niej potrzeb zdrowotnych, które stanowią podstawę kształtowania polityki zdrowotnej.

W wyniku rozwoju epidemiologii i jej coraz większego obszaru badawczego wyróżniono kolejne dziedziny, których zakres tematyczny jest węższy i dokładniejszy. Można wymienić epidemiologię: wojskową, chorób zawodowych czy katastrof, a także geografię epidemiologiczną. To pokazuje, że podejmowana problematyka obejmuje niemal każdą sferę życia populacji.

Jednostką sprawującą nadzór nad bezpieczeństwem sanitarno-epidemiologicznym w Polsce jest Państwowa Inspekcja Sanitarna (nazwa zwyczajowa: sanepid) będąca centralnym organem administracji rządowej. Podlega ministrowi właściwemu ds. zdrowia, kieruje nią główny inspektor sanitarny. Na mocy Ustawy z dnia 14 marca 1985 r. o Państwowej Inspekcji Sanitarnej oraz Rozporządzenia Ministra Zdrowia z dnia 17 października 2014 r. w sprawie systemów wymiany informacji w zakresie dotyczącym zadań Państwowej Inspekcji Sanitarnej została ona powołana do realizacji zadań z zakresu zdrowia publicznego. Sprawuje ona prewencyjny i bieżący nadzór sanitarny oraz prowadzi działalność o charakterze zapobiegawczym

i przeciwepidemicznym w zakresie chorób zakaźnych i innych chorób powodowanych warunkami środowiskowymi, a także działalność oświatowo-zdrowotną.

Państwowa Inspekcja Sanitarna ustawowe zadania realizuje za pośrednictwem terenowych stacji sanitarno-epidemiologicznych na poziomie województwa (wojewódzka stacja sanitarno-epidemiologiczna), powiatu (powiatowa stacja sanitarno-epidemiologiczna) oraz obszarów przygranicznych (graniczna stacja sanitarno-epidemiologiczna), tj. lądowych oraz morskich, które podlegają jurysdykcji państwowego granicznego inspektora sanitarnego.

Zadania Państwowej Inspekcji Sanitarnej mogą być również realizowane przez Wojskową Inspekcję Sanitarną, która podlega ministrowi obrony narodowej. Kieruje nią główny inspektor sanitarny Wojska Polskiego za pomocą organów terenowych, tj. komendantów i wojskowych inspektorów sanitarnych wojskowych ośrodków medycyny prewencyjnej. Podmioty Wojskowej Inspekcji Sanitarnej wykonują ustawowe zadania przy udziale wojskowych ośrodków medycyny prewencyjnej, które są centrami leczniczymi finansowanymi z budżetu państwa oraz jednostkami wojskowymi.

Wojskowa Inspekcja Sanitarna realizuje zadania w jednostkach organizacyjnych podległych ministrowi obrony narodowej bądź przez niego nadzorowanych oraz w podmiotach, w tym spółkach, utworzonych przez te jednostki. Dodatkowo pełni obowiązki obsługi sanitarno-epidemiologicznej w rejonach zakwaterowania przejściowego jednostek wojskowych oraz w stosunku do wojsk obcych przebywających na terytorium Rzeczypospolitej Polskiej lub przemieszczających się przez nie. Wojskowa Inspekcja Sanitarna realizuje również zadania Państwowej Inspekcji Sanitarnej poza terenem jednostek i podmiotów wobec → ż o ł n i e r z y [t. 4] służby czynnej, funkcjonariuszy Służby Kontrwywiadu Wojskowego oraz Służby Wywiadu Wojskowego, a także żołnierzy wojsk obcych i ich personelu cywilnego przemieszczających się przez terytorium Rzeczypospolitej Polskiej lub przebywających na tym terytorium.

Państwowa Inspekcja Sanitarna, gromadząc → i n f o r m a c j e [t. 2] oraz dane statystyczne w obszarze swoich kompetencji, począwszy od 2006 r. (pierwsze udostępnione podsumowanie do otwartego wglądu), rokrocznie wydaje raporty o stanie sanitarnym kraju. W ostatnim dostępnym dokumencie został przeanalizowany 2021 r., poświęcono w nim szczególną uwagę pandemii COVID-19 oraz problemom i wyzwaniom wynikającym z zaistniałej sytuacji epidemiologicznej na terenie całego państwa. Oprócz tego rozwinięto zagadnienia dotyczące m.in. bezpieczeństwa sanitarnego żywności, jakości wody pitnej, zapobiegania zakażeniom i chorobom zakaźnym u ludzi oraz zwalczania ich, stanu sanitarnego kąpielisk oraz pływalni, a także obiektów użyteczności publicznej czy podmiotów leczniczych. Dokument ten zawiera również opis wdrożonych programów edukacyjnych na rzecz bezpieczeństwa sanitarno-epidemiologicznego. Podobne raporty wydają też wojewódzkie stacje sanitarno-epidemiologiczne, przedstawiona jest w nich analogiczna analiza problemów zdrowotnych oraz stanu sanitarnego badanych podmiotów na terenie województwa.

Państwowa Inspekcja Sanitarna w zależności od okoliczności badanej sprawy ma prawo do przeprowadzenia kontroli wobec danego podmiotu, w formie:

- kompleksowej kontroli sanitarnej – charakteryzuje się całościowym sprawdzeniem danej placówki;
- kontroli tematycznej – w zakresie określonego produktu lub określonej grupy podmiotów;
- kontroli interwencyjnej przeprowadzanej na skutek otrzymania zawiadomienia o nieprawidłowościach higieniczno-sanitarnych;
- kontroli laboratoryjnej próbek żywności;
- kontroli sprawdzającej – w celu zweryfikowania, czy rekomendacje wydane podczas poprzedniej kontroli zostały wdrożone przez podmiot.

Bezpośrednio z bezpieczeństwem sanitarno-epidemiologicznym związane jest pojęcie nadzoru epidemiologicznego, który oznacza bieżącą ocenę zagrożeń godzących w zdrowie populacji. Nadzór polega na zbieraniu, interpretacji, analizie i udostępnianiu informacji na temat obecnie występujących zachorowań lub innych zdarzeń związanych ze zdrowiem. Jego celem jest umożliwienie decydentom efektywniejszego zarządzania przez dostarczanie aktualnych danych epidemiologicznych. Dzieli się na:

- nadzór epidemiologiczny bierny – dozór, w którym zachorowania zgłaszają uprawnione osoby (np. lekarze, pielęgniarki), które je rozpoznali. Instytucje zajmujące się gromadzeniem danych nie wyszukują ich czynnie, ale mogą zwracać się do zgłaszającycho weryfikację zgłoszeń;
- nadzór epidemiologiczny czynny – kontrola epidemiologów sprawujących nadzór w celu wyszukania zachorowań w populacji lub w podmiotach medycznych.

Bezpieczeństwo sanitarno-epidemiologiczne to nie tylko wartość, ale także potrzeba, ponieważ dbałość o higienę, profilaktykę oraz uświadamianie o → z a g r o ż e n i a c h [t. 4] stanowi o sile danego państwa. Jednym z katalizatorów pomyślnego rozwoju narodu jest właśnie zdrowie. Zagrożenie dla bezpieczeństwa sanitarno-epidemiologicznego może pośrednio i bezpośrednio wpływać na całokształt funkcjonowania państwa, tym samym hamując jego rozwój oraz powodując poważne konsekwencje dla teraźniejszych i przyszłych pokoleń w wymiarze zdrowia publicznego i →b e z p i e c z e ń s t w a n a r o d o w e g o [t. 1].

Żaneta Zając

S. Czechowicz, *Pojęcie bezpieczeństwa sanitarno-epidemiologicznego i jego konteksty prawne*, „Opolskie Studia Administracyjno-Prawne" 2020, t. 18, nr 3; *Definicja, przedmiot, cele i zadania epidemiologii*, https://www.wnoz.cm.umk.pl/panel/ wp-content/uploads/1.pdf (dostęp 20.04.2023); Główny Inspektorat Sanitarny, https://www.gov.pl/web/gis (dostęp 20.04.2023); W. Jędrychowski, *Podstawy epidemiologii. Metody badań ora materiały ćwiczeniowe*, Wydawnictwo UJ, Kraków 2002; J.M. Last, *Public Health*, [w:] *A Dictionary of Epidemiology*, J.M. Last, R.A. Spasoff, S.S. Harris (eds.), Oxford University Press, New York 2001; Rozporządzenie Ministra Zdrowia z dnia 17 października 2014 r. w sprawie systemów wymiany informacji w zakresie dotyczącym zadań Państwowej Inspekcji Sanitarnej, Dz.U. 2014, poz.

1474; *Sanitarny*, Słownik języka polskiego PWN, https:// sjp.pwn.pl/slowniki/sanitarny.html (dostęp 20.04.2023); *Słowniczek terminów epidemiologicznych*, http://www.przeglepidemiol.pzh.gov.pl/slowniczek-terminow-epidemiologicznych (dostęp 20.04.2023); *Stan Sanitarny w Kraju w 2021 roku*, Główny Inspektorat Sanitarny, Warszawa 2022; Ustawa z dnia 14 marca 1985 r.o Państwowej Inspekcji Sanitarnej, Dz.U. 1985, nr 12, poz. 49.

BEZPIECZEŃSTWO SPOŁECZNE (ang. *social security*) – jeden z podstawowych rodzajów (typów, sektorów, dziedzin) → b e z p i e c z e ń s t w a rozumianego jako kategoria badawcza oraz przestrzeń realizacji polityki, w której dominującą rolę w zakresie wypełniania potrzeb społeczeństwa odgrywa państwo (polityka społeczna). Społeczny, priorytetowy wymiar bezpieczeństwa łączy w pewnym sensie różne jego sektory (→ b e z p i e c z e ń s t w o p o l i t y c z n e , → b e z p i e c z e ń s t w o m i l i t a r n e , → b e z p i e c z e ń s t w o e k o n o m i c z n e , → b e z p i e c z e ń s t w o k u l t u r o w e , → b e z p i e c z e ń s t w o i d e o l o g i c z n e , → b e z p i e c z e ń s t w o i n f o r m a c y j n e , → b e z p i e c z e ń s t w o e k o l o g i c z n e itd.) i choć trudno jest polemizować ze stwierdzeniem o wzajemnym uzupełnianiu się wyszczególnionych rodzajów bezpieczeństwa, to jednak współczesne definicje bezpieczeństwa społecznego wyraźnie podkreślają jego państwocentryczny charakter, a właściwie nadrzędną rolę państwa w jego zapewnieniu. Nie umniejsza to jednak znaczenia zaradności społecznej i obywatelskiego zaangażowania na rzecz realizacji pomocy i wsparcia w tych problemach społecznych, w których działalność państwa jest niewystarczająca. Według jednej z najprostszych definicji bezpieczeństwa społecznego, trafnie oddającej istotę pojęcia, jest ono ujmowane jako pewien stan społeczeństwa, który zapewnia jednostkom (grupom społecznym, społeczeństwu, narodowi, obywatelom) tzw. progresywną kontynuację życia, a więc warunki do przetrwania, egzystencji i rozwoju. W ujęciu procesualnym (bezpieczeństwo jako pewien proces) bezpieczeństwo społeczne jawi się także jako permanentnie utrzymywana pewność przetrwania określonej grupy społecznej w obliczu ewoluujących → z a g r o ż e ń [t. 4] godzących w interes społeczny (potrzeby, dążenia, pragnienia). Bezpieczeństwo społeczne może być także rozpatrywane z punktu widzenia konkretnego człowieka (jako bezpieczeństwo społeczne jednostki, zaspokajane na poziomie egzystencjalno-emocjonalnym, psychiczno-emocjonalnym, edukacyjno-kulturalnym i interakcyjnym) oraz wspólnoty państwowej (jako bezpieczeństwo społeczne państwa definiowane przez obszary takie jak struktura społeczna, kultura danego społeczeństwa czy system podziału pracy).

W literaturze przedmiotu zaznacza się, że po raz pierwszy terminu bezpieczeństwa społecznego użyto oficjalnie w USA w tytule ustawy z 1935 r., odnoszącej się do programów społecznych mających zastosowanie w przypadku starości, śmierci, inwalidztwa oraz bezrobocia. Natomiast w Polsce pojęcie to wybrzmiało w 2001 r. z uwagi na ujęcie go w zestawieniu terminów umieszczonych w *Leksykonie polityki społecznej* (red. B. Rysz-Kowalczyk) na oznaczenie pewnego stanu wolności od

ryzyka i zagrożeń nie tylko społecznych, ale także socjalnych i psychospołecznych. Bezpieczeństwo socjalne należy odnieść przy tym do gwarancji zaspokojenia podstawowych potrzeb życiowych (egzystencjalnych, ekonomicznych), bezpieczeństwo psychospołeczne zaś – do gwarancji stabilnego rozwoju i realizacji podstawowych celów życiowych (poczucia wolności, uznania w grupie, samorealizacji). Istota bezpieczeństwa społecznego (w sensie generalnym) uwidacznia się więc w potrzebie skupienia uwagi państwa, jego instytucji oraz samego społeczeństwa (rodziny, grup społecznych, stowarzyszeń i organizacji pozarządowych) na zapewnieniu obywatelom określonego poziomu egzystencji, warunków do rozwoju, odpowiednich warunków zatrudnienia, edukacji, świadczeń zdrowotnych i socjalnych oraz realizacji żywotnych → i n t e r e s ó w n a r o d o w y c h [t. 2]. Według A. Skrabacz bezpieczeństwo społeczne jest bowiem obszarem wpisującym się w ramy bezpieczeństwa narodowego, rozumianym jako ochrona egzystencjalnych podstaw ludzkiego życia, możliwość zaspokajania indywidualnych potrzeb (zarówno materialnych, jak i duchowych), realizacja aspiracji duchowych poprzez tworzenie odpowiednich warunków do pracy i nauki, → o c h r o n a z d r o w i a [t. 3] oraz zagwarantowanie świadczeń emerytalnych przy zachowaniu zasady sprzężenia zwrotnego występującego pomiędzy działaniami instytucji państwowych, a obowiązującym systemem normatywnym, symbolicznym, zwyczajowym, etycznym, religijnym i filozoficznym. Do współczesnych uwarunkowań bezpieczeństwa społecznego Polski zalicza się przy tym następujące czynniki: → z a g r o ż e n i a s p o ł e c z n e [t. 4], charakter narodowy, aspekty tożsamościowo-kulturowe, rozwój społeczeństwa obywatelskiego, poziom kapitału społecznego, wyzwania w zakresie demografii oraz migrację zarobkową.

W teorii bezpieczeństwa dominującym poglądem jest przekonanie, że dany rodzaj bezpieczeństwa (w tym przypadku społecznego) jest silnie skorelowany z odpowiadającym mu rodzajem zagrożeń. Celem zaś bezpieczeństwa społecznego jest zapewnienie przetrwania, dobrobytu oraz → z r ó w n o w a ż o n e g o r o z w o j u [t. 4] społeczeństwa poprzez zapewnienie wysokiego standardu życia jednostkom, rodzinom i grupom społecznym oraz niedopuszczenie do marginalizacji i wykluczenia społecznego. Natomiast do zagrożeń, które determinują stan bezpieczeństwa społecznego oraz decydują o jego charakterze, zalicza się: trwałe wykluczenie społeczne, bezrobocie, brak środków na utrzymanie rodziny i mieszkania, ubóstwo, bezdomność, narkomanię, alkoholizm, upadek wartości rodzinnych, naruszane → p r a w c z ł o w i e k a [t. 3] i podstawowych wolności, dyskryminację na tle narodowościowym, religijnym, kulturowym i etnicznym, zagrożenie szowinizmem, ksenofobią i → f u n d a m e n t a l i z m e m r e l i g i j n y m [t. 2], medialną manipulację świadomością i psychiką, alienację społeczną, → p a t o l o g i e s p o ł e c z n e [t. 3], zagrożenia demograficzne, masowe migracje ekonomiczne, absorpcję obcych wartości kulturowych, dewaluację wartości, brutalizację stosunków międzyludzkich, brak perspektyw rozwoju itd. Tego typu ujęcia teoretyczne kładą nacisk głównie na pomocniczą rolę

państwa, które po pierwsze chroni jednostki przed niekorzystnym wpływem wyżej wymienionych zagrożeń społecznych, po drugie przeciwdziała skutkom przez nie wywołanym, po trzecie ma narzędzia do skutecznego zapewnienia i realizacji potrzeby bezpieczeństwa społecznego i ekonomicznego jednostek, tj. dostęp do rent, emerytur, powszechnej służby zdrowia itp. Szczególnie ostatni z wymienionych aspektów działalności państwa w ramach prowadzonej polityki społecznej często skłania teoretyków bezpieczeństwa do ujmowania kategorii bezpieczeństwa społecznego w kontekście funkcjonowania państwa opiekuńczego. W tym aspekcie unaocznienia wymaga również fakt zwrócenia uwagi współczesnych badaczy sfery bezpieczeństwa na koncepcje mające w założeniu poprawić poziom bezpieczeństwa społecznego, tj. *workfare state* (państwo zorientowane na pracę), *welfare society* (społeczeństwo opiekuńcze), *welfare pluralism* (pluralizm, wielosektorowość sfery społecznej) oraz *welfare mix* (stosowanie mieszanych form w polityce społecznej).

Bezpieczeństwo społeczne jest także kategorią/dziedziną → b e z p i e c z e ń s t w a n a r o d o w e g o i bywa rozpatrywane przez pryzmat polityki społecznej i ekonomicznej danego państwa. Kompatybilność założeń polityki dotyczącej bezpieczeństwa narodowego i społecznego zauważyć można na przykładzie definicji bezpieczeństwa społecznego rozumianego jako zbiór przedsięwzięć normatywno-organizacyjnych podejmowanych przez instytucje państwowe (ponadpaństwowe również) różnego szczebla służących zapobieganiu „wyrzucania" jednostek poza nawias życia społecznego (m.in. poprzez zagospodarowanie przestrzeni dotychczas zdezorganizowanej, leczenie dolegliwości, niwelowanie sprzeczności i przeciwdziałanie niewydolności funkcji społecznych będących w obszarze działalności instytucji państwa). Ponadto we współczesnej politologii i → n a u k a c h o b e z p i e c z e ń s t w i e [t. 3] pojęcie bezpieczeństwa narodowego wyprowadza się z egzystencjalnych potrzeb i interesów społeczeństwa zamieszkującego dane państwo, a więc z potrzeb i interesów, których zaspokojenie i realizacja są domeną bezpieczeństwa społecznego. Pokrywa się to poniekąd z podziałem bezpieczeństwa społecznego wg zakresu realizowanych wartości na pozytywne (aksjologia wartości społecznych) i negatywne (przetrwanie narodowej substancji). Wewnętrzny charakter bezpieczeństwa społecznego jako zadania dla administracji rządowej, samorządowej oraz każdego człowieka odzwierciedlają też zasady nawiązujące do interesów i korzyści wszystkich członków społeczeństwa (lokalnych społeczności, narodu, obywateli), tj. zasady solidarności społecznej, subsydiarności, przezorności, samopomocy, partycypacji, dobra wspólnego oraz wielosektorowości. Ponadto, na co wskazuje R. Jakubczak, bezpieczeństwo społeczne w sensie ogólnym dotyczy sytuacji wewnętrznej państwa oraz odnosi się do zagrożeń takich jak: zakłócenie ładu społeczno-politycznego, destabilizacja demokratyzacji państwa i budowy → s p o ł e c z e ń s t w a o b y w a t e l s k i e g o [t. 4], istnienie barier integracyjnych w stosunkach międzynarodowych, godzenie w interesy żywotne państwa oraz hamowanie rozwoju narodu i społeczeństwa. Należy także podkreślić, że

traktując bezpieczeństwo społeczne jako zintegrowany system i płaszczyznę realizacji zadań z zakresu egzystencjalnych potrzeb społeczeństwa, wyróżnić można kilka jego podsystemów. K. Loranty wymienia następujące: publiczny (działalność instytucji rządowych i samorządowych), nieformalny (wsparcie społeczne w ramach relacji z rodziną, przyjaciółmi, sąsiadami), ochotniczy (wsparcie ze strony podmiotów uskuteczniających ideę samopomocy i inicjatywności społeczności lokalnych, tj. wolontariatu, organizacji pozarządowych itp.), rynkowy (funkcjonujący na zasadzie kupna i sprzedaży, do którego dostęp uzależniony jest od zamożności obywateli) i obejmujący działalność podmiotów gospodarczych (zapewniający rozwój, ochronę zdrowia i poprawiający efektywność pracy w grupie pracowniczej).

Bezpieczeństwo społeczne, co zaznaczono powyżej, utożsamiane bywa także z bezpieczeństwem socjalnym rozumianym jako zapewnienie uzyskania ze strony instytucji zewnętrznych pomocy na wypadek zdarzeń losowych i innych wyszczególnionych przez prawo. Bezpieczeństwo socjalne jest kategorią węższą od bezpieczeństwa społecznego, ponieważ wszelkie zabiegi na jego rzecz koncentrują się na zapewnieniu jedynie wystarczających środków do życia oraz odnoszą się do ryzyka socjalnego związanego z możliwością wystąpienia choroby, choroby zawodowej, wypadku przy pracy czy zgonu żywiciela rodziny (a w konsekwencji poszerzaniem się obszaru biedy, nierówności czy wyłączenia socjalnego). Dlatego też podchodząc systemowo do bezpieczeństwa społecznego (jako jednej ze składowych bezpieczeństwa narodowego), nierzadko w świecie nauki zwraca się uwagę zarówno na aspekt socjalny (instytucjonalno-prawne gwarancje minimalnych standardów dotyczących płac, dochodów, transferów itp.), rozwojowy (szanse i możliwości rozwoju obywateli w danym państwie), jak i wspólnotowy (oparta na kapitale społecznym świadomość bycia częścią większej zbiorowości). Uwzględniając powyższe aspekty, J. Gierszewski traktuje bezpieczeństwo społeczne jako zbiór regulacji normatywno-prawnych mających na celu zapewnienie bezpieczeństwa przez wykorzystanie czynników (wewnętrznych i zewnętrznych) rozwoju społeczno-gospodarczego i organizację instytucji, gwarantujących niezagrożony rozwój oraz ład społeczny w kontekście bezpieczeństwa państwa. Zatem wieloaspektowość bezpieczeństwa społecznego i jego duże znaczenie dla zapewnienia bezpieczeństwa narodowego są płaszczyzną, która znajduje odzwierciedlenie w wielu dokumentach o strategicznym dla państwa charakterze.

Jednym z dokumentów, które podkreślają znaczenie społecznego rodzaju bezpieczeństwa, jest *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*. W → s t r a t e g i i [t. 4] z 2007 r., w części poświęconej zagrożeniom i → w y z w a n i o m b e z p i e c z e ń s t w a [t. 4] narodowego, sygnalizuje się problem negatywnych zmian demograficznych, czyli skali migracji z kraju, malejącego przyrostu naturalnego oraz różnic związanych z poziomem zamożności i stopy życiowej obywateli.

Bezpieczeństwu społecznemu poświęcono osobny podrozdział, w którym uwypuklono sprawy nauki i edukacji (społeczeństwo oparte na wiedzy), aktywnego

i sprawnego społeczeństwa (rozwój kultury fizycznej) oraz właśnie pracy i polityki społecznej. Natomiast w strategii z 2014 r. zawarto szereg czynników mających wpływ na bezpieczne warunki godziwego życia obywateli oraz rozwoju duchowego i materialnego narodu. We wspomnianym dokumencie zawarto następujące elementy odwołujące się do społecznej sfery funkcjonowania państwa: ochrona i umacnianie tożsamości narodowej (zachowanie tożsamości narodowej poprzez pielęgnowanie kultury narodowej oraz ciągłości historycznej i pokoleniowej, wzmacnianie postaw patriotycznych oraz aktywne i świadome obywatelstwo), → e d u k a c j a d l a b e z p i e c z e ń s t w a [t. 2] (zdobywanie przez obywateli wiedzy i umiejętności z zakresu bezpieczeństwa, podnoszenie zdolności do identyfikowania zagrożeń i reagowania na nie), działania mediów na rzecz bezpieczeństwa (budowanie i pogłębianie współpracy administracji i służb z mediami, prowadzenie działalności o charakterze edukacyjnym), przeciwdziałanie zagrożeniom dla → b e z p i e c z e ń s t w a d e m o g r a f i c z n e g o (zahamowanie obecnych niekorzystnych zmian demograficznych w kraju oraz prognozowanie przyszłych i zapobieganie im, umiejętnie prowadzona polityka prorodzinna, zatrudnienia, mieszkaniowa, emerytalna i migracyjna) oraz zapewnienie bezpieczeństwa socjalnego (zmniejszenie strefy ubóstwa i wykluczenia społecznego poprzez aktywizację osób zagrożonych tymi stanami, wsparcie ze strony instytucji pomocy społecznej, instytucji rynku pracy i służby zdrowia).

Bezpieczeństwo społeczne (nierzadko zestawiane z bezpieczeństwem socjalnym, ekonomicznym i publicznym) jest jedną z elementarnych potrzeb i wartości, których realizacja stanowi nie tylko odzwierciedlenie poszanowania godności ludzkiej w wymiarze czysto egzystencjalnym, ale także służy do opisu zjawisk i procesów mających bezpośrednie przełożenie na prawidłowy rozwój społeczeństwa oraz poziom skuteczności państwa i jego instytucji w ramach realizowanej polityki społecznej. Dlatego określenie istoty tego rodzaju bezpieczeństwa oraz jego współczesnych uwarunkowań wydaje się tak ważnym zadaniem, zwłaszcza z punktu widzenia reprezentantów nauk o bezpieczeństwie czy nauk o polityce i administracji. Nie ulega wątpliwości, że bezpieczeństwo społeczne jest niezwykle ważkim elementem każdej koncepcji bezpieczeństwa narodowego i w pewien sposób warunkuje jego charakter oraz określa istotę jego społecznego (socjalnego) wymiaru.

Paweł Łubiński

J. Gierszewski, *Bezpieczeństwo społeczne. Studium z zakresu teorii bezpieczeństwa narodowego*, Difin, Warszawa 2013; tenże, *Społeczne zagrożenia (social security) bezpieczeństwa państwa*, [w:] *Nauka o bezpieczeństwie. Istota, przedmiot badań i kierunki rozwoju. Studia i materiały*, t. 2, L. Grochowski, A. Letkiewicz, A. Misiuk (red.), Wydawnictwo Wyższej Szkoły Policji w Szczytnie, Szczytno 2011; B. Jagusiak, *Bezpieczeństwo socjalne współczesnego państwa*, Difin, Warszawa 2015; R. Jakubczak, *Charakter i dynamika zjawisk i procesów społecznych zagrażających stabilności wewnętrznej państwa*, [w:] *Wyzwania, szanse, zagrożenia i ryzyko dla bezpieczeństwa narodowego RP o charakterze wewnętrznym*, R. Jakubczak, B. Wiśniewski (red.), Wydawnictwo Wyższej Szkoły Policji w Szczytnie, Szczytno 2016; M. Leszczyński,

Bezpieczeństwo społeczne Polaków wobec wyzwań XXI wieku, Difin, Warszawa 2011; K. Loranty, *Bezpieczeństwo społeczne*, [w:] *Podstawy bezpieczeństwa narodowego (państwa)*, J. Pawłowski (red.), Akademia Sztuki Wojennej, Warszawa 2017; P. Łubiński, *Bezpieczeństwo społeczne*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; P. Łubiński, P. Dubiński, *Społeczny priorytet bezpieczeństwa państwa. Coaching jako narzędzie walki z bezrobociem*, [w:] *Bezpieczeństwo współczesnego świata. Uwarunkowania bezpieczeństwa narodowego*, M. Kosman, W. Stach (red.), Wydawnictwo Naukowe Wyższej Szkoły Handlu i Usług, Poznań 2013; A. Skrabacz, *Bezpieczeństwo społeczne. Podstawy teoretyczne i praktyczne*, Dom Wydawniczy Elipsa, Warszawa 2012; taż, *Uwarunkowania tworzenia bezpieczeństwa społecznego w XXI wieku*, [w:] *Bezpieczeństwo społeczne. Pojęcia – uwarunkowania – wyzwania*, A. Skrabacz, S. Sulowski (red.), Dom Wydawniczy Elipsa, Warszawa 2012; *Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej*, Biuro Bezpieczeństwa Narodowego, Warszawa 2014; D. Svyrydenko, O. Yatsenko, *A Social Security in Experience of Possibility*, [w:] *Wielowymiarowość kategorii bezpieczeństwa. Wymiar społeczny*, t. 1, K. Sygidus, P. Łubiński, D. Svyrydenko (red.), Wydawnictwo Bookmarked Publishing & Editing, Olsztyn–Kraków–Kijów 2018; K. Szewior, *Bezpieczeństwo społeczne jednostki. Założenia i polska rzeczywistość*, ASPRA-JR, Warszawa 2016; *Vademecum bezpieczeństwa wewnętrznego – społeczny wymiar bezpieczeństwa*, M.Z. Kulisz (red.), Oficyna Wydawnicza PWSZ w Nysie, Nysa 2019; *Współczesne bezpieczeństwo społeczne*, M. Kubiak, M. Minkina (red.), Wydawnictwo Naukowe UPH, Warszawa–Siedlce 2013.

BEZPIECZEŃSTWO SZKOLNE (BEZPIECZEŃSTWO W SZKOLE) – definiując bezpieczeństwo szkolne, należy spojrzeć na nie z perspektywy czynników, zasad → b e z p i e c z e ń s t w a oraz wyzwań, które mogą determinować przekształcenie danego zjawiska w szansę lub → z a g r o ż e n i e [t. 4]. Taki układ czynników (patrz: L.F. Korzeniowski, A. Pieczywok, Z. Ścibiorek, B. Wiśniewski, R.B. Kuc, A. Dawidczyk) określa się mianem → ś r o d o w i s k a b e z p i e c z e ń s t w a [t. 4] w szkole, które uwarunkowane jest współdziałaniem, partycypacją wszystkich podmiotów odpowiedzialnych za realizację celów i zadań edukacyjnych w danej placówce: dyrekcji, nauczycieli, uczniów, rodziców, pracowników administracyjnych szkoły, podmiotów zewnętrznych współpracujących ze szkołą, organów administracji samorządowej oraz społeczności lokalnej.

Kształtowanie tak rozumianego środowiska bezpieczeństwa w szkole wymaga formułowania celów w zakresie przeciwdziałania zagrożeniom, reagowania na wyzwania współczesnego świata oraz umożliwiania rozwoju zarówno uczniom, jak i nauczycielom. Działania oparte na powyższych założeniach wpisują się w holistyczne rozumienie bezpieczeństwa, które w literaturze opisywane jest jako stan i proces. Jako takie powinno być analizowane w wymiarach: pozytywnym i negatywnym, subiektywnym i obiektywnym oraz wewnętrznym i zewnętrznym (zob. → e d u k a c j a d l a b e z p i e c z e ń s t w a [t. 2]). Szczegółowy zakres działań związanych z kształtowaniem bezpieczeństwa szkolnego uregulowano w dokumentach ministerialnych, w tym w Ustawie z dnia 14 grudnia 2016 r. – Prawo oświatowe oraz rozporządzeniach wykonawczych Ministerstwa Edukacji Narodowej, jak również aktach prawnych funkcjonujących w obrębie innych resortów.

Zgodnie z Rozporządzeniem z dnia 31 grudnia 2002 r. w sprawie bezpieczeństwa i higieny w publicznych i niepublicznych szkołach i placówkach (z późn. zm.) osobą odpowiedzialną za bezpieczeństwo w szkole jest zawsze dyrektor. Jednoosobowa odpowiedzialność nie powinna jednak determinować prób jednoosobowego ustalania zasad i procedur bezpieczeństwa w placówce, jeśli działania takie mają być efektywne. Współczesne teorie psychologiczne (np. teoria wyznaczania celów E.A. Locke'a) oraz wybrane teorie pedagogiczne wpisują w ideał zarządzania bezpieczeństwem zasadę podmiotowości (zob: → z a r z ą d z a n i e p a r t y c y p a c y j n e b e z p i e c z e ń s t w e m [t. 4]), która zakłada aktywność i partycypację wszystkich uczestników procesu kształcenia i wychowania. Społeczność szkolna powinna współdziałać w procesie kształtowania bezpieczeństwa szkolnego, ponieważ bezpieczeństwo szkolne jest wspólną wartością i wspólnym (choć często odmiennie definiowanym) celem każdego jej członka. W związku z powyższym działania ukierunkowane na bezpieczeństwo szkolne powinny uwzględniać opinie wszystkich podmiotów funkcjonujących w placówce i przebiegać 3-etapowo, kolejnymi etapami są:

- diagnoza poczucia bezpieczeństwa i zagrożeń w grupie nauczycieli, uczniów oraz innych pracowników szkoły;
- wyjaśnienie przyczyn ewentualnych zagrożeń;
- współdziałanie wszystkich podmiotów funkcjonujących w szkole i poza nią podczas projektowania zasad oraz ewaluacji działań ukierunkowanych na poprawę poczucia bezpieczeństwa (uwzględniając opinie uczniów, rodziców, władz samorządowych, partnerów zewnętrznych, np. lokalnej jednostki → P o l i c j i [t. 3] i społeczności lokalnej).

Procedury bezpieczeństwa wypracowane w toku tej współpracy muszą być zaakceptowane przez każdego uczestnika procesu dydaktyczno-wychowawczego, zrozumiałe i szczegółowe, a ich coroczna modyfikacja determinowana jest ustawicznymi nowelizacjami w obszarze obowiązujących aktów prawnych. Procedury bezpieczeństwa mogą dotyczyć zasad np. rozpoczęcia i zakończenia zajęć, obecności w szkole osób niepowołanych, odbierania uczniów ze szkoły, samowolnego opuszczenia szkoły przez ucznia, organizacji zajęć dydaktycznych, korzystania z szatni szkolnej, bezpiecznego użytkowania sprzętu sportowego i szkolnych obiektów sportowych, postępowania z uczniem stwarzającym problemy wychowawcze uniemożliwiające prowadzenie zajęć, przechowywania w szkole substancji chemicznych (w pracowni chemicznej), organizacji i przeprowadzania wycieczek szkolnych, postępowania w sytuacji uzasadnionego podejrzenia, że wobec ucznia stosowana jest → p r z e m o c [t. 3], postępowania w sytuacji uzasadnionego podejrzenia, że uczeń jest sprawcą → a g r e s j i lub przemocy w szkole, postępowania w przypadku stwierdzenia posiadania i/lub palenia przez ucznia papierosów, spożywania alkoholu lub stosowania innych substancji odurzających, postępowania w stosunku do ucznia przejawiającego zachowania świadczące o demoralizacji, postępowania w sytuacji podejrzenia, że na terenie szkoły znajduje

się uczeń będący pod wpływem alkoholu, narkotyków lub innych środków odurzających, postępowania w sytuacji znalezienia na terenie szkoły substancji przypominającej swym wyglądem narkotyk lub inną substancję odurzającą, postępowania w sytuacji, gdy uczeń ma przy sobie substancję przypominającą narkotyk lub inną substancję odurzającą, postępowania w sytuacji, gdy zachowanie ucznia zagraża bezpieczeństwu, zdrowiu i życiu jego oraz innych osób.

Złożoność problematyki bezpieczeństwa szkolnego wymusza konieczność kompleksowego podejścia do tego zagadnienia. Zapewnienie bezpieczeństwa osobom przebywającym na terenie danej placówki jest uwarunkowane wieloma czynnikami. Wpływ na ten stan mają wspomniane już podmioty tworzące społeczność szkolną (m.in. dyrekcja, grono pedagogiczne i uczniowie), akty normatywne i wytyczne ministra oświaty (ustawy, rozporządzenia, zarządzenia, programy) oraz wewnątrzszkolne dokumenty (statuty, regulaminy, procedury, programy profilaktyczne i wychowawcze). Z uwagi na złożoność tych wpływów można wyszczególnić 3 kategorie uwarunkowań bezpieczeństwa szkolnego:

- instytucjonalne – prawo oświatowe, funkcjonowanie i organizacja pracy szkoły, rodzaj sprawowanego nadzoru pedagogicznego, miejsce i warunki lokalowe placówki, przynależność administracyjna;
- psychospołeczne – kompetencje zawodowe i psychospołeczne kadry pedagogicznej, atmosfera i relacje międzyludzkie;
- etyczne – cenione i uznawane wartości, postawy nauczycieli, dyrekcji, rodziców i uczniów.

Powyższy katalog podkreśla wyraźnie, że bezpieczeństwo szkolne ma wieloaspektowy wymiar, dlatego zasadne wydaje się regulowanie tego obszaru przez liczne akty normatywne z zakresu prawa oświatowego, cywilnego, pracy oraz karnego. Każdy z tych dokumentów podejmuje odrębne kwestie: prawo oświatowe dotyczy głównie funkcji dydaktycznej, opiekuńczej i wychowawczej szkoły; prawo pracy (w przypadku gdy nie obowiązuje Karta Nauczyciela) obejmuje prawa i obowiązki stron; prawo cywilne reguluje cywilnoprawną ochronę dóbr osobistych; prawo karne dotyczy czynów noszących znamiona zabronionych i podlegających karze.

Szczególne znaczenie dla statutowej działalności placówek oświatowych, z uwagi na pełnione przez nie funkcje (dydaktyczną, wychowawczą i opiekuńczą), ma art. 19 Konwencji o prawach dziecka w brzmieniu:

> Państwa-Strony będą podejmowały wszelkie właściwe kroki w dziedzinie ustawodawczej, administracyjnej, społecznej oraz wychowawczej dla ochrony dziecka przed wszelkimi formami przemocy fizycznej bądź psychicznej, krzywdy lub zaniedbania bądź złego traktowania lub wyzysku, w tym wykorzystywania w celach seksualnych dzieci pozostających pod opieką rodzica(ów) prawnego(ych) lub innej osoby sprawującej opiekę nad dzieckiem.

Konieczność zapewnienia bezpieczeństwa dzieciom (→ bezpieczeństwo dzieci) została również podkreślona w najważniejszym akcie prawnym

Rzeczypospolitej Polskiej – Konstytucji RP, w której można znaleźć kwestie dotyczące: ochrony prawnej życia, zakazu poddawania torturom oraz poniżającemu traktowaniu i karaniu, prawa do bezpiecznych i higienicznych warunków pracy czy też gwarancji ochrony praw dziecka. Problem przemocy wobec dzieci jest z kolei regulowany przez ustawę o przeciwdziałaniu przemocy w rodzinie, która uwzględnia sposób postępowania wobec osób stosujących przemoc (w tym również wychowawców placówek opiekuńczo-wychowawczych). Należy podkreślić, że w myśl Rozporządzenia Rady Ministrów z dnia 13 września 2011 r. w sprawie procedury „Niebieskie Karty" oraz wzorów formularzy „Niebieska Karta" każdy nauczyciel został zobligowany do wszczęcia procedury w sytuacji, gdy istnieje przypuszczenie, że uczeń może być ofiarą przemocy w rodzinie. W razie popełnienia czynu karalnego przez ucznia szkoły, który ma skończone 17 lat (lub w wyjątkowych sytuacjach – 15), należy stosować się do zapisów Ustawy z dnia 6 czerwca 1997 r. – Kodeks karny. W innych problematycznych przypadkach należy powołać się na Ustawę z dnia 26 października 1982 r. o postępowaniu w sprawach nieletnich.

Z uwagi na to, że dzieci i młodzież stanowią szczególnie wrażliwy podmiot bezpieczeństwa, podlegają one ochronie przewidzianej w art. 1 Ustawy o systemie oświaty z dnia 7 września 1991 r.:

> System oświaty zapewnia w szczególności […] utrzymywanie bezpiecznych i higienicznych warunków nauki, wychowania i opieki w szkołach i placówkach; […] upowszechnianie wśród dzieci i młodzieży wiedzy o bezpieczeństwie oraz kształtowanie właściwych postaw wobec zagrożeń i sytuacji nadzwyczajnych.

W tekście tego nadrzędnego dokumentu, na podstawie którego funkcjonuje cały system szkolny, można odnaleźć wiele kwestii odnoszących się do spraw bezpieczeństwa. Wśród nich należy wymienić: art. 1 pkt 10, art. 5 ust. 7, art. 33 ust. 2, art. 34a ust. 2, art. 39 ust. 1, art. 82 ust. 2 pkt 3. Dokument ten nakłada również na pracowników szkoły obowiązek powiadomienia odpowiednich organów w sytuacji, gdy dany uczeń uchyla się od obowiązku szkolnego lub obowiązku nauki. O bezpieczeństwie szkolnym szeroko traktuje też Rozporządzenie Ministra Edukacji Narodowej z dnia 21 maja 2001 r. w sprawie ramowych statutów publicznego przedszkola i publicznych szkół. Ważnym dokumentem poświęconym bezpieczeństwu w placówkach oświatowych jest Rozporządzenie Ministra Edukacji Narodowej i Sportu z dnia 31 grudnia 2002 r. w sprawie bezpieczeństwa i higieny w publicznych i niepublicznych szkołach i placówkach, które powierzyło główną rolę w zakresie zapewnienia tego stanu dyrektorom. W myśl rozporządzenia osoba kierująca placówką oświatową jest zobligowana do zapewnienia bezpiecznych warunków, w tym opracowania planów i wyjść ewakuacyjnych, jak również procedur postępowania w razie wypadku itp. W dokumencie tym wyszczególniono obowiązki dyrektorów w zakresie BHP, takie jak np.: troska o czystość i funkcjonalność pomieszczeń szkolnych, dbanie o stan techniczny

urządzeń i wszelkiego innego wyposażenia szkoły, zapewnienie właściwej temperatury, wentylacji i oświetlenia, udostępnienie instrukcji i regulaminów w widocznych miejscach, zabezpieczenie wyjść i ciągów schodowych, troska o równą nawierzchnię przejść i dróg, zapewnienie nadzoru pedagogicznego nad uczniami. O dużej odpowiedzialności dyrektorów za stan bezpieczeństwa kierowanych przez nich placówek mówi również inny dokument prawa oświatowego – Ustawa z dnia 26 stycznia 1982 r. – Karta Nauczyciela, stanowiący, że obowiązkiem dyrektorów jest:

> zapewnienie w miarę możliwości odpowiednich warunków organizacyjnych do realizacji zadań dydaktycznych i opiekuńczo-wychowawczych; zapewnienie bezpieczeństwa uczniom i nauczycielom w czasie zajęć organizowanych przez szkołę.

Działania te powinny być wspierane przez wszystkich nauczycieli, na co wskazują fragmenty Karty Nauczyciela oraz ustawy o systemie oświaty. Odpowiedzialność za bezpieczeństwo szkolne spoczywa również na organach prowadzących, które formalnie odpowiadają za działalność i funkcjonowanie podlegających im placówek.

Wśród aktów prawnych regulujących bezpieczeństwo szkolne znajdują się również takie, które podejmują problematykę profilaktyki uzależnień. Przykładem są: Ustawa z dnia 9 listopada 1995 r. o ochronie zdrowia przed następstwami używania tytoniu i wyrobów tytoniowych, Ustawa z dnia 24 kwietnia 1997 r. o przeciwdziałaniu narkomanii i Ustawa z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi oraz Rozporządzenie Ministra Edukacji Narodowej z dnia 18 sierpnia 2015 r. w sprawie zakresu i form prowadzenia w szkołach i placówkach systemu oświaty działalności wychowawczej, edukacyjnej, informacyjnej i profilaktycznej w celu przeciwdziałania narkomanii.

O bezpieczeństwie szkolnym traktuje też Rozporządzenie Rady Ministrów z dnia 12 maja 2008 r. zmieniające rozporządzenie w sprawie form i zakresu finansowego wspierania organów prowadzących w zapewnieniu bezpiecznych warunków nauki, wychowania i opieki w publicznych szkołach i placówkach.

Oprócz wyżej wymienionych ustaw i rozporządzeń dużą rolę w zapewnianiu bezpieczeństwa szkolnego odgrywają też ministerialne programy, takie jak np.: „Program Zapobiegania Niedostosowaniu Społecznemu i Przestępczości wśród Dzieci i Młodzieży", „Zero tolerancji dla przemocy w szkole", „Bezpieczna i przyjazna szkoła", „Szkoła przyjaźnie wymagająca", „Monitoring wizyjny w szkołach i placówkach", czy też „Bezpieczna+".

W trosce o zapewnienie bezpieczeństwa szkolnego oprócz stosowania się do wielu regulacji prawnych, przepisów, programów i zaleceń należy też uwzględnić wewnętrzny system bezpieczeństwa, który – odnosząc się do specyfiki danej placówki – może stanowić skuteczne narzędzie naprawcze. Ważne jest, by opracowanie wewnątrzszkolnych dokumentów (np. statutu, programu profilaktycznego i wychowawczego) było poprzedzone szczegółową diagnozą danej placówki oraz określeniem jej mocnych

i słabych stron w zakresie bezpieczeństwa. Istotne jest też włączenie samych uczniów w proces konstruowania zasad i procedur związanych z kreowaniem środowiska bezpieczeństwa szkolnego, co zaowocować może lepszym zrozumieniem zapisów i ich respektowaniem.

Reasumując, liczne regulacje prawne, mnogość programów i zasad dotyczących bezpieczeństwa szkolnego wskazują na szczególną wagę tego obszaru. Dzięki jednak wypracowanym schematom, nawiązywaniu sieci współpracy z różnymi podmiotami – takimi jak Policja, → S t r a ż M i e j s k a / G m i n n a) [t. 4], Straż Pożarna, poradnie psychologiczno-pedagogiczne, sądy rodzinne, poradnie profilaktyki i leczenia uzależnień, stacje sanitarno-epidemiologiczne, poradnie zdrowia psychicznego, komitety ochrony praw dziecka, ośrodki pomocy społecznej, Towarzystwo Rodzin i Przyjaciół Dzieci Uzależnionych, parafie, kluby sportowe, domy kultury czy organizacje młodzieżowe – i zdobytemu doświadczeniu urealnia się szansa na wyeliminowanie wielu negatywnych zjawisk i poprawę bezpieczeństwa w środowisku szkolnym.

Ewelina Włodarczyk, Magdalena Szumiec

K. Denek, *Ku dobrej edukacji*, Wydawnictwo Wyższej Szkoły Humanistycznej w Lesznie, Toruń–Leszno 2005; Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r., Dz. U. 1997, nr 78, poz. 483 (z późn. zm.); Konwencja o prawach dziecka, Dz. U. 1991, nr 120, poz. 526; L.F. Korzeniowski, *Podstawy nauk o bezpieczeństwie*, Difin, Warszawa 2017; A. Kusztelak, *Bezpieczeństwo dzieci i młodzieży – ważnym problemem każdej polskiej szkoły*, [w:] *Edukacja dla bezpieczeństwa – w rodzinie, szkole i pracy*, A. Zduniak, M. Kryłowicz (red.), Dom Wydawniczy Elipsa, Warszawa–Poznań 2004; E. Nerwińska, *Psychospołeczne uwarunkowania bezpieczeństwa w szkole*, ORE.edu.pl, Warszawa 2014; A. Pieczywok, *Wybrane problemy z zakresu edukacji dla bezpieczeństwa. Konteksty, zagrożenia, wyzwania*, AON, Warszawa 2011; Rozporządzenie Ministra Edukacji Narodowej i Sportu z dnia 31 grudnia 2002 r. w sprawie bezpieczeństwa i higieny w publicznych i niepublicznych szkołach i placówkach (z późn. zm.), Dz. U. 2003, nr 6, poz. 69; Rozporządzenie Ministra Edukacji Narodowej z dnia 11 sierpnia 2017 r. w sprawie wymagań wobec szkół i placówek (z późn. zm.), Dz. U. 2017, poz. 1611, Dz. U. 2019, poz. 1575; Rozporządzenie Ministra Edukacji Narodowej z dnia 14 lutego 2017 r. w sprawie podstawy programowej wychowania przedszkolnego oraz podstawy programowej kształcenia ogólnego dla szkoły podstawowej, w tym dla uczniów z niepełnosprawnością intelektualną w stopniu umiarkowanym lub znacznym, kształcenia ogólnego dla branżowej szkoły I stopnia, kształcenia ogólnego dla szkoły specjalnej przysposabiającej do pracy oraz kształcenia ogólnego dla szkoły policealnej, Dz. U. 2017, poz. 356; Rozporządzenie Ministra Edukacji Narodowej z dnia 18 sierpnia 2015 r. w sprawie zakresu i form prowadzenia w szkołach i placówkach systemu oświaty działalności wychowawczej, edukacyjnej, informacyjnej i profilaktycznej w celu przeciwdziałania narkomanii, Dz. U. 2015, poz. 1249; Rozporządzenie Ministra Edukacji Narodowej z dnia 21 maja 2001 r. w sprawie ramowych statutów publicznego przedszkola i publicznych szkół, Dz. U. 2001, nr 61, poz. 624; Rozporządzenie Ministra Edukacji Narodowej z dnia 30 stycznia 2018 r. w sprawie podstawy programowej kształcenia ogólnego dla liceum ogólnokształcącego, technikum oraz branżowej szkoły II stopnia, Dz. U. 2018, poz. 467; Rozporządzenie Rady Ministrów z dnia 12 maja 2008 r. zmieniające rozporządzenie w sprawie form i zakresu finansowego wspierania

organów prowadzących w zapewnieniu bezpiecznych warunków nauki, wychowania i opieki w publicznych szkołach i placówkach, Dz. U. 2008, nr 94, poz. 598; Rozporządzenie Rady Ministrów z dnia 13 września 2011 r. w sprawie procedury „Niebieskie Karty" oraz wzorów formularzy „Niebieska Karta", Dz. U. 2011, nr 209, poz. 1245; J. Stefanowicz, *Bezpieczeństwo współczesnych państw*, Wydawnictwo Pax, Warszawa 1984; M. Szumiec, *Zagrożenia w środowisku szkolnym i działania ukierunkowane na poprawę stanu bezpieczeństwa*, „Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate et Educatione Civili" 2018, nr 8; Z. Ścibiorek i in., *Bezpieczeństwo wewnętrzne. Podręcznik akademicki*, Wydawnictwo Adam Marszałek, Toruń 2017; Ustawa z dnia 14 grudnia 2016 r. – Prawo oświatowe, Dz. U. 2017, poz. 59; Ustawa z dnia 24 kwietnia 1997 r. o przeciwdziałaniu narkomanii, Dz. U. 1997, nr 75, poz. 468; Ustawa z dnia 26 października 1982 r. o postępowaniu w sprawach nieletnich, Dz. U. 1982, nr 35, poz. 228; Ustawa z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi, Dz. U. 1982, nr 35, poz. 230; Ustawa z dnia 26 stycznia 1982 r. – Karta Nauczyciela, Dz. U. 2018, poz. 967; Ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu przemocy w rodzinie, Dz. U. 2005, nr 180, poz. 14930; Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, Dz. U. 1997, nr 88, poz. 553; Ustawa z dnia 7 września 1991 r. o systemie oświaty, Dz. U. 2016, poz. 1943; Ustawa z dnia 9 listopada 1995 r. o ochronie zdrowia przed następstwami używania tytoniu i wyrobów tytoniowych, Dz. U. 1996, nr 10, poz. 55; P. Wachowiak, *Motywowanie pracowników*, [w:] *Podstawy zarządzania*, M. Strużycki (red.), Oficyna Wydawnicza SGH, Warszawa 2014; E. Włodarczyk, *Bezpieczeństwo szkolne*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; R. Zięba, *O tożsamości nauk o bezpieczeństwie*, „Zeszyty naukowe AON" 2012, nr 1.

BEZPIECZEŃSTWO TELEINFORMATYCZNE – inaczej bezpieczeństwo teleinformacyjne (ang. *information and communication technology security*) – pojęcie węższe znaczeniowo od terminu bezpieczeństwa informacyjnego, które dotyczy sposobu pozyskiwania dobrej jakości → i n f o r m a c j i [t. 2] oraz metod ochrony przed jej utratą. → B e z p i e c z e ń s t w o i n f o r m a c y j n e w praktyce jest utożsamiane przede wszystkim z podmiotem narażonym na brak dostępu do informacji lub ewentualną utratę mniej lub bardziej istotnych zasobów informacyjnych. W sensie negatywnym gwarantuje poufność, integralność i powszechność w zakresie dostępności informacji poprzez eliminację wszelkich zakłóceń i potencjalnych → z a g r o ż e ń [t. 4].

Współcześnie terminów bezpieczeństwa teleinformatycznego i bezpieczeństwa teleinformacyjnego używa się zamiennie. Jak słusznie zauważył K. Liderman, jesteśmy świadkami zacierania się istotnych różnic między bezpieczeństwem teleinformacyjnym a teleinformatycznym, czego odzwierciedleniem jest chociażby diametralna zmiana funkcji telefonu komórkowego, który przestał być wyłącznie narzędziem umożliwiającym komunikację. W XXI w. telefony komórkowe stały się również terminalami zapewniającymi dostęp do sieci komputerowej, wyposażonymi w nowoczesne technologie łączenia elementów sieci komputerowej poprzez łączność radiową (np. Bluetooth).

Postępująca digitalizacja życia współczesnych społeczeństw przyniosła istotne zmiany w postrzeganiu zagrożeń, co w konsekwencji doprowadziło do redefinicji bezpieczeństwa w ogóle oraz ewolucji pojmowania bezpieczeństwa państwa. Daje się

zauważyć wyraźne korelacje bezpieczeństwa państwa i bezpieczeństwa informacyjnego związanego z funkcjonowaniem obszarów takich jak siły zbrojne, energetyka, ekonomia, media, systemy transportowe, finansowe i → o c h r o n a z d r o w i a [t. 3], bazujących na systemach informatycznych. Upowszechnienie się technologii teleinformatycznych oraz wykorzystywanie komputerów i sieci na masową skalę niewątpliwie przyniosło realne korzyści, zarówno w sferze publicznej, jak i prywatnej. Niestety, w → c y b e r p r z e s t r z e n i uaktywnili się również terroryści, międzynarodowe grupy przestępcze, → h a k e r z y [t. 2], a tym samym cyberprzestrzeń stała się obszarem działań zakłócających funkcjonowanie państw. Pojawiające się nowe zagrożenia, związane bezpośrednio z informacją, udowodniły, że pojmowanie bezpieczeństwa informacyjnego wyłącznie w kategoriach negatywnych staje się niewystarczające i wymaga podejścia z uwzględnieniem aspektu pozytywnego, zgodnie z którym polityka ma gwarantować ochronę funkcjonujących w państwie systemów przy jednoczesnym umożliwieniu dalszego swobodnego rozwoju wszystkich podmiotów → s p o ł e c z e ń s t w a i n f o r m a c y j n e g o [t. 4].

Wraz z digitalizacją utrzymuje się nielogiczna tendencja do przeceniania → c y b e r b e z p i e c z e ń s t w a i równoczesnego deprecjonowania bezpieczeństwa informacyjnego. Jest to niezrozumiałe, → c y b e r a t a k i bowiem są niejednokrotnie zamachami informacyjnymi. Po pierwsze, przyglądając się wnikliwie obszarowi bezpieczeństwa teleinformacyjnego, można zauważyć, że nie jest możliwa polemika na jego temat bez odwołania się do bezpieczeństwa informacyjnego, gdyż jest to niezgodne chociażby ze standardami określonymi normą ISO/IEC 17799 (systemowe podejście do bezpieczeństwa informacji). Po drugie, informacja jest poniekąd zasobem strategicznym i istotnym czynnikiem produkcyjnym współczesnych podmiotów. Po trzecie, sektor informacyjny stał się głównym obszarem pozyskiwania większości dochodów państw współczesnych. Po czwarte, wszelkie systemy informacyjne związane z pozyskiwaniem i przetwarzaniem informacji będą implikować procesy decyzyjne w pozostałych sektorach funkcjonowania państwa i społeczeństwa. Po piąte, dezorganizacja systemów informacyjnych nie jest kosztowna, a rozgrywki pomiędzy przeciwnikami mogą przybrać formę → w a l k i i n f o r m a c y j n e j [t. 4].

Jak już wcześniej wspomniano, w zakres bezpieczeństwa informacyjnego wchodzi tzw. bezpieczeństwo teleinformatyczne/teleinformacyjne, odnoszące się do zakresu form wymiany informacji z wykorzystaniem konkretnych technicznych środków łączności, takich jak telefony komórkowe i stacjonarne, radiostacje, sieci komputerowe, telefaksy, wideotelefony, sieci i systemy teleinformatyczne itp. Bezpieczeństwo teleinformacyjne jest rozumiane także w kategoriach uzasadnionego poziomu zaufania, że podmiot nie poniesie strat wynikających z niepożądanego ujawnienia, zmiany bądź zniszczenia informacji. Rozpatrywane w aspekcie organizacyjnym, technicznym oraz prawnym, stanowi syntezę aktywności interdyscyplinarnego zespołu ekspertów. Nie może być zatem sprowadzone do jednorazowej procedury wdrażania konkretnych

zabezpieczeń, bezpieczeństwo teleinformatyczne to bowiem dynamiczny, wielokierunkowy i skomplikowany proces, który należy permanentnie kontrolować i dostosowywać do zmieniającej się rzeczywistości. Na ów rodzaj bezpieczeństwa składa się szereg procesów ukierunkowanych na zdefiniowanie, osiągnięcie oraz utrzymanie atrybutów bezpieczeństwa w systemach teleinformatycznych, a zatem zachowanie planowanego poziomu poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności.

Bezpieczeństwo teleinformatyczne jest bezpośrednio związane z bezpieczeństwem systemów komputerowych, danych elektronicznych, a także transmisji danych przesyłanych za pośrednictwem sieci teleinformatycznych. Sam termin jest stosowany na określenie systemów wykorzystywanych przez konkretne kręgi podmiotów (jednostki, państwa, organizacje rządowe, wojskowe, publiczne, przedsiębiorstwa itp.). W wybranych organizacjach i przedsiębiorstwach, zwłaszcza tych o strategicznym znaczeniu dla bezpieczeństwa państwa, stosuje się normatywny system zarządzania bezpieczeństwem informacji. System ten zapewnia poufność, dostępność i integralność danych, więc jest wdrażany na rzecz ochrony informacji oraz jej przetwarzania w systemach i sieciach teleinformatycznych. Procedura zarządzania bezpieczeństwem teleinformatycznym wymaga wykreowania specyficznej polityki bezpieczeństwa dla wykorzystywanych systemów komputerowych oraz wskazania klasy bezpieczeństwa danego systemu. Istotne są również działania polegające na monitorowaniu i nadzorowaniu zabezpieczeń, chociażby poprzez uwierzytelnianie użytkowników, analizę ryzyka oraz właściwe reagowanie na incydenty zagrażające bezpieczeństwu systemów operacyjnych.

Bezpieczeństwo teleinformatyczne jest związane z ochroną informacji na etapie jej przetwarzania, przechowywania i przekazywania poprzez systemy teleinformatyczne. Celem tak rozumianej ochrony jest zabezpieczenie informacji (nie komputerów) przed potencjalnym ujawnieniem (zwłaszcza danych poufnych), modyfikacją, utratą lub destrukcją. Informacja wymaga ochrony, ponieważ może mieć znaczenie strategiczne dla konkretnych podmiotów, stanowi podstawowy element procesów gospodarczych, politycznych, militarnych i społecznych. Ponadto ochronę informacji wymuszają obowiązujące regulacje prawne. Zgodnie z §5.1 Rozporządzenia Prezesa Rady Ministrów z 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego → b e z p i e c z e ń s t w o i n f o r m a c j i n i e j a w n y c h przetwarzanych w systemie teleinformatycznym zapewnia się poprzez implementację spójnego zbioru zabezpieczeń w celu zapewnienia poufności, integralności i dostępności tych informacji. Usługi świadczone w zakresie bezpieczeństwa teleinformatycznego obejmują zarówno telekomunikację, jak i informatykę, a polegają w głównej mierze na ocenie i kontroli ryzyka podejmowanego w związku z korzystaniem z komputerów, sieci komputerowych, przesyłaniem danych do zdalnych lokalizacji. Działania z zakresu bezpieczeństwa teleinformatycznego/teleinformacyjnego polegają na ochronie

systemów teleinformatycznych przed włamaniami, kradzieżą lub zniszczeniem danych i oprogramowania. Kluczowe w zakresie jego zapewnienia wydaje się sformułowanie zasad autoryzacji oraz kontroli dostępu do systemów, gromadzonych zasobów i oferowanych usług. Ponadto obligatoryjne jest określenie procedur podnoszenia stopnia dostępu do informacji, a także ustalenie właściwych uprawnień.

Pomimo podejmowanych wysiłków na rzecz udoskonalenia systemów teleinformatycznych oraz ze względu na wielowymiarowość wdrożonych rozwiązań w dalszym ciągu istniejące luki w zabezpieczeniach stanowią poważny problem dla wszystkich użytkowników sieci teleinformatycznych. Pojawiło się nawet odrębne zagrożenie w postaci tzw. phreakingu, wykorzystujące wspomniane luki w systemach teleinformatycznych, co może prowadzić do licznych nadużyć niekorzystnych dla wielu dziedzin aktywności instytucji państwowych.

Konstruowanie bezpiecznych, a zarazem efektywnych systemów teleinformatycznych i aplikacji stało się kluczowe dla funkcjonowania współczesnej gospodarki, biznesu, armii oraz dla właściwej realizacji ustawowych zadań jednostek administracji publicznej. Liczne próby usprawnienia systemów teleinformatycznych przyczyniły się do wypracowania określonych metod oceny bezpieczeństwa i analizy potencjalnych zagrożeń, różnych dla poszczególnych państw i podmiotów funkcjonujących w cyberprzestrzeni. Niestety, wdrożenie w pełni bezpiecznego systemu nie jest możliwe, nie tylko z uwagi na ryzyko wystąpienia standardowych usterek i błędów, ale także ze względu na dylemat określenia i spełnienia niekiedy sprzecznych oczekiwań podmiotów systemów teleinformatycznych. Pojawiające się w cyberprzestrzeni zagrożenia są wielowymiarowe, skomplikowane, o zasięgu transnarodowym, a nawet globalnym. Efektywne przeciwdziałanie zjawiskom zagrażającym bezpieczeństwu wymaga podejścia interdyscyplinarnego oraz podjęcia współpracy w wymiarze międzynarodowym, co jest niezwykle utrudnione z uwagi na różnice w poziomie rozwoju poszczególnych państw oraz ze względu na priorytety polityki bezpieczeństwa i → i n t e r e s y n a r o d o w e [t. 2]. Wypracowanie wspólnych mechanizmów jest w zasadzie niewykonalne, ponieważ każde ze współczesnych państw stosuje własne rozwiązania, zależne od posiadanych sił i środków. Nieudanymi próbami wdrożenia jednolitych procedur w zakresie przeciwdziałania zagrożeniom dla bezpieczeństwa teleinformatycznego/teleinformacyjnego było opracowanie w 2001 r. Konwencji Rady Europy o cyberprzestępczości, a także rewizja przepisów Międzynarodowych Regulacji Telekomunikacyjnych, dokonana podczas Światowej Konferencji Międzynarodowej Telekomunikacji (World Conference on International Telecommunications, WCIT-12) w Dubaju w 2012 r. Aktualizacji przepisów nie poparło wówczas 55 państw, w tym Polska, USA, Wielka Brytania, a także Szwecja.

Najbardziej powszechnymi zagrożeniami dla bezpieczeństwa teleinformatycznego są osoby bagatelizujące ustalone zasady bezpieczeństwa danego systemu, błędy w programach i → z ł o ś l i w e o p r o g r a m o w a n i e [t. 4], przerwy w łączach sieci

teleinformatycznych, nieprzewidywalne zjawiska losowe, → c y b e r p r z e s t ę p c z o ś ć , → c y b e r t e r r o r y z m, → c y b e r s z p i e g o s t w o, haking, → h a k t y w i z m [t. 2], a także *cyberwarfare* (wykorzystywanie cyberprzestrzeni do działań zbrojnych). Współczesne wydarzenia i tendencje stają się swoistym wyzwaniem dla państw w zakresie zagwarantowania szeroko pojętego bezpieczeństwa teleinformatycznego/teleinformacyjnego.

Julia Anna Gawęcka

A. Białas, *Bezpieczeństwo informacji i usług*, Wydawnictwa Naukowo-Techniczne, Warszawa 2006; J. Gawęcka, *Bezpieczeństwo teleinformatyczne*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; J. Janczak, A. Nowak, *Bezpieczeństwo informacyjne. Wybrane problemy*, AON, Warszawa 2013; K. Liderman, *Standardy w ocenie bezpieczeństwa teleinformatycznego*, „Biuletyn Instytutu Automatyki i Robotyki" 2002, nr 17; K. Liedel, *Bezpieczeństwo informacyjne jako element bezpieczeństwa narodowego*, 27.11.2008, Liedel.pl (dostęp 12.04.2019); L.F. Korzeniowski, *Podstawy nauk o bezpieczeństwie*, Difin, Warszawa 2012; M. Klimek, *Bezpieczeństwo teleinformatyczne i bezpieczeństwo informacji w przedsiębiorstwach budownictwa inżynieryjnego*, „Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach. Seria: Administracja i Zarządzanie" 2015, nr 105; M. Lakomy, *Zagrożenia dla bezpieczeństwa teleinformatycznego państw – przyczynek do typologii*, „Kwartalnik Naukowy OAP UW «e-Politikon»" 2013, nr 6; *Metodyka – Standard ISO/IEC 17799*, Security.dga.pl (dostęp 12.04.2019); Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego, Dz. U. 2011, nr 159, poz. 948.

BEZPIECZEŃSTWO USTROJOWE – część systemu → b e z p i e c z e ń s t w a w e w n ę t r z n e g o p a ń s t w a , organów władzy publicznej i instytucji państwowych, których zadaniem jest ochrona organizacji państwa. Bywa utożsamiane z bezpieczeństwem konstytucyjnym, gdyż jest bezpośrednio związane z przestrzeganiem prawa, a więc i zapisów konstytucji. Ma charakter polityczny, ponieważ dotyczy mechanizmów sprawowania władzy. Jak podaje M. Brzeziński, „bezpieczeństwo ustrojowe występuje w 3 modelowych odmianach: demokratycznej, totalitarnej i autorytarnej, które stanowią pochodne zróżnicowania systemów politycznych".

Bezpieczeństwo konstytucyjne (bezpieczeństwo ustrojowe) związane jest z przestrzeganiem prawa w państwie, którego rdzeniem jest ustawa zasadnicza – konstytucja (od łac. *constituo*, urządzać, ustanawiać, regulować). Jak podaje internetowa *Encyklopedia PWN*, to podstawowy akt ustrojowy państwa, całościowo określający strukturę państwa, system jego organów oraz sytuację prawną jednostki wobec władz publicznych. Głównymi cechami wyróżniającymi konstytucję są sprecyzowane podstawy ustroju politycznego państwa, ranga aktu o najwyższej mocy prawnej, nadrzędne miejsce w hierarchii aktów prawnych oraz jej charakter jako jedynej w swoim rodzaju ustawy zasadniczej.

Funkcje konstytucji obejmują:

- określenie ładu społeczno-instytucjonalnego i normatywnego państwa poprzez akty prawne w zakresie stosunków społecznych i politycznych zapobiegające chaosowi prawnemu;
- tworzenie prawnych gwarancji swobód i wolności obywatelskich, wpływających na identyfikowanie się obywateli z państwem i jego instytucjami oraz na procesy integracyjne społeczeństwa, konstytucja jest gwarantem politycznego ustroju państwa;
- konieczność działania zgodnie z prawem (dotyczy całego urządzenia państwa, w tym powoływania tylko organów przewidzianych w konstytucji), konstytucja stanowi ucieleśnienie społecznie akceptowanych idei, określa model państwa.

Stosowanie konstytucji oznacza wykorzystywanie określonych w konstytucji kompetencji przez organy w niej wyszczególnione i przez nią upoważnione lub uzyskiwanie kompetencji przez organy władzy publicznej do dokonywania aktów prawnych. Konstytucja ogranicza organom państwa pole podejmowania decyzji, a zarazem określa jego ustrój, porządek prawny, relacje pomiędzy instytucjami władzy, obowiązki oraz prawa i wolności obywatelskie. Jest podstawą porządku prawnego w państwie i jednocześnie wykładnikiem bezpieczeństwa ustrojowego. Określa system władzy, hierarchizuje jego organy, przypisuje im stosowne właściwości, mówiąc inaczej – stanowi porządek konstytucyjny w kraju, rozumiany jako zbiór reguł, na podstawie których funkcjonuje państwo.

Bezpieczeństwo konstytucyjne ma wymiar państwowy i społeczny. Obszarem jego zainteresowania w ujęciu państwowym jest ochrona organów władzy, prawnych procedur ich wyłaniania oraz zapewnienie warunków niezakłóconego funkcjonowania. Jego społeczny wymiar sprowadza się do stworzenia przez państwo prawnych gwarancji chroniących obywateli w istotnych sferach ich życia, zabezpieczając tym samym ich interesy i wolność.

W odniesieniu do państwa polskiego, zgodnie z definicją bezpieczeństwa ustrojowego W. Kitlera, polega ono na ochronie konstytucyjnego ustroju państwa, a więc norm ustalających: ustrój Rzeczypospolitej Polskiej, zasady pluralizmu politycznego, ustrój społeczno-gospodarczy, status prawny jednostki, wolności i obowiązki człowieka i obywatela, system prawny i proces legislacyjny w państwie oraz ochronę systemu prawnego.

Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 r. określa naczelne zasady porządku konstytucyjnego i chronione wartości. W zakresie ustroju politycznego są nimi: suwerenność narodu (art. 4); republikańska forma państwa prawnego (art. 1); demokratyczne państwo prawne (art. 2); podział władzy i równowaga władz (art. 10); reprezentacja polityczna; dwuizbowość parlamentu (art. 10 ust. 2); pluralizm polityczny (art. 11); zasada decentralizacji władzy publicznej (art. 15); ustanowienie samorządu terytorialnego (art. 16); wzajemna niezależność i współdziałanie państwa i kościołów

oraz związków wyznaniowych (art. 25); wolności i → p r a w a c z ł o w i e k a [t. 3] i obywatela (rozdział II); odrębność władzy sądowniczej oraz niezawisłość sądów i trybunałów (art. 173). Dobra chronione, które nie dotyczą ustroju politycznego, to: społeczna gospodarka rynkowa (art. 20); własność prywatna (art. 21) i wolność gospodarcza (art. 22).

Wyróżnia się instytucjonalny i prawny wymiar państwa, co oznacza, że państwo do ochrony porządku konstytucyjnego powołuje instytucje na podstawie prawa, które działają wg prawa i w celu ochrony prawa. Zatem ochrona porządku konstytucyjnego/ustrojowego to ochrona instytucji/ organów władzy w państwie, prawnych procedur ich wyłaniania oraz zapewnienie warunków, w których funkcjonują one w sposób niezakłócony.

Dla zapewnienia ochrony porządku konstytucyjnego państwa ważna jest zasada legalizmu – każdy czyn, który podlega karze, musi być zakazany przez prawo obowiązujące w czasie jego popełnienia. Wyklucza ona działanie prawa wstecz oraz tworzy prawne gwarancje ochrony praw obywateli. Obszar ochrony ogranicza środki mające charakter prawny, które mogą być stosowane przez państwo i jego instytucje do wykonywania zadań związanych z zapewnieniem bezpieczeństwa.

Drugą ważną zasadą jest zasada praworządności (art. 7), która oznacza, że „organy władzy publicznej działają na podstawie prawa i w granicach prawa". Normy prawne określające zakres zadań instytucji państwa oraz zakres uprawnień jego przedstawicieli najczęściej mają charakter ustawowy. Ważna dla zapewnienia stabilizacji funkcjonowania organów państwa jest stabilność prawa, co oznacza, że prawo stanowione powinno być stabilne i przewidywalne, a wyraża się to stworzeniem przez państwo prawnych gwarancji dla obywateli. Państwo chroni działalność obywateli w wielu żywotnych sferach życia, a zakres podstawowych wolności i praw obywatelskich jest szeroki i obejmuje ochronę wolności osobistych, praw politycznych i socjalnych.

Próba indywidualnego i powszechnego naruszenia porządku ustrojowego skutkuje odpowiedzialnością karną.

Przypadek indywidualnego naruszenia porządku ustrojowego, za który sprawca lub sprawcy mogą ponieść odpowiedzialność, znajduje się w art. 127 kk. Dotyczy on zamachu stanu. Z treści tego przepisu prawa wynika, że odpowiedzialności karnej, a dokładnie karze pozbawienia wolności na czas nie krótszy od lat 3, podlega ten, kto w celu usunięcia → p r z e m o c ą [t. 3] konstytucyjnego organu Rzeczypospolitej Polskiej podejmuje działalność zmierzającą bezpośrednio do urzeczywistnienia tego celu. Bezpieczeństwo ustrojowe gwarantuje również Ustawa z dnia 21 czerwca 2001 r. o stanie wyjątkowym, precyzująca zakres ograniczeń praw i wolności człowieka i obywatela, przez co obejmuje obowiązkiem ich przestrzegania nie tylko obywateli Rzeczypospolitej Polskiej, ale także cudzoziemców przebywających na terenie kraju.

Na mocy przywołanych ustaw zastosowanie określonych środków w razie → z a g r o ż e n i a [t. 4] pomoże przywrócić stan poprzedni.

A. Moroska-Bonkiewicz wskazuje, że bezpieczeństwo ustrojowe ma na celu ochronę przed zagrożeniami wymierzonymi w porządek konstytucyjny państwa, zapewnienie niezakłóconego funkcjonowania jego organów oraz wartości i norm określających charakter państwa, a także w szerszym ujęciu zapewnienie integralności terytorialnej, → s u w e r e n n o ś c i p a ń s t w a [t. 4] oraz stabilności społecznej.

Jeżeli ustrojowemu komponentowi bezpieczeństwa wewnętrznego przypisuje się ochronę porządku konstytucyjnego, czyli realizację zbioru zasad i wartości zapisanych w ustawie zasadniczej, a ta określa ustrój państwa, porządek prawno-instytucjonalny, relacje pomiędzy władzą ustawodawczą, wykonawczą i sądowniczą, obowiązki, prawa i wolności obywateli, to zagrożeniami dla bezpieczeństwa ustrojowego będą zwłaszcza próby zburzenia struktur państwa, dezorganizacja procesów decyzyjnych poszczególnych organów, ograniczanie lub łamanie praw i wolności obywatelskich oraz destabilizacja ładu politycznego.

Bezpieczeństwo konstytucyjne dotyczy sfery zarówno powszechnej (obywatelskiej), jak i jednostkowej, więc bywa dookreślane również pojęciem znacznie szerszym, mianowicie bezpieczeństwem wewnętrznym. Z tego punktu widzenia podstawowymi źródłami zagrożeń w tym obszarze są wewnętrzne napięcia w państwie powodowane balansowaniem elit i jednostek na pograniczu prawa, łamaniem przepisów i oszustwami oraz słaba skuteczność wymiaru sprawiedliwości, które podważają zaufanie obywateli do władzy. W wymiarze zewnętrznym zasadniczym źródłem zagrożeń bezpieczeństwa ustrojowego jest wszelka działalność obcych służb skierowana na struktury władzy (decyzyjne) państwa, a szczególnie → t e r r o r y z m [t. 4], którego zamiarem jest wywarcie presji na sprawujących władzę w celu uzyskania określonego ich zachowania.

Uogólniając, zagrożeniem dla bezpieczeństwa ustrojowego państwa będą próby zaburzenia struktur państwa oraz procesów decyzyjnych jego organów władzy, działalność ruchów ekstremistycznych i skrajnych, słabość → s p o ł e c z e ń s t w a o b y w a t e l s k i e g o [t. 4] (podatność na manipulację), niska sprawność wymiaru sprawiedliwości i → p r o k u r a t u r y [t. 3].

Podsystem porządku konstytucyjnego obejmuje organy władzy ustawodawczej, wykonawczej i sądowniczej, których działania koncentrują się na zapewnieniu ochrony organizacji państwa. Władzę ustawodawczą sprawują Sejm i Senat, realizujące funkcje:

- ustawodawczą, polegającą na stanowieniu, w drodze procedury legislacyjnej, aktów prawnych decydujących m.in. o zasadach funkcjonowania podstawowych dziedzin państwa, kluczowych dla jego porządku konstytucyjnego;
- kreacyjną, polegającą na bezpośrednim powoływaniu i odwoływaniu organów konstytucyjnych państwa oraz osób, które wchodzą w skład tych organów, a także egzekwowaniu ich odpowiedzialności;
- kontrolną, polegającą na kontroli działalności Rady Ministrów, głównie poprzez kontrolę wykonywania ustawy budżetowej, komisje śledcze, stałe i nadzwyczajne oraz procedury interpelacyjne.

Organami władzy wykonawczej w zakresie zapewnienia porządku konstytucyjnego są Prezydent Rzeczypospolitej Polskiej i Rada Ministrów. Prezydent zgodnie z zapisami Konstytucji RP jest gwarantem ciągłości władzy państwowej, czuwa nad przestrzeganiem konstytucji, stoi na straży suwerenności i bezpieczeństwa państwa oraz nienaruszalności i niepodzielności jego terytorium, natomiast Rada Ministrów prowadzi politykę wewnętrzną i zagraniczną, a ponadto m.in. zapewnia wykonanie ustaw, koordynuje i kontroluje prace organów administracji rządowej, zapewnia bezpieczeństwo wewnętrzne oraz zewnętrzne państwa, sprawuje ogólne kierownictwo w dziedzinie stosunków z innymi państwami i organizacjami międzynarodowymi, zawiera umowy międzynarodowe wymagające ratyfikacji oraz zatwierdza i wypowiada inne umowy międzynarodowe oraz sprawuje ogólne kierownictwo w dziedzinie obronności kraju.

Ważnymi podmiotami władzy wykonawczej w aspekcie zapewnienia porządku konstytucyjnego są → służby specjalne [t. 4], takie jak → Agencja Bezpieczeństwa Wewnętrznego, która współpracuje z → Policją [t. 3], Strażą Graniczną, → Służbą Ochrony Państwa [t. 4] i Żandarmerią Wojskową; → Agencja Wywiadu, → Służba Kontrwywiadu Wojskowego [t. 4], → Służba Wywiadu Wojskowego [t. 4] czy → Centralne Biuro Antykorupcyjne. Służby te podlegają bezpośrednio lub w określonym zakresie uprawnień Prezesowi Rady Ministrów, a ich działalność jest koordynowana przez niego lub przez ministra koordynatora służb specjalnych w przypadku jego powołania. Działalność tych służb podlega również kontroli Sejmu. Niezwykle ważną rolę w zakresie zapewnienia ochrony porządku konstytucyjnego odgrywa władza sądownicza, sprawowana przez sądy i trybunały, które są władzą odrębną i niezależną od innych władz. Funkcje organów władzy sądowniczej w zakresie ochrony porządku konstytucyjnego obejmują sądownictwo powszechne (w tym Sąd Najwyższy), Naczelny Sąd Administracyjny oraz, a może przede wszystkim, Trybunał Konstytucyjny.

Zadania ochrony bezpieczeństwa ustrojowego realizują również: Najwyższa Izba Kontroli, Rzecznik Praw Obywatelskich, Państwowa Inspekcja Pracy i Główny Inspektor Ochrony Danych Osobowych.

Współcześnie dylematy związane z bezpieczeństwem ustrojowym dotyczą zakresu władzy, jaki współczesna demokracja powinna posiadać w stosunku do własnych obywateli.

Danuta Kaźmierczak

L. Grosicki, K. Grosicka, P. Grosicki, *Organizacja i kierowanie instytucjami bezpieczeństwa wewnętrznego państwa*, Akademia Humanistyczna im. Aleksandra Gieysztora, Pułtusk 2013; W. Kitler, *Organizacja bezpieczeństwa narodowego RP w kontekście ochrony ładu wewnętrznego w państwie*, „Zeszyty Naukowe AON" 2013, nr 4 (93); Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia

1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r., Dz. U. 1997, nr 78, poz. 483 (z późn. zm.); M. Kopczewski, J.M. Krawczyk, *Wybrane elementy bezpieczeństwa wewnętrznego państwa na podstawie założeń „Strategii bezpieczeństwa narodowego Rzeczypospolitej Polskiej"*, „Doctrina. Studia Społeczno-polityczne" 2011, nr 8; P. Łubiński, *Bezpieczeństwo publiczne jako element bezpieczeństwa wewnętrznego – kategoryzacja, uwarunkowania, zależności*, [w:] *Współczesne uwarunkowania zarządzania bezpieczeństwem wewnętrznym państwa*, J. Falecki, R. Kochańczyk, P. Sowizdraniuk (red.), Szkoła Policji w Katowicach, Katowice 2018; A. Moroska-Bonkiewicz, *„Urząd Ochrony Konstytucji" jako organ bezpieczeństwa ustrojowego RFN. Problematyka funkcjonowania w Państwie Demokratycznym*, „Rocznik Bezpieczeństwa Międzynarodowego" 2013, nr 1 (7); A. Sęk, M. Róg, *Prawo a bezpieczeństwo. Analiza wybranych aspektów*, „Studia Prawnicze. Rozprawy i Materiały" 2017, nr 1 (20); Z. Ścibiorek i in., *Bezpieczeństwo wewnętrzne. Podręcznik akademicki*, Wydawnictwo Adam Marszałek, Toruń 2017.

BEZPIECZEŃSTWO W EKSPORCIE ZABYTKÓW – jednym z ważniejszych problemów w zakresie bezpieczeństwa kultury materialnej w Polsce jest zabezpieczenie zabytków i dzieł sztuki przed kradzieżami. Dwie największe (historycznie) grabieże dzieł sztuki, które dotknęły Polskę, nastąpiły podczas potopu szwedzkiego i II wojny światowej. Według Fundacji Odbudowy Zniszczeń Dokonanych w Czasie Potopu Szwedzkiego straty spowodowane przez wojska szwedzkie w Polsce w latach 1655–1660 wyniosły ok. 4 mld zł. Zniszczono całkowicie: 188 miast, 186 wsi, 81 zamków, 89 pałaców, 136 kościołów, 30 młynów, 10 browarów. Z kolei zgodnie z raportem o stratach poniesionych przez Polskę w wyniku → a g r e s j i [t. 1] i okupacji niemieckiej w czasie II wojny światowej szkody szacuje się na 235,48 mln dolarów. Z powyższych przyczyn Polska ma bardzo restrykcyjne przepisy dotyczące wywozu dzieł sztuki za granicę. Niektórzy ekonomiści twierdzą, że cierpi na tym rynek sztuki, gdyż rygorystyczne przepisy ograniczają promocję niektórych artystów za granicą. Zważywszy jednak na wyżej wspomnianą historyczną skalę zniszczeń oraz fakt, że nakaz strzeżenia dziedzictwa kulturowego jest wartością wpisaną do ustawy zasadniczej (np. art. 5 Konstytucji RP z dnia 2 kwietnia 1997 r.), warto dążyć do zachowania jak największej liczby dzieł w kraju. Polskie przepisy są więc skonstruowane tak, aby chronić dziedzictwo oraz kontrolować wywóz dzieł sztuki z kraju.

Wywóz zabytku za granicę na gruncie prawa polskiego ma rangę ustawową i następuje na podstawie pozwolenia wydawanego przez odpowiednie organy w formie decyzji administracyjnej. Istnieją 4 rodzaje pozwoleń, które mogą dotyczyć odpowiednio:

1) jednorazowego pozwolenia na stały wywóz zabytku za granicę;
2) jednorazowego pozwolenia na czasowy wywóz zabytku za granicę;
3) wielokrotnego pozwolenia indywidualnego na czasowy wywóz zabytku za granicę;
4) wielokrotnego pozwolenia ogólnego na czasowy wywóz zabytków za granicę.

Wymienione pozwolenia nie obejmują każdego cennego przedmiotu bądź dzieła sztuki, a jedynie przedmioty spełniające ustawową definicję zabytku (nieruchomość lub rzecz ruchoma, ich części lub zespoły będące dziełem człowieka albo związane

z jego działalnością i stanowiące świadectwo minionej epoki bądź zdarzenia, których zachowanie leży w interesie społecznym ze względu na posiadaną wartość historyczną, artystyczną lub naukową).

Zgodnie z obowiązującym prawem jednorazowego pozwolenia na stały wywóz zabytku za granicę wymagają zabytki zaliczane do jednej z następujących kategorii:

1) zabytki archeologiczne, które mają więcej niż 100 lat i wchodzą w skład zbiorów archeologicznych lub zostały pozyskane w wyniku badań archeologicznych bądź przypadkowych odkryć;
2) elementy, które stanowią integralną część zabytków architektury, wystroju wnętrz, pomników, posągów i dzieł rzemiosła artystycznego i które mają więcej niż 100 lat;
3) wykonane dowolną techniką i na dowolnym materiale dzieła malarstwa, nieobjęte kategoriami wskazanymi w pkt 4 i 5, które mają więcej niż 50 lat i ich wartość jest wyższa niż 40 tys. zł;
4) wykonane na dowolnym materiale akwarele, gwasze i pastele, które mają więcej niż 50 lat i ich wartość jest wyższa niż 16 tys. zł;
5) mozaiki nieobjęte kategoriami wskazanymi w pkt 1 i 2 oraz rysunki wykonane dowolną techniką i na dowolnym materiale, mające więcej niż 50 lat i o wartości wyższej niż 12 tys. zł;
6) oryginalne dzieła grafiki i matryce do ich wykonania oraz oryginalne plakaty, które mają więcej niż 50 lat i ich wartość jest wyższa niż 16 tys. zł;
7) oryginalne rzeźby, posągi lub ich kopie wykonane tą samą techniką, co oryginał, nieobjęte kategorią wskazaną w pkt 1, mające więcej niż 50 lat i o wartości wyższej niż 20 tys. zł;
8) pojedyncze fotografie, filmy oraz ich negatywy, które mają więcej niż 50 lat i ich wartość jest wyższa niż 6 tys. zł;
9) pojedyncze lub znajdujące się w zbiorach rękopisy, które mają więcej niż 50 lat i ich wartość jest wyższa niż 4 tys. zł;
10) pojedyncze lub znajdujące się w zbiorach książki, które mają więcej niż 100 lat i ich wartość jest wyższa niż 6 tys. zł;
11) pojedyncze mapy drukowane i partytury, które mają więcej niż 150 lat i ich wartość jest wyższa niż 6 tys. zł;
12) kolekcje i przedmioty z kolekcji zoologicznych, botanicznych, mineralnych lub anatomicznych o wartości wyższej niż 16 tys. zł;
13) kolekcje o znaczeniu historycznym, paleontologicznym, etnograficznym lub numizmatycznym, których wartość jest wyższa niż 16 tys. zł;
14) środki transportu, które mają więcej niż 50 lat i ich wartość jest wyższa niż 32 tys. zł;
15) inne kategorie niewymienione w pkt 1–14, obejmujące zabytki, które mają więcej niż 50 lat i ich wartość jest wyższa niż 16 tys. zł.

Prawo polskie przewiduje również grupę zabytków całkowicie wyłączonych z możliwości stałego wywozu za granicę. Są to dzieła wpisane do rejestru zabytków,

na Listę Skarbów Dziedzictwa, wchodzące w skład zbiorów publicznych, które stanowią własność Skarbu Państwa, jednostek samorządu terytorialnego lub innych jednostek organizacyjnych zaliczanych do sektora finansów publicznych, bądź zarejestrowane w inwentarzu muzeum albo w narodowym zasobie bibliotecznym. W wypadku tych przedmiotów prawo dopuszcza jedynie możliwość wywozu czasowego.

Osoba lub jednostka ubiegająca się o uzyskanie pozwolenia na wywóz zabytku za granicę składa wniosek do ministra właściwego do spraw kultury i ochrony dziedzictwa narodowego za pośrednictwem wojewódzkiego konserwatora zabytków. Wniosek taki każdorazowo zawiera imię, nazwisko, miejsce zamieszkania i adres wnioskodawcy albo nazwę, siedzibę i adres jednostki organizacyjnej będącej wnioskodawcą, określenie zabytku wraz z opisem umożliwiającym jego identyfikację, uzasadnienie wniosku. W wypadku wniosków czasowych konieczne jest również wskazanie okresu, na jaki ma zostać wydane pozwolenie. Do wniosku dołącza się 2 kolorowe fotografie zabytku o formacie nie mniejszym niż 9 cm na 13 cm oraz oświadczenie właściciela zabytku, że zgłoszony artefakt jest jego własnością, jest wolny od obciążeń prawa i nie podlega zajęciu w trybie przepisów o egzekucji sądowej lub o postępowaniu egzekucyjnym w administracji. Wojewódzki konserwator zabytków przed rozpatrzeniem wniosku dokonuje oględzin zabytku. Mogą być one dokonane w siedzibie organu bądź w miejscu, w którym przedmiotowy zabytek się znajduje. Na podstawie uzyskanego w ten sposób pozwolenia może nastąpić wywózdzieła za granicę, nie później jednak niż w terminie 12 miesięcy od uzyskania pozwolenia.

Ustawa z dnia 23 lipca 2003 r. o ochronie zabytków i opiece nad zabytkami daje ministrowi właściwemu do spraw kultury i ochrony dziedzictwa narodowego możliwość odmowy wydania jednorazowego pozwolenia na stały wywóz zabytku za granicę, jeśli dzieło ma szczególną wartość dla dziedzictwa kulturowego. Przepis ten nakłada niejako na organ obowiązek wnikliwej analizy przedstawionego w sprawie materiału dowodowego, aby każdorazowo zbadać zaistnienie przesłanki. Ustalenie jej wystąpienia pociąga bowiem za sobą nieodwracalne konsekwencje w postaci wywozu zabytku za granicę Polski na stałe. Potwierdzenie szczególnej wartości danego zabytku dla dziedzictwa kulturowego powinno wiązać organ co do skutku, tj. każdorazowo powinno determinować odmowę wydania pozwolenia wywozowego. Pogląd ten znajduje uzasadnienie z uwagi na konieczność ochrony doniosłej wartości, mającej również umocowanie konstytucyjne, wynikające z art. 5 Konstytucji RP, zgodnie z którym Rzeczpospolita Polska strzeże dziedzictwa narodowego, oraz powiązanej z celem komentowanych przepisów, jakim jest zapewnienie integralności zasobu zabytkowego. Innymi słowy, decyzja podjęta w przedmiotowym postępowaniu wywozowym staje się ostateczna i prawomocna. Co istotne, skutek w postaci wywozu zabytku za granice na stałe jest nieodwracalny. Dopiero po wnikliwej analizie zebranego w sprawie materiału dowodowego i wykluczeniu sytuacji, że przedmiotowy zabytek ma szczególną wartość dla dziedzictwa kulturowego, organ może wydać pozwolenie na wywóz obiektu za granicę na stałe.

Pozwolenia na wywóz za granicę nie wymagają:

1) zabytki nieobjęte kategoriami opisanymi powyżej, niewpisane do rejestru, na Listę Skarbów Dziedzictwa, do inwentarzy muzeów albo niewchodzące w skład narodowego zasobu bibliotecznego;
2) zabytki podlegające zwrotowi na terytorium państwa Unii Europejskiej na podstawie prawomocnego wyroku nakazującego zwrot zagranicznego narodowego dobra kultury, o którym mowa w Ustawie z dnia 25 maja 2017 r. o restytucji narodowych → d ó b r k u l t u r y [t. 2];
3) zabytki przywiezione z terytorium państwa niebędącego członkiem Unii Europejskiej, objęte procedurą odprawy czasowej lub procedurą uszlachetniania czynnego w rozumieniu przepisów prawa celnego;
4) zabytki przywiezione z terytorium państwa niebędącego członkiem Unii Europejskiej, objęte procedurą dopuszczenia do obrotu ze zwolnieniem od należności celnych przywozowych, jeżeli wywóz tych zabytków następuje przed upływem 5 lat od dnia dopuszczenia do obrotu;
5) zabytki przywiezione z terytorium państwa członkowskiego Unii Europejskiej na okres nie dłuższy niż 3 lata, jeżeli wywozu tych zabytków dokonuje się na terytorium państwa członkowskiego Unii Europejskiej;
6) zabytki przywiezione z zagranicy przez osoby korzystające z przywilejów lub immunitetów dyplomatycznych, w tym przywiezione w celu urządzenia wnętrz przedstawicielstw dyplomatycznych i urzędów konsularnych;
7) dzieła twórców żyjących niewpisane do inwentarzy muzeów albo niewchodzące w skład narodowego zasobu bibliotecznego;
8) dzieła twórców żyjących podlegające zwrotowi na terytorium państwa Unii Europejskiej na podstawie prawomocnego wyroku nakazującego zwrot zagranicznego narodowego dobra kultury, o którym mowa w ustawie o restytucji narodowych dóbr kultury;
9) zabytki przemieszczane przez terytorium Rzeczypospolitej Polskiej z terytorium państwa członkowskiego Unii Europejskiej na terytorium państwa niebędącego członkiem Unii Europejskiej i objęte kategoriami A.1–A.15 wymienionymi w załączniku do Rozporządzenia Rady (WE) nr 116/2009 z dnia 18 grudnia 2008 r. w sprawie wywozu dóbr kultury, jeżeli ich wartość jest niższa od progów finansowych wymienionych w pkt B tego załącznika (150 tys. euro w wypadku obrazów, 50 tys. euro w wypadku rzeźb, 30 tys. euro w wypadku akwareli, gwaszy i pasteli oraz 15 tys. euro w przypadku rycin, rysunków i fotografii);
10) zabytki, które mają zgodne z przepisami potwierdzenie wwozu wystawione przez organ celny lub Straż Graniczną.

Brak obowiązku posiadania pozwolenia na wywóz niektórych zabytków nie powoduje, że przedmioty o mniejszej wartości mogą być wywożone za granicę całkowicie bez żadnej kontroli. W wypadku wywozu zabytków o mniejszej wartości, jeżeli

czynność ta jest dokonywana bez pozwolenia, a cechy dzieła sztuki wskazują, że jego wywóz może wymagać pozwolenia, organ Straży Granicznej lub organ celny może zażądać od osoby dokonującej wywozu zabytku okazania dokumentu potwierdzającego fakt, że wywożony artefakt nie wymaga pozwolenia.

Ewa Durek

Z. Cieślik i in., *Ustawa o muzeach. Komentarz*, Wolters Kluwer, Warszawa 2021; P. Dobosz, *Administracyjnoprawne instrumenty kształtowania ochrony zabytków*, Oficyna Wydawnicza „Dajwór", Kraków 1997; D. Folga-Januszewska, *Zasady wypożyczania obiektów i współpracy między muzeami w krajach UE*, „Muzealnictwo" 2005, nr 46; A. Gerecka-Żołyńska, *Międzynarodowa ochrona dziedzictwa kulturowego a działalność muzeów*, [w:] *Prawo muzeów*, J. Włodarski, K. Zeidler (red.), Wolters Kluwers business, Warszawa 2008; P. Gwoździewicz-Matan, *Wypożyczenia dzieł sztuki. Zalecenia międzynarodowe*, „Opolskie Studia Administracyjno-Prawne" 2012, nr 3; Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U. 1997, nr 78, poz. 483; W. Pływaczewski, B. Gadecki, *Ochrona dziedzictwa kulturowego i naturalnego. Perspektywa prawna i kryminologiczna*, C.H. Beck, Warszawa 2015; *Prawo wobec kultury i sztuki*, J. Sobczak, K. Chałubińska-Jentkiewicz, K. Kakareko (red.), Wolters Kluwer, Warszawa 2018; P. Rosik, *Zagranica niechętnie kupuje polską sztukę, wszystko przez złe prawo i postawę urzędników*, 7.05.2022, https://strefainwestorow.pl/artykuly/inwestycje-alternatywne/20220507/polska-sztuka-inwestowanie-eksport-dziel-ograniczenia-prawo (dostęp 15.04.2023); Rozporządzenie Rady (WE) nr 116/2009 z dnia 18 grudnia 2008 r. w sprawie wywozu dóbr kultury, Dz.Urz. UE L 39 z 10.02.2009; strona Małopolskiego Wojewódzkiego Urzędu Ochrony Zabytków, https://www.wuoz. malopolska.pl/poradnikmwkz/ (dostęp 15.04.2023); Ustawa z dnia 23 lipca 2003 r.o ochronie zabytków i opiece nad zabytkami, Dz.U. 2003, nr 162, poz. 1568; Ustawa z dnia 25 maja 2017 r. o restytucji narodowych dóbr kultury, Dz.U. 2017, poz. 1086; K. Zalasińska, *Ustawa o ochronie zabytków i opiece nad zabytkami. Komentarz*, C.H. Beck, Warszawa 2020.

BEZPIECZEŃSTWO W KAMPANIACH WYBORCZYCH – ogół problemów i zagadnień odnoszących się do problematyki → b e z p i e c z e ń s t w a, które podejmowane są w toku kampanii poprzedzającej wybory parlamentarne, prezydenckie, samorządowe lub europejskie. Kampania wyborcza to działania, za pomocą których partie polityczne, sojusze, koalicje i kandydaci przekazują swoje programy wyborcze potencjalnym wyborcom w formie manifestu lub programu wyborczego. Ten ostatni określa zakres planów, które partie lub kandydaci zamierzają wdrożyć, jeśli zostaną wybrani. Podejmowanie zagadnień dotyczących bezpieczeństwa w kampaniach wyborczych wynika z faktu, że ta grupa problemów znajduje się na ogół w centrum zainteresowania potencjalnych wyborców, ponadto większość podmiotów uczestniczących w wyborach ma swoje stanowisko w odniesieniu do najistotniejszych kierunków działań związanych z bezpieczeństwem. Kampania wyborcza z uwagi na skalę medialnego nagłośnienia ma też wpływ na kształtowanie się → o p i n i i p u b l i c z n e j [t. 3], stanowiąc przyczynek do licznych debat i dyskusji.

To, że problematyka bezpieczeństwa jest uznawana przez wyborców za istotną, znajduje potwierdzenie w licznych badaniach opinii publicznej. Z badań przeprowadzonych w Polsce w 2015 r. wynika, że → z a g r o ż e n i e [t. 4] → t e r r o r y z m e m

[t. 4] w Polsce jest w odczuciu społecznym poważniejsze niż przed laty. Ankietowani na ogół sceptycznie odnoszą się do kompetencji władz i instytucji państwowych w zakresie bezpieczeństwa. Poza terroryzmem Polacy przywiązywali dużą wagę do problematyki bezpieczeństwa także w związku z wydarzeniami w Ukrainie. 75% Polaków wyrażało niepokój, że konflikt w Ukrainie zagrozi bezpieczeństwu Polski, 67% widziało w nim zagrożenie dla Europy, a 55% uważało, że wydarzenia te zaburzą światowy porządek. Ponadto z badań wynika, że prawie połowa badanych Polaków czuła się osobiście zagrożona → p r z e s t ę p c z o ś c i ą [t. 3]. Jeszcze częściej ankietowani obawiają się o bezpieczeństwo swoich najbliższych (58%). → Za g r o ż e n i e b e z p i e c z e ń s t w a [t. 4] dla badanych Polaków wiązało się także z perspektywą przyjęcia w Polsce uchodźców. Osoby, które uzasadniały swój sprzeciw strachem, odwoływały się do różnego rodzaju obaw. Najczęściej bardzo ogólnie twierdziły, że uchodźcy stanowiliby zagrożenie albo że są niebezpieczni. W związku z przedstawionymi wynikami badań opinii można uznać, że zagadnienia bezpieczeństwa, w wielu różnych kontekstach, obecne są w obszarze zainteresowań Polaków. Także większość podmiotów biorących udział w wyborach wypowiada się w swoich programach wyborczych, w czasie spotkań z wyborcami oraz w mediach na tematy dotyczące bezpieczeństwa państwa, problematyki → b e z p i e c z e ń s t w a l o k a l n e g o czy → b e z p i e c z e ń s t w a e u r o p e j s k i e g o .

R.M. Perloff wskazuje, że media zajmują centralne miejsce we współczesnych kampaniach wyborczych. Programy informacyjne, reklamy wyborcze, debaty czy blogi polityków są głównym komunikacyjnym pasem transmisyjnym pomiędzy wyborcami a ubiegającymi się o urząd. Ewolucja mediów – w szczególności rozwój technologii opierający się na internecie i aplikacjach cyfrowych – zasadniczo zmieniły sposób, w jaki funkcjonują kampanie polityczne. Promowanie swojego programu, także odnoszącego się do zagadnień dotyczących bezpieczeństwa, nie może już opierać się wyłącznie na → m e d i a c h t r a d y c y j n y c h [t. 3] i → s t r a t e g i a c h [t. 4] kampanii przedinternetowych, ale aby wygrać wybory, ich uczestnicy muszą prowadzić kampanię, w której odbiorcy i potencjalni wyborcy znajdują się w środowisku cyfrowym. Rozwiązania związane z wykorzystaniem internetu doprowadziły do znacznych zmian w sposobie prowadzenia kampanii. Wyborcy nie są już biernymi członkami publiczności, którzy muszą czekać na informacje. Internet zmienił wyborców w aktywnych odbiorców, a także twórców → i n f o r m a c j i [t. 2]. Rozwiązania te pozwalają na selektywne adresowanie treści kampanijnych oraz interaktywność, które były ograniczone przez większość tradycyjnych formatów środków masowego przekazu, a pozwalają na szerokie zaangażowanie odbiorców w sformalizowany dotąd system polityczny. Nowe środowiska mediów interaktywnych zachęcają do tworzenia sieci, organizacji, kreowania nowych przestrzeni i powstawania nowych typów społeczności. Dzięki forom wyborcy mogą stać się integralną częścią kampanii cyfrowych. Ponadto powszechny i niedrogi dostęp do internetu, technologii mobilnych

i innych tanich, popularnych narzędzi technologicznych zapewnia wyborcom więcej informacji i możliwości zaangażowania. W miarę rozwoju technologii komunikacyjnych narzędzia cyfrowe, takie jak streaming, i możliwość publikowania materiałów wideo w sieci, portale społecznościowe, strony internetowe kandydatów i aplikacje mobilne stały się niezbędnymi elementami kampanii wyborczych.

Niejednokrotnie zwraca się uwagę na odmienne relacjonowanie kampanii wyborczej w mediach publicznych i prywatnych. Dotyczy to także problematyki bezpieczeństwa. Dzieje się tak, ponieważ partia lub koalicja rządząca często wywiera wpływ na media publiczne, aby działały w sposób bardziej stronniczy. Działania takie są zwykle łagodzone przez kodeksy postępowania mediów, zgodnie z którymi harmonogram czasu przeznaczonego dla partii i kandydatów jest regulowany określonymi przepisami lub zasadami. Tematyka dotycząca bezpieczeństwa z uwagi na fakt, że część zagadnień z tego obszaru ma charakter niejawny, częściej bywa podejmowana przez ugrupowania już sprawujące władzę, mające dostęp do danych, do których partie i kandydaci niesprawujący żadnych funkcji w państwie mogą nie mieć dostępu. Z drugiej strony aktorzy polityczni będący w opozycji i pretendujący do przejęcia władzy mają szerokie możliwości krytyki prowadzonej polityki, wykorzystując niejawność niektórych danych i wyolbrzymiając krytyczne oceny działań swoich przeciwników politycznych.

Popularność oraz wzrost znaczenia problematyki bezpieczeństwa wynikające w równej mierze z zagrożeń takich jak terroryzm, spadek stabilności otoczenia międzynarodowego czy przestępczość, co z samego subiektywnego poczucia bezpieczeństwa, sprawiają, że tematyka bezpieczeństwa stanowi bardzo często element obecny w kampaniach wyborczych w internecie. Daje ona duże możliwości prezentacji w formie filmów, które odpowiednio skonstruowane i umieszczone w internecie mogą tanio, szybko i skutecznie dotrzeć do szerokiego grona odbiorców, łatwo generując tysiące wyświetleń, polubień i udostępnień. W internecie za pośrednictwem portali społecznościowych powstają także ogromne sieci zwolenników i przeciwników zgromadzone wokół problemów i pomysłów odnoszących się do określonych kwestii z zakresu bezpieczeństwa. Kampanie wykorzystują polubienia milionów „przyjaciół" kandydatów, komentarze i tweety wygenerowane na portalach społecznościowych w celu przekształcenia entuzjastycznych uczestników w aktywnych wyborców, popierających nie tylko dane rozwiązanie, ale także kandydata lub partię. Wybrane zagadnienia odnoszące się do bezpieczeństwa – od koncepcji zbudowania nowej drogi w kampaniach lokalnych po rozwiązania dotyczące modernizacji sił zbrojnych czy zawarcia strategicznego sojuszu z określonym państwem – znakomicie nadają się do prezentacji na internetowych stronach kandydujących polityków i ugrupowań politycznych oraz w wytworzonych na potrzeby kampanii aplikacjach mobilnych.

W okresie kampanii wyborczej komunikacja odbywająca się za pośrednictwem mediów – od programów informacyjnych po rozrywkowe – odgrywa szczególną rolę. Nie tylko dostarcza ona informacji o kandydatach i programach politycznych, lecz

także kreuje perspektywy oceny rozmaitych kwestii związanych z bezpieczeństwem. Przekazy medialne w tym okresie stymulują także rozmowy toczone między przyjaciółmi czy nieznajomymi w miejscach publicznych, tworząc platformę ofert wyboru politycznego, a także stanowią społecznie autorytatywne źródło i ramy kampanijnych tematów będących przedmiotem debaty publicznej.

Rafał Klepka

W. Benoit, *Political Election Debates: Informing Voters about Policy and Character*, Lexington Books, Lanham 2013; F. Esser, J. Strömbäck, C.H. De Vreese, *Reviewing Key Concepts in Research on Political News Journalism: Conceptualizations, Operationalizations, and Propositions for Future Research*, „Journalism" 2011, vol. 13, no. 2; S. Hjarvard, *The Mediatization of Culture and Society*, Routledge, London–New York 2013; R. Klepka, *Bezpieczeństwo jako temat prezydenckiej i parlamentarnej kampanii wyborczej w relacjach Wiadomości TVP*, [w:] *Współczesne problemy bezpieczeństwa państwa*, O. Wasiuta, P. Mazur (red.), Katolicki Uniwersytet Lubelski Jana Pawła II w Lublinie, Stalowa Wola 2017; tenże, *Bezpieczeństwo w kampaniach wyborczych w internecie*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; tenże, *Bezpieczeństwo w kampaniach wyborczych*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; R. Perloff, *The Dynamics of Political Communication: Media and Politics in a Digital Age*, Routledge, New York–London 2013; L. Ricke, *Campaigns, Digital*, [w:] *Encyclopedia of Social Media and Politics*, K. Harvey (ed.), Sage, Los Angeles 2011.

BEZPIECZEŃSTWO W SIECI – zespół zagadnień związanych z takim korzystaniem z internetu, które pozwala unikać → z a g r o ż e ń [t. 4] zarówno w wymiarze prywatnym, jak i publicznym; jednostkowym, państwowym i międzynarodowym. W szerszym ujęciu bezpieczeństwo w sieci można analizować, koncentrując się na systemach teleinformatycznych oraz danych i → i n f o r m a c j a c h [t. 2], które są w nich tworzone, przechowywane, przetwarzane i wymieniane. W węższym ujęciu skupiamy się na użytkowniku i jego kompetencjach cyfrowych oraz wiedzy i świadomości dotyczącej potencjalnych ryzykownych sytuacji, jakie mogą się pojawić w wirtualnym świecie, a także umiejętności identyfikacji groźnych incydentów i właściwego reagowania na nie. Oba ujęcia należy traktować komplementarnie, ponieważ nieodzowne jest zapewnienie bezpieczeństwa zarówno w pierwszym, jak i w drugim aspekcie.

Bezpieczeństwo w sieci interesuje naukowców nie od dziś. Przykładowo blisko 2 dekady temu przebadano pod tym kątem ponad 0,5 tys. szkół podstawowych i średnich w Anglii. Okazało się, że w większości szkół uczono bezpiecznego użytkowania internetu, głównie w ramach przedmiotu ICT (ang. *information and communication technologies*, → t e c h n o l o g i e i n f o r m a c y j n o - k o m u n i k a c y j n e [t. 4]). W podobnym czasie badania wykazały, że blisko połowa rodziców w Irlandii i zdecydowana większość w Kanadzie była zdania, że szkoły powinny zapewniać taką wiedzę. Ostatnia dekada w Polsce przyniosła wg GUS wzrost dostępu do internetu w gospodarstwach domowych z dziećmi z 61,4% do 99,2%. Tendencje zwyżkowe

związane z powszechnością internetu, a wraz z tym zjawiskiem – z wielością szans i zagrożeń – odnoszą się nie tylko do Polski.

Dane wskazują, że globalny rozwój cyfrowy nie ustaje. Na całym świecie na początku 2021 roku z internetu korzystało 4,66 mld osób (59,5% globalnej populacji) i każdego dnia do wirtualnego świata dołącza milion nowych użytkowników. Wzrost ten wyraźnie napędza korzystanie z mediów społecznościowych, które skupiają 4,2 mld ludzi, czyli aż 53,6% ludzi żyjących na Ziemi. Średni czas spędzany każdego dnia online wynosi 7 godz., w trakcie których użytkownicy sieci głównie wyszukują informacje, oglądają filmy i inne materiały, odwiedzają portale społecznościowe oraz grają w gry. Coraz więcej osób kupuje wszelkiego rodzaju dobra konsumpcyjne za pośrednictwem handlu elektronicznego (*e-commerce*) – liczba ta obejmuje 77% osób od 16 do 64 lat.

Powyższe dane świadczą o ogromnej popularności internetu, który stał się nieodłączną częścią życia olbrzymich rzesz ludzi na całym świecie. W tej sytuacji zasadne jest pytanie o to, czy aktywność użytkowników sieci na pewno spełnia kryteria bezpieczeństwa.

Reagowaniem na incydenty mogące powodować zagrożenia w internecie oraz propagowaniem bezpiecznego korzystania z tego medium zajmuje się CERT (Computer Emergency Response Team). Zespół ten funkcjonuje w Polsce już od 1996 r. w ramach NASK (Naukowa i Akademicka Sieć Komputerowa), państwowego instytutu badawczego nadzorowanego przez Ministerstwo Cyfryzacji, który m.in. prowadzi całodobową obsługę incydentów, wspierając przedsiębiorców oraz obywateli w przeciwdziałaniu zagrożeniom teleinformatycznym, tworzy dobre praktyki i analizy strategiczne dotyczące → c y b e r b e z p i e c z e ń s t w a i gospodarki cyfrowej, podejmuje współpracę i wymianę informacji między sektorem prywatnym i publicznym oraz zajmuje się badaniami i rozwojem cyberbezpieczeństwa.

Główne zadania zespołu CERT Polska to:

- rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo sieci;
- reagowanie w przypadku pojawienia się bezpośrednich zagrożeń dla użytkowników;
- współpraca z innymi zespołami CERT/CSIRT (Computer Security Incident Response Team) w Polsce i na świecie;
- udział w krajowych i międzynarodowych projektach poświęconych → b e z p i e c z e ń s t w u t e l e i n f o r m a t y c z n e m u ;
- prowadzenie badań nad metodami wykrywania incydentów bezpieczeństwa, analizy → z ł o ś l i w e g o o p r o g r a m o w a n i a [t. 4] i systemów wymiany informacji dotyczącej zagrożeń;
- rozwijanie narzędzi do wykrywania, monitorowania, analizy i korelacji tych zagrożeń;
- regularne publikowanie raportów o bezpieczeństwie polskich zasobów internetu;

- działania informacyjno-edukacyjne mające na celu zwiększenie świadomości w zakresie bezpieczeństwa teleinformatycznego, w tym publikacja informacji o bezpieczeństwie na blogu Cert.pl oraz w serwisach społecznościowych Facebook i Twitter;
- cykliczna organizacja konferencji SECURE i nadzór merytoryczny nad nią;
- sporządzanie niezależnych analiz i testów rozwiązań z dziedziny bezpieczeństwa teleinformatycznego.

W 2018 r. najczęstszymi typami niebezpiecznych incydentów były: → p h i s h i n g [t. 3] (czyli oszustwo polegające na podszywaniu się pod inną osobę lub instytucję, aby wyłudzić poufne informacje, np. numer karty kredytowej, w celu kradzieży), dystrybucja złośliwego oprogramowania oraz spam. Liczba zgłaszanych incydentów w sieci wzrasta, co może świadczyć nie tylko o tym, że jest coraz więcej zagrożeń w wirtualnym świecie, ale być może i o tym, że wzrasta świadomość społeczna w tym zakresie. Jednak przypadki osób poszkodowanych, wykorzystanych bądź oszukanych w internecie są bardzo liczne, co uzasadnia konieczność podejmowania prac dotyczących zarówno przeciwdziałania, jak i profilaktyki.

Warto w tym miejscu wspomnieć, że NASK prowadzi również działalność informacyjną, edukacyjną, szkoleniową i popularyzatorską związaną z zastosowaniem nowoczesnych technologii w → s p o ł e c z e ń s t w i e i n f o r m a c y j n y m [t. 4] oraz z przeciwdziałaniem wykluczeniu cyfrowemu. W strukturach tej sieci funkcjonuje bowiem Akademia NASK, która zajmuje się kwestią bezpieczeństwa internetu, skupiająca szczególną uwagę na najmłodszych internautach. Ponadto w ramach IT Szkoły prowadzi studia e-learningowe w zakresie teorii oraz zastosowań technologii informacyjno-komunikacyjnych (ICT). Akademia realizuje zarówno projekty niekomercyjne, jak i kursy oraz szkolenia skierowane do instytucji czy przedsiębiorstw. Spośród głównych działań można wymienić organizację akcji edukacyjnych dla dzieci i młodzieży mających na celu rozwijanie ich kompetencji w zakresie technologii informacyjno-komunikacyjnych, a także budowanie świadomości o zagrożeniach internetowych. Poza działaniami poświęconymi uczniom Akademia opracowuje programy i scenariusze dla nauczycieli, aby zwiększyć ich wiedzę dotyczącą wykorzystywania nowoczesnych technologii i multimediów w dydaktyce. Ponadto prowadzi szkolenia i seminaria dla przedstawicieli wymiaru sprawiedliwości, poruszające tematykę profilaktyki i zwalczania → c y b e r p r z e s t ę p c z o ś c i , zwłaszcza w kontekście bezpieczeństwa dzieci i młodzieży. Akademia NASK organizuje również szkolenia eksperckie, konkursy, inicjatywy przeciwdziałające wykluczeniu społecznemu (np. dla seniorów niemających dostępu do sieci), tworzy interaktywne projekty multimedialne i współpracuje z różnymi ośrodkami edukacyjnymi.

Spośród kluczowych przedsięwzięć Akademii należy wyróżnić koordynowanie (współtworzonego z Fundacją Dajemy Dzieciom Siłę) Polskiego Centrum Programu Safer Internet (PCPSI), tworzonego w ramach projektu Komisji Europejskiej Safer

Internet. Cele zakładające edukację i propagowanie postaw dzieci sprzyjających kreowaniu internetu jako bezpiecznego i przyjaznego miejsca realizuje się we współpracy z również funkcjonującym w strukturach NASK Zespołem Dyżurnet.pl, który odpowiada za przeciwdziałanie szkodliwym i nielegalnym treściom w internecie (bazując na zgłoszeniach użytkowników). Dodatkowo Centrum każdego roku organizuje międzynarodową konferencję „Bezpieczeństwo dzieci i młodzieży w internecie" oraz ogólnoświatowy Dzień Bezpiecznego Internetu.

Poza rozwiązaniami technicznymi oraz wyzwaniami legislacyjno-organizacyjnymi konieczne jest opracowywanie przepisów prawnych odnoszących się do szeroko pojętego cyberbezpieczeństwa. Internauci dokonują mentalnej kalkulacji – rachunku zysków i strat pojawiających się zarówno w wyniku bezpiecznych, jak i niebezpiecznych zachowań. Korzyści z tych pierwszych nie zawsze są oczywiste, co więcej, istnieją negatywne aspekty związane z zachowywaniem bezpieczeństwa. Przykładowo, starania o uzyskanie ochronnego oprogramowania i aktualizowanie go mogą zniechęcać, gdyż wymagają czasu i pieniędzy. Należy zatem w miarę możliwości eliminować czynniki negatywne. Ważne jest również dyskredytowanie nieracjonalnych zachowań, np. niezbyt rozsądnego ulegania obietnicom zdobycia „nagrody", jeśli kliknie się we wskazane (niekoniecznie wiarygodne) miejsce. Warto zwracać uwagę na pozytywne skutki bezpiecznego zachowania. Wyeliminowaniu złośliwego oprogramowania towarzyszą również drugorzędne korzyści osobiste związane z wydajniejszą pracą komputera, rzadszą koniecznością napraw i większą produktywnością.

Kluczową sprawą jest zaangażowanie użytkowników w kwestię bezpieczeństwa w sieci w taki sposób, aby czuli się za nie osobiście odpowiedzialni. Kiedy to zaangażowanie jest niskie, użytkownicy nie będą skłonni wdawać się w szczegóły, np. zapoznawać się z polityką prywatności danej strony. Zagadnienia związane z prywatnością stanowią zresztą czynnik, dzięki któremu można zwiększyć zaangażowanie w bezpieczeństwo w sieci. Innymi źródłami regulacji mogą być normy społeczne, zatem korzystne w omawianym zakresie jest krzewienie pożądanych postaw. Pomocne będzie także kształtowanie odpowiednich nawyków. Wreszcie, należy zachęcać użytkowników, by korzystali z aplikacji, które wykrywają problemy, ostrzegają o zagrożeniach oraz informują o sposobach ochrony przed nimi.

Dbałość o bezpieczeństwo w sieci to obszar, który wzbudza coraz większe zainteresowanie naukowców i specjalistów z różnych dziedzin, co przekłada się na rosnącą liczbę prowadzonych badań i powstających publikacji (naukowych i popularyzatorskich, np. poradników dla szkół i indywidualnych odbiorców), a także stron internetowych oraz instruktaży poświęconych omawianej problematyce. W trosce o najmłodszych użytkowników → Światowa Organizacja Zdrowia [t. 4] (World Health Organization, WHO) w ostatnim czasie wydała zalecenie, aby dzieci poniżej 2. roku życia nie miały kontaktu z ekranami urządzeń elektronicznych (włączając w to telewizję), tym mającym poniżej 5 lat powinno się zaś ograniczać dostęp

do maksymalnie godziny dziennie, a najlepiej mniej. W wytycznych kładzie się nacisk m.in. na kluczową, zwłaszcza w tym wieku, aktywność fizyczną, co ma zapobiegać w przyszłości różnym chorobom związanym z otyłością. Trudno jednak stwierdzić, na ile oświadczenie WHO wpłynie na rzesze rodziców, dla których zajmowanie dzieci mediami mobilnymi stało się rutynowym sposobem zapobiegania przeszkadzaniu osobom dorosłym podczas załatwiania sprawunków, dłuższej jazdy samochodem czy jedzenia, co może być szkodliwe dla późniejszych kompetencji społeczno-emocjonalnych wychowanków, jeśli jest stosowane jako główny sposób, w jaki uczy się ich uspokajać. W przypadku starszych dzieci powinna mieć miejsce (niewystarczająca zwykle) rodzicielska kontrola czasu i treści, do jakich młodzi internauci mają dostęp. Specjaliści podkreślają, że rodzice powinni umieć rozpoznawać zagrożenia w sieci, zarówno te napotykane, jak i te tworzone przez ich dzieci, po to, by chronić je przed złem, ale również, aby wpoić im zasady właściwego poruszania się w wirtualnym świecie. Przy czym wcale nie jest niezbędne (chociaż korzystne), by rodzice mieli wyspecjalizowaną wiedzę informatyczną; wystarczy ich świadome i odpowiedzialne podejście do tematu oraz zaangażowanie w to, czym zajmują się dzieci, które mimo znacznej biegłości w korzystaniu z komputera i internetu nie mają wystarczającej świadomości zagrożeń.

Równolegle z edukacją związaną z bezpiecznym korzystaniem z internetu odbywającą się w domu rodzinnym powinna funkcjonować wieloaspektowa edukacja medialna i informacyjna w szkołach (niestety podstawa programowa w naszym kraju nie uwzględnia przedmiotu ICT). Nie będzie to jednak możliwe bez kształcenia w tym zakresie również rodziców opiekujących się dziećmi i nauczycieli przekazujących swoją wiedzę uczniom (a niekiedy także ich rodzicom). Konieczna zatem jest wielowymiarowa → e d u k a c j a d l a b e z p i e c z e ń s t w a w s i e c i [t. 2].

Korzystne byłoby wdrażanie takiej edukacji w ramach systematycznej i holistycznej edukacji medialnej i informacyjnej, niezbędnej we współczesnym społeczeństwie informacyjnym, aby ewoluowało ono w społeczeństwo wiedzy. W raporcie poświęconym tej edukacji, powstałym w ramach otwartego projektu „Cyfrowa przyszłość" Fundacji Nowoczesna Polska, autorzy dogłębnie scharakteryzowali to pojęcie, opisali stan kompetencji w tym zakresie w Polsce, przedstawili rolę organizacji międzynarodowych w tej kwestii, uwzględniając w szczególności UE i → U N E S C O [t. 4], przybliżyli istniejące już w innych krajach rozwiązania (w Kanadzie, na Węgrzech, w Wielkiej Brytanii, we Francji), opracowali katalog inicjatyw Polsce, podejmowanych m.in. przez instytucje publiczne i prywatne, oraz przeanalizowali proces kształtowania omawianych kompetencji w podstawach programowych Ministerstwa Edukacji Narodowej. Z raportu wynika, że powstaje wiele inicjatyw dotyczących edukacji medialnej i informacyjnej, w tym dotyczących bezpieczeństwa w sieci, jednak zarówno ich treści, jak i podejmowane działania są rozproszone i brakuje spójnego podejścia czy programu obejmującego w sposób całościowy i skoordynowany to zagadnienie.

Dodatkowo różnymi aspektami tego obszaru zajmują się różne instytucje – Ministerstwo Kultury i Dziedzictwa Narodowego, Ministerstwo Edukacji Narodowej, Ministerstwo Administracji i Cyfryzacji (w 2015 r. przekształcone w Ministerstwo Cyfryzacji), media publiczne, Narodowy Instytut Audiowizualny oraz instytucje samorządowe – przez co odpowiedzialność za tę problematykę jest niejako rozmyta. Ponadto potrzebne są kompleksowe badania poświęcone kompetencjom medialnym Polaków, aby na podstawie uzyskanej rzetelnej diagnozy móc stworzyć właściwy projekt będący odpowiedzią na wszystkie potrzeby w tym zakresie.

Wracając do węższego zagadnienia krzewienia postaw korzystnych z punktu widzenia bezpieczeństwa w sieci, cenne jest również wspieranie działań oświatowych przez kampanie w mass mediach, inicjatywy rozpowszechniające zasady bezpiecznego zachowania w wirtualnym świecie podejmowane przez organizacje i stowarzyszenia zajmujące się cyberbezpieczeństwem, literatura naukowa i popularyzacyjna. Wreszcie ważną rolę w tym względzie odgrywają raporty (np. CBOS) i badania naukowe umożliwiające formułowanie diagnozy służącej w dalszej kolejności opracowywaniu projektów związanych z edukacją czy rozwiązaniami w zakresie bezpiecznego korzystania z zasobów internetowych.

Małgorzata Bereźnicka

CERT.pl (dostęp 23.11.2019); *Cyfrowa przyszłość. Edukacja medialna i informacyjna w Polsce – raport otwarcia*, J. Lipszyc (red.), Fundacja Nowoczesna Polska, Warszawa 2012; M. Bereźnicka, R. Klepka, *Pedagogizacja medialna rodziny w społeczeństwie informacyjnym*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; M. Bereźnicka, P. Motylińska, *Bezpieczeństwo w sieci*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; R. LaRosse, N.J. Rifon, R. Enbody, *Promoting Personal Responsibility for Internet Safety*, „Communications of the ACM" 2008, vol. 51, iss. 3; NASK.pl (dostęp 20.11.2019); J. Plis, *Ochrona dziecka przed zagrożeniami w sieci*, [w:] *Współczesne determinanty profilaktyki i resocjalizacji nieletnich*, S. Bębas (red.), Wyższa Szkoła Handlowa w Radomiu, Radom 2010; J.S. Radesky, J. Schumacher, B. Zuckerman, *Mobile and Interactive Media Use by Young Children: The Good, the Bad, and the Unknown*, „Pediatrics" 2015, vol. 135, iss. 1; S. Kemp, *Digital 2021: Global Overview Report*, 27 January 2021, https://datareportal.com/reports/ digital-2021-global-overview-report (dostęp 21.03.2021);WHO, *Safety and Security on the Internet: Challenges and Advances in Member States: Based on the Findings of the Second Global Survey on eHealth*, WHO, Geneva 2011; J. Wishart, *Internet Safety in Emerging Educational Contexts*, „Computers & Education" 2004, vol. 43.

BEZPIECZEŃSTWO W TRADYCYJNYCH I NOWYCH MEDIACH – należy je wiązać z szerokim zakresem relacji między → b e z p i e c z e ń s t w e m jako tematem obecnym w mediach a problematyką bezpieczeństwa w użytkowaniu mediów. Same media stanowią zwykle główne źródło → i n f o r m a c j i [t. 2] o → z a g r o ż e n i a c h [t. 4], katastrofach, → w o j n a c h [t. 4], ale i zaleceniach dotyczących postępowania w razie → k r y z y s u [t. 2], a także komunikatów perswazyjnych, które mają oddziaływać na emocje, postawy i wywoływać określone działania związane

z bezpieczeństwem jednostki. Medialne przekazy o bezpieczeństwie dają szanse na bycie dobrze poinformowanym i dzięki temu gotowym, by podejmować właściwe decyzje.

Tradycyjne paradygmaty bezpieczeństwa oraz rola komunikowania masowego przeszły znaczną metamorfozę w erze postzimnowojennej charakteryzującej się globalizacją i rewolucją informacyjną. Ta na nowo zdefiniowała rolę środków masowego przekazu, przenosząc je z pokoju redaktora do szerszego grona odbiorców na poziomie globalnym za pośrednictwem technologii, mobilnej telefonii komórkowej, telewizji kablowej i satelitarnej oraz internetu. Środki masowego przekazu odgrywają zarówno pozytywną, jak i negatywną rolę w stosunku do bezpieczeństwa. Wyzwania związane z → b e z p i e c z e ń s t w e m n a r o d o w y m mają głównie charakter niemilitarny i zazwyczaj dotyczą krajowych, a nie zewnętrznych zagrożeń. W związku z tym wielokrotnie podnoszono problem odpowiedzialności środków masowego przekazu. Media takie jak internet, które nie mają reżimu regulacyjnego do monitorowania jego zawartości, mogą łatwo zagrozić bezpieczeństwu. Jednak zarówno media, jak i instytucje bezpieczeństwa wciąż aklimatyzują się w zmieniającym się otoczeniu gwałtownie rozprzestrzeniających się technologii i towarzyszących im wyzwań.

Wśród negatywnych konsekwencji komunikowania związanego z bezpieczeństwem wymienić należy → t e r r o r y z m [t. 4]. Powszechnie uznaje się, że istnieje niemal symbiotyczny związek między terroryzmem a mediami, ponieważ terroryzm zapewnia ekscytujące i brutalne historie, które pomagają w sprzedaży produktu medialnego, a media zapewniają grupom terrorystycznym możliwość rozpowszechniania ich wiadomości i wywoływania strachu wśród ogółu społeczeństwa. Jeżeli media informacyjne są kluczowe dla strategii terrorystycznej, by zdobyć publiczną uwagę i szerzyć strach wśród ludności, pojawiają się pytania o możliwości zakazania prezentowania doniesień medialnych o terroryzmie. Jakikolwiek rodzaj takich ograniczeń mediów podczas ataków terrorystycznych napotyka 2 poważne problemy, jeden normatywny i jeden praktyczny. W kontekście normatywnego problemu cenzurowania (→ c e n z u r a) i ograniczania doniesień medialnych na temat terroryzmu należy podkreślić, że wolne media, choć nie zawsze są bastionem liberalnych wartości demokratycznych, są jednak kluczową cechą społeczeństw demokratycznych. Jak zauważył P. Wilkinson, pionier badań nad terroryzmem, powszechnie uznaje się, że ważne jest unikanie zawłaszczenia przez terrorystów środków masowego przekazu i manipulowania nimi, ale jeśli wolność mediów zostanie poświęcona w imię walki z terroryzmem, oznaczać to będzie zniszczenie jednej z kluczowych podstaw demokratycznego społeczeństwa. Komunikowanie o bezpieczeństwie napotyka także zagrożenia związane z manipulacją i stronniczością medialną, a zwłaszcza jej najdalej idącą formą, czyli → p r o p a g a n d ą [t. 3]. Komunikowaniem o wojnie i zagrożeniach można przeciwdziałać stratom w ludziach, ale także wywoływać konflikty etniczne, narodowościowe, → w o j n y d o m o w e [t. 4] oraz rewolucje. Najlepszych

przykładów takiego tworzenia i wykorzystywania komunikatów związanych z bezpieczeństwem dostarcza → w o j n a h y b r y d o w a [t. 4] Rosji przeciwko Ukrainie, w której → m a n i p u l a c j a i n f o r m a c j ą [t. 3] wywołuje oraz pogłębia chaos i → p r z e c i ą ż e n i e i n f o r m a c y j n e [t. 3].

Medialne relacje na temat wydarzeń dotyczących bezpieczeństwa są zdominowane przez doniesienia o wojnie i wiadomości o konfliktach zbrojnych. Tego typu newsy są często silnie upolitycznione, co może odzwierciedlać rzeczywiste stosunki międzynarodowe i równowagę sił. → K u l t u r y i n f o r m a c y j n e [t. 2] różnią się znacznie pod względem uwagi poświęcanej wiadomościom międzynarodowym i zagranicznym. Podczas gdy newsy w USA są mocno skoncentrowane na sprawach krajowych, newsy w wielu krajach europejskich mają często międzynarodowy charakter. Ten wzór jest w dużej mierze konsekwencją faktu, że wiele międzynarodowych wiadomości spoza USA dotyczy USA. W istocie świat jest bardzo nierównomiernie reprezentowany w światowych newsach, a regionalne problemy Afryki i Azji często zajmują o wiele mniej miejsca w Europie i USA w porównaniu z liczbą newsów dotyczących Europy i USA nadawanych w programach informacyjnych w Afryce i regionach azjatyckich. Pierwszeństwo w politycznych serwisach często dotyczy spraw wewnętrznych, ale w czasie → z a g r o ż e n i a b e z p i e c z e ń s t w a [t. 4], a więc wojny, ataków terrorystycznych lub konfliktów, wiadomości zagraniczne mogą dominować. Sprawy zagraniczne zazwyczaj trafiają do serwisów informacyjnych, gdy dotyczą elit, gdy wydarzenia rozgrywają się blisko państwa, w którym mają być nadawane, gdy mają określony poziom znaczenia i pociągają za sobą ofiary. Wydźwięk przekazów medialnych o wojnie i → k o n f l i k t a c h m i ę d z y n a r o d o w y c h [t. 2] często jest uzależniony od poglądu na pozycję państwa w wojnie. Bliski związek między oficjalnymi źródłami a treścią relacji wojennych (zob. → m e d i a l n e r e l a c j e w o j e n n e [t. 3]) został udokumentowany w USA oraz w krajach z autorytarnymi → r e ż i m a m i [t. 3] i silnymi powiązaniami strukturalnymi między polityką a prasą. Wiadomości z zagranicy są kosztownym elementem organizacji medialnych i często ich zakres uzależniony jest zarówno od posiadania sieci korespondentów, jak i od dostępności sprzętu. Niewątpliwie konkurencja między organizacjami medialnymi i cięcia finansowe doprowadziły do spadku liczby wiadomości międzynarodowych.

Newsy dotyczące bezpieczeństwa bardzo często odnoszą się także do wydarzeń krajowych, a nawet lokalnych. W pierwszej grupie można odnaleźć materiały dotyczące → p r z e s t ę p c z o ś c i [t. 3], wydarzeń niosących za sobą niebezpieczne skutki, kataklizmów czy katastrof. Z kolei wydarzenia lokalne dotyczą wypadków komunikacyjnych oraz indywidualnych działań człowieka, które najczęściej wiążą się z bagatelizowaniem zagrożeń, rzadziej zaś z wydarzeniami pozbawionymi negatywnego wpływu człowieka. W wiadomościach dotyczących bezpieczeństwa szczególnie wyraźnie rysuje się negatywizm medialny – oznaczający, że złe wieści są zwykle preferowane i o wiele chętniej omawiane od dobrych wiadomości – co w skrajnym

przypadku może prowadzić nawet do sytuacji wskazywanej przez sławnego teoretyka medialnego M. McLuhana, który zauważył, że często reklamy stanowią jedyną „dobrą nowinę" w gazecie.

Szereg specyficznych funkcji media mają do spełnienia w → s y t u a c j a c h k r y z y s o w y c h [t. 4], mogą one bowiem przyspieszyć rozwiązanie kryzysu oraz wpłynąć na sposób zażegnania sytuacji kryzysowej. Tempo oddziaływania mediów daje ogromne możliwości informowania czy przestrzegania o nadchodzącym kryzysie, działania medialne nie ograniczają się jedynie do informowania po zdarzeniu, a wręcz dają możliwość tworzenia wiadomości ostrzegawczych przez użytkowników, a nie tylko ich odbierania, jak ma to miejsce w przypadku → m e d i ó w t r a d y c y j n y c h [t. 3].

Sposób, cele i zakres oddziaływania mediów uzależniony jest od typu kryzysu. Istnieje wiele definicji kryzysu, ale większość zawiera 3 elementy: zagrożenie, nagłe wystąpienie i niepewność. Uwzględniając te elementy, można traktować kryzys jako poważne zagrożenie dla elementarnych struktur lub podstawowych wartości i stanów społeczeństwa, które wymagają podejmowania kluczowych decyzji pod presją czasu i w wysoce niepewnych okolicznościach. Konieczność działania mediów występuje w razie tak różnorodnych przeciwności, jak klęski żywiołowe i zagrożenia środowiskowe, krach finansowy, ataki terrorystyczne, epidemie, eksplozje, katastrofy infrastrukturalne czy upadki organizacji. Wszystkie te wydarzenia charakteryzują się trudnymi warunkami dla tych, którzy starają się zarządzać operacją reagowania i podejmować pilne decyzje. Zwykle podstawowe informacje o przyczynach i konsekwencjach kryzysu są wówczas niedostępne.

Rola mediów w sytuacji kryzysowej polega w pierwszej kolejności na informowaniu, ale także przestrzeganiu oraz prezentowaniu racjonalnych i prawdopodobnych, wynikających z istnienia kryzysu zagrożeń dla jednostki. Niezwykle ważne pozostaje w takiej sytuacji odejście od typowej dla mediów praktyki eskalowania sensacji na rzecz pragmatycznego informowania – zwłaszcza w kontekście potencjalnych wydarzeń w następstwie kryzysu lub w odniesieniu do jego bieżących skutków. W dalszej kolejności rola mediów polega na relacjonowaniu akcji ratowniczej, działania instytucji, organów, podmiotów, sztabów, które pracują na rzecz zażegnania skutków kryzysu bądź ograniczenia jego konsekwencji. Media następnie podejmują dyskusję nad przyczynami kryzysu, jego genezą i poprzedzającymi go wydarzeniami. Nierzadko na tym etapie rozważania dziennikarzy i mediów mają charakter interpretacji, często uczestniczą w nich dziennikarze śledczy, pojawiają się komentarze ekspertów, specjalistów. Bardzo istotne jest, aby etap dziennikarskiej ewaluacji kryzysu nie przesłonił, zwłaszcza na wstępnym etapie, podstawowej funkcji mediów, czyli informowania o wydarzeniu. Później rolą mediów pozostaje edukowanie, a więc informowanie antycypujące możliwe działania odbiorców i kierunkujące tę aktywność w sposób, który ułatwi akcję ratunkową, a także już po jej zakończeniu będzie stanowił instruktaż działań

możliwych do podjęcia, aby uniknąć podobnych kryzysów w przyszłości. Wreszcie, już po upływie określonego czasu od zakończenia kryzysu, media mogą podjąć działania aktywizujące odbiorców na rzecz kroków, które przeciwdziałałyby wystąpieniu podobnego kryzysu w przyszłości.

Należy wskazać, że media często tylko do pewnego stopnia realizują zarysowany tu model działania. Cele mediów, zwłaszcza komercyjnych, wiążą się z aktywnością na rzecz utrzymania jak największej oglądalności lub poczytności, a to sprawia, że działania mediów niejednokrotnie ograniczają się do sensacyjnego informowania o kryzysie oraz emocjonalnego tłumaczenia przyczyn, poszukiwania winnych i spekulowania o poniesieniu przez nich kary czy o możliwych konsekwencjach politycznych, ekonomicznych lub karnych dla osób, którym będzie można przypisać odpowiedzialność za zaistniałe zdarzenie.

Nie ulega wątpliwości, że w sytuacjach kryzysowych coraz większą rolę odgrywają nowe media (zob. → m e d i a t r a d y c y j n e i k o n w e r g e n t n e [t. 3]) wykorzystujące internet, szczególnie media społecznościowe. Facebook i Twitter dają możliwość bardzo szybkiej reakcji, sformułowania ostrzeżenia, poinformowania o zaistniałej sytuacji. Mogą także stanowić forum dyskusji nad danym wydarzeniem.

Internet jest przełomową technologią, której wpływ w XXI w. na komunikację między ludźmi jest porównywalny tylko z zastosowaniem ruchomej czcionki przez Gutenberga. Dla agencji wywiadowczych na całym świecie, chcących dowiedzieć się więcej o ludzkich celach, ich tożsamości, lokalizacji, ruchach, finansach i intencjach, internet jest źródłem, które ciągle daje nowe możliwości pozyskiwania danych. Cyfrowy charakter wszystkich informacji w sieci sprawia, że możliwe jest czerpanie ich zarówno z treści komunikacji internetowej, jak i na podstawie efektywnego gromadzenia danych przechowywanych w sposób, który nigdy wcześniej nie był możliwy, po przystępnej cenie.

Szczególną rolę w odniesieniu do przekazów dotyczących bezpieczeństwa odgrywają → m e d i a s p o ł e c z n o ś c i o w e [t. 3] zaprojektowane specjalnie w celu ułatwienia interakcji między osobami, zarówno w formie informacji rozgłoszeniowej (takiej jak Twitter), jak i jako informacje wspólne dla członków grupy (takich jak Facebook i LinkedIn) lub jako platforma, na której materiały wideo lub inne mogą być łatwo udostępniane (np. YouTube). Media społecznościowe stały się ważną częścią ludzkiego życia. Począwszy od dzielenia się informacjami takimi jak tekst, zdjęcia, wiadomości, przez działania podejmowane przez wiele osób udostępniających najnowsze wiadomości i zdjęcia pochodzące z innych mediów, dokumenty z pytaniami, umieszczających zadania i warsztaty edukacyjne, ankiety internetowe, podejmujących w mediach społecznościowych działania marketingowe oraz wykazujących aktywność kierowaną do klientów biznesowych, po żarty, udostępnianie muzyki, filmów i innych treści o charakterze rozrywkowym. Ze względu na wykorzystanie social mediów przez internautów na wiele możliwych sposobów mówi się nierzadko o mediach społecznościowych jako o istocie kultury współczesnego internetu.

Zagrożenia związane z wykorzystaniem mediów społecznościowych wiążą się z opracowaniem w ostatnich latach skutecznych narzędzi do ekstrakcji i analizy cyfrowych danych. Przyczyniła się do tego dynamiczna interakcja – z jednej strony wzrosło zapotrzebowanie na informacje o osobach jako jednostkach, w szczególności po atakach z 11 września i powstaniu Al-Kaidy, a następnie ISIS (zob. → P a ń s t w o I s l a m s k i e [t. 3]), z drugiej zaś zwiększyła się potencjalna podaż takich informacji, wynikająca z rosnącego wykorzystania internetu przez społeczeństwo, firmy i rządy. Media społecznościowe generują ogromne ilości danych o osobach będących przedmiotem zainteresowania przedsiębiorstw komercyjnych, rządów, które chcą poprawić jakość usług publicznych, organów ścigania, które usiłują identyfikować przestępców, wykorzystując internet, i krajowych agencji wywiadowczych poszukujących informacji o osobach kluczowych dla ich misji związanych z bezpieczeństwem narodowym. Trudność w utrzymaniu bezpieczeństwa wiąże się z silną adaptacją mediów społecznościowych jako narzędzia nowoczesnej wojny rozumianej zarówno w sposób tradycyjny, jak i w sensie → w o j n y i n f o r m a c y j n e j [t. 4]. Wykorzystując media społecznościowe, można w sposób sztuczny spopularyzować dany temat, uczynić go ważnym i szeroko komentowanym.

Istnieją 3 metody pomagające kontrolować trendy w mediach społecznościowych:

- dystrybuowanie trendów,
- przejęcie trendów,
- tworzenie trendów.

Pierwsza metoda jest stosunkowo łatwa i wymaga najmniej zasobów. Dystrybucja trendów polega po prostu na wysyłaniu wiadomości do każdego tematu, który ma stać się popularny. Na przykład można wstawić na Twitterze zdjęcie prezydenta z komunikatem w postaci mema, które stosuje kulturowo odpowiedni żart do danego zdjęcia lub filmu, wraz z niepowiązanym hashtagiem #SuperBowl. Każdy, kto kliknie na listę trendów, spodziewając się zobaczyć coś na temat piłki nożnej, zobaczy mema prezydenta. Przejęcie trendu wymaga więcej zasobów w postaci większej liczby obserwujących, którzy rozpowszechniają komunikat, lub sieci botów, czyli autonomicznych programów, które mogą wchodzić w interakcje z systemami komputerowymi lub użytkownikami, zaprojektowanych w celu automatycznego rozprzestrzeniania wiadomości. Spośród 3 metod zdobywania wiedzy na temat trendu tworzenie trendów wymaga największego wysiłku. Wymaga pieniędzy na promowanie trendu lub znajomości środowiska mediów społecznościowych zbudowanego wokół tematu, a najprawdopodobniej również sieci kilku automatycznych kont botów. Konta botów automatycznie tweetują i przesyłają tweety dalej na podstawie zestawu zaprogramowanych reguł. W 2014 r. Twitter oszacował, że tylko 5% kont to boty, liczba ta wzrosła wraz z całkowitą liczbą użytkowników i w 2017 r. wynosiła już 15%.

Doskonały przykład zagrożenia w mediach społecznościowych wynikającego z przesyłania fałszywych wiadomości pochodzi z najbardziej popularnych wiadomości

publikowanych na Facebooku podczas wyborów prezydenckich w USA w 2016 r. Źródłem fałszywych wiadomości był rzekomo patriotyczny amerykański blog End the Fed, strona prowadzona przez rumuńskiego biznesmena O. Drobota. Jeden z newsów przekazywanych przez sieci społecznościowe, wg którego papież poparł D. Trumpa jako kandydata na prezydenta, uzyskał ponad milion reakcji na samym Facebooku. Inne fałszywe wiadomości z tej strony przekazywane przez media społecznościowe miały pod koniec 2016 r. więcej odbiorców niż materiały pochodzące z tradycyjnych źródeł.

Można wskazać szerokie zastosowania mediów społecznościowych mające wpływ na bezpieczeństwo i poczucie bezpieczeństwa na całym świecie. Przestępcy, terroryści i uczestnicy zamieszek używają mediów społecznościowych do prezentacji swoich głosów, rekrutacji i planowania działań. Podczas arabskiej wiosny protestujący na całym Bliskim Wschodzie wykorzystywali media społecznościowe do organizowania protestów i pomocy w obaleniu rządów w ich krajach. Podczas zamieszek w Londynie młodzi ludzie używali lokalnych platform mediów społecznościowych do koordynowania grabieży i przeciwstawiania się → p o l i c j i [t. 3]. Terroryści używają mediów społecznościowych do rozpowszechniania propagandy na temat swojej sprawy, demonizowania celów ataku i rekrutowania innych do ich przeprowadzania. Gangi używają mediów społecznościowych, aby grozić sobie nawzajem, rekrutować członków, planować → p r z e m o c [t. 3] i inne działania przestępcze. Z powodu zamieszek, terroryzmu i kryminalnego wykorzystania mediów społecznościowych rządy na całym świecie stoją przed nowymi, silniejszymi zagrożeniami niepaństwowymi, których w coraz większym stopniu nie rozumieją. Tylko niektóre grupy i rządy skutecznie wykorzystują media społecznościowe do zapewnienia bezpieczeństwa społecznościom. Jednak większość z nich jest w dużej mierze nieświadoma potencjalnych możliwości mediów społecznościowych i tego, jak mogą i powinny z nich korzystać.

Media odgrywają także kluczową rolę w zakresie promowania działań i postaw, dlatego to za ich pośrednictwem prowadzone są zwykle kampanie na rzecz bezpieczeństwa obejmujące planowane działania, które mają wpływ na wiedzę, postawy i zachowania odnoszące się do różnych obszarów bezpieczeństwa. Kampanie takie nastawione są na cel działania, w odniesieniu do którego próbuje się informować, przekonywać lub motywować zmiany zachowań u stosunkowo dobrze zdefiniowanej i dużej publiczności. W kampaniach dotyczących bezpieczeństwa cel działania jest stosunkowo ogólny i ma przynieść niekomercyjne korzyści dla jednostek i/lub społeczeństwa jako całości w danym okresie poprzez zorganizowane działania komunikacyjne obejmujące media masowe i internetowe o charakterze interaktywnym, często uzupełniane wsparciem interpersonalnym.

Projektowanie kampanii rozpoczyna się od konceptualnej oceny sytuacji w celu określenia szans i barier oraz wskazania segmentów populacji, których praktyki mają zostać zmienione, a także podstawowych zachowań, na które kampania ostatecznie stara się wpłynąć. Następnym krokiem jest prześledzenie występowania takich zachowań,

aby zidentyfikować ich najbliższe i dalsze determinanty, a następnie stworzyć modele ścieżek wpływu poprzez postawy, przekonania, wiedzę, wpływy społeczne i siły środowiskowe. Kolejną fazą jest badanie modelu z perspektywy komunikacji i określenie odbiorców docelowych oraz zachowań docelowych, na które mogą bezpośrednio wpływać komunikaty kampanii.

Większość kampanii ma na celu przekazywanie wiadomości bezpośrednio w głównych podgrupach, zagrożonych subpopulacjach, które mogą skorzystać z kampanii. Potencjał bezpośrednich efektów zależy od względnej otwartości docelowych grup odbiorców. Kampanie zazwyczaj osiągają najsilniejszy wpływ, jeśli uruchamiają lub wzmacniają komunikaty przeznaczone dla osób, które są już korzystnie predysponowane. Następny kluczowy segment odbiorców obejmuje tych, którzy jeszcze nie próbowali niepożądanych zachowań, ale ich charakterystyka tła sugeruje, że są nimi zagrożeni w najbliższej przyszłości, wielu z nich może być podatnych na perswazyjne przekazy. Osoby zaangażowane w niewłaściwe praktyki nie podlegają bezpośrednio ukierunkowanym kampaniom, więc duża inwestycja w zasoby, które skłoniłyby do przerwania działalności, prowadzi do marginalnych zysków.

Wywierając wpływ na zachowania, kampanie albo próbują promować pozytywne działania, np. zapinanie pasów bezpieczeństwa, przestrzeganie ograniczeń prędkości, tolerowanie mniejszości, albo zapobiegać problematycznym zachowaniom, takim jak jazda pod wpływem alkoholu, palenie lasów czy przemoc w rodzinie. W wielu wariantach kampanii ważną rolę odgrywają komunikaty informacyjne, mające na celu uświadamianie lub dostarczanie instrukcji. Komunikaty uświadamiające przedstawiają zwykle stosunkowo proste treści, które informują ludzi, co mają robić, określają, kto powinien to robić, lub zapewniają wskazówki dotyczące tego, kiedy i gdzie należy podejmować działania. Nawet powierzchowne wiadomości mogą zachęcić odbiorców do szukania bogatszych dogłębnych treści z opracowanych zasobów informacyjnych, takich jak strony internetowe, książki czy liderzy opinii. Bardziej złożone komunikaty instruktażowe przedstawiają informacje, jak coś zrobić.

W rozpowszechnianiu medialnych kampanii na rzecz bezpieczeństwa większość projektantów kampanii nadal wybiera tradycyjne kanały medialne, czyli prasę, radio i telewizję. Strony internetowe były również popularnym nośnikiem kampanii medialnych od końca lat 90. W ostatnim dziesięcioleciu kampanie coraz częściej wykorzystywały technologię interaktywną, a więc blogi i mikroblogi, płyty CD i DVD, dostosowane wiadomości i strony internetowe, gry komputerowe oraz aplikacje na telefony komórkowe.

Większość ekspertów twierdzi, że kampanie medialne osiągnęły raczej skromny niż silny wpływ, zwłaszcza w zakresie poprawy bezpieczeństwa. Jest to częściowo spowodowane skromnymi budżetami upowszechniającymi, błędnym zastosowaniem teorii i modeli oraz źle opracowanymi podejściami strategicznymi. Jest to również wynikiem skomplikowanego zadania stojącego przed twórcą kampanii, który może promować złożone lub trudne zachowania, celować w odporne segmenty odbiorców

lub radzić sobie z ograniczonymi zasobami, podczas gdy zagrożona publiczność jest stale narażona na relacje w mediach i reklamy, które mają negatywny wpływ na zachowania.

Kampanie medialne na rzecz bezpieczeństwa obecnie coraz częściej wykorzystują możliwości, jakie daje internet, a w szczególności sieci społecznościowe, takie jak Facebook, Twitter czy YouTube. Social media odzwierciedlają sposób, w jaki użytkownicy komunikują się ze sobą, mają bardzo interaktywny charakter, a użytkownicy mogą łatwo udostępniać informacje innym osobom. Ponadto umożliwiają bardziej złożony, dwukierunkowy sposób komunikowania się, co jest bezpośrednim efektem demokratyzacji informacji. W konsekwencji nie tylko twórcy kampanii rozmawiają ze swoimi odbiorcami, ale ci rozmawiają też bezpośrednio ze sobą. Podstawowe zmiany, jakie rodzi dla kampanii dotyczących bezpieczeństwa wykorzystanie mediów społecznościowych, dotyczą kilku kluczowych elementów: bezpośredniego dotarcia do tożsamości odbiorcy, stałej obecności w jego sieci społecznościowej, możliwości ciągłego utrzymania kontaktu, prowadzenia rozmowy, budowania relacji, kreowania grupy zainteresowanych wokół kampanii, budowania reputacji oraz dalszego udostępniania treści. Od twórców kampanii medialnych wymagane jest strategiczne podejście do obecności w social mediach, ponieważ – podobnie jak w przypadku mediów tradycyjnych – tu również o uwagę odbiorców walczą inne komunikaty oraz treści.

Jakub Idzik, Rafał Klepka

Ch. Atkin, R. Rice, *Advances in Public Communication Campaigns*, [w:] *The International Encyclopedia of Media Studies*, A. Valdivia (ed.), Wiley, Malden 2013; A. Boin, M. Ekengren, M. Rhinard, *The Study of Crisis Management*, [w:] *The Routledge Handbook of Security Studies*, M. Cavelty, V. Mauer (eds.), Routledge, New York–London 2010; M. Cross, *Social Media Security: Leveraging Social Networking While Mitigating Risk*, Elsevier, Amsterdam, 2014; R. Gupta, H. Brooks, *Using Social Media for Global Security*, Wiley, Indianapolis 2013; J. Idzik, R. Klepka, *News na temat bezpieczeństwa*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 2: *N–Z*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; R. Klepka, *Bezpieczeństwo w mediach społecznościowych*; *Kampanie medialne na rzecz bezpieczeństwa*; *Media w sytuacjach kryzysowych*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; tenże, *Bezpieczeństwo w mediach społecznościowych*; *Kampanie medialne na rzecz bezpieczeństwa*; *Komunikowanie o bezpieczeństwie*; *News na temat bezpieczeństwa*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; tenże, *Wojna w mediach: wybrane zagadnienia dotyczące relacjonowania konfliktów zbrojnych*, „Wojny i Konflikty. Przeszłość – Teraźniejszość – Przyszłość" 2016, nr 1; O. Wasiuta, S. Wasiuta, *Medialna manipulacja informacją w wojnie hybrydowej Rosji przeciwko Ukrainie*, [w:] *Medialne obrazy świata*, R. Klepka (red.), Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2018.

BEZPIECZEŃSTWO WEWNĘTRZNE PAŃSTWA (bezpieczeństwo krajowe) – w literaturze przedmiotu dyskutowane jako układ (system) i/lub stan równowagi jednostki ludzkiej; jest to pojęcie wieloznaczne. Według *Słownika terminów z zakresu bezpieczeństwa* to stan osiągnięty w rezultacie działania organów państwa zmierzających

do zapewnienia jego stabilności wewnętrznej i odporności na możliwe → z a g r o ż e n i a [t. 4] wywołane przez przyrodę lub człowieka. W opracowaniu Z. Ścibiorka można odnaleźć nieco szersze ujęcie, w którym bezpieczeństwo wewnętrzne to stan, ale także proces uzyskany w efekcie spełniania przez państwo funkcji wewnętrznej realizowanej w ramach strategicznej polityki → b e z p i e c z e ń s t w a n a r o d o w e g o, przejawiającej się → o c h r o n ą z d r o w i a [t. 3], życia ludzi i majątku narodowego przed bezprawnymi działaniem, skutkami klęsk naturalnych i awarii technicznych. Realizacja polityki powinna urzeczywistniać się poprzez tworzenie odpowiednich struktur. Niektórzy autorzy utożsamiają bezpieczeństwo wewnętrzne ze stabilnym i harmonijnym funkcjonowaniem struktur państwa, wskazując na struktury władzy, procedury decyzyjne w ramach tych struktur i relacje między władzą i obywatelami. P. Majer uważa, że bezpieczeństwo wewnętrzne to stan niezakłóconego funkcjonowania państwa, związany z bezpieczeństwem jego organów oraz stabilnością życia społecznego. Harmonijność funkcjonowania jest wyznacznikiem bezpieczeństwa wewnętrznego w klasycznej definicji J. Symonidesa, który wskazuje, że bezpieczeństwo wewnętrzne to stan stabilności i równowagi wewnętrznej.

Należy zwrócić również uwagę na dychotomię podziału bezpieczeństwa narodowego wynikającą z zewnętrznej i wewnętrznej sfery działalności państwa, która ma swe źródła historyczne.

W okresie Rzeczypospolitej szlacheckiej ostatecznie uformowane zalążki administracji terenowej były oznaką zrozumienia, że bezpieczeństwo państwa zależy nie tylko od czynników zewnętrznych, ale też wewnętrznych. W 1764 r. król Stanisław August utworzył Radę Nieustającą z Departamentem Policji, któremu przyznano prawo nadzoru nad miastami w zakresie dbałości o infrastrukturę i czuwania nad finansami. Formalne zapisy dotyczące działań centralnej i lokalnej administracji publicznej znalazły się w Konstytucji 3 maja (1791 r.). Po odzyskaniu niepodległości w 1918 r. minister spraw wewnętrznych w demokratycznie powołanym rządzie był odpowiedzialny za ogólny zarząd w kraju, stan porządku i bezpieczeństwa, a także nadzór nad samorządem terytorialnym. 24 lipca 1919 r. powołano Policję Państwową. Po zakończeniu II wojny światowej działania administracji bezpieczeństwa wewnętrznego skupiały się na realizacji funkcji policyjnych i ochrony porządku prawno-politycznego państwa. W okresie transformacji ustrojowej odpolitycznio no powstałą formację policyjną w miejsce rozwiązanej Milicji Obywatelskiej. W 1996 r. utworzono Ministerstwo Spraw Wewnętrznych i Administracji, które funkcjonowało do 2011 r. Wszelkie zmiany dokonywane w toku wieków miały dostosować organy administracyjne do istniejącej rzeczywistości. Tak rozumiane bezpieczeństwo wewnętrzne obejmowało wszystko to, co wiązało się ze stabilnością i porządkiem na danym terytorium, a jego zapewnianie leżało w kompetencjach instytucji policyjnych. Bezpieczeństwo zewnętrzne natomiast obejmowało ochronę i obronę przed zagrożeniami z zewnątrz, za co odpowiadały struktury wojskowe. Ta klasyfikacja, jak twierdzi Majer, okazała

się zbyt schematyczna i uproszczona, gdyż na bezpieczeństwo narodowe składają się zarówno bezpieczeństwo wewnętrzne, jak i zewnętrzne. Te 2 rodzaje bezpieczeństwa powinny być traktowane jako wartości uzupełniające się, a samo bezpieczeństwo wewnętrzne warunkowane jest poprzez zagrożenia zewnętrzne oraz wewnętrzne.

Przesłankę do używania terminu bezpieczeństwa wewnętrznego państwa stanowi fakt, że pojęcie bezpieczeństwa wewnętrznego odnosi się do procesu zaspokajania potrzeb i interesów społeczeństwa danego kraju. Jak dowodzą J. Zawisza i S. Trzmiel, w strukturze bezpieczeństwa narodowego świadomie zostało wydzielone bezpieczeństwo wewnętrzne – to bezpieczeństwo wewnętrzne w swojej istocie stoi na straży konstytucji, → s u w e r e n n o ś c i [t. 4], spokoju społecznego, bytu narodowego, wolności i niepodległości oraz → p r a w c z ł o w i e k a [t. 3]. Bezpieczeństwo wewnętrzne zapewnia trwanie, przetrwanie i rozwój jednostki, grup społecznych i państwa w jego granicach. Rozpatrując znaczenie i zakres bezpieczeństwa wewnętrznego państwa, należy uwzględniać wyzwania i zagrożenia na danym etapie rozwoju oraz kryteria wartościowania, a także to, że podmiotem bezpieczeństwa jest człowiek. Człowiek jako jednostka ludzka ma właściwe sobie wartości i tworzy różnego rodzaju więzi wymagające stosownej obrony i ochrony (grupy ludzi o różnej wielkości i skali począwszy od rodziny, na społeczności międzynarodowej skończywszy). Jak podaje W. Pokruszyński, procesy rozwoju dowodzą, że instytucją w miarę skutecznie zapewniającą potrzeby jednostki w zakresie bezpieczeństwa jest państwo ze wszystkimi jego atrybutami w układzie międzynarodowym. Terminy bezpieczeństwa wewnętrznego państwa i bezpieczeństwa zewnętrznego znalazły swe miejsce w polskim prawodawstwie. Art. 146 Konstytucji RP brzmi:

> Rada Ministrów prowadzi politykę wewnętrzną i zagraniczną Rzeczypospolitej Polskiej. […] W zakresie i na zasadach określonych w Konstytucji i ustawach Rada Ministrów w szczególności […] zapewnia bezpieczeństwo wewnętrzne państwa oraz porządek publiczny.

W Ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu nie zdefiniowano bezpieczeństwa wewnętrznego wprost, ale treść art. 5 ustawy pozwala ją odtworzyć, biorąc pod uwagę dziedziny, którymi ABW się zajmuje. Zadania obejmują:

- rozpoznawanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny, a w szczególności w suwerenność i międzynarodową pozycję, niepodległość i nienaruszalność jego terytorium, a także obronność państwa, zapobieganie im i ich zwalczanie;
- rozpoznawanie i wykrywanie następujących przestępstw oraz zapobieganie im:
  - szpiegostwa, → t e r r o r y z m u [t. 4], bezprawnego ujawnienia lub wykorzystania → i n f o r m a c j i n i e j a w n y c h [t. 2] i innych przestępstw godzących w bezpieczeństwo państwa,

  - godzących w podstawy ekonomiczne państwa,
  - → k o r u p c j i [t. 2] osób pełniących funkcje publiczne,
  - w zakresie produkcji towarów, technologii i usług o znaczeniu strategicznym dla bezpieczeństwa państwa oraz obrotu nimi,
  - w zakresie nielegalnego wytwarzania i posiadania broni, amunicji i materiałów wybuchowych, broni masowej zagłady, środków odurzających i substancji psychotropowych, udział w obrocie międzynarodowym,
  - przeciwko wymiarowi sprawiedliwości;
- rozpoznawanie i wykrywanie zagrożeń godzących w bezpieczeństwo, istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład → i n f r a s t r u k t u r y k r y t y c z n e j [t. 2], a także systemów teleinformatycznych właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej oraz zapobieganie im, ujawnianie mienia zagrożonego przepadkiem w związku z przestępstwami;
- realizowanie, w granicach swojej właściwości, zadań związanych z ochroną informacji niejawnych oraz wykonywanie funkcji krajowej władzy bezpieczeństwa w zakresie ochrony informacji niejawnych w stosunkach międzynarodowych;
- uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom → i n f o r m a c j i [t. 2] mogących mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego.

Ustawa ta traktuje bezpieczeństwo wewnętrzne szerzej niż ustawa zasadnicza, gdyż odnosi się do zagadnień ekonomicznych.

Zagrożenia definiowane jako zjawiska fizyczne lub społeczne powodujące stan niepewności i obaw mogą zaistnieć zarówno w obrębie terytorium (wewnątrz), jak i na zewnątrz państwa. Do zagrożeń wewnętrznych należą:

- zamieszki lub strajki w skali regionu lub całego kraju;
- klęski żywiołowe;
- → k a t a s t r o f y t e c h n i c z n e [t. 2];
- → k r y z y s y [t. 2] ekonomiczne;
- zbrojne przewroty polityczne i powstania;
- kryzysy polityczne zagrażające demokratycznemu porządkowi w państwie;
- terroryzm i → p r z e s t ę p c z o ś ć z o r g a n i z o w a n a [t. 3].

Zagrożenia dla bezpieczeństwa wewnętrznego powodowane przez czynniki zewnętrzne to:

- masowe migracje;
- prowokacje zbrojne lub incydenty graniczne;
- → w o j n a d o m o w a [t. 4] lub → w o j n a [t. 4] między sąsiadującymi państwami;

- konflikt zbrojny między państwami oddalonymi geograficznie, jednak zagrażającymi pośrednio lub bezpośrednio interesom narodu;
- interwencja zbrojna mocarstwa;
- interwencja państwa w ramach sojuszu wynikająca ze zobowiązań międzynarodowych.

Zagrożenia nieznające granic to terroryzm i ataki w → c y b e r p r z e s t r z e n i oraz → w a l k a i n f o r m a c y j n a [t. 4].

W Decyzji ramowej Rady UE z dnia 13 czerwca 2002 r. w sprawie zwalczania terroryzmu za przestępstwa terrorystyczne uznano:

> przestępstwa, które ze względu na swój charakter i kontekst mogą wyrządzić poważne szkody krajowi lub organizacji międzynarodowej, gdy zostają popełnione w celu:
> - poważnego zastraszenia ludności, lub
> - bezprawnego zmuszenia rządu lub organizacji międzynarodowej do podjęcia lub zaniechania działania, lub
> - poważnej destabilizacji lub zniszczenia podstawowych politycznych, konstytucyjnych, gospodarczych lub społecznych struktur kraju lub organizacji międzynarodowej.

Cyberprzestrzeń jest obszarem aktywności sprzyjającej rozwojowi gospodarki, bezpieczeństwa, komunikacji społecznej i edukacji, ale także aktywności rodzącej szereg zagrożeń, takich jak:

- cyberinwigilacja – kontrola społeczeństwa za pośrednictwem narzędzi teleinformatycznych;
- → c y b e r p r z e s t ę p c z o ś ć – wykorzystanie cyberprzestrzeni do celów kryminalnych w ramach → p r z e s t ę p c z o ś c i [t. 3] zorganizowanej i przestępczości ekonomicznej;
- → c y b e r t e r r o r y z m – wykorzystanie cyberprzestrzeni do działań terrorystycznych;
- → c y b e r w o j n a – wykorzystanie cyberprzestrzeni do działań wojennych;
- walka informacyjna – działania podjęte w celu osiągnięcia dominacji informacyjnej poprzez wpływ na informację przeciwnika, jego procesy oparte na informacji, systemy informacyjne i sieci komputerowe.

Narzędziami wykorzystywanymi w walce informacyjnej są: dyplomacja, → p r o p a g a n d a [t. 3], kampanie psychologiczne, działania na poziomie wpływania na procesy polityczne lub kulturowe, → d e z i n f o r m a c j a [t. 2], manipulowanie lokalnymi mediami, infiltracja sieci komputerowych i baz danych.

Zagwarantowanie odpowiedniego poziomu bezpieczeństwa wewnętrznego zależy od harmonijnego działania instytucji, urzędów i organów państwa tworzących system bezpieczeństwa wewnętrznego. Podobnie W. Fehler postrzega system bezpieczeństwa wewnętrznego jako uporządkowany zbiór rozwiązań prawnych, organizacyjnych

i materialnych, którego celem jest osiąganie i utrzymywanie optymalnego w danych okolicznościach poziomu bezpieczeństwa wewnętrznego państwa oraz realizowanie zadań wynikających z prowadzonej przez państwo polityki bezpieczeństwa wewnętrznego. Zgodnie z klasyfikacją tego autora system bezpieczeństwa wewnętrznego jest podsystemem systemu bezpieczeństwa państwa. Podsystem bezpieczeństwa wewnętrznego zawiera kolejne podsystemy: bezpieczeństwa ustrojowego, bezpieczeństwa publicznego i porządku publicznego, ochrony granic, ratowniczy, sanitarno-epidemiologiczny, bezpieczeństwa informacyjnego, → z a r z ą d z a n i a k r y z y s o w e g o [t. 4]. Również w broszurze *Aspekte der Inneren Sicherheit* (Bonn 1996) wydanej przez Federalne Ministerstwo Spraw Wewnętrznych Niemiec bezpieczeństwo wewnętrzne jest traktowane jako część bezpieczeństwa narodowego wraz z następującymi jego elementami:

- → b e z p i e c z e ń s t w o p o l i t y c z n e, określane jako zachowanie ładu i porządku konstytucyjnego, a w szczególności praw i obowiązków obywateli oraz uprawnień organów państwa;
- poziom przestępczości kryminalnej, a w szczególności przestępczości zorganizowanej i terroryzmu międzynarodowego, handlu i rozpowszechniania narkotyków i środków psychotropowych wśród młodzieży, przestępczości w zakresie środowiska, korupcji wśród pracowników państwowych, przestępczości związanej z pornografią dziecięcą;
- bezpieczeństwo tajemnic państwowych i przemysłowych;
- → b e z p i e c z e ń s t w o e k o n o m i c z n e;
- ekstremizmy polityczne i pseudowyznaniowe wewnętrzne i zagraniczne;
- bezpieczeństwo i szczelność granic państwa, a w tym: polityka imigracyjna, system zabezpieczenia i kontroli granic, zabezpieczenie interesów ekonomicznych państwa na jego granicach (system kontroli celnej i skarbowej, sanitarnej, weterynaryjnej, fitosanitarnej);
- współpraca międzynarodowa organów funkcjonujących w systemie bezpieczeństwa państwa;
- stan środowiska oddziałującego bezpośrednio na zdrowie społeczeństwa.

Zdaniem A. Pieczywoka poziom bezpieczeństwa wewnętrznego jest silnie związany z poziomem bezpieczeństwa zewnętrznego (międzynarodowego). J. Zaborowski zaś utożsamia bezpieczeństwo wewnętrzne z → b e z p i e c z e ń s t w e m p u b l i c z n y m:

> bezpieczeństwo wewnętrzne to taki stan faktyczny wewnątrz państwa, który umożliwia – bez narażania na szkody z jakiegokolwiek źródła – normalne funkcjonowanie organizacji państwowej i realizację jej interesów, zachowanie życia, zdrowia i mienia jednostek żyjących w tej organizacji oraz korzystanie przez te jednostki z praw i swobód zagwarantowanych konstytucją i innymi przepisami prawa.

Majer wyodrębnia 3 podstawowe obszary bezpieczeństwa wewnętrznego: obszar bezpieczeństwa osobistego, organów państwa i egzystencji.

J. Gierszewski proponuje podział systemu bezpieczeństwa wewnętrznego na:

- podsystem bezpieczeństwa publicznego – stanowiący zbiór organów władzy i administracji publicznej, metod oraz sposobów działania związanych z ochroną życia i zdrowia obywateli, majątku narodowego przed bezprawnymi działaniami; wiodącą częścią podsystemu jest minister właściwy ds. wewnętrznych oraz komendant główny Policji;
- podsystem bezpieczeństwa powszechnego – stanowiący zbiór organów władzy i administracji publicznej, metod oraz sposobów działania związanych z ochroną życia i zdrowia obywateli, majątku narodowego przed skutkami klęsk żywiołowych i katastrof technicznych; wiodącą częścią podsystemu jest minister właściwy ds. wewnętrznych oraz komendant główny → Państwowej Straży Pożarnej [t. 3] (szef Obrony Cywilnej Kraju);
- podsystem bezpieczeństwa ustrojowego – będący zbiorem podmiotów, organów władzy publicznej i instytucji państwowych, których zadania koncentrują się na ochronie organizacji państwa; wiodącą rolę odgrywają organy władzy ustawodawczej, wykonawczej i sądowniczej.

W systemie bezpieczeństwa wewnętrznego funkcjonują również prywatne podmioty, np. agencje ochrony osób i mienia.

M. Lutostański wymienia organy i jednostki organizacyjne, zaliczając je do wyodrębnionych sektorów architektury ochrony bezpieczeństwa wewnętrznego i porządku publicznego.

- Parlamentarny sektor architektury ochrony bezpieczeństwa wewnętrznego i porządku publicznego obejmuje: Najwyższą Izbę Kontroli, Rzecznika Praw Obywatelskich, Państwową Inspekcję Pracy (wykonują one zadania finansowane ze środków publicznych).
- Rządowy sektor uzupełniający bezpieczeństwa wewnętrznego i porządku publicznego obejmuje podmioty wykonujące zadania publiczne finansowane ze środków publicznych. Są to: Agencja Rezerw Materiałowych, Państwowa Agencja Atomistyki, Główny Urząd Nadzoru Budowlanego, Inspekcja Jakości Handlowej Artykułów Rolno-Spożywczych, → Inspekcja Transportu Drogowego [t. 2], Inspekcja Weterynaryjna, Instytut Meteorologii i Gospodarki Wodnej – Państwowy Instytut Badawczy, Państwowa Inspekcja Farmaceutyczna, Państwowa Inspekcja Sanitarna, Państwowa Straż Łowiecka, Państwowa Straż Rybacka, Służba Leśna oraz Straż Leśna, Służba Parku Narodowego oraz Straż Parku, Służba Więzienna, Straż Ochrony Kolei.
- Samorządowy sektor architektury ochrony bezpieczeństwa wewnętrznego i porządku publicznego obejmuje podmioty podległe administracji samorządu terytorialnego lub przez nie administrowane, np. → straże gminne [t. 4].
- Społeczny sektor architektury ochrony mienia i osób obejmuje stowarzyszenia, do których przynależność polega na zasadzie dobrowolności, a działalność na celach

niezarobkowych mających często charakter prac społecznych, np. ochotnicze straże pożarne.

- Prywatno-komercyjny sektor architektury ochrony bezpieczeństwa osób i mienia to różnego rodzaju formy organizacyjno-prawne działalności gospodarczej w zakresie ochrony osób i mienia.
- Sektor przedsiębiorców to wewnętrzne służby ochrony powoływane przez kierowników jednostek organizacyjnych do ochrony obowiązkowo chronionych obiektów, obszarów.
- Sektor prawa jednostki do samoobrony jako element architektury ochrony bezpieczeństwa to indywidualna obrona konieczna odpierająca bezpośredni i bezpodstawny zamach na dobro chronione prawem, życie i zdrowie.

Współczesne zagrożenia przenikają się, ich podział na zagrożenia wewnętrzne i zewnętrzne staje się coraz mniej aktualny. Zadania systemu bezpieczeństwa wewnętrznego to zapewnienie bezkonfliktowego rozwoju społeczeństwa poprzez utrzymanie zdolności do reagowania (odpowiednio do zaistniałej sytuacji) w przypadku zagrożenia porządku publicznego, wystąpienia klęski, katastrofy, zagrożeń porządku konstytucyjnego i każdego innego zdarzenia powodującego lub mogącego spowodować → s y t u a c j ę k r y z y s o w ą [t. 4] w drodze zorganizowanych i zespolonych działań (tak w układzie funkcjonalnym, jak terytorialnym, wszystkich szczebli władzy i społeczności lokalnych). A. Szymonik konkretyzuje te działania, wymieniając: tworzenie spójnych przepisów prawnych, kształtowanie postaw społecznych, doskonalenie działalności wszystkich podmiotów państwowych i społecznych, których aktywność związana jest z bezpieczeństwem wewnętrznym. Będzie to jego zdaniem możliwe dzięki zwiększeniu efektywności działań administracji publicznej, podniesieniu poziomu profesjonalizmu funkcjonariuszy i pracowników administracji publicznej realizujących zadania w tej sferze oraz dzięki upowszechnianiu wiedzy o zagrożeniach bezpieczeństwa wewnętrznego państwa.

Bezpieczeństwo wewnętrzne państwa i zapewnienie jego odpowiednio wysokiego poziomu jest domeną polityki wewnętrznej kraju. Polityka ta jest ciągle udoskonalana i dostosowywana do zmieniających się uwarunkowań funkcjonowania państwa tak, aby utrzymać jak najwyższy poziom bezpieczeństwa.

Danuta Kaźmierczak

Aspekte der Inneren Sicherheit, *Bundesministerium des Innern*, Bundesministerium des Innern, Bonn 1996; A. Barcikowski, *Bezpieczeństwo wewnętrzne – różne perspektywy analityczne i doktrynalne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, t. 6, nr 11; Decyzja ramowa Rady z dnia 13 czerwca 2002 r. w sprawie zwalczania terroryzmu (2002/475/WSISW), Dz. Urz. L 164 z 22.6.2002; W. Fehler, *Bezpieczeństwo wewnętrzne współczesnej Polski*. *Aspekty praktyczne i teoretyczne*, Wydawnictwo Arte, Warszawa 2012; tenże, *Pojęcie i istota bezpieczeństwa wewnętrznego państwa*, „Przedsiębiorczość i Zarządzanie" 2009, t. 10, nr 3; J. Gierszewski, *Bezpieczeństwo wewnętrzne. Zarys systemu*, Difin, Warszawa 2013; D. Kaźmierczak, *Bezpieczeństwo wewnętrzne*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka,

R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; taż, *Cyberterrorism, Cybercrime and Cybersecurity*, [w:] *Współczesne zagrożenia w zarządzaniu i bezpieczeństwie*, J. Kuck (red.), UKiP J&D Gębka, Gliwice 2014; Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r., Dz. U. 1997, nr 78, poz. 483 (z późn. zm.); *Leksykon bezpieczeństwa wewnętrznego*, W. Fehler, J.J. Piątek, R. Podgórzańska (red.), Wydawnictwo Naukowe Wydziału Humanistycznego US Minerwa, Szczecin 2017; M. Lutostański, *Bezpieczeństwo. Uzupełniający komponent architektury ochrony bezpieczeństwa narodu i państwa*, Difin, Warszawa 2016; P. Majer, *W poszukiwaniu uniwersalnej definicji bezpieczeństwa wewnętrznego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2012, t. 7, nr 4; A. Pieczywok, *Edukacja dla bezpieczeństwa wobec zagrożeń i wyzwań współczesności*, AON, Warszawa 2012; W. Pokruszyński, *Filozoficzne aspekty bezpieczeństwa*, Wydawnictwo WSGE w Józefowie, Józefów 2011; tegoż, *Polityka i strategia bezpieczeństwa*, Wydawnictwo WSGE w Józefowie, Józefów 2011; A. Szymonik, *Organizacja i funkcjonowanie systemów bezpieczeństwa. Zarządzanie bezpieczeństwem*, Difin, Warszawa 2011; *Słownik terminów z zakresu bezpieczeństwa narodowego*, B. Zdrodowski (red.), AON, Warszawa 2008; Z. Ścibiorek i in., *Bezpieczeństwo wewnętrzne. Podręcznik akademicki*, Wydawnictwo Adam Marszałek, Toruń 2017; Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, Dz. U. 2018, poz. 2387, 2245, 2399; Dz. U. 2019, poz. 53, 125, 1091, 1726.

BEZPIECZEŃSTWO W ZAKRESIE EFEKTYWNOŚCI ENERGETYCZNEJ – całościowe podejście mające na celu zapewnienie optymalnego wykorzystania energii przy minimalnym → r y z y k u dla ludzi, środowiska i infrastruktury. Obejmuje ono zarówno zapewnienie bezpieczeństwa dostaw energii, jak i tego, że wykorzystanie tej energii jest efektywne i zgodne z zasadami → z r ó w n o w a ż o n e g o r o z w o j u [t. 4]. W praktyce bezpieczeństwo w zakresie efektywności energetycznej (zob. → b e z p i e c z e ń s t w o e n e r g e t y c z n e [t. 1]) wiąże się z identyfikacją potencjalnych zagrożeń dla systemów energetycznych oraz wdrażaniem odpowiednich środków zaradczych, które zmniejszają ryzyko wystąpienia awarii, zwiększają niezawodność i efektywność systemów oraz minimalizują negatywne skutki dla środowiska.

Efektywność energetyczna jest kluczowym elementem dążenia do zrównoważonego rozwoju i osiągnięcia globalnych celów dotyczących ochrony środowiska i ograniczenia zmian klimatycznych. Obejmuje ona wykorzystanie energii w sposób, który minimalizuje straty i zużycie zasobów, jednocześnie dostarczając potrzebne usługi energetyczne. Efektywność energetyczna jest związana z różnymi sektorami gospodarki, takimi jak budownictwo, transport, przemysł czy usługi, które wymagają energii do swojego funkcjonowania.

Ważnym czynnikiem wpływającym na efektywność energetyczną jest technologia. Innowacyjne rozwiązania, takie jak zaawansowane systemy zarządzania energią, inteligentne sieci czy wykorzystanie → o d n a w i a l n y c h ź r ó d e ł e n e r g e t y c z n y c h, mogą znacznie zwiększyć efektywność wykorzystania energii w różnych sektorach. Innymi istotnymi czynnikami wpływającymi na efektywność

energetyczną są świadomość społeczna, edukacja oraz regulacje prawne, które upowszechniają oszczędność energii i racjonalne wykorzystanie zasobów.

Poprawa efektywności energetycznej niesie liczne korzyści dla społeczeństwa i środowiska. Przede wszystkim zmniejsza emisję gazów cieplarnianych i innych substancji szkodliwych dla atmosfery, co przyczynia się do ograniczenia zmian klimatycznych. Ponadto efektywność energetyczna przyczynia się do oszczędności zasobów naturalnych, takich jak paliwa kopalne czy woda. Redukuje również koszty energii w gospodarstwach domowych, przedsiębiorstwach i instytucjach, co przekłada się na wzrost konkurencyjności, zmniejszenie ubóstwa energetycznego oraz lepszą jakość życia.

Polityki i regulacje dotyczące efektywności energetycznej są niezwykle istotne dla propagowania zrównoważonego wykorzystania energii oraz osiągania globalnych celów związanych z ochroną środowiska. Zapewnienie skutecznych i odpowiednich ram prawnych i regulacyjnych jest kluczowe dla zachęcania sektora zarówno publicznego, jak i prywatnego do podejmowania działań mających na celu zwiększenie efektywności energetycznej.

Na poziomie krajowym rządy podejmują różne środki mające na celu upowszechnianie efektywności energetycznej. Jednym z przykładów jest wprowadzenie wymogów dotyczących efektywności energetycznej dla budynków. Warunki te obejmują stosowanie nowoczesnych technologii, izolację termiczną czy wydajne systemy grzewcze i chłodzące. Stosowane są także programy dotacyjne i ulgi podatkowe, aby zachęcić przedsiębiorstwa i obywateli do inwestowania w energooszczędne technologie oraz modernizację istniejących systemów.

Na świecie istnieje wiele organizacji, które angażują się w propagowanie efektywności energetycznej na skalę globalną. Międzynarodowa Agencja Energetyczna (International Energy Agency, IEA) prowadzi badania, publikuje raporty i rekomendacje na ten temat. Organizacje, takie jak ONZ czy Unia Europejska, również tworzą dyrektywy i regulacje mające na celu zwiększenie efektywności energetycznej oraz wspierają kraje rozwijające się w osiąganiu ich celów w tym obszarze.

Analiza skuteczności istniejących polityk i regulacji jest niezbędna, aby ocenić ich wpływ na efektywność energetyczną. Wartościowe wnioski można wyciągnąć przez badanie zmian w zużyciu energii, udziału odnawialnych źródeł energii czy poprawy wydajności poszczególnych sektorów gospodarki. Te → i n f o r m a c j e [t. 2] pozwalają na identyfikację obszarów, w których można wprowadzić ulepszenia, takie jak dostosowanie regulacji, wprowadzenie nowych bodźców finansowych czy poprawa systemów monitorowania i raportowania.

Technologie i innowacje odgrywają istotną rolę w dążeniu do zrównoważonego wykorzystania energii. Inteligentne sieci energetyczne są jednym z rozwiązań, które integruje technologie informatyczne i komunikacyjne z sektorem energetycznym. Sieci te pozwalają na sprawne zarządzanie produkcją, dystrybucją i konsumpcją energii, co umożliwia optymalne wykorzystanie zasobów energetycznych. Dzięki zastosowaniu

zaawansowanych algorytmów i systemów monitoringu inteligentne sieci energetyczne mogą dynamicznie dostosowywać się do zmieniających się warunków, tym samym minimalizując straty i zwiększając efektywność systemu.

Systemy zarządzania energią, takie jak Energy Management Systems (EMS), są kolejnym ważnym narzędziem służącym poprawie efektywności energetycznej. Umożliwiają monitorowanie, kontrolę i optymalizację zużycia energii w budynkach, zakładach przemysłowych oraz infrastrukturze. Dzięki precyzyjnej analizie danych, takich jak zużycie energii, temperatura czy oświetlenie, systemy zarządzania energią identyfikują obszary, w których można wprowadzić oszczędności i efektywnie zarządzać zasobami energetycznymi.

Odnawialne źródła energii, takie jak energia słoneczna, wiatrowa czy geotermalna, również przyczyniają się do poprawy efektywności energetycznej. Postęp w technologiach umożliwia coraz bardziej efektywne i ekonomiczne wykorzystanie tych źródeł energii, co prowadzi do redukcji emisji gazów cieplarnianych i zmniejszenia zależności od paliw kopalnych.

Z kolei inwestycje w prace badawcze przyczyniają się do powstawania nowych technologii i innowacji związanych z efektywnością energetyczną. Badania koncentrują się na identyfikowaniu i opracowywaniu przyszłościowych technologii, które mogą prowadzić do dalszego zwiększenia efektywności energetycznej. Przykłady, jakie można tu wymienić, to rozwój bardziej wydajnych paneli fotowoltaicznych, zaawansowanych baterii magazynujących energię czy technologii efektywnego oświetlenia LED. Wprowadzenie nowych technologii związanych z efektywnością energetyczną wiąże się zarówno z korzyściami, jak i wyzwaniami. Analiza aspektów oraz strategie → z a r z ą d z a n i a r y z y k i e m są niezbędne, aby skutecznie wdrożyć innowacje. Korzyści obejmują redukcję emisji gazów cieplarnianych, oszczędność kosztów energii oraz wzrost niezależności energetycznej. Wdrożenie nowych technologii może jednak wymagać znacznych inwestycji finansowych, zmiany infrastruktury i reorganizacji procesów. Zarządzanie ryzykiem, takie jak analiza kosztów i korzyści, ocena stabilności systemu i identyfikacja potencjalnych zagrożeń, jest kluczowe dla zminimalizowania potencjalnych negatywnych skutków i zwiększenia szans powodzenia wprowadzanych technologii.

Związek między efektywnością energetyczną a → b e z p i e c z e ń s t w e m e n e r g e t y c z n y m [t. 1] stanowi istotny obszar badań i działań podejmowanych w zakresie globalnego systemu energetycznego. Efektywność energetyczna ma bezpośredni wpływ na zapewnienie bezpiecznego dostępu do energii. Kluczowa jest tu dywersyfikacja źródeł energii oraz redukcja zależności od jednego rodzaju paliwa. Dywersyfikacja, obejmująca wykorzystanie odnawialnych źródeł energii, energii jądrowej oraz innych alternatywnych technologii, ma na celu zmniejszenie ryzyka wystąpienia braków w dostawach energii oraz minimalizację skutków potencjalnych zakłóceń na rynku energetycznym.

Istotnym zagadnieniem w odniesieniu do efektywności energetycznej jest bezpieczeństwo cybernetyczne, ponieważ rozwój systemów energetycznych o zwiększonej efektywności niesie ze sobą nowe wyzwania i → z a g r o ż e n i a [t. 4]. Przegląd tych kwestii pozwala na lepsze zrozumienie potrzeby ochrony infrastruktury energetycznej oraz zastosowania odpowiednich metod i praktyk bezpieczeństwa cybernetycznego.

Systemy energetyczne o zwiększonej efektywności często opierają się na zaawansowanych technologiach informatycznych, takich jak systemy zarządzania energią, inteligentne sieci energetyczne czy urządzenia internetu rzeczy (Internet of Things, IoT). Wprowadzenie tych technologii niesie ze sobą ryzyko ataków cybernetycznych, które mogą prowadzić do zakłóceń w dostawie energii, utraty danych czy zagrożenia dla bezpieczeństwa osób i mienia.

Ochrona infrastruktury energetycznej przed atakami cybernetycznymi i innymi zagrożeniami wymaga zastosowania odpowiednich środków. Są to m.in. wdrożenie skutecznych systemów wykrywania incydentów i reagowania na nie, zastosowanie silnych mechanizmów uwierzytelniania i kontroli dostępu, regularne audyty bezpieczeństwa oraz szkolenia personelu w zakresie ochrony przed zagrożeniami cybernetycznymi. Metody, techniki i praktyki bezpieczeństwa cybernetycznego stosowane w sektorze energetycznym obejmują również: monitorowanie ruchu sieciowego, szyfrowanie danych, tworzenie kopii zapasowych, segmentację sieci, weryfikację oprogramowania czy ciągłe aktualizacje i łatki zabezpieczeń. Istotnym aspektem jest również współpraca między podmiotami sektora energetycznego, organami regulacyjnymi oraz służbami odpowiedzialnymi za bezpieczeństwo cybernetyczne w celu wymiany informacji, analizy zagrożeń i opracowania skutecznych strategii obronnych.

Wymogi prawne i regulacje dotyczące bezpieczeństwa cybernetycznego w sektorze energetycznym mają na celu zapewnienie ochrony infrastruktury i danych przed atakami. Organizacje odpowiedzialne za dostarczanie energii są zobligowane do spełniania określonych standardów bezpieczeństwa, które są wskazane w odpowiednich regulacjach prawnych. Przykładem jest Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (tzw. → d y r e k t y w a N I S). Określa ona wymogi dotyczące → o c h r o n y i n f r a s t r u k t u r y k r y t y c z n e j [t. 5], w tym sektora energetycznego, przed zagrożeniami cybernetycznymi.

Z punktu widzenia efektywności energetycznej konieczne jest uwzględnienie aspektów bezpieczeństwa cybernetycznego. Ochrona infrastruktury energetycznej przed atakami i zagrożeniami wymaga zastosowania odpowiednich metod, technik i praktyk bezpieczeństwa oraz przestrzegania obowiązujących regulacji i wymogów prawnych. Wprowadzenie skutecznych rozwiązań → c y b e r b e z p i e c z e ń s t w a [t. 1] pozwoli zapewnić stabilność i niezawodność systemów energetycznych oraz chronić

dane i infrastrukturę przed atakami, przyczyniając się tym samym do dalszego rozwoju efektywności energetycznej w sposób bezpieczny i zrównoważony.

Obok aspektu technologicznego niezmiernie ważne jest zagadnienie wpływu efektywności energetycznej na społeczeństwo i gospodarkę. Przegląd społecznych i ekonomicznych aspektów efektywności energetycznej pozwala na lepsze zrozumienie korzyści, wyzwań i analizy kosztów z nią związanych.

Jednym z kluczowych społecznych zagadnień w tym obszarze jest tworzenie miejsc pracy. Wdrażanie nowych technologii i rozwiązań, takich jak odnawialne źródła energii czy innowacyjne systemy zarządzania energią, generuje zapotrzebowanie na wykwalifikowaną siłę roboczą. Tworzenie miejsc pracy w sektorze energetycznym przyczynia się do wzrostu zatrudnienia, poprawy warunków życia i redukcji bezrobocia. Dodatkowo rozwój lokalnych branż związanych z efektywnością energetyczną, takich jak producenci urządzeń energooszczędnych czy firmy świadczące usługi audytu energetycznego, przyczynia się do wzrostu zatrudnienia na poziomie lokalnym.

Efektywność energetyczna odgrywa również istotną rolę w redukcji ubóstwa energetycznego. Jej poprawa może pomóc w obniżeniu kosztów energii, szczególnie w wypadku osób o niższych dochodach, co pozwala na dostęp do niezbędnej energii bez nadmiernego obciążenia finansowego. Ponadto wdrażanie efektywności energetycznej może wpływać na poprawę jakości życia przez zapewnienie lepszych warunków termicznych w budynkach, co ma znaczenie szczególnie w okresach ekstremalnych temperatur.

Efektywność energetyczna ma także istotny wpływ na gospodarkę. Jej poprawa przyczynia się do wzrostu konkurencyjności przedsiębiorstw przez obniżenie kosztów operacyjnych. Redukcja zużycia energii prowadzi do oszczędności, które mogą być reinwestowane w inne obszary gospodarki. Dzięki temu wzrasta inwestycyjna zdolność przedsiębiorstw, co sprzyja rozwojowi i tworzeniu nowych miejsc pracy.

Wdrożenie efektywności energetycznej wiąże się jednak z różnymi wyzwaniami społecznymi i ekonomicznymi. Jednym z nich jest dostępność finansowania. Inwestycje w nowe technologie i systemy energetyczne mogą wymagać znacznych nakładów, które nie zawsze są łatwo dostępne dla wszystkich podmiotów. Konieczne jest opracowanie skutecznych mechanizmów finansowania i zachęt, takich jak subsydia, ulgi podatkowe czy instrumenty wsparcia finansowego, aby umożliwić szerokie wdrożenie efektywności energetycznej. Również inwestycje publiczne w infrastrukturę energetyczną mogą odegrać istotną rolę w upowszechnianiu efektywności energetycznej.

Kolejny ważny aspekt to świadomość społeczna i edukacja. Wiele osób nie zdaje sobie sprawy z korzyści, jakie płyną z efektywności energetycznej, ani z możliwości wdrożenia odpowiednich rozwiązań. Wzrost świadomości społecznej i edukacja są kluczowe dla rozpropagowania zmiany postaw i zachowań, co przyczyni się do zwiększenia efektywności energetycznej na szeroką skalę. Kampanie informacyjne i programy edukacyjne poszerzają wiedzę społeczeństwa na temat efektywności energetycznej, mogąteż zachęcić do podejmowania działań na rzecz oszczędzania energii.

Analiza kosztów i korzyści odgrywa istotną rolę przy podejmowaniu decyzji dotyczących inwestycji w efektywność energetyczną. Właściwa ich ocena pozwala określić opłacalność inwestycji, zwrot z inwestycji oraz efekty ekonomiczne i społeczne wynikające z poprawy efektywności energetycznej. Czynniki, takie jak koszty wdrożenia, oszczędności operacyjne, korzyści środowiskowe czy społeczne, muszą być uwzględniane w analizie, aby można było podjąć świadomą decyzję i maksymalnie wykorzystać potencjał efektywności energetycznej.

Ryzyko związane z niewydolnością lub awarią systemów energetycznych to kolejny ważny aspekt, który ma wpływ na efektywność energetyczną oraz bezpieczeństwo energetyczne. Systemy energetyczne są podatne na różnego rodzaju zagrożenia, takie jak awarie infrastruktury, zakłócenia w dostawach energii czy ataki cybernetyczne. Te ryzyka mogą prowadzić do przerw w dostawach energii, spadku efektywności energetycznej oraz naruszenia bezpieczeństwa energetycznego. Dlatego istotne jest opracowanie strategii zarządzania ryzykiem, które uwzględniają aspekty zarówno efektywności energetycznej, jak i bezpieczeństwa energetycznego.

Aby zapewnić bezpieczeństwo energetycznego przy jednoczesnym propagowaniu efektywności energetycznej, konieczne jest opracowanie odpowiednich → s t r a t e g i i [t. 5]. Jednym z głównych podejść jest zwiększenie elastyczności i zdolności adaptacyjnych systemu energetycznego, co pozwala na lepsze radzenie sobie z potencjalnymi zagrożeniami. Ważnym elementem jest również rozwój inteligentnych sieci energetycznych, które umożliwiają efektywne zarządzanie energią, monitorowanie systemów oraz szybką reakcję na ewentualne problemy. Ponadto niezbędne są inwestycje w rozwój i modernizację infrastruktury energetycznej oraz upowszechnianie innowacyjnych rozwiązań technologicznych.

Związki między efektywnością energetyczną a bezpieczeństwem energetycznym są nieodłącznymi elementami globalnego systemu energetycznego. Dywersyfikacja źródeł energii, zarządzanie ryzykiem oraz rozwój nowoczesnych technologii stanowią kluczowe czynniki, które pozwalają na osiągnięcie zarówno efektywności energetycznej, jak i bezpieczeństwa energetycznego. Świadome podejście do tych zagadnień jest niezbędne dla zrównoważonego rozwoju oraz stabilności systemu energetycznego w długiej perspektywie czasowej.

Aleksander Wasiuta

A. Bieńkowska i in., *Bezpieczeństwo energetyczne – koordynacja działań na regionalnym i lokalnym rynku energii*, „Rynek Energii" 2011, nr 2; W. Dołęga, *Efektywność energetyczna w aspekcie bezpieczeństwa dostaw energii i bezpieczeństwa ekologicznego*, „Rynek Energii" 2014, nr 2; tenże, *Wybrane aspekty efektywności energetycznej*, „Polityka Energetyczna" 2017, t. 20, z. 4; Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz.Urz. UE L 194 z 19.07.2016; I.M. Jankowska, *Bezpieczeństwo energetyczne w polityce bezpieczeństwa państwa*, „Studia Lubuskie" 2015, t. 11; M. Mastalerska, *Znaczenie efektywności energetycznej dla bezpieczeństwa energetycznego*

kraju, „Polityka Energetyczna" 2011, t. 14, z. 1; J. Misiągiewicz, *Bezpieczeństwo energetyczne Unii Europejskiej. Implikacje nowych projektów infrastruktury gazociągowej w Europie*, Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, Lublin 2019; T. Młynarski, *Bezpieczeństwo energetyczne i ochrona klimatu w drugiej dekadzie XXI wieku. Energia – środowisko – klimat*, Wydawnictwo UJ, Kraków 2017; K. Olczak, *Odnawialne źródła energii jako przesłanka prawna bezpieczeństwa energetycznego*, „Studia Prawno-Ekonomiczne" 2020, nr 117; J. Paska, T. Surma, *Wpływ polityki energetycznej Unii Europejskiej na funkcjonowanie przedsiębiorstw energetycznych w Polsce*, „Rynek Energii" 2016, nr 2/123; R. Rolbiecki, *Bezpieczeństwo energetyczne Unii Europejskiej a polityka energetyczna w transporcie*, „Współczesna Gospodarka" 2015, t. 6, nr 2; T. Skoczkowski, S. Bielecki, *Efektywność energetyczna – polityczno-formalne uwarunkowania rozwoju w Polsce i Unii Europejskiej*, „Polityka Energetyczna" 2016, t. 19, z. 1; R. Szczerbowski, *Bezpieczeństwo energetyczne Polski – mix energetyczny i efektywność energetyczna*, „Polityka Energetyczna" 2013, t. 16, z. 4; M. Zajączkowska, *Efekty realizacji założeń Europejskiej strategii bezpieczeństwa energetycznego dotyczących efektywności energetycznej w Polsce*, „Horyzonty Polityki" 2017, t. 8, nr 23.

BEZPIECZEŃSTWO W ZAKRESIE WYDOBYCIA SUROWCÓW ENERGETYCZNYCH – jeden z kluczowych obszarów, które mają ogromne znaczenie dla globalnej gospodarki i → b e z p i e c z e ń s t w a e n e r g e t y c z n e g o [t. 1] państw. Wydobycie surowców energetycznych, takich jak paliwa kopalne czy surowce nuklearne, jest nieodzowne dla zaspokojenia rosnącego zapotrzebowania na energię na całym świecie. Wraz ze wzrostem znaczenia sektora wydobycia surowców energetycznych pojawiają się jednak liczne wyzwania związane z bezpieczeństwem pracowników, ze środowiskiem naturalnym i stabilnością społeczną.

Surowce energetyczne to wszelkie substancje, materiały lub zasoby, które są wykorzystywane do produkcji energii. Obejmują one zarówno → k o n w e n c j o n a l n e ź r ó d ł a e n e r g i i , takie jak paliwa kopalne (węgiel, ropa naftowa, gaz ziemny), jak i surowce nuklearne (uran). Definicje surowców energetycznych mogą się różnić w zależności od uwarunkowań i rodzaju energii, którą mają generować.

Znaczenie surowców energetycznych dla gospodarki światowej jest nieocenione. To właśnie dzięki nim możemy napędzać maszyny, ogrzewać nasze domy, oświetlać miasta i rozwijać technologie, które przyczyniają się do postępu społecznego i ekonomicznego. Paliwa kopalne od dziesięcioleci stanowiły główne źródło energii, jednak w ostatnich latach rosnące obawy dotyczące zmian klimatycznych i potrzeba ograniczenia emisji gazów cieplarnianych skierowały naszą uwagę na → o d n a w i a l n e ź r ó d ł a e n e r g e t y c z n e oraz surowce nuklearne.

Do paliw kopalnych zalicza się węgiel, ropę naftową i gaz ziemny. Są one wykorzystywane zarówno do produkcji energii elektrycznej, jak i jako paliwa w transporcie. Stanowią one główne źródło energii w wielu krajach na świecie, jednak ich wydobycie, a potem spalanie wiąże się z emisją gazów cieplarnianych oraz negatywnymi skutkami dla środowiska.

Surowce nuklearne, głównie uran, są wykorzystywane w elektrowniach jądrowych do generowania energii elektrycznej. Energia jądrowa charakteryzuje się wysoką

wydajnością i niską emisją gazów cieplarnianych, jednak wydobycie i przetwarzanie uranu powodują poważne → z a g r o ż e n i a [t. 4] związane zarządzaniem odpadami radioaktywnymi. Odnawialne źródła energii obejmują energię słoneczną, wiatrową, wodną, geotermalną i biomasy. Aby wygenerować energię, wykorzystuje się naturalne procesy i zasoby, takie jak promieniowanie słoneczne, wiatr czy ruch wody. Zainteresowanie tymi źródłami energii rośnie ze względu na ich niewyczerpalność i minimalny wpływ na środowisko, jednak wydobycie i przetwarzanie niektórych surowców potrzebnych do produkcji technologii odnawialnych mogą wiązać się z pewnymi wyzwaniami i skutkami środowiskowymi.

Wzrost światowej populacji, rozwój gospodarczy oraz postęp technologiczny prowadzą do coraz większego zapotrzebowania na surowce energetyczne. Zwiększa się popyt zarówno na tradycyjne, jak i alternatywne źródła energii. Bezpieczne i efektywne wydobycie surowców energetycznych jest niezbędne, aby zapewnić stabilność dostaw energii, zaspokoić potrzeby przemysłu, transportu oraz sektora energetycznego. Właściwe zarządzanie wydobyciem surowców ma duże znaczenie dla bezpieczeństwa energetycznego państw i stabilności światowej gospodarki. Wyzwania związane z przemysłem wydobywczym wymagają podejścia, które uwzględnia aspekty zarówno techniczne, jak i społeczne, ekonomiczne oraz środowiskowe.

Bezpieczeństwo w zakresie wydobycia surowców energetycznych jest niezwykle istotnym zagadnieniem, które wiąże się z wieloma wyzwaniami i zagrożeniami. Wydobycie surowców energetycznych, takich jak paliwa kopalne, surowce nuklearne czy odnawialne źródła energii, może prowadzić do potencjalnych zagrożeń dla pracowników, środowiska naturalnego oraz społeczności lokalnych. Aby osiągnąć bezpieczne i zrównoważone wydobycie surowców energetycznych, konieczne jest dokładne zidentyfikowanie zagrożeń i → r y z y k a, które są z nim bezpośrednio związane, oraz opracowanie odpowiednich strategii zarządzania nimi. Wśród niebezpieczeństw w tym obszarze znajdują się:

- wypadki i obrażenia pracowników – praca w trudnych warunkach oraz używanie ciężkiego sprzętu i substancji chemicznych mogą prowadzić do wypadków i obrażeń pracowników;
- eksplozje i pożary – niektóre surowce energetyczne, zwłaszcza paliwa kopalne, mogą być podatne na eksplozje i pożary;
- skutki górnicze – wydobycie surowców energetycznych często wiąże się z wykopywaniem ziemi i zniszczeniem krajobrazu. Może to prowadzić do erozji gleby, degradacji środowiska naturalnego oraz zmian w krajobrazie, co negatywnie wpłynie na lokalne ekosystemy;
- emisja gazów cieplarnianych i zanieczyszczenie powietrza – niektóre procesy wydobycia i spalania surowców energetycznych mogą prowadzić do emisji gazów cieplarnianych i zanieczyszczenia powietrza, co przyczynia się do zmian klimatycznych i negatywnie wpływa na jakość powietrza;

- z agrożenie dla wód podziemnych i powierzchniowych – wydobycie surowców energetycznych może prowadzić do zanieczyszczenia wód podziemnych i powierzchniowych, zwłaszcza w wypadku nieszczelności infrastruktury górniczej lub wycieków substancji chemicznych stosowanych w procesach wydobywczych.

Odpowiednie środki bezpieczeństwa i → o c h r o n y z d r o w i a [t. 3]pracowników są niezwykle istotne w sektorze wydobycia surowców energetycznych. Wprowadzenie szkoleń, procedur bezpieczeństwa i nadzoru nad stanem zdrowia pracowników może znacznie zmniejszyć ryzyko wypadków i chorób zawodowych. Ochrona przed substancjami chemicznymi, odpowiednie wyposażenie ochronne i monitorowanie warunków pracy to kluczowe aspekty, które należy uwzględnić.

Wydobycie surowców energetycznych często prowadzi do negatywnych skutków środowiskowych. Wycinka lasów, degradacja siedlisk, zmiany hydrologiczne czy emisja substancji chemicznych do środowiska to tylko niektóre z możliwych konsekwencji. Konieczne jest podejmowanie odpowiednich działań, takich jak rekultywacja terenów górniczych czy zastosowanie metod wydobywczych minimalizujących wpływ na środowisko, aby zmniejszyć negatywne oddziaływanie przemysłu wydobywczego na lokalne ekosystemy.

W niektórych regionach wydobycie surowców energetycznych może prowadzić do poważnych konfliktów społecznych. Często dochodzi do sporów o prawa własności, korzystanie z zasobów naturalnych czy sprawiedliwy podział zysków. Konieczne jest uwzględnienie aspektów społecznych i dialogu z lokalnymi społecznościami, aby minimalizować konflikty i propagować zrównoważone podejście do wydobycia surowców energetycznych. Bezpieczeństwo w zakresie wydobycia surowców energetycznych jest zagadnieniem wielowymiarowym, które wymaga całościowego podejścia. Proces wydobycia ropy naftowej, gazu ziemnego i węgla wiąże się z wieloma zagrożeniami i ryzykiem dla pracowników oraz środowiska naturalnego. Aby zapewnić bezpieczne i zrównoważone wydobycie paliw kopalnych, konieczne jest zrozumienie technik wydobywczych (np. odwierty, szczelinowanie hydrauliczne skał, górnictwo) oraz stosowanie odpowiednich technologii i procedur mających na celu minimalizację ryzyka i poprawę → b e z p i e c z e ń s t w a [t. 1] w tym sektorze. Każda z tych technik niesie specyficzne zagrożenia. Na przykład odwierty mogą prowadzić do wycieków ropy naftowej, skażeń wód podziemnych lub uszkodzenia geologicznego. Szczelinowanie hydrauliczne może spowodować wycieki chemikaliów, skażenie wód powierzchniowych oraz trzęsienia ziemi. Górnictwo niesie ryzyko tąpnięć, zawalania się chodników czy wystąpienia pożarów podziemnych.

Aby minimalizować ryzyko i poprawić bezpieczeństwo w sektorze paliw kopalnych, stosuje się różne technologie i innowacyjne rozwiązania, np.:

- zaawansowane techniki wiertnicze i monitorowanie geologiczne, co zmniejsza ryzyko wycieków i uszkodzeń geologicznych;

- technologię bezpiecznego szczelinowania hydraulicznego skał, co minimalizuje ryzyko wycieków i wpływu na środowisko;
- zaawansowane systemy monitorowania i kontroli, co pozwala na szybką reakcję na pojawiające się zagrożenia, takie jak wycieki czy pożary;
- nowoczesne urządzenia ochrony osobistej, które zwiększają bezpieczeństwo pracowników podczas wydobywania paliw kopalnych;
- szkolenia pracowników zwiększające ich świadomość zagrożeń i umiejętności zarządzania sytuacjami awaryjnymi.

Bezpieczeństwo w wydobyciu paliw kopalnych jest kluczowym aspektem, który musi być priorytetem dla branży. Identyfikacja zagrożeń i zarządzanie nimi oraz stosowanie odpowiednich technologii mogą pomócw minimalizacji ryzyka i poprawie bezpieczeństwa w tym sektorze. Wdrażanie innowacyjnych rozwiązań, monitorowanie środowiska naturalnego i ciągłe doskonalenie procedur są niezbędne dla zagwarantowania bezpiecznego i zrównoważonego wydobycia paliw kopalnych.

Wydobycie surowców nuklearnych również wiąże się z różnymi zagrożeniami i ryzykiem zarówno dla pracowników, jak i dla środowiska. Aby zapewnić bezpieczne wydobycie tych surowców, ważne jest także zrozumienie procedur, technologii oraz stosowanie rygorystycznych norm i regulacji mających na celu minimalizację ryzyka i ochronę zdrowia ludzi oraz środowiska.

Wydobycie uranu wymaga korzystania z różnych technik, takich jak wydobycie w kopalniach podziemnych lub odkrywkowych, a każda z nich niesie ze sobą specyficzne ryzyko. Zagrożenia związane z wydobyciem uranu obejmują wypadki górnicze, skażenie środowiska, narażenie pracowników na promieniowanie jonizujące oraz problemy zdrowotne związane z długotrwałą ekspozycją na uran i jego produkty rozpadu. Ponadto transport uranu musi odbywać się zgodnie z odpowiednimi normami, aby minimalizować ryzyko wypadków, kradzieży czy nieautoryzowanego dostępu do materiałów nuklearnych.

Ochrona pracowników w zakładach wydobywczych uranu jest niezwykle istotna. Pracownicy są narażeni na promieniowanie jonizujące i skażenie chemikaliami, wypadki z użyciem maszyn i sprzętu czy szkodliwe warunki pracy. Konieczne jest wprowadzenie odpowiednich procedur bezpieczeństwa, takich jak noszenie odpowiedniego sprzętu ochronnego, regularne badania medyczne, szkolenia z zakresu bezpiecznej pracy, a także monitorowanie warunków pracy w celu zapewnienia pracownikom jak najwyższego poziomu ochrony.

Ważne jest również właściwe zarządzanie odpadami radioaktywnymi, tak aby zapobiec ich niekontrolowanemu rozprzestrzenianiu się i minimalizować wpływ na środowisko i → z d r o w i e p u b l i c z n e [t. 4]. Wymaga to przestrzegania restrykcyjnych przepisów, odpowiedniego składowania i utylizacji odpadów oraz monitorowania środowiska wokół zakładów przetwarzających uran.

Wyzwania i zagrożenia środowiskowe pojawiają się również w związku z wydobyciem surowców niezbędnych do produkcji urządzeń wykorzystywanych w energetyce

odnawialnej, takich jak lit, kobalt czy cynk. Procesy wydobywcze niejednokrotnie realizowane są w trudno dostępnych obszarach geograficznych. Ponadto mogą powodować negatywne skutki dla środowiska naturalnego, np. wyciek substancji chemicznych do gleby lub wód, degradację ekosystemów, emisję gazów cieplarnianych czy znaczne zużycie wody. Tu również potrzebne są odpowiednie procedury, by minimalizować ryzyko wypadków, skażenia środowiska i negatywnego wpływu na zdrowie pracowników. Ważne jest także kontrolowanie łańcucha dostaw surowców od ich wydobycia do przetwarzania, aby zapewnić zrównoważone i odpowiedzialne praktyki na każdym etapie produkcji.

Wydobycie surowców dla technologii energii odnawialnej niejednokrotnie ma wpływ na społeczności lokalne. Może wywoływać konflikty dotyczące własności ziemi, wypierania ludności lokalnej, braku udziału społecznego czy naruszenia → p r a w c z ł o w i e k a [t. 3]. W związku z tym ważne jest uwzględnienie społecznych i etycznych aspektów przemysłu wydobywczego, dążenie do transparentności, odpowiedzialności społecznej i dialogu z miejscową ludnością oraz uwzględnienie interesów lokalnych społeczności.

Zapobieganie → k r y z y s o m [t. 2] w sektorze wydobywczym i zarządzanie nimi to kwestia o kluczowym znaczeniu dla utrzymania bezpiecznego i niezakłóconego procesu wydobycia. Aby skutecznie zarządzać kryzysami w tym sektorze, konieczne jest zastosowanie odpowiednich systemów monitorowania, wczesnego ostrzegania oraz planowania awaryjnego. Monitorowanie pozwala wykryć wczesne sygnały nadchodzących zagrożeń, co umożliwia szybką reakcję. Takie systemy mogą obejmować monitoring parametrów technicznych, środowiskowych oraz zdrowotnych pracowników. Gdy dojdzie do → s y t u a c j i k r y z y s o w y c h [t. 4], takich jak wypadki, awarie lub inne nieprzewidziane zdarzenia, wdrażane są plany awaryjne i procedury reagowania. Powinny one zawierać wytyczne działania na wypadek różnych scenariuszy kryzysowych, określać odpowiedzialność i zadania oraz precyzować komunikację wewnętrzną i zewnętrzną. Ważne, aby pracownicy byli przeszkoleni w zakresie tych procedur i regularnie uczestniczyli w ćwiczeniach, co pozwoli zapewnić skuteczność planów awaryjnych w rzeczywistych sytuacjach kryzysowych.

Bezpieczeństwo w sektorze wydobycia surowców energetycznych często wymaga współpracy na poziomie międzynarodowym. Wymiana → i n f o r m a c j i [t. 2], doświadczeń i najlepszych praktyk między państwami oraz współpraca techniczna mogą przyczynić się do poprawy bezpieczeństwa w sektorze wydobywczym. Organizacje międzynarodowe, takie jak Międzynarodowa Agencja Energii Atomowej czy Organizacja Narodów Zjednoczonych ds. Wyżywienia i Rolnictwa, odgrywają istotną rolę w koordynowaniu działań w tym zakresie.

Przyszłość bezpieczeństwa w zakresie wydobycia surowców energetycznych jest dynamicznie kształtowana przez trendy rozwojowe, wśród których można wymienić:

- zmiany popytu na surowce energetyczne w związku z transformacją energetyczną i dążeniem do → z r ó w n o w a ż o n e g o r o z w o j u [t. 4];

- wpływ nowych technologii i osiągnięć technicznych, takich jak sztuczna inteligencja, automatyka czy analiza danych, na procesy wydobycia surowców energetycznych;
- rozwój nowych obszarów wydobycia, takich jak wydobycie gazu łupkowego czy ropy naftowej z trudno dostępnych złóż.

Nie do przecenienia są także innowacyjne rozwiązania, które poprawiają bezpieczeństwo w przemyśle wydobywczym:

- zastosowanie zaawansowanych technologii i urządzeń monitorujących w celu poprawy bezpieczeństwa pracowników oraz ograniczenia ryzyka wystąpienia wypadków;
- wykorzystanie systemów wczesnego ostrzegania i monitorowania parametrów środowiskowych w celu zapobiegania potencjalnym katastrofom ekologicznym;
- wdrażanie nowoczesnych rozwiązań → z a r z ą d z a n i a r y z y k i e m, takich jak analiza predykcyjna czy modelowanie matematyczne, aby lepiej prognozować i minimalizować zagrożenia.

Coraz większe znaczenie zyskują alternatywne źródła energii, które również wpływają na bezpieczeństwo wydobycia surowców energetycznych:

- rozwój technologii odnawialnych, takich jak energia słoneczna, wiatrowa czy geotermalna jako alternatywy dla tradycyjnych surowców energetycznych;
- rola recyklingu i odzysku surowców w zmniejszaniu zapotrzebowania na nowe wydobycie;
- skutki transformacji energetycznej na sektor wydobycia surowców energetycznych i potrzeba dostosowania procesów wydobycia do zmieniających się warunków rynkowych i technologicznych.

Przyszłość bezpieczeństwa w zakresie wydobycia surowców energetycznych jest dynamiczna i wymaga ciągłego monitorowania trendów, wprowadzania innowacyjnych rozwiązań oraz dostosowania się do zmieniających się warunków. Ważne jest również podejmowanie działań mających na celu minimalizację negatywnego wpływu wydobycia surowców na środowisko, zapewnienie bezpieczeństwa pracownikom oraz uwzględnienie interesów społeczności lokalnych.

Aleksander Wasiuta

V. Drábik, K. Galicki, I. Protasowicki, *Wpływ systemów przesyłowych surowców energetycznych na kształtowanie bezpieczeństwa energetycznego Polski*, „Zeszyty Naukowe WSIZiA" 2016, t. 14, z. 2(35); A. Gawęda, *Przyszłość polskiej energetyki z wykorzystaniem bazy zasobowej surowców energetycznych*, „Systemy Wspomagania w Inżynierii Produkcji" 2018, vol. 1, no. 7; P. Majchrzak, *Bezpieczeństwo energetyczne Polski ze szczególnym uwzględnieniem województwa małopolskiego*, praca licencjacka, Kraków 2013; J. Mazurkiewicz. *Bezpieczeństwo energetyczne Polski*, „Polityka Energetyczna" 2008, t. 11, z. 1; E. Mokrzycki, R. Ney, J. Siemek, *Światowe zasoby surowców energetycznych – wnioski dla Polski*, „Rynek Energii" 2008, nr 6; A. Mrozowska, *Organizacja pracy przy wydobyciu surowców energetycznych spod dna morskiego*, „Zeszyty Naukowe Akademii Marynarki Wojennej" 2011, R. 52, nr 4(187);

T. Olkuski i in., *Prognozy wydobycia, konsumpcji i salda wymiany surowców energetycznych w Polsce*, „Polityka Energetyczna" 2017, t. 20, z. 2; M. Paszkowski, *Specyfika badań politologicznych nad myślą polityczną w zakresie bezpieczeństwa energetycznego państwa*, „Humanities and Social Sciences" 2015, t. 20, nr 2; J. Sokołowski, *Rozważania o stanie bezpieczeństwa energetycznego państwa*, „Technika Poszukiwań Geologicznych" 2002, R. 41, nr 3; T. Szubrycht, *Współczesne aspekty bezpieczeństwa państwa*, „Zeszyty Naukowe Akademii Marynarki Wojennej" 2006, R. 47, nr 4(167).

BEZPIECZEŃSTWO ZDROWOTNE – zdrowie stanowi jedną z najważniejszych wartości w życiu człowieka, a bezpieczeństwo zdrowotne jest prawem każdego obywatela. Prawo to reguluje Konstytucja Rzeczypospolitej Polskiej. Z nim połączony jest wynikający z art. 68 ustawy zasadniczej:

> obowiązek zapewnienia przez państwo równego dostępu do świadczeń zdrowotnych, opieki zdrowotnej kobietom ciężarnym, dzieciom, niepełnosprawnym oraz osobom starszym, zwalczania epidemii i degradacji środowiska naturalnego oraz rozwoju kultury fizycznej.

Zdrowie klasyfikuje się jako wartość odczuwaną (wówczas jest postrzegane przez jednostkę jako cenne) i/lub uznawaną (bazującą na powszechnym przekonaniu, że należy je cenić). Dla jednych jest wartością uroczystą (wyższą, publicznie manifestowaną), a dla innych wartością codzienną (uwzględnianą podczas realizacji prywatnych celów). W literaturze przedmiotu jest także postrzegane jako wartość deklarowana bądź realizowana. Gruntowne zrozumienie istoty bezpieczeństwa zdrowotnego wymaga odwołania się do wielu dyscyplin naukowych, takich jak: → n a u k i o b e z p i e c z e ń s t w i e [t. 3], nauki medyczne, nauki o zdrowiu, nauki o polityce, pedagogika, psychologia, nauki o zarządzaniu, nauki przyrodnicze, nauki rolnicze, nauki o kulturze fizycznej czy prawo (na podstawie wykazu obszarów wiedzy, dziedzin nauki i sztuki oraz dyscyplin naukowych i artystycznych opublikowanego przez Ministerstwo Nauki i Szkolnictwa Wyższego). Obecność tak wielu obszarów dociekań naukowych czyni bezpieczeństwo zdrowotne zagadnieniem interdyscyplinarnym.

Bezpieczeństwo zdrowotne zostało sklasyfikowane w międzynarodowych raportach i w literaturze przedmiotu, choć niewiele dostępnych materiałów pozwala spojrzeć na jego problematykę w sposób kompleksowy. W Raporcie o rozwoju społecznym (Human Development Programme, HDR) Programu Organizacji Narodów Zjednoczonych ds. Rozwoju (United Nations Development Programme, UNDP) z 1994 r. bezpieczeństwo zdrowotne zostało wyodrębnione tuż obok → b e z p i e c z e ń s t w a e k o n o m i c z n e g o, żywności, środowiskowego, osobistego, → b e z p i e c z e ń s t w a s p o ł e c z n e g o oraz → b e z p i e c z e ń s t w a p o l i t y c z n e g o. Szczególne zasługi w zakresie promowania założeń bezpieczeństwa zdrowotnego w ramach dyscypliny nauk o bezpieczeństwie należy przypisać M. Cieślarczykowi, który dokonał klasyfikacji rodzajów bezpieczeństwa człowieka. Bezpieczeństwo zdrowotne i → b e z p i e c z e ń s t w o e k o l o g i c z n e znalazło się u podstaw stworzonej

przez autora piramidy bezpieczeństwa. Podobnego zabiegu dokonał H. Kromołowski. W przedmiotowym wymiarze bezpieczeństwa wskazał on bezpieczeństwo zdrowotne obok bezpieczeństwa politycznego, ekonomicznego, ekologicznego, społecznego, socjalnego, biologicznego, → b e z p i e c z e ń s t w a p u b l i c z n e g o, żywnościowego, → b e z p i e c z e ń s t w a k u l t u r o w e g o, → b e z p i e c z e ń s t w a i d e o l o g i c z n e g o, → b e z p i e c z e ń s t w a m i l i t a r n e g o, → b e z p i e c z e ń s t w a e n e r g e t y c z n e g o, → b e z p i e c z e ń s t w a i n f o r m a c y j n e g o oraz atomowego/jądrowego.

Zrozumienie istoty i uwarunkowań bezpieczeństwa zdrowotnego wymaga zdefiniowania pojęć → b e z p i e c z e ń s t w a oraz zdrowia. Definicję bezpieczeństwa zdrowotnego należy odnieść do 2 sposobów rozumienia bezpieczeństwa, które określa się jako stan oraz proces. Ujęcie pierwsze obejmuje zarówno subiektywne odczucia podmiotu, jak i obiektywnie istniejące → z a g r o ż e n i a [t. 4]. Drugie ujęcie bezpieczeństwa zdrowotnego dotyczy działań ustawicznie podejmowanych w celu diagnozowania zagrożeń zdrowotnych, rozwijania umiejętności właściwego reagowania na wyzwania i zagrożenia zdrowotne, jak również postawy troski o zapewnienie społeczeństwu takiej jakości życia, która umożliwi samorealizację. Wyodrębniając za R. Ziębą 2 wymiary bezpieczeństwa – negatywny i pozytywny – należy dodatkowo akcentować w ramach bezpieczeństwa zdrowotnego z jednej strony potrzebę eliminacji choroby i czynników ryzyka, natomiast z drugiej konieczność wsparcia człowieka w dążeniu do dobrostanu oraz wzmacniania czynników chroniących go przed zagrożeniami zdrowotnymi. Podobne orientacje prezentowane są w definicji i typologii zdrowia.

Wśród definicji zdrowia najbardziej aktualne, a zarazem powszechne jest wyjaśnienie proponowane przez → Ś w i a t o w ą O r g a n i z a c j ę Z d r o w i a [t. 4] (World Health Organization, WHO). Zdrowie w ujęciu WHO stanowi podstawę bezpieczeństwa i pokoju na całym świecie. Złożony charakter tego pojęcia wymaga odniesienia go do fizycznego, psychicznego i społecznego dobrostanu człowieka, nie zaś wyłącznie do braku choroby czy kalectwa. Stąd w literaturze spotykamy klasyfikację opartą na patogenetycznym i salutogenetycznym modelu zdrowia (A. Antonovsky). Pierwszy koncentruje się na chorobach i czynnikach ryzyka, a drugi na sposobach osiągania zdrowia i szczęścia.

Kryteria oceny zdrowia można porównać do kryteriów oceny bezpieczeństwa. Wśród nich M. Sygit wyodrębnił:

- kryteria subiektywne – osobiste odczucia dotyczące zdrowia i samopoczucia;
- kryteria obiektywne – zjawiska fizjologiczne zachodzące w organizmie;
- kryteria społeczne – zmiany w pełnionych rolach społecznych dostrzegane przez otoczenie.

Zdrowie może być zatem odmiennie oceniane w zależności od pewnych uwarunkowań, wśród których D. Cianciara wskazała:

- indywidualne – w związku z wiekiem i osobistymi doświadczeniami (np. choroba) rozumienie oraz stosunek człowieka do zdrowia bywają różne,
- społeczne – różne grupy społeczne, mające odmienne wykształcenie bądź status ekonomiczny, mogą interpretować zdrowie w odrębny sposób,
- sytuacyjne – związane ze stanem funkcjonowania państwa (ocena zdrowia w czasie pokoju oraz → w o j n y [t. 4] jest inna),
- historyczne – na które wpływa rozwój medycyny, przyrost wiedzy, rozwój profilaktyki zdrowotnej,
- kulturowe – nawiązujące do tradycji danego regionu (np. medycyna Wschodu),
- naukowe – wynikające z kwalifikacji zawodowych (np. filozof, psycholog, lekarz).

Zdrowie człowieka – zdaniem Sygita – determinowane jest przez styl życia, jakość otoczenia i funkcjonowania służb zajmujących się → oc h r o n ą z d r o w i a [t. 3], posiadane kompetencje, rozwój psychospołeczny człowieka, realizowaną politykę zdrowotną oraz promocję zdrowia. Wśród czynników wpływających na zdrowie wyodrębnić należy także – sygnalizowane w Narodowym Programie Zdrowia na lata 2007–2015 – czynniki genetyczne.

Podobne czynniki (sprawność fizyczna, funkcjonowanie układu immunologicznego, predyspozycje genetyczne, styl życia, zewnętrzne zasoby gwarantujące zdrowie, np. środowisko, warunki życia, charakter pracy, rodzaj więzi społecznych) wskazał P. Grzywna. Opisał on za ich pośrednictwem pojęcie kapitału zdrowotnego. Jest to ważny element bezpieczeństwa zdrowotnego człowieka, pozwala na „prowadzenie rozumnego, kreatywnego oraz satysfakcjonującego życia". W wyniku niewłaściwego stylu życia (używki, stres, wypadki) wraz z wiekiem kapitał zdrowotny człowieka zmniejsza się. Niekorzystny wpływ na bezpieczeństwo i kapitał zdrowotny mają też nierówności w stanie zdrowia oraz nierówny dostęp do zasobów (np. styl życia, środowisko, praca, warunki socjalne, więzi społeczne). Jego odbudowa możliwa jest wyłącznie przez podejmowanie zachowań prozdrowotnych.

B. Woynarowska opisała pojęcie zdrowia z perspektywy:

- → z d r o w i a p u b l i c z n e g o [t. 4] – zorganizowanego wysiłku na rzecz zapobiegania chorobom oraz promowania zdrowia;
- populacyjnego – które – będąc rozszerzeniem zdrowia publicznego – wskazuje wpływające na zdrowie czynniki oraz adekwatne do nich sposoby reagowania;
- międzynarodowego – będącego w obszarze zainteresowań organizacji międzynarodowych;
- globalnego – mającego na celu poprawę zdrowia całego społeczeństwa;
- społecznościowego – odnoszącego się do norm i wartości właściwych dla danej społeczności, np. dostępu do żywności, opieki zdrowotnej;
- środowiskowego – dotyczącego czynników środowiskowych oddziałujących na zdrowie;

- jednostkowego – w tym fizycznego, psychicznego, społecznego, duchowego, emocjonalnego i seksualnego/prokreacyjnego.

Parafrazując B. Hołysta, holistyczne podejście do zdrowia wymaga uwzględnienia w definicji jego 3 kategorii: zdrowia fizycznego, psychicznego oraz duchowego. Autor wyodrębnił szereg zagrożeń zdrowia człowieka, wśród których szczególne znaczenie mają:

> zagrożenia naturalne (kataklizmy, epidemie i pandemie, zagrożenia kosmiczne), zagrożenia cywilizacyjne (fale elektromagnetyczne, choroby cywilizacyjne, manipulacje genetyczne, sztuczną inteligencję, toksyczne właściwości żywności, niewłaściwą gospodarkę zasobami Ziemi, skażenie gleby, powietrza i wody, niewłaściwą gospodarkę odpadami, ambiwalentną rolę postępu technicznego, patologie genetyczne, zagrożenia mikrobiologiczne), zagrożenia społeczne (terroryzm, konflikty społeczne, działania wojenne, nadmierną rywalizację, zagrożenia demograficzne, migracje, wykluczenie, postawy fundamentalistyczne, konsumpcjonizm, wypadki, katastrofy technologiczne i inżynieryjne, niewłaściwe odżywianie się, brak aktywności fizycznej) oraz zaburzenia psychiczne człowieka (stres i chroniczne zmęczenie, zakłócenia rytmów biologicznych, utratę tożsamości wraz ze skutkami, jakie one powodują, np. depresja).

Bezpieczeństwo zdrowotne wg Grzywny zmierza do:

> zapewnienia przez państwo oraz jego agendy warunków (społecznych, ekonomicznych i środowiskowych) pozwalających na realizację prawa do ochrony zdrowia, prawa, którego istotny element stanowi gwarancja dostępu do świadczeń medycznych na równych dla beneficjenta zasadach.

Dostęp do świadczeń zdrowotnych determinuje bezpieczeństwo zdrowotne, co skłania autora do wyeksponowania 2 płaszczyzn tak rozumianego bezpieczeństwa. Płaszczyzna obiektywna dotyczy realizacji przez państwo → p r a w a c z ł o w i e k a [t. 3] do ochrony zdrowia. Płaszczyzna subiektywna obejmuje oczekiwania, jakie obywatele kierują w stronę tego systemu.

Odnosząc się do powyższych rozważań i czyniąc podstawą rozumienia bezpieczeństwa zdrowotnego definicję zdrowia wg WHO oraz holistyczne ujęcie pojęcia bezpieczeństwa (zob. → e d u k a c j a d l a b e z p i e c z e ń s t w a [t. 2]), powinniśmy istotę bezpieczeństwa zdrowotnego traktować w sposób szeroki, uwzględniając problematykę dostępu obywateli do świadczeń zdrowotnych i mając na uwadze, że pojęcie to nie obejmuje jedynie czasu pokoju.

W ujęciu procesualnym bezpieczeństwo zdrowotne interpretować należy jako:

> ustawicznie podejmowane działania w zakresie diagnozy zagrożeń zdrowotnych (subiektywnych i obiektywnych), wspierania rozwiązań pozwalających właściwie reagować na wyzwania i zagrożenia dla zdrowia i życia człowieka, wzmacniania troski społeczeństwa o zdrowie i życie własne oraz innych osób oraz dążenie do zapewnienia wysokiej jakości życia i możliwości samorealizacji każdemu człowiekowi. Wiąże się ono także z diagnozą stanu – subiektywnego poczucia

bezpieczeństwa podmiotu i obiektywnie istniejących zagrożeń. Tak pojmowane bezpieczeństwo zdrowotne należy ujmować w dwóch wymiarach. Bezpieczeństwo negatywne, dotyczące działań zorientowanych na eliminację choroby i czynników ryzyka, oraz bezpieczeństwo pozytywne, skoncentrowane na wzmacnianiu czynników chroniących człowieka przez zagrożeniami zdrowotnymi i wspieraniu jednostki w dążeniu do dobrostanu.

Realizacja tak sformułowanych celów wymaga podjęcia kompleksowych działań w zakresie edukacji zdrowotnej wchodzącej w zakres szeroko pojętej edukacji dla bezpieczeństwa.

W działania zmierzające do poprawy bezpieczeństwa zdrowotnego społeczeństwa zaangażowane są poszczególne resorty oraz wszystkie sektory działalności społeczno-gospodarczej (także podmioty i instytucje państwowe, administracja samorządowa, podmioty funkcjonujące komercyjnie oraz organizacje pozarządowe non profit). Efektywność podejmowanych działań wymaga uwzględniania zewnętrznego oraz wewnętrznego (związanego z aktywnością podmiotu) aspektu bezpieczeństwa. Skłonność do przyjęcia postawy osobistej odpowiedzialności za bezpieczeństwo zdrowotne społeczeństwa jest podstawą działania dla innych osób i instytucji, współodpowiedzialnych za kapitał zdrowotny. W tych działaniach troska o zdrowie własne musi być powiązana z troską o zdrowie innych osób. Bezpieczeństwo zdrowotne zostało zasygnalizowane w najważniejszych dokumentach regulujących cele strategiczne działań ukierunkowanych na bezpieczeństwo Polski. W *Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* bezpieczeństwo zdrowotne zostało uznane za → interes narodowy [t. 2] państwa. Zaakcentowano w niej wewnętrzny i zewnętrzny aspekt bezpieczeństwa, uzasadniając konieczność podejmowania indywidualnej oraz zbiorowej ochrony obywateli przed zagrożeniami dla ich zdrowia i życia. Odniesiono się także do pozytywnego wymiaru bezpieczeństwa zdrowotnego, wskazując potrzebę zagwarantowania społeczeństwu → zrównoważonego rozwoju [t. 4] i umożliwienia ludziom zdrowego oraz satysfakcjonującego życia. Tak rozumiane bezpieczeństwo zdrowotne – zgodnie z podstawowymi założeniami semantycznymi – „nie koncentruje się jedynie na przeciwdziałaniu zagrożeniom. Równie ważne są wyzwania współczesnego świata". Podobny charakter powinna mieć → profilaktyka bezpieczeństwa [t. 3] zdrowotnego. Przeciwdziałanie zagrożeniom i eliminacja ryzyka stanowi jedynie fragment potrzebnych działań profilaktycznych. Tak samo istotne jest wspieranie człowieka w rozwoju (w tym rozwijanie jego samooceny, szacunku do siebie i otoczenia oraz empatii).

Kształtowanie → środowiska bezpieczeństwa [t. 4] zdrowotnego w zgodzie ze *Strategią Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* realizowane jest w obrębie podsystemów wsparcia (społecznego i gospodarczego) oraz podsystemów wykonawczych (obronnego i ochronnego) systemu → bezpieczeństwa narodowego. Podsystemy wsparcia koncentrują się na edukacji

dla bezpieczeństwa i bezpieczeństwie socjalnym (podsystem wsparcia społecznego) oraz ochronie środowiska naturalnego i bezpieczeństwie żywności (podsystem wsparcia gospodarczego). Działania ochronne w kontekście bezpieczeństwa zdrowotnego dotyczą: wymiaru sprawiedliwości, → c y b e r b e z p i e c z e ń s t w a, bezpieczeństwa i porządku publicznego, przeciwdziałania → t e r r o r y z m o w i [t. 4] i ekstremizmowi, funkcjonowania systemu ratownictwa i → o c h r o n y l u d n o ś c i [t. 3], → z a r z ą d z a n i a k r y z y s o w e g o [t. 4] oraz ochrony zdrowia poprzez rozpoznawanie zagrożeń zdrowotnych i przeciwdziałanie im. Powyższe działania poddano charakterystyce w *Białej Księdze Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*.

Kluczowe cele strategiczne wyodrębnione zostały także w Narodowym Programie zdrowia na lata 2016–2020, który stanowi załącznik do Rozporządzenia Rady Ministrów z dnia 4 sierpnia 2016 r. Priorytetem ustanowiono w nim wydłużenie i poprawę jakości życia ludzi oraz poprawę ich stanu zdrowia. Realizację tych celów umożliwi rozwój kultury fizycznej społeczeństwa i poprawa sposobu żywienia, profilaktyka w zakresie korzystania z substancji psychoaktywnych, profilaktyka zdrowia psychicznego, minimalizowanie zagrożeń fizycznych, chemicznych i biologicznych w środowisku zewnętrznym, promocja aktywnego i zdrowego starzenia się oraz troska o zdrowie prokreacyjne. Odzwierciedleniem działań krajowych są inicjatywy międzynarodowe, podejmowane w podobnych zakresach. Kształtowanie środowiska bezpieczeństwa zdrowotnego, opartego na wskazanych powyżej celach strategicznych, w ujęciu Grzywny wymaga diagnozy i monitorowania stanu zdrowia społeczeństwa, prowadzenia kompleksowej profilaktyki zdrowotnej oraz modernizacji w obrębie systemu bezpieczeństwa socjalnego.

Świat stoi przed wieloma wyzwaniami zdrowotnymi. Obejmują one ogniska chorób takich jak odra czy błonica, którym można zapobiegać za pomocą szczepionek, rosnące doniesienia o patogenach odpornych na leki, rosnące wskaźniki otyłości i braku aktywności fizycznej, a także skutki zdrowotne zanieczyszczenia środowiska i zmian klimatu oraz liczne → k r y z y s y h u m a n i t a r n e [t. 2]. Aby zaradzić tym i innym zagrożeniom, w 2019 r. rozpoczął się nowy 5-letni plan strategiczny Światowej Organizacji Zdrowia – 13 Generalny Program Prac (Thirteenth General Programme of Work, GPW 13). Plan ten koncentruje się na celu „potrójnego miliarda" – polegającego na zapewnieniu 1 mld ludzi więcej korzyści związanych z dostępem do powszechnego ubezpieczenia zdrowotnego, 1 mld więcej ludzi ma być chronionych przed zagrożeniami zdrowotnymi, a 1 mld więcej ludzi ma cieszyć się lepszym zdrowiem i dobrym samopoczuciem. Osiągnięcie tego celu będzie wymagało zajęcia się zagrożeniami dla zdrowia z różnych punktów widzenia.

Ewelina Włodarczyk

Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Biuro Bezpieczeństwa Narodowego, Warszawa 2013; D. Cianciara, *Zarys współczesnej promocji zdrowia*, Wydawnictwo PZWL, Warszawa 2010; M. Cieślarczyk, *Kultura bezpieczeństwa i obronności*, Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Siedlce 2011; tenże, *Teoretyczne i metodologiczne*

podstawy badania problemów bezpieczeństwa i obronności państwa, Wydawnictwo Akademii Podlaskiej, Siedlce 2009; P. Grzywna, *Bezpieczeństwo zdrowotne w nauce o polityce społecznej. Wprowadzenie do dyskusji*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2017; B. Hołyst, *Bezpieczeństwo gatunku ludzkiego*, Wydawnictwo Naukowe PWN, Warszawa 2016; tenże, *Bezpieczeństwo jednostki*, Wydawnictwo Naukowe PWN, Warszawa 2014; tenże, *Przeciwko życiu. Perspektywy badawcze problematyki zagrożeń życia*, t. 1, Wydawnictwo Naukowe PWN, Warszawa 2017; Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r., Dz. U. 1997, nr 78, poz. 483 (z późn. zm.); L.F. Korzeniowski, *Podstawy nauk o bezpieczeństwie*, Difin, Warszawa 2017; S. Koziej, *Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja*, „Bezpieczeństwo Narodowe" 2011, nr 18; H. Kromołowski, *Problematyka bezpieczeństwa zdrowotnego ludności w Polsce w latach 1918–2017 w świetle wybranych reform w systemach ochrony zdrowia*, Wydawnictwo Wydziału Zarządzania Politechniki Częstochowskiej, Częstochowa 2017; J. Mazur, *Zdrowie publiczne i globalne*, [w:] *Edukacja zdrowotna*, B. Woynarowska (red.), Wydawnictwo Naukowe PWN, Warszawa 2017; Narodowy Program Zdrowia na lata 2007–2015. Załącznik do Uchwały nr 90/2007 Rady Ministrów z dnia 15 maja 2007 r.; Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 8 sierpnia 2011 r. w sprawie obszarów wiedzy, dziedzin nauki i sztuki oraz dyscyplin naukowych i artystycznych, Dz. U. 2011, nr 179, poz. 1065; Rozporządzenie Rady Ministrów z dnia 4 sierpnia 2016 r. w sprawie Narodowego Programu Zdrowia na lata 2016–2020, Dz.U. 2016, poz. 1492; *Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej*, Biuro Bezpieczeństwa Narodowego, Warszawa 2014; M. Sygit, *Zdrowie publiczne*, Wolters Kluwer Polska, Warszawa 2017; UNDP, *Human Development Report 1994*, UNDP, Oxford University Press, New York 1994; WHO, *Constitution of the World Health Organization*, WHO.int (dostęp 1.01.2020); WHO, *Draft Thirteenth General Programme of Work 2019–2023*, 1.11.2017, WHO.int (dostęp 1.01.2020); E. Włodarczyk, *Bezpieczeństwo zdrowotne*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; taż, *Edukacja filarem bezpieczeństwa zdrowotnego człowieka*; *Wskaźniki kultury bezpieczeństwa zdrowotnego w Polsce*, [w:] *Współczesne konteksty bezpieczeństwa zdrowotnego*, O. Wasiuta, E. Włodarczyk, M. Szumiec (red.), Wydawnictwo Naukowe Uniwersytetu Pedagogicznego w Krakowie, Kraków 2020; taż, *Wskaźniki kultury bezpieczeństwa zdrowotnego w Polsce*, [w:] *Współczesne konteksty bezpieczeństwa zdrowotnego*, O. Wasiuta, E. Włodarczyk, M. Szumiec (red.), Wydawnictwo Naukowe Uniwersytetu Pedagogicznego w Krakowie, Kraków 2020; B. Woynarowska, *Zdrowie – podstawowe pojęcie w edukacji zdrowotnej*, [w:] *Edukacja zdrowotna*, B. Woynarowska (red.), Wydawnictwo Naukowe PWN, Warszawa 2017; R. Zięba, *O tożsamości nauk o bezpieczeństwie*, „Zeszyty Naukowe AON" 2012, nr 1.

BEZPIECZEŃSTWO ŻYWNOŚCI – według definicji znajdującej się w Ustawie z dnia 25 sierpnia 2006 r. o bezpieczeństwie żywności i żywienia to ogół warunków, które muszą być spełniane, dotyczących szczególnie:

- stosowanych substancji dodatkowych (substancje pomagające w przetwarzaniu, celowo dodawane do żywności ze względów np. technologicznych, takie jak barwniki, substancje słodzące) i aromatów;
- poziomu substancji zanieczyszczających (np. azotany, mykotoksyny, dioksyny, wielopierścieniowe węglowodany aromatyczne czy metale ciężkie);
- pozostałości pestycydów;
- warunków napromieniania żywności;

- cech organoleptycznych;
- działań, jakie muszą być podejmowane na wszystkich etapach produkcji żywności lub obrotu nią w celu zapewnienia zdrowia i życia człowieka.

Podstawy regulacji prawnych związanych z jakością i bezpieczeństwem żywności stanowią wymogi krajowe oraz Unii Europejskiej, określają one zakres działalności sektora rolno-spożywczego i obejmują cały łańcuch żywnościowy „od pola do stołu".

Biorąc pod uwagę bezpieczeństwo żywności, akcentuje się przede wszystkim zdrowotność oraz walory odżywcze środków spożywczych. Kategorię tę odnosi się do takich zagadnień jak jakość żywności, jej zgodność z normami handlowymi i standardami rynkowymi z uwzględnieniem właściwości organoleptycznych (zespół cech obejmujących smak, zapach, wygląd, w tym barwę i konsystencję środków spożywczych, co można wyodrębnić i ocenić za pomocą zmysłów człowieka), fizykochemicznych i mikrobiologicznych żywności oraz występujących w tym zakresie nieprawidłowości, związanych przede wszystkim z jej fałszowaniem.

Środek spożywczy zafałszowany, zgodnie z ustawą o bezpieczeństwie żywności i żywienia, to taki, którego skład lub inne właściwości zostały zmienione, a konsument nie został o tym poinformowany, albo taki, w którym zostały wprowadzone zmiany mające na celu ukrycie jego rzeczywistego składu lub innych właściwości. Do praktyk fałszowania żywności zalicza się np.: podawanie przez producenta żywności nieprawdziwych danych dotyczących składu, zaniżanie masy, zawyżanie lub zaniżanie wartości odżywczych produktów.

Pojęcie bezpieczeństwa żywności często jest mylone z bezpieczeństwem żywnościowym. Według definicji Departamentu Rolnictwa Stanów Zjednoczonych oraz ustaleń → Organizacji Narodów Zjednoczonych ds. Wyżywienia i Rolnictwa [t. 5] przez bezpieczeństwo żywnościowe należy rozumieć fizyczny i ekonomiczny dostęp do bezpiecznej, odpowiednio zbilansowanej żywności w takiej ilości, która zaspokoi codzienne potrzeby żywnościowe społeczeństwa i zapewni aktywne i zdrowe życie człowieka. Gwarancją bezpieczeństwa żywnościowego będzie spełnienie następujących warunków:

- fizyczna dostępność żywności, co oznacza, że krajowa gospodarka żywnościowa gwarantuje pokrycie co najmniej minimalnego zapotrzebowania fizjologicznego, import zaś dostarcza żywność ponad to minimalne zapotrzebowanie;
- ekonomiczna dostępność żywności, co jest równoznaczne z tym, że również najsłabsze ekonomicznie gospodarstwa domowe mają dostęp do niezbędnej żywności;
- zdrowotna odpowiedniość pojedynczego produktu żywnościowego (brak zanieczyszczeń) i spożywanej racji żywnościowej (niezbędny poziom energii i właściwa proporcja składników pokarmowych).

Bezpieczeństwo żywnościowe odnosi się więc przede wszystkim do dostępności żywności. W wypadku bezpieczeństwa żywności chodzi głównie o jej jakość pod

względem zarówno zdrowotnym, jak i handlowym. Określając żywność jako bezpieczną, mamy na myśli taką, która spełnia szczegółowe wymagania wspólnotowego (unijnego) prawa żywnościowego, a w razie ich braku – wymogi krajowego prawa żywnościowego państwa członkowskiego. Z kolei środek spożywczy szkodliwy dla zdrowia lub życia człowieka to taki, którego spożycie w warunkach normalnych i zgodnie z przeznaczeniem może spowodować negatywne skutki dla zdrowia lub życia człowieka, zwłaszcza gdy nie spełnia wymagań zdrowotnych określonych w przepisach i (lub) zawiera:

- substancje zanieczyszczające lub zanieczyszczenia mikrobiologiczne w ilościach przekraczających dopuszczalne poziomy określone w rozporządzeniach UE oraz inne zanieczyszczenia;
- pozostałości skażeń promieniotwórczych w ilościach przekraczających poziomy określone w rozporządzeniach UE;
- weterynaryjne produkty lecznicze w ilościach przekraczających dopuszczalne poziomy lub zabronione określone w rozporządzeniach UE;
- inne substancje szkodliwe dla zdrowia lub życia człowieka określone w przepisach UE.

Należy tutaj również rozróżnić środek spożywczy szkodliwy od zepsutego. Żywność zepsuta to żywność, której skład lub właściwości uległy zmianom wskutek nieprawidłowości zaistniałych na etapie produkcji, obrotu lub pod wpływem działań czynników naturalnych, takich jak: wilgotność, czas, temperatura lub światło, albo wskutek obecności drobnoustrojów, a także zanieczyszczeń sprawiających, że nie nadaje się ona do spożycia zgodnie z jego przeznaczeniem.

Mając na uwadze powyższe definicje, żywnością niebezpieczną będziemy zatem określać środek spożywczy szkodliwy dla zdrowia lub zepsuty w rozumieniu przepisów wspólnotowych. Z kolei bezpieczeństwo żywności to przede wszystkim zapewnienie, że dostępna żywność nie spowoduje uszczerbku na zdrowiu konsumenta, jeśli jest przygotowywana zgodnie z zamierzonym zastosowaniem.

Bezpieczeństwo środków spożywczych jest warunkowane przez wiele czynników. Zależy ono m.in. od: skuteczności funkcjonowania inspekcji odpowiedzialnych za bezpieczeństwo żywości (ta determinowana jest np. liczbą etatów, przygotowaniem merytorycznym, jakością i intensywnością współpracy między poszczególnymi organami urzędowej kontroli żywności czy jakością wyposażenia laboratoriów inspekcji), jakości regulacji prawnych w obszarze prawa żywnościowego, jakości i intensywności współpracy inspekcji z organami ścigania, reakcji konsumentów na sytuacje nadużyć oraz świadomego wybierania produktów podczas zakupów (np. przez zapoznanie się z opiami zamieszczonymi na etykietach). Ponadto bezpieczeństwo żywności zależy od postaw producentów przejawiających się przede wszystkim w dbałości o własne produkty oraz samokontroli branżowej, a także od stanu gospodarki w obszarze sektora spożywczego.

Największe → z a g r o ż e n i a [t. 4] dla bezpieczeństwa żywności to przede wszystkim jej świadome fałszowanie, zaniedbania sanitarne podczas produkcji oraz związane z przechowywaniem i transportem żywności w nieodpowiednich warunkach, to również niedopatrzenia dotyczące złej jakości produktów pierwotnych używanych w produkcji. Niebezpieczeństwo tkwi także w produkcji artykułów spożywczych przez niezarejestrowane przedsiębiorstwa lub nieewidencjonowaniu produkcji przez podmioty, które działają legalnie.

Zagrożenia wynikające z pojawienia się na rynku niepełnowartościowych produktów mogą dotyczyć wielu aspektów funkcjonowania państwa i społeczeństwa. Skutki wiążą się z reakcją rynków zewnętrznych – obejmują przede wszystkim ograniczenia handlowe ze strony rządów krajów importujących polską żywność (decyzje w tym zakresie mogą mieć podłoże czysto polityczne) oraz zwyczajny spadek popytu w tych krajach na żywność, co do której często stwierdza się nieprawidłowości, lub żywność, do której zagraniczni konsumenci tracą zaufanie na skutek negatywnej kampanii medialnej (często podsycanej przez grupy interesu, którym szczególnie zależy na zniszczeniu wizerunku polskiej żywności). Konsekwencje mogą także oddziaływać bezpośrednio na rynek wewnętrzny – przez tworzenie się nieuczciwej konkurencji lub spadek popytu na kwestionowaną żywność. Sytuacja taka może wpłynąć na finanse publiczne przez zmniejszenie wpływu do budżetu oraz konieczność utrzymywania rozbudowanych instytucji chroniących konsumentów przed niebezpieczną żywnością. Najistotniejszym negatywnym skutkiem są jednak konsekwencje zdrowotne związane ze spożywaniem niepełnowartościowych, niebezpiecznych produktów przez konsumentów.

Wiedząc, jakie determinanty określają bezpieczną żywność oraz jakie następstwa wynikają z obecności na rynku niepełnowartościowej żywności, konieczne jest przestrzeganie określonych wymagań prawa żywnościowego, zgodnego z przepisami Unii Europejskiej i polskim ustawodawstwem, aby zapewnić → b e z p i e c z e ń s t w o [t. 1] konsumentom. Wśród tych wymagań najważniejsze jest niedopuszczenie do obrotu żywności szkodliwej lub zepsutej, czyli takiej, która nie spełnia wymagań zdrowotnych. Kolejnym warunkiem jest przestrzeganie w produkcji żywności i jej obrocie wymogów higieniczno-sanitarnych dotyczących pomieszczeń i urządzeń. Normy te zapewniają właściwą jakość zdrowotną żywności, ich spełnienie powinno być potwierdzone przez organy urzędowej kontroli żywności przed rozpoczęciem działalności. Następnym elementem jest dopilnowanie, aby kontakt z żywnością miały tylko osoby dopuszczone pod względem zdrowotnym oraz te, które odbyły szkolenie w zakresie przestrzegania zasad higieny, w tym stosowania zasad HACCP (Hazard Analysis and Critical Control Points).

→ S y s t e m H A C C P [t. 4], zgodnie z definicją Codex Alimentarius (międzynarodowe normy żywnościowe), to system, który identyfikuje, ocenia oraz kontroluje zagrożenia istotne dla bezpieczeństwa żywności. Z kolei ustawa o bezpieczeństwie

żywności i żywienia określa system HACCP jako postępowanie mające na celu zapewnienie bezpieczeństwa żywności przez identyfikację i oszacowanie skali zagrożeń z punktu widzenia wymagań zdrowotnych żywności oraz → r y z y k a wystąpienia zagrożeń podczas przebiegu wszystkich etapów produkcji i obrotu żywnością. System ma także na celu określenie metod eliminacji lub ograniczania zagrożeń oraz ustalenie działań korygujących.

Wśród ogólnych wymagań jest także konieczność przestrzegania i ścisłej kontroli zasad w stosowaniu substancji dodatkowych w produkcji oraz nieprzekraczanie określonych poziomów substancji obcych, czyli zanieczyszczeń, w tym zanieczyszczeń mikrobiologicznych i substancji zanieczyszczających, jak również pozostałości pestycydów, produktów leczniczych oraz skażeń promieniotwórczych. Ponadto obowiązkiem jest posiadanie stosownych administracyjnych zezwoleń lub powiadamianie określonych organów administracyjnych (zezwolenia Komisji Europejskiej, przy udziale Głównego Inspektoratu Sanitarnego – GIS) w wypadku wprowadzania do obrotu niektórych środków spożywczych (np. nowa żywność, żywność genetycznie zmodyfikowana). Żywność przywożona z zagranicy musi być zgodna z wymogami prawa unijnego i polskim prawem żywnościowym.

Zgodnie z zaleceniami prawa żywnościowego żywność powinna być odpowiednio znakowana, tak aby nie wprowadzać konsumenta w błąd a dostarczać mu określonych → i n f o r m a c j i [t. 2] o zakupionych produktach. Wymogi wskazują również na cywilną odpowiedzialność przedsiębiorcy za szkody wyrządzone przez wprowadzone przez niego do obrotu niebezpieczne środki spożywcze. Określono również wymóg identyfikowalności, czyli prowadzenia i przechowywania dokumentacji lub innych danych umożliwiających identyfikację podmiotów, które dostarczyły i którym dostarczono surowce lub inne komponenty do produkcji żywności lub gotowe środki spożywcze w celu wprowadzenia do obrotu. Ostatnim elementem wśród określonych wymogów jest obowiązek podwójnej kontroli jakości zdrowotnej żywności czyli zewnętrznej urzędowej kontroli oraz kontroli wewnętrznej (samokontroli zakładowej).

Celem kontroli wewnętrznej jest przede wszystkim zapewnienie jakości zdrowotnej żywności oraz zasad higieny w procesie produkcji i w obrocie żywnością w zakładach produkujących żywność lub wprowadzających ją do obrotu. Obowiązek kontroli wewnętrznej jest realizowany m.in. przez wdrażanie zasad dobrej praktyki higienicznej (Good Hygienic Practice, GHP), dobrej praktyki produkcyjnej (Good Manufacturing Practice, GMP) oraz systemu HACCP. W ramach kontroli przestrzegania GHP ocenia się m.in. stan techniczny budynków, maszyn i urządzeń wykorzystywanych w produkcji, procesy dotyczące higieny i szkolenia personelu, jakość wody, obecność szkodników, procesy mycia i dezynfekcji oraz sposób i prawidłowości usuwania odpadów i ścieków. Z kolei w kontroli GMP chodzi głównie o ocenę jakości zdrowotnej surowców poprawności procesów technologicznych, przestrzegania identyfikacji i identyfikowalności wyrobów gotowych.

Cel kontroli wewnętrznej jest właściwie tożsamy z celem i zakresem urzędowej kontroli żywności. Podstawą organizacji polskiego systemu urzędowej kontroli żywności jest Rozporządzenie (WE) Nr 882/2004 Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. w sprawie kontroli urzędowych przeprowadzanych w celu sprawdzenia zgodności z prawem paszowym i żywnościowym oraz regułami dotyczącymi zdrowia zwierząt i dobrostanu zwierząt. W celu zrealizowania powyższego obowiązku konieczne stało się wydzielenie zasobów instytucjonalnych, prawnych, organizacyjnych i finansowych oraz utworzenie systemu funkcjonującego zgodnie z normami prawa unijnego. Ogólny zakres urzędowej kontroli żywności dotyczy oceny stanu faktycznego w porównaniu ze stanem postulowanym w przepisach prawa żywnościowego. Obejmuje ona: stan techniczno-sanitarny zakładu, higienę produkcji dystrybucji i sprzedaży, zarządzanie zakładem, kontrolę wewnętrzną i wdrożone systemy zarządzania bezpieczeństwem żywności oraz profil działalności – zgodnie z kategoryzacją zakładów. W Polsce obowiązki z zakresu zewnętrznej kontroli żywności są realizowane w ramach krajowego systemu bezpieczeństwa i jakości żywności, który stanowią następujące podmioty: Państwowa Inspekcja Sanitarna (PIS), Inspekcja Weterynaryjna (IW) – instytucje kompetentne w zakresie jakości zdrowotnej – oraz Inspekcja Jakości Handlowej Artykułów Rolno-Spożywczych (IJHARS) i Inspekcja Handlowa (IH) – instytucje kompetentne w zakresie jakości handlowej. Państwowa Inspekcja Sanitarna kontroluje bezpieczeństwo żywności pochodzenia niezwierzęcego na etapie produkcji oraz wszystkich produktów na sklepowych półkach, a Inspekcja Weterynaryjna odpowiedzialna jest za żywność pochodzenia zwierzęcego na etapie produkcji oraz w obrocie hurtowym. Z kolei IJHARS kontroluje jakość handlową żywności u producenta oraz w obrocie hurtowym, zaś Inspekcja Handlowa dba o jakość handlową żywności w obrocie detalicznym. Zakres i częstotliwość urzędowych kontroli oraz ich rodzaj zależą od stopnia ryzyka dla zdrowia lub życia człowieka wynikającego z rodzaju prowadzonej w zakładach działalności, biorąc pod uwagę m.in. wyniki uprzednich kontroli, wiarygodność kontroli wewnętrznej (zakładowej) oraz wszelkie informacje mogące wskazywać na naruszenia prawa żywnościowego.

Żaneta Mrożek, Magdalena Szumiec

Bezpieczeństwo żywności i żywienia. Komentarz, A. Szymecka-Wesołowska (red.), Lex a Wolters Kluwer business, Warszawa 2013; M. Korzycka, P. Wojciechowski, *System prawa żywnościowego*, Wolters Kluwer, Warszawa 2017; S. Kowalczyk, *Bezpieczeństwo i jakość żywności*, Wydawnictwo Naukowe PWN, Warszawa 2016; K. Leśkiewicz, *Prawo żywnościowe*, C.H. Beck, Warszawa 2020; R. Płocki, *Bezpieczeństwo żywności w kontekście jej fałszowania*, Wydawnictwo Wyższej Szkoły Policji, Szczytno 2017; Rozporządzenie (WE) nr 178/2002 Parlamentu Europejskiego i Rady z dnia 28 stycznia 2002 r. ustanawiające ogólne zasady i wymagania prawa żywnościowego, powołujące Europejski Urząd ds. Bezpieczeństwa Żywności oraz ustanawiające procedury w zakresie bezpieczeństwa żywności, Dz.Urz. UE L 31 z 1.02.2002; Rozporządzenie (WE) nr 854/2004 Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2006 r. ustanawiające szczególne przepisy dotyczące organizacji urzędowych kontroli w odniesieniu do produktów pochodzenia zwierzęcego przeznaczonych do spożycia przez

ludzi, Dz.Urz. UE L 139 z 30.04.2004; Rozporządzenie (WE) nr 882/2004 Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. w sprawie kontroli urzędowych przeprowadzanych w celusprawdzenia zgodności z prawem paszowym i żywnościowym oraz regułami dotyczącymi zdrowia zwierząt i dobrostanu zwierząt, Dz.Urz. UE L 165 z 30.04.2004; A. Serlikowska, *Opłaty i inne należności ustalane lub pobierane przez organy urzędowej kontroli żywności*, Wolters Kluwer, Warszawa 2020; M. Taczanowski, *Prawo żywnościowe*, Wolters Kluwer, Warszawa 2017; *Urzędowa kontrola żywności. Teoria i praktyka*, M. Korzycka, P. Wojciechowski (red.), Wydawnictwa Uniwersytetu Warszawskiego, Warszawa 2018; Ustawa z dnia 25 sierpnia 2006 r. o bezpieczeństwie żywności i żywienia, Dz.U. 2006, nr 171, poz. 1225.

BIAŁA KSIĘGA BEZPIECZEŃSTWA NARODOWEGO RZECZYPOSPOLITEJ POLSKIEJ (BK) – jedno z niewielu stworzonych dotąd przez administrację państwową opracowań obejmujących całościową diagnozę stanu → b e z p i e c z e ń s t w a państwa polskiego.

BK została opracowana przez Komisję Strategicznego Przeglądu Bezpieczeństwa, powołaną w listopadzie 2010 r. przez Prezydenta RP na podstawie → S t r a t e g i c z n e g o P r z e g l ą d u B e z p i e c z e ń s t w a N a r o d o w e g o [t. 4]. Przegląd zakończono we wrześniu 2012 r., dokument zaś, który powstał na bazie niejawnego raportu opracowanego w ramach wspomnianych prac, został opublikowany w maju 2013 r. W skali Polski to stosunkowo nowatorskie opracowanie. W jednym dokumencie został bowiem przedstawiony i oceniony cały system bezpieczeństwa państwa – obejmujący sferę obronną, ochronną, społeczną i gospodarczą, wskazujący jednocześnie pewne wzajemne relacje i zależności pomiędzy tymi elementami.

W perspektywie dwudziestolecia zaprezentowane zostały prognozy rozwoju sytuacji wraz z wariantami działań (kierunków strategicznych), jakie powinna podjąć Polska z uwzględnieniem różnych opcji rozwoju organizacji i zasad funkcjonowania systemu kierowania → b e z p i e c z e ń s t w e m n a r o d o w y m. Pod uwagę zostały wzięte również warianty zmian systemowych na najwyższym, prezydenckim i rządowym szczeblu kierowania bezpieczeństwem państwa.

Opracowanie składa się z 4 głównych rozdziałów, są to:

1. Diagnoza stanu bezpieczeństwa narodowego.
   - W rozdziale przedstawiono historyczną ewolucję bezpieczeństwa Polski, począwszy od państwa Piastów, a skończywszy na III Rzeczypospolitej. Zaprezentowano również potencjał Polski w dziedzinie bezpieczeństwa, na który składają się: potencjał obronny (służba dyplomatyczna, → S i ł y Z b r o j n e R z e c z y p o s p o l i t e j P o l s k i e j [t. 4], przemysł obronny, wojskowe służby specjalne), potencjał ochronny (wymiar sprawiedliwości, → p r o k u r a t u r a [t. 3], → s ł u ż b y s p e c j a l n e [t. 4], służby (systemy) zapewniające → b e z p i e c z e ń s t w o p u b l i c z n e, powszechne, elementy → s y s t e m u z a r z ą d z a n i a k r y z y s o w e g o [t. 4]), potencjał społeczno-gospodarczy (potencjał demograficzny, kapitał społeczny, media,

służba zdrowia, energetyka, dług publiczny itp.) W proponowanym katalogu interesów i celów za punkt wyjścia przyjęto interesy konstytucyjne, czyli wymienione w art. 5 Konstytucji RP podstawowe funkcje Rzeczypospolitej Polskiej, którymi są: istnienie niepodległego państwa polskiego, w nienaruszalnych granicach, wolne i bezpieczne życie obywateli, → z r ó w n o w a ż o n y r o z w ó j [t. 4] społecznego i gospodarczego potencjału państwa, z konstytucyjnym podkreśleniem spraw dziedzictwa narodowego i ochrony środowiska. Realizacja → i n t e r e s ó w n a r o d o w y c h [t. 2] w dziedzinie bezpieczeństwa ma wg twórców opracowania opierać się na 2 wymiarach: operacyjnym i preparacyjnym. W obu można zidentyfikować konkretne cele strategiczne w dziedzinie bezpieczeństwa.

2. Prognoza rozwoju środowiska bezpieczeństwa.

   W rozdziale dokonano analizy bieżącego stanu i nakreślono prognozy kształtowania się strategicznego → ś r o d o w i s k a b e z p i e c z e ń s t w a [t. 4] w aspekcie zewnętrznym (międzynarodowym) i wewnętrznym (krajowym), militarnym i pozamilitarnym (zob. → p o z a m i l i t a r n e p r z y g o t o w a n i e o b r o n n e p a ń s t w a [t. 3]). Treścią analizy są szanse, wyzwania, ryzyka i → z a g r o ż e n i a [t. 4], przed jakimi stanie RP w perspektywie 20 lat. Przedstawiono 3 strategiczne scenariusze rozwoju warunków bezpieczeństwa Polski w perspektywie następnych 20 lat:

   - Optymistyczny scenariusz integracyjny, który zakłada przewagę korzystnych dla Polski zjawisk i trendów związanych ze środowiskiem bezpieczeństwa w wymiarze globalnym, europejskim i wewnątrzkrajowym. Obecność polityczno-wojskowa USA na naszym kontynencie zostałaby utrzymana. → N A T O [t. 3] pozostawałoby nadal najpotężniejszym sojuszem wojskowym, zachowując swoją wiarygodność i spoistość. W tym wariancie kraje UE wzmocniłyby konstrukcję unii walutowej, wprowadziłyby skuteczną dyscyplinę budżetową i fiskalną, zapewniono by bezpieczeństwo surowcowe i energetyczne oraz stworzono warunki do dalszego rozwoju UE.
   - Pesymistyczny scenariusz dezintegracyjny jest bardziej rozbudowany. Zakłada przewagę występowania niekorzystnych dla Polski zjawisk, w pierwszym rzędzie utrwalenie, a nawet pogłębienie się → k r y z y s u [t. 2] politycznego wskutek narastających problemów gospodarczych i finansowych. Prowadziłoby to do narastającej rozbieżności interesów państw UE, w wariancie skrajnie pesymistycznym do rozpadu UE. Osłabieniu uległoby również NATO, z jednej strony na skutek coraz mniejszego zainteresowania USA kontynentem europejskim, z drugiej zaś w wyniku postępującej utraty znaczenia USA w polityce światowej. Opisanym zjawiskom towarzyszyłoby nieuchronnie nasilanie się asertywnej i neoimperialnej polityki Rosji oraz częściowe odbudowywanie przez nią wpływów w obszarze poradzieckim.

- Scenariusz ewolucyjny – uznany za najbardziej prawdopodobny – zakłada kontynuację procesów integracyjnych w Europie, choć przy jednoczesnym ich dużym spowolnieniu. Najprawdopodobniej osłabieniu ulegnie globalna pozycja gospodarcza UE na korzyść gospodarek wschodzących. Wariant ten zakłada pewne, choć mniejsze niż w wariancie pesymistycznym, zmniejszenie się zaangażowania USA w Europie. Rosja wg tego scenariusza mimo kontynuacji prób nie dokonałaby żadnej radykalnej zmiany w swojej polityce wewnętrznej i zagranicznej.

3. Koncepcja działań strategicznych (→ s t r a t e g i a [t. 4] operacyjna). 3 scenariuszom rozwoju warunków bezpieczeństwa Polski w perspektywie następnych 20 lat zostały podporządkowane 3 opcje „strategii preparacyjnej":
   - Opcja umiędzynarodowienia → s y s t e m u b e z p i e c z e ń s t w a n a r o d o w e g o [t. 4], która odpowiada najbardziej optymalnemu dla Polski scenariuszowi integracyjnemu, czyli umiędzynarodowienia bezpieczeństwa RP.
   - Opcja usamodzielnienia systemu bezpieczeństwa narodowego, która jest odpowiedzią na drugi, najmniej dla RP korzystny scenariusz dezintegracyjny, oznacza przyjęcie opcji samowystarczalności strategicznej.
   - Opcja zrównoważonego integrowania systemu bezpieczeństwa narodowego odpowiada trzeciemu, „realistycznemu" scenariuszowi zrównoważonego umiędzynarodowienia i jednocześnie usamodzielnienia bezpieczeństwa Polski.
4. Koncepcja przygotowania systemu bezpieczeństwa.
   Autorzy BK słusznie zwrócili uwagę, że na poziomie rządowym brak jest struktur zajmujących się kierowaniem całością bezpieczeństwa narodowego. Do pewnego stopnia funkcje te pełnią Rządowy Zespół Zarządzania Kryzysowego (RZZK) jako organ doradczy Rady Ministrów i → R z ą d o w e C e n t r u m B e z p i e c z e ń s t w a [t. 3] (RCB), które obsługuje RZZK, pełniące funkcję jego sekretariatu. Jednak zadania i kompetencje zarówno RZZK, jak i RCB dotyczą tylko → z a r z ą d z a n i a k r y z y s o w e g o [t. 4], które jest jedynie częścią większej całości, tj. systemu bezpieczeństwa narodowego. Stąd postulat zastąpienia ciała doradczego, jakim obecnie jest RZZK, przez obdarzony szerszymi kompetencjami Komitet Rady Ministrów ds. Bezpieczeństwa Narodowego, zastąpienie obecnego, odpowiadającego tylko za → o c h r o n ę l u d n o ś c i [t. 3] RCB przez Rządowe Centrum Bezpieczeństwa Narodowego, które integrowałoby wszystkie zagadnienia bezpieczeństwa. Te rozwiązania proponowane były dla obecnie istniejącego porządku konstytucyjnego RP. Jednak autorzy *Białej Księgi* wskazują, że ów ustrojowy dualizm równoległej władzy prezydenta i premiera jest podstawowym elementem utrudniającym kierowanie systemem bezpieczeństwa kraju. Dualizm ten jest sprzeczny z podstawowym uniwersalnym modelem kierowania przywoływanym przez autorów *Białej Księgi*. W modelu tym mamy do czynienia z tylko jednym decydentem wspieranym przez kolegialny organ doradczy

i obsługiwanym przez organ sztabowy, któremu podlegają poszczególne ogniwa wykonawcze.

Twórcy opracowania zapisali również, że służy ono upowszechnieniu wiedzy o bezpieczeństwie i krzewieniu świadomości społecznej w tej dziedzinie – w myśl idei, że bezcennym kapitałem każdego nowoczesnego państwa są obywatele rozumiejący jego potrzeby, w tym tę żywotną, jaką jest troska o wspólne bezpieczeństwo. Dokument ze względu na swój język, objętość i twórców jest po części opracowaniem publicystycznym, w którym nie brak odniesień do bieżących problemów politycznych i gospodarczych, po części zaś dziełem akademickim. Dwoistość charakteru dokumentu nie odbiera mu jednak merytoryczności i trafności sformułowanych w nim tez i problemów.

Łukasz Szewczyk

Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Biuro Bezpieczeństwa Narodowego, Warszawa 2013; B. Bieliszczuk i in., *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej – wybrane zagadnienia*, „Poliarchia" 2014, nr 2 (3); P. Soloch, *Wizja bezpieczeństwa narodowego w 2013 roku w dokumentach Prezydenta RP i Rządu. Biała Księga Bezpieczeństwa Narodowego*, Instytut Sobieskiego, Warszawa 2013.

BIAŁY WYWIAD (wywiad ze źródeł otwartych, ang. *open-source intelligence*, OSINT) – w sposób ogólny może być zdefiniowany jako zorganizowana i zaplanowana działalność prowadzona w celu pozyskania określonego rodzaju → i n f o r m a c j i [t. 2] z szerokiego zakresu źródeł dostępnych publicznie. Określany bywa także jako → w y w i a d [t. 4] jawny albo wywiad jawnoźródłowy. Może być traktowany jako forma pracy wywiadowczej w postaci pozyskiwania informacji ze źródeł otwartych czy ogólnodostępnych (w rozumieniu wąskim) lub jako uporządkowany sposób pozyskiwania, przetwarzania i analizy informacji pochodzących z otwartych źródeł przez określone podmioty w celu wykorzystania ich w interesie tych podmiotów (w rozumieniu szerokim). Co do zasady taka działalność nie powinna stanowić naruszenia prawa do prywatności osób fizycznych (ochrony danych osobowych) oraz tajemnic państwowych (→ i n f o r m a c j i n i e j a w n y c h [t. 2]) i innych tajemnic prawnie chronionych.

Biały wywiad jest przede wszystkim jednym z podstawowych narzędzi państwowych służb wywiadowczych i kontrwywiadowczych, ale też służb typu policyjnego, stanowiącym tzw. rozpoznanie oficjalne – obok HUMINT (osobowych źródeł informacji) i SIGINT (rozpoznania technicznego). Ta forma wywiadowczej działalności pozwala gromadzić ok. 80% ilości wszystkich pozyskiwanych danych, a wartość informacji uzyskiwanych w ten sposób oceniana jest na 10–15% ogólnej wartości gromadzonych informacji. W miarę rozwoju → s p o ł e c z e ń s t w a i n f o r m a c y j n e g o [t. 4] oraz coraz większej transparentności funkcjonowania różnych podmiotów (urzędów administracji publicznej, podmiotów gospodarczych i pozarządowych) ten wymiar działalności informacyjnej nabiera coraz większego znaczenia.

W literaturze przedmiotu oraz w dorobku różnych organizacji można spotkać odmienne typologie w ramach tak rozumianego białego wywiadu, w odniesieniu do otwartych źródeł informacji. Na podstawie klasyfikacji prezentowanej przez → N A T O [t. 3] ze względu na stopień opracowania i weryfikacji dostępnych w ten sposób informacji można w tym zakresie wyróżnić:

- dane jawne (*open-source data*, ODT) – dotyczą otwartych, dostępnych publicznie danych, występujących w postaci czystej, surowej, nieopracowanej; są to wszystkie dane pochodzące ze źródeł pierwotnych (np. notatki, korespondencja prywatna lub służbowa, nagrania radiowe lub telewizyjne, zdjęcia drukowane bądź udostępnione w internecie, informacje zamieszczone na stronach internetowych, akty prawne, komercyjne zdjęcia satelitarne, mapy);
- informacje ze źródeł otwartych (*open-source information*, OSINF) – poddane procesom wstępnej oceny i wartościowania zestawienia, analizy, raporty, artykuły, książki i innego rodzaju materiały opracowane na podstawie danych jawnych (otwartych, publicznie dostępnych), które są szeroko rozpowszechniane;
- wywiad ze źródeł otwartych/jawnoźródłowy (*open-source intelligence*, OSINT) – dotyczy działalności zorganizowanej i zaplanowanej, uporządkowanego i usystematyzowanego procesu pozyskiwania i przetwarzania, a następnie rozpowszechniania wśród właściwych odbiorców informacji, na które zgłosili oni wcześniej zapotrzebowanie;
- zweryfikowany wywiad ze źródeł otwartych/jawnoźródłowy (*validated open-source intelligence*, OSINT-V) – obejmuje informacje wywiadowcze pochodzące ze źródeł otwartych, które zostały w odpowiednim, wysokim stopniu potwierdzone w wyniku weryfikacji przez inne źródła informacji wywiadu (np. przez osobowe źródła informacji, wiedzę innych funkcjonariuszy czy pracowników), lub pochodzące ze źródła, co do którego autentyczności i wiarygodności nie ma żadnych wątpliwości (np. przekaz audiowizualny określonego wydarzenia w czasie rzeczywistym w kilku różnych mediach).

Inna klasyfikacja białego wywiadu prezentowana przez NATO, dokonana ze względu na rodzaj otwartego źródła informacji, obejmuje następujące obszary pozyskiwania jawnych informacji:

- → m e d i a t r a d y c y j n e [t. 3] – → a g e n c j e p r a s o w e, czasopisma, gazety, stacje radiowe i telewizyjne, książki (w zakresie zawartych w nich faktów lub autorskich komentarzy oraz analiz, a także wywiadów z ekspertami, publicystyki czy przeprowadzonych śledztw dziennikarskich);
- media elektroniczne (internet) – serwisy agencji informacyjnych, serwisy, portale i wortale informacyjne, portale eksperckie, naukowe i akademickie serwisy społecznościowe, blogi (również fotoblogi, wideoblogi, blogi korporacyjne i organizacyjne, blogi tematyczne, pamiętniki internetowe), serwisy multimedialne, fora, listy dyskusyjne, czaty, strony domowe prywatnych użytkowników,

podmiotów gospodarczych, organizacji pozarządowych, think tanków, serwisy aukcyjne, sieci wymiany plików i udostępniania informacji, internetowe bazy danych oraz tzw. głęboka sieć itp. (w tym również tzw. metadane dokumentów w formie elektronicznej);

- internetowe usługi komercyjne – portale informacji prawnej, portale eksperckie, branżowe, portale akademickie, biblioteki elektroniczne, specjalistyczne agencje lub fundacje informacyjno-analityczne, programy dostarczające informacji przestrzennej w postaci różnego rodzaju map itp. (informacje lub ich fachowe opracowania, zebrane i przetworzone przez prywatne podmioty, które są udostępniane na określonych warunkach komercyjnych);
- literatura niszowa (ang. *grey literature*) – dokumenty robocze, przedruki, raporty i dokumenty techniczne, dysertacje, badania rynkowe, niepublikowane tłumaczenia, instrukcje, poradniki, biuletyny, newslettery itp. (literatura udostępniana tylko poprzez specjalistyczne kanały lub poprzez bezpośredni dostęp lokalny, np. z sektora akademickiego, organizacji non profit, przedsiębiorstw handlowych tworzących dokumenty na użytek wewnętrzny oraz dla klientów i dostawców, ze stowarzyszeń, fundacji, klubów itp.);
- eksperci i obserwatorzy – uczestnicy ekspedycyjnych projektów naukowych, badacze poszczególnych krajów i kultur, pracownicy organizacji międzynarodowych, pracownicy i wolontariusze organizacji humanitarnych, świadkowie wydarzeń itp. (osoby mające wiedzę merytoryczną w określonym przedmiocie ze względu na uczestnictwo w pewnych wydarzeniach, wiedzę i zainteresowania naukowe czy branżowe lub po prostu znajdujące się w określonym miejscu i czasie);
- komercyjne bazy zdjęć i obrazów satelitarnych – ujęcia różnych fragmentów powierzchni ziemi (np. mostów, dróg, portów, fragmentów wybrzeża, zakładów), które mogą być udostępniane na określonych warunkach przez podmioty świadczące tego typu usługi.

Na podstawie tego samego kryterium (źródła pochodzenia informacji) w polskiej literaturze przedmiotu podkreśla się z kolei znaczenie źródeł otwartych z sektora publicznego. B. Saramak wyróżnia w tym kontekście 5 podstawowych kanałów informacyjnych:

- środowisko naukowe i akademickie – wykłady, szkolenia, prace dyplomowe, publikacje, opracowania, wyniki badań i analiz;
- administracja publiczna, organizacje międzynarodowe i pozarządowe – przepisy prawa, procedury, regulaminy, ogólnodostępne rejestry, ogłoszenia sądowe i urzędowe, raporty, dokumentacja udostępniana na podstawie przepisów prawa, systemy informacji przestrzennej, systemy informacji publicznej, systemy informacji gospodarczej itp.;
- środki masowego przekazu i podmioty komercyjne – transmisje i relacje dotyczące bieżących wydarzeń, zgromadzone materiały archiwalne, produkty marketingowe

(biuletyny, prospekty, informatory, ulotki, reklamy) oraz wyniki analizy różnego rodzaju produktów (w tym tzw. inżynieria odwrotna);
- biblioteki – zbiory tradycyjne i elektroniczne zawierające książki, czasopisma, starodruki itp., a także stosowne bazy danych oraz specjalne systemy pozwalające na ich wyszukiwanie;
- osoby fizyczne – przekaz ustny i dystrybucja informacji podczas posiedzeń, spotkań, dyskusji w zakresie obserwacji określonych zjawisk, które nie zostały jeszcze ujęte w żadnych innych sformalizowanych źródłach.

Poza obszarem funkcjonowania służb państwowych biały wywiad ma również szerokie zastosowanie w działalności różnego rodzaju podmiotów pozapaństwowych funkcjonujących w różnych obszarach, zarówno legalnie, jak i w sposób nielegalny. Dotyczy to działalności takich podmiotów, jak np.:
- prywatne agencje wywiadowcze – głównie w zakresie politycznym, militarnym i ekonomicznym, na poziomie strategicznym; dostarczanie różnego rodzaju opracowań analitycznych na zasadach komercyjnych;
- wywiadownie gospodarcze – przede wszystkim o charakterze ekonomicznym; profesjonalna działalność informacyjna na zlecenie podmiotów gospodarczych ukierunkowana na zabezpieczenie interesów zleceniodawców i osiągnięcie przez nich przewagi konkurencyjnej;
- przedsiębiorstwa prywatne – działalność w zakresie analizy sytuacji rynkowej i możliwości rozwojowych własnej organizacji, działalności konkurencji, możliwości pozyskania klientów i analizy ich preferencji;
- organizacje pozarządowe – szczególnie zajmujące się ważnymi sprawami społeczno-politycznymi, przede wszystkim w obszarze ochrony → p r a w c z ł o w i e k a [t. 3], ochrony praw zwierząt, ochrony środowiska czy broniące interesów określonych grup społecznych; w kręgu ich zainteresowań mogą pozostawać informacje dotyczące funkcjonowania administracji publicznej, środowiska naturalnego, występowania → z a g r o ż e ń [t. 4], możliwości w zakresie współpracy międzynarodowej itp.;
- brokerzy informacji (infobrokerzy) – działalność komercyjna w przedmiocie oceny, selekcji, analizy oraz udostępniania określonych informacji będących w zainteresowaniu zleceniobiorcy;
- pracownicy naukowi – powszechne korzystanie z wielu ogólnodostępnych źródeł informacji dotyczących szerokiego spektrum zagadnień na potrzeby realizacji badań naukowych;
- dziennikarze śledczy – w ramach prowadzonych śledztw dziennikarskich, najczęściej dotyczących tematów kontrowersyjnych; informacje będące w zasięgu zainteresowania dotyczyć mogą powiązań między różnymi osobami i grupami, funkcjonowania określonych organizacji, zarówno w odniesieniu do podmiotów publicznych, jak i prywatnych;

- informatycy śledczy – działalność ukierunkowana na pozyskiwanie dowodów przestępstw, oszustw i nadużyć, które mogą zagrażać interesom osób fizycznych lub prawnych;
- specjaliści w zakresie → b e z p i e c z e ń s t w a systemów i sieci informatycznych – w zakresie informacji ogólnodostępnych w → c y b e r p r z e s t r z e n i, m.in. poszukiwania luk bezpieczeństwa i wykonywania tzw. testów penetracyjnych;
- organizacje terrorystyczne – działalność mająca na celu pozyskanie wszechstronnych informacji, najczęściej dotyczących funkcjonowania administracji publicznej, → i n f r a s t r u k t u r y k r y t y c z n e j [t. 2] danego państwa, organizacji międzynarodowych, organizowanych wydarzeń, ukierunkowana na wykorzystanie ich w celach nielegalnych, przestępczych o charakterze politycznym (w tym ideologicznym);
- organizacje przestępcze – wyszukiwanie w ogólnodostępnych źródłach informacji, które mogą przyczynić się do nielegalnej działalności przestępczej lub uniknięcia kary, przede wszystkim w obszarze funkcjonowania służb systemu bezpieczeństwa państwa, organów administracji rządowej i samorządowej, funkcjonowania podmiotów publicznych i prywatnych, stosowanych zabezpieczeń itp. (cel ekonomiczny, kryminalny).

Piotr Swoboda

B. Jakubus, M. Ryszkowski, *Ochrona informacji niejawnych*, Wydawnictwo Projekt, Warszawa 2001; J. Hughes-Wilson, *Największe błędy wywiadów świata*, tłum. J. Rosiński, Bellona, Warszawa 2002; K. Liedel, T. Serafin, *Otwarte źródła informacji w działalności wywiadowczej*, Difin, Warszawa 2011; P. Maciołek, *Internet a OSINT – szanse i praktyczne zastosowania*, [w:] *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, W. Filipowski, W. Mądrzejowski (red.), Wydawnictwo C.H.Beck, Warszawa 2012; *NATO Open Source Intelligence Handbook*, Norfolk 2001; *NATO Open Source Intelligence Reader*, Brussels 2002; B. Saramak, *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej. Historia, praktyka, perspektywy*, Wydział Dziennikarstwa i Nauk Politycznych Uniwersytetu Warszawskiego, Warszawa 2015; B. Stromczyński, P. Waszkiewicz, *Biały wywiad w praktyce pracy organów ścigania na przykładzie wykorzystania serwisów społecznościowych*, „Prawo i Prokuratura" 2014, nr 5; P. Swoboda, *Biały wywiad*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; tenże, *Wywiad i kontrwywiad w Polsce w procesie przemian systemowych (1989–2007)*, Wydawnictwo Avalon, Kraków 2016; K. Wiciak, *ESOM jako narzędzie „białego wywiadu"*, [w:] *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, W. Filipowski, W. Mądrzejowski (red.), Wydawnictwo C.H.Beck, Warszawa 2012; A. Żebrowski, *Wywiad i kontrwywiad w XXI wieku*, Innovatio Press, Lublin 2010.

BIG DATA – technologia służąca do gromadzenia, analizowania i przetwarzania danych o dużych objętościach, pochodzących ze źródeł tradycyjnych i nowo tworzonych, np. → m e d i ó w s p o ł e c z n o ś c i o w y c h [t. 3], zarówno o określonej, częściowo określonej, jak i nieokreślonej strukturze. Odnosi się do danych, które przekraczają typowe pojemności przechowywania i przetwarzania, dlatego też dotychczasowa

analiza i sposoby zarządzania danymi stają się niewystarczające i konieczne jest zastosowanie specjalnych metod i narzędzi służących do określenia korelacji między nimi (stosuje się analizę opisową, analitykę predykcyjną, diagnostyczną, preskryptywną).

Pojęcie to jest używane od lat 90. XX w., a niektórzy uznają za popularyzatora tego terminu J. Masheya. Duże zbiory danych zwykle obejmują zestawy danych o rozmiarach przekraczających możliwości powszechnie używanych narzędzi do przechwytywania, selekcjonowania i przetwarzania danych oraz zarządzania nimi w dopuszczalnym czasie.

Big data jest zjawiskiem wszechobecnym we współczesnym świecie, w którym ilość danych dostępnych użytkownikowi rośnie w sposób wykładniczy, a także odznacza się coraz większą heterogenicznością formatów, złożonością i siecią powiązań utrudniającą zarządzanie danymi. Polimorficzność zjawiska, zależnego od obszaru występowania, prowadzi do trudności definicyjnych. Koncepcję big data z uwagi na jej złożoność należy rozpatrywać zatem wyłączenie w kategoriach inter-, a nawet multidyscyplinarnych. Gartner opiera jej definicję na 3 filarach:

- objętości (ang. *volume*) – oznacza ilość danych generowanych, przechowywanych i obsługiwanych w systemie, współcześnie objętość cały czas wzrasta; tempo przetwarzania wiąże się głównie z szybkim napływem strumieniowym;
- różnorodności (ang. *variety*) oraz zmienności (ang. *variability*) – dotyczy zarówno źródeł danych, jak i ich formy; zwielokrotnienie danych prowadzi do powstania wielu powiązań;
- szybkości przetwarzania (ang. *velocity*) – odnosi się do prędkości, z jaką współcześnie dane są generowane, rejestrowane i udostępniane.

Termin big data ulega ciągłej zmianie, często opisuje się także kompleks technologii wykorzystywanych do gromadzenia i oceny tej ilości danych. Wzrost ilości i znaczenia danych we współczesnym świecie związany jest z globalizacją gospodarki, rozwojem internetu oraz nowych technologii odgrywających znaczącą rolę w urządzeniach związanych z przesyłem i przekazem danych, a także przejściem od formy analogowej – przez przyspieszającą cyfryzację – do zdigitalizowanej masowej rzeczywistości. Ilość danych z dnia na dzień powiększa się tak szybko, że mówi się już o środowisku prawdziwie zrewolucjonizowanym przez → i n f o r m a c j ę [t. 2]. Analitycy twierdzą, że w ostatnim czasie ich przyrost stanowi 90% przyrostu dotychczasowego. W tej sytuacji znane techniki służące do analizy danych stają się niewystarczające (za tą teorią opowiadają się W. Fan i A. Bifet, twierdzący, że aktualnymi ich zbiorami nie da się zarządzać za pomocą dostępnych i używanych dotąd narzędzi). Klasyczny schemat analizy danych staje się zupełnie nieadekwatny, a globalny świat informacji stanowi nowe wyzwanie dla współczesnej technologii i myśli analitycznej. Duże zbiory danych wymagają zestawu technik i technologii z nowymi formami integracji w celu ujawnienia wglądu w zbiory danych, które są różnorodne i złożone.

Big data są dziś wszechobecne. Podmiotami, które wykorzystują je w swoich działaniach, są np.:

- banki – gromadzą dane związane z operacjami wykonywanymi na kontach użytkowników, dotyczące np. dokonanych płatności, ich wielkości i rodzaju kupowanych przedmiotów;
- firmy – udostępniają własne aplikacje, które są pobierane przez użytkowników na smartfony lub tablety; instalując produkt na urządzeniu, najczęściej automatycznie wyraża się zgodę na dostęp aplikacji do własnych danych;
- właściciele portali internetowych – poprzez świadczone usługi również mogą gromadzić takie dane; najczęściej zgoda na taką czynność znajduje się w regulaminie.

Big data rozpatrywana jest jako płaszczyzna tworząca szanse rozwoju wielu dziedzin związanych z funkcjonowaniem jednostek i społeczeństwa, począwszy od gospodarki i biznesu, na świecie nauki skończywszy. Jest jednocześnie ogromnym wyzwaniem stanowiącym symbol wieku informacji, konieczne staje się pochylenie nad tą problematyką, podjęcie próby utworzenia jednolitej terminologii oraz metod badania, a także zminimalizowanie szumu informacyjnego wokół tematu.

Edyta Sadowska

B. Doyd, K. Crawford, *Critical Questions for Big Data: Provocation for a Cultural, Technological, and Scholarly Phenomenon*, „Information, Communication & Society" 2012, no. 15 (5); *Internet. Publiczne bazy danych i big data*, G. Szpor (red.), Wydawnictwo C.H.Beck, Warszawa 2014; V. Mayer-Schroberger, K. Cukier, *Big data. Rewolucja, która zmieni nasze myślenie, pracę i życie*, tłum. M. Głoatki, MT Biznes, Warszawa 2014; T. Protasowicki, J. Stanik, *Big data w analizie zagrożeń bezpieczeństwa narodowego*, „Ekonomiczne Problemy Usług" 2016, nr 123; Y. Riahi, S. Riahi, *Big Data and Big Analytics: Concepts, Types, and Technologies*, „International Journal of Research and Technologies" 2018, vol. 5, no. 9; E. Sadowska, *Big data*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; M. Tabakow, J. Korczak, B. Franczyk, *Big data. Definicje, wyzwania i technologie informatyczne*, „Informatyka Ekonomiczna" 2014, nr 1; J. Woźniczka, *Big Data w marketingu. Szansa i zagrożenia*, „Studia Oeconomica Posnaniensia" 2018, vol. 6, no. 6.

BIOMETRIA – termin rozumiany dwojako: jako nauka zajmująca się badaniem zmienności populacji organizmów oraz jako technika rozpoznawania i identyfikacji organizmów żywych, oparta zarówno na indywidualnych mierzalnych cechach fizycznych, jak i na behawioralnych człowieka. Obecnie to drugie rozumienie jest podejściem dominującym. Sam termin pochodzi z języka greckiego, w którym bios oznacza 'życie', metron – 'mierzyć'. Biometria ma na celu automatyczne uwierzytelnienie tożsamości człowieka na podstawie jego unikatowych cech i umiejętności, mających charakter mierzalny. Dotychczasowe tradycyjne metody sprawdzania tożsamości człowieka, opierające się na weryfikacji dokumentów tożsamości, haseł czy też numerów PIN, zostały wyparte. Trudno było wszakże zapamiętać hasła, numery PIN, łatwo też

zgubić karty identyfikacyjne. Biometria wyszła naprzeciw tym problemom, a stosowane przez nią metody bazują na tym, kim jest użytkownik. Nie wymagają one od niego znajomości żadnych specjalnych procedur, ponieważ wykorzystują fakt, że dana osoba może być rozpoznana na podstawie jej własnych unikatowych cech osobistych. Współcześnie biometria jest wykorzystywana m.in. w → k r y m i n o l o g i i [t. 2], antropologii, genetyce, medycynie sądowej, a także jako instrument zapewnienia szeroko rozumianego → b e z p i e c z e ń s t w a [t. 1] w wielu obszarach życia społecznego.

Dane biometryczne to właściwości biologiczne, cechy fizjologiczne, życiowe lub powtarzalne i wymierne czynności konkretnej osoby. Na ich podstawie możliwa okazuje się automatyczna identyfikacja lub weryfikacja danej osoby za pomocą tzw. systemów biometrycznych. Polegają one na cyfrowym mierzeniu pewnych anatomicznych lub behawioralnych cech człowieka i porównywaniu ich z cechami wzorcowymi (szablonem/ wzorcem). Biometryczny system identyfikacji ma dostęp do biometrycznej bazy danych zawierającej próbki biometryczne lub reprezentacje próbek biometrycznych.

Nowoczesne technologie biometryczne identyfikują osobę za pomocą ciała, przy użyciu charakterystyk właściwych każdej istocie ludzkiej. Cała gama wskaźników wykorzystywanych przez biometrię daje niezaprzeczalne potwierdzenie tożsamości, ponieważ są one jednostkowymi biologicznymi cechami charakterystycznymi, odróżniającymi jedną osobę od drugiej i mogą być przypisane jednej osobie.

Biometria bada:

- cechy fizyczne/genotypowe organizmów, takie jak:
  - linie papilarne,
  - geometria ucha,
  - owal twarzy, rozkład punktów charakterystycznych (oczy, usta) lub wartości temperatur na twarzy, faktura powierzchni twarzy lub skóry,
  - tęczówka oka, siatkówka (dno oka),
  - kształt dłoni,
  - kształt i rozmieszczenie zębów,
  - układ naczyń krwionośnych na dłoni lub przegubie ręki,
  - kształt linii zgięcia wnętrza dłoni,
  - zapach,
  - fale mózgowe EEG,
  - identyfikacja DNA;
- cechy behawioralne/fenotypowe (związane z zachowaniem):
  - barwa głosu, sposób mówienia,
  - sposób chodzenia, siedzenia, sylwetka,
  - ruch oka,
  - podpis odręczny i sposób pisania na klawiaturze,
  - cechy charakterystyczne ruchu ust i poruszania gałki ocznej,

– fala P300 – reakcja mózgu powstająca w czasie 300 milisekund od bodźca, charakterystyczna dla każdego człowieka.

Wszystkie modalności wykorzystywane w biometrycznym rozpoznawaniu powinny charakteryzować się następującymi właściwościami:

- unikatowością – dla każdej osoby owe cechy są unikalne, wyróżniające ja od innych;
- uniwersalnością – wszystkie istoty ludzkie mają te same właściwości fizyczne, tj. DNA, tęczówka, twarz itd., które mogą być podstawą identyfikacji;
- niezmiennością w czasie – właściwości te pozostają w dużej części niezmienne przez całe życie danej osoby;
- łatwą akwizycją – osoby nadają się do pobrania w stosunkowo łatwy sposób, co umożliwia szybką identyfikację;
- wydajnością – stopień dokładności identyfikacji musi być stosunkowo wysoki;
- akceptowalnością – sukces zastosowania systemu zależy od poziomu akceptacji społecznej wobec stosowania danych biometrycznych;
- o dpornością na oszustwa – w celu zapewnienia bezpieczeństwa system powinien być dobrze zabezpieczony, aby udaremnić ewentualne oszustwa.

Wykorzystanie biometrii w praktyce nie jest jednoznaczne i proste. Spora część danych biometrycznych ma charakter mieszany fizyczno-biologiczno-behawioralny. Trudno zatem jednoznacznie oddzielić parametry głosu ludzkiego podlegającego zmianom emocjonalnym lub obraz kształtu rysów twarzy od jej mimiki zależnej od stanów pobudzenia emocjonalnego. Niektóre wskaźniki identyfikacji mogą podlegać pewnym zmianom w czasie cyklu życia człowieka, podczas choroby itd. Nie zmienia to jednak faktu, że biometria jest aktualnie najbardziej wiarygodną metodą identyfikacji i cały czas podlega rozwojowi.

Gwałtowny rozwój biometrycznych metod rozpoznawania osób nastąpił na początku XXI w., ale sposoby identyfikacji człowieka towarzyszyły ludzkości od najdawniejszych czasów. W przeszłości były zdecydowanie mniej skomplikowane niż współcześnie i opierały się najczęściej na stosowaniu odcisków palców. W Babilonii odcisk palca na glinianej tabliczce stanowił potwierdzenie zawarcia transakcji, a w starożytnych Chinach palce odciskano na urzędowych pieczęciach. Oficjalne dokumenty w czternastowiecznej Persji były natomiast sygnowane przez decydenta kciukiem maczanym w farbie, a następnie weryfikowane przez lekarza zatrudnionego na dworze władcy. Pierwsze próby biometrycznego oznaczania osób zastosowano w Imperium Rzymskim, gdzie nacinano, wypalano lub tatuowano skórę najemników, aby utrudnić im → d e z e r c j ę [t. 2].

Największy rozwój w zakresie ustalania tożsamości człowieka nastąpił w XIX i XX w. w Europie. Biometria zaczęła się rozwijać we Francji, gdzie w 1893 r. Alphonse Bertillon, francuski uczony i funkcjonariusz policji, wydał książkę pt. *Identification anthropomérique*. Zawierała ona wyniki badań w zakresie antropometrii

kryminalnej, fotografii kryminalistycznej oraz „portretu mówionego". Była to pierwsza publikacja w zakresie sposobów i metod weryfikacji tożsamości człowieka. W ramach fotografii kryminalistycznej badacz zlecił, aby zdjęcie było wykonywane w 2 pozach – *en face* oraz z profilu, a jednocześnie twierdził, że najbardziej wiarygodne są fotografie wykonywane z profilu. Bertillon podkreślał, że należy je zawsze wykonywać z takiej samej odległości, przy takim samym ustawieniu głowy oraz przy takim samym oświetleniu. Opracował również antropometryczną kartotekę rejestracyjną opartą na pomiarach ludzkiego ciała. Bazowała ona na pomiarze niektórych cech anatomicznych człowieka, tj. średnicy czaszki, długości ramion i stóp, które były zapisywane na specjalnej karcie wraz z dołączonym zdjęciem. Jego autorska metoda ustalania tożsamości człowieka opierała się na kilku założeniach:

1) wymiary ludzkiego kośćca po 20. roku życia nie ulegają zmianie;
2) zachodzi małe prawdopodobieństwo znalezienia 2 osób o takich samych wymiarach kilkunastu zewnętrznych części ciała;
3) przeprowadzenie pomiarów ciała nie jest skomplikowanym procesem i polega na zmierzeniu pomiaru:
   - całego ciała – wzrostu w pozycji stojącej i siedzącej oraz rozwartości ramion,
   - głowy – długości i szerokości głowy, największej szerokości twarzy oraz długości i szerokości prawego ucha,
   - długości niektórych części ciała – lewego przedramienia, lewej stopy oraz środkowego i małego palca lewej ręki.

Metoda antropometrii kryminalistycznej Bertillona wzbudziła wielkie zainteresowanie kryminologów. Najpierw wdrożono ją we Francji, a następnie – w innych państwach Europy.

Interesujące aspekty zastosowania elementów biometrii w kryminologii można odnaleźć w kontrowersyjnej koncepcji antropologicznej znanej jako →teoria zbrodniarza z urodzenia, którą stworzył Cesare Lambroso – włoski psychiatra, antropolog i kryminolog, twórca szkoły kryminologii pozytywistycznej. W swojej książce pt. *Człowiek –zbrodniarz* z 1876 r. dowodził, że istnieją związki między budową twarzy a budową czaszki człowieka, które mogą wpływać na właściwości jego psychiki, w tym – na zdolności biologiczne do popełnienia przestępstwa. Chociaż badacz nie był zainteresowany wykorzystywaniem biometrii do identyfikacji czy weryfikacji człowieka, to starał się udowodnić, że kryminaliści mieli pewne cechy fizjologiczne i dymorficzne, które w pewnym stopniu mogą determinować ich skłonność do popełniania przestępstw.

Prawdziwym przełomem w sposobach ustalania tożsamości człowieka okazała się **daktyloskopia** – technika śledcza zajmująca się badaniami porównawczymi linii papilarnych dłoni w celu ustalenia sprawcy czynu zabronionego. Linie papilarne sklasyfikował już w XVII w. Marcello Malpighi, ale dopiero w XIX w. Jan Purkinje opracował zestaw 9 głównych wzorów linii papilarnych. Ogromne zasługi w zakresie

badań nad odciskami palców dla potrzeb praktyki kryminalistycznej należy przypisać m.in. Edwardowi Richardowi Henry'emu, który opracował system identyfikacji odcisków palców – w 1901 r. wdrożony przez londyński Scotland Yard, a wykorzystywany z powodzeniem także przez organy policji na całym świecie. Przełomem w historii rozwoju biometrii stały się prace badawcze Francisa Galtona, który pogłębił metody badań daktyloskopijnych i w rezultacie wyróżnił 3 podstawowe zasady tej techniki: niezmienność, niezniszczalność oraz indywidualność. Stwierdził ponadto, że rysunek tworzony przez linie papilarne człowieka jest niezmienny przez całe życie i kształtuje się ostatecznie w szóstym miesiącu życia płodowego. Opracował także metodę klasyfikacji odcisków palców, a tym samym udowodnił, że żaden człowiek nie jest anonimowy. Posługiwanie się odciskami palców, znane już od czasów starożytnych, zostało upowszechnione w XX w. i zyskało status obiektywnej podstawy ustalania tożsamości. Metoda opracowana przez Galtona ostatecznie wyparła system identyfikacji kryminalistycznej Bertillona.

Rozwój biometrii na szeroką skalę, oparty zwłaszcza na wykorzystywaniu odcisków palców, nastąpił w latach 60. XX w. i zbiegł się w czasie z rozwojem komputeryzacji na świecie. Rozpoczęto wówczas prace nad stworzeniem systemu daktyloskopijnego AFIS (ang. *Automated Fingerprint Identification System*), pozwalającego na gromadzenie i automatyczne przeszukiwanie obrazów linii papilarnych palców rąk i dłoni w celu szybkiej identyfikacji osób. W latach 80. XX w. rozwinęła się także technologia skanowania dokumentów, a coraz bardziej powszechne stawało się wykorzystanie komputerów osobistych. W następstwie tych okoliczności rozpoznawanie odcisków palców znalazło swoje zastosowanie nie tylkow kryminalistyce czy w medycynie sądowej, lecz także w życiu codziennym,np. w celu kontrolowania czasu pracy, na lotniskach, by zapewnić szybką odprawę pasażerów, oraz jako metoda kontroli dostępu do strzeżonychpomieszczeń.

Od tego momentu rozwój biometrii stał się coraz bardziej zaawansowany i obejmował swoim zasięgiem coraz więcej sfer życia ludzkiego. Obecnie biometria jest bardzo powszechnym instrumentem zapewnienia bezpieczeństwa. Jako rozwiązanie wspierające walkę z → terroryzmem [t. 4] oraz kontrolę granic było proponowane od początku lat 90. XX w., czyli jeszcze przed zamachami z 11 września 2001 r. Atak na World Trade Center zdecydowanie przyśpieszył wdrażanie identyfikacji na podstawie danych biometrycznych jako jednej z metod ochrony przed → zagrożeniami globalnymi [t. 4] związanymi z terroryzmem, → przestępczością zorganizowaną [t. 3] oraz związanymi z zapewnieniem skutecznej polityki imigracyjnej i azylowej. Stąd też główna rola Stanów Zjednoczonych w promowaniu tej metody i koncentracja wysiłków na rzecz stworzenia efektywnego mechanizmu kontroli granicznej chroniącej zainteresowane kraje przed napływem niepożądanych osób z zewnątrz. W 2003 r. Międzynarodowa Organizacja Lotnictwa Cywilnego wprowadziła nowe standardy dokumentów odczytywanych automatycznie

MRTD (ang. *Machine Readable Travel Documents*). Wprowadziły one do dokumentów technologie biometryczne, a podstawowym parametrem stał się obraz kształtu i rysów twarzy człowieka – w formie obrazu cyfrowego o wysokiej rozdzielczości.

Obecnie biometria stanowi stałe, a zarazem najważniejsze ogniwo łańcucha wartości dokumentów identyfikacyjnych. Paszport biometryczny w zasadzie stał się już standardem w wielu krajach na świecie. Biometria nie tylko jest już wykorzystywana przez instytucje publiczne, lecz także pozostaje również w spektrum zainteresowania przedsiębiorstw prywatnych: coraz częściej znajduje zastosowanie w sektorze bankowym, finansowym, zdrowia, handlu i kształcenia. Ten rozwój przyśpieszają nowe właściwości uzyskane w wyniku połączenia z nowoczesną technologią. Szczególnie ciekawe rozwiązania w tym zakresie wprowadza sektor bankowy, a cechą biometryczną, która jest coraz bardziej doceniana przez instytucje finansowe, jest układ krwionośny palca oraz układ naczyń krwionośnych dłoni. Państwem, które pierwsze wdrożyło biometrię układu naczyń krwionośnych palca, stała się Japonia, a dostawcą tej technologii pod koniec lat 90. XX w. była firma Hitachi. W Polsce biometria oparta na układzie krwionośnym palca została wprowadzona po raz pierwszy w 2013 r. w oddziałach Banku BPH.

Wdrażanie rozwiązań technologicznych w biometrii z pewnością ułatwia społeczeństwom funkcjonowanie w wielu obszarach życia. Jednak masowe zastosowanie rozwiązań biometrycznych w wielu krajach budzi kontrowersje natury etycznej, moralnej i społecznej. Często postrzega się ją jako →za g r o żenie [t. 4] dla podstawowych → p r a w c z ł o w i e k a [t. 3], tj. prawo do prywatności, prawo do ochrony danych osobowych czy godności ludzkiej. Szczególnie niebezpieczne okazuje się wykorzystywanie technologii biometrycznych, które opierają się na informatycznych bazach danych. Przetwarzanie → i n f o r m a c j i [t. 2] zawartych w takich bazach stwarza ryzyko ich utraty, wykorzystania przez osoby nieuprawnione lub niezgodnie z celami przewidzianymi pierwotnie. Dlatego zbieranie i przetwarzanie danych biometrycznych powinno pozostawać w zgodzie z zasadami prawa do ochrony danych osobowych. Należy jednak pamiętać, że prawo do ochrony danych osobowych nie ma charakteru bezwzględnego i w pewnych warunkach może zostać ograniczone w przypadku m.in.: konieczności zapewnienia → b e z p i e c z e ń s t w a p u b l i c z n e g o [t. 1], → b e z p i e c z e ń s t w a n a r o d o w e g o [t. 1], → o b r o n n o ś c i oraz w działaniach prewencyjnych, prowadzonych czynności dochodzeniowo-śledczych i prokuratorskich w sprawach karnych. Rozwoju biometrii nie da się zatrzymać, należy jednak podjąć działania w zakresie ochrony prawnej, tak aby był on w odpowiedni sposób regulowany i kontrolowany.

Sabina Olszyk

D. Jaroszewska-Choraś, *Biometria. Aspekty prawne*, Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2016; K. Krasowski, I. Sołtyszewski, *Biometria – zarys problematyki*, „Problemy Kryminalistyki" 2006, nr 252; R. Lewandowski, *Biometria –nowe zastosowania*, „Przegląd Bezpieczeństwa Wewnętrznego" 2017, vol. 9, z. 17.

BIOTERRORYZM – rodzaj → t e r r o r y z m u [t. 4], który definiowany jest jako bezprawne, nielegalne użycie czynników biologicznych wobec ludzi, zwierząt lub spowodowanie uszkodzeń roślin z zamiarem wymuszenia jakiegoś działania bądź zastraszenia rządu, → l u d n o ś c i c y w i l n e j [t. 3] w celu osiągnięcia celów politycznych, społecznych lub religijnych. Bioterroryzm jest formą terroryzmu z użyciem środków pochodzenia biologicznego. Czynnikiem rażenia mogą być mikroorganizmy, bakterie, wirusy, grzyby lub toksyny produkowane przez żywe organizmy.

Celem bioterroryzmu jest skuteczne wywołanie lęku i paniki wśród ludności i ratowników oraz chaos w wielu dziedzinach życia i ogromne straty ekonomiczne. Według ekspertów z Centrum Kontroli i Prewencji Chorób (Centers for Disease Control and Prevention, CDC) w Atlancie ogólne koszty związane z zakażeniem 100 tys. ludzi np. laseczką wąglika (postać płucna) to straty w wysokości ok. 26,2 mld USD, a w przypadku tularemii 5,5 mld USD. Sama → b r o ń b i o l o g i c z n a jest najtańszą do uzyskania → b r o n i ą m a s o w e g o rażenia (BMR). Cechuje się również dużą skutecznością, słabą wykrywalnością oraz możliwością preparowania w szczególny sposób, np. poprzez modyfikację genetyczną, aby zwiększyć jej siłę rażenia i zdolność do przetrwania w środowisku.

Wiele zarazków można łatwo wyprodukować, kłopot pojawia się w chwili użycia danego patogenu jako broni biologicznej. Najwięcej trudności wiąże się z mechanizmem rozpylania oraz przechowywania zarodków. Niemniej jednak rozwój technologii zmniejsza bariery utrudniające produkcję oraz daje możliwość jej zastosowania przez terrorystów. Drobnoustroje mogą być rozprzestrzenianie za pomocą pocisków rakietowych, bomb lotniczych, pojemników lub przesyłek listowych. Rozprzestrzenianie może odbywać się także za pomocą nosicieli, np. owadów, zwierząt i ludzi, którzy podróżując, zwiększają możliwość przenoszenia niebezpiecznego patogenu do nieuodpornionych części populacji. Zastosowanie broni biologicznej w ataku terrorystycznym może nastąpić np. poprzez rozpylenie aerozolu, skażenie żywności, wody i gleby. Miejscem ataku najczęściej są obszary skupisk ludzkich, takie jak centra handlowe, porty lotnicze, stacje kolejowe, metro, budynki rządowe i publiczne oraz tereny wojskowe. Wybór miejsca zależy też od czynników takich jak dobra wentylacja lub specyficzne prądy powietrzne (warunki takie występują np. w metrze) albo ujście wody pitnej. Bioterroryści mogą również skazić żywność poprzez wprowadzenie patogenu do fabryk, hurtowni lub dużych sklepów. Wybór broni biologicznej w aktach terrorystycznych może wynikać z dostępności surowców i technologii do ich produkcji m.in. dlatego, że surowce te mają zastosowanie w produkcji szczepionek dla ludzi, zwierząt i roślin, stąd możliwość ich pozyskania jest tak łatwa. Atrakcyjność zastosowania broni biologicznej w ataku terrorystycznym wynika nie tylko z łatwości dostępu czy minimalnego kosztu, ale także z możliwości ukrycia i transportu oraz niewidoczności w trakcie przeprowadzenia zamachu ze względu na brak zapachu i koloru.

Według klasyfikacji CDC wykorzystywane w atakach niebezpieczne czynniki biologiczne zostały podzielone z uwagi na stopień stwarzanego → z a g r o ż e n i a [t. 4] na 4 kategorie:

- Kategoria A – patogeny o wysokiej zjadliwości i śmiertelności, łatwe do emisji i utrzymania w środowisku w postaciach możliwych do militarnego wykorzystania. Zakażenie odbywa się poprzez kontakt bezpośredni, powoduje panikę i konsekwencje psychologiczne w społeczeństwie. Stanowią one duże ryzyko dla → z d r o w i a p u b l i c z n e g o [t. 4]. Choroby wywoływane przez patogen kategorii A to np. dżuma, wąglik, botulizm, wirusowe gorączki krwotoczne, tularemia, ospa prawdziwa.
- Kategoria B – patogeny o niższej zjadliwości i śmiertelności, łatwe do rozprzestrzeniania, średnio trudne do utrzymania w środowisku. Wymagają specjalistycznych metod diagnostycznych oraz nadzoru nad przebiegiem choroby. Zakażenie może odbywać się poprzez wodę lub pokarm. Choroby wywoływane przez patogen kategorii B to np. bruceloza, dur plamisty, zatrucie rycyną, salmonelloza, czerwonka, gorączka Q, wirusowe zapalenie mózgu, cholera.
- Kategoria C – czynniki charakteryzujące się potencjalnie dużą chorobotwórczością i śmiertelnością. Mogą być przeznaczone do zastosowania w przyszłości na bardzo dużych skupiskach ludności, gdyż są łatwe do nabycia oraz rozprzestrzeniania. Mogą stać się przedmiotem modyfikacji genetycznej. Choroby wywoływane przez patogen kategorii C to np. żółta febra, kleszczowe zapalenie mózgu, gorączka krwotoczna z zespołem nerkowym, gruźlica lekoodporna, malajskie zapalenia mózgu.
- Kategoria D – czynniki, które najprawdopodobniej nie zostaną wykorzystane jako broń biologiczna (np. wirus grypy).

Ataki z użyciem czynnika biologicznego odbywają się najczęściej bez ostrzeżenia, osoby porażone nie zdają sobie sprawy z ekspozycji na śmiercionośny czynnik. Podejrzenie epidemii pojawia się dopiero w sytuacji identyfikacji pojawienia się skupisk zachorowań. Wykluczenie ataku czynnikiem biologicznym odbywa się przy udziale → p o l i c j i [t. 3] oraz nadzoru epidemiologicznego. Cechy epidemiologiczne zachorowań, które powinny wzbudzać niepokój pracowników służby zdrowotnej, to:

- zwiększona liczba zachorowań (na danym terenie) z podobnym zespołem objawów wśród dotychczas zdrowej populacji;
- przebieg zachowań charakteryzujący się najczęściej wysoką temperaturą, objawami ze strony układu oddechowego, pokarmowego oraz przypadki śmiertelne;
- niska skuteczność podczas zastosowania rutynowego leczenia;
- wystąpienie jednostki chorobowej nietypowej dla danej populacji oraz w nietypowym terenie lub w okresie, w którym nie obserwowano wcześniej tego typu zachorowań;
- pojawienie się chorób rzadkich, takich jak ospa prawdziwa, gorączka krwotoczna, dżuma, tularemia;

- nietypowe drogi przenoszenia: woda, żywność, aerozol;
- skupiska przypadków zachorowań po zawietrznej (tj. biorąc pod uwagę kierunek wiatru).

Skutki ataku bioterrorystycznego mogą pojawić się z czasem. Trudno jest przewidzieć i zlokalizować atak terrorystyczny z użyciem patogenu biologicznego oraz zapobiec mu, gdyż zatrucia pojawiają się w wielu wypadkach w różnych miejscach. Bez posiadania → i n f o r m a c j i [t. 2] o możliwości ataku działania zapobiegawcze są praktycznie niemożliwe. Efekty działania bioterroryzmu rozpatruje się w aspekcie finansowym, najczęściej określa się koszty związane z leczeniem osób zakażonych oraz koszty związane z zapobieganiem rozprzestrzeniania się patogenu. Lekceważone są natomiast koszty związane ze skutkami psychologicznymi. Wraz z atakiem bioterrorystycznym pojawia się panika, lęk, strach i obawa o zdrowie i życie własne i najbliższych. Nikt nie czuje się bezpieczny, co przedkłada się w dalszej konsekwencji na ludzkie zachowania, które mogą mieć istotny z ekonomicznego punktu widzenia wymiar. Zagrożenie bioterrorystyczne jest jak najbardziej realne. Jego nieprzewidywalność i okrucieństwo jest szczególnie pożądane przez terrorystów. Możliwość użycia mikroorganizmów w ataku terrorystycznym deklarowały m.in. ugrupowania takie jak: Al-Kaida, Hamas (Muzułmański Ruch Oporu), baskijska ETA (bask. Euskadi Ta Askatasuna, Baskonia i Wolność), Palestyński Islamski Dżihad (→ d ż i h a d [t. 2]) czy Hezbollah.

Według → Ś w i a t o w e j O r g a n i z a c j i Z d r o w i a [t. 4] (World Health Organization, WHO) Al-Kaida może być w posiadaniu np. zarodników laseczki wąglika, laseczki C. botulinum, a także wirusa ospy.

Definicja terroryzmu i bioterroryzmu jest stosunkowo nowa, natomiast użycie broni biologicznej nie jest wynalazkiem XX w. Pierwsze wzmianki o jej wykorzystaniu sięgają starożytności. Polegały na zatruciu wody pitnej, np. Rzymianie wrzucali do wody pitnej padlinę. Uważa się, że pierwsi w 1346 r. użyli broni biologicznej Tatarzy, wśród których wybuchła epidemia dżumy – wykorzystali oni ciała zmarłych na tę chorobę → ż o ł n i e r z y [t. 4] i katapultami przerzucali je na teren oblężonej Kaffy (dzisiejsza Teodozja, Krym) nad Morzem Czarnym. Mieszkańcy portu uciekli m.in. do Wenecji, Konstantynopola i Genui, przywieźli ze sobą dżumę i wywołali pandemię czarnej śmierci w Europie, w wyniku której zmarło 25 mln ludzi. Czynnika biologicznego używali również hiszpański konkwistador F. Pizarro czy – kilka wieków później – dowódca wojsk angielskich J. Amherst. Wykorzystywali oni zarazki ospy, rozdając lub pozostawiając zainfekowaną wirusem odzież i bieliznę, a tym samym doprowadzili do wybuchu epidemii. Zarażanie wroga aktualnie panującą chorobą było wykorzystywane aż do XIX w., później naukowcom udało się wyizolować i wyhodować niektóre bakterie i drobnoustroje. Podczas I wojny światowej Niemcy wykorzystali patogen wąglika do zniszczenia transportów mułów i koni z USA czy Argentyny. W latach 1932–1945 Japonia prowadziła badania nad rozwojem broni biologicznej, od

1933 r. w wyniku tych eksperymentów zmarły dziesiątki tysięcy osób. Do 1945 r. zgromadzono 400 kg bakterii wąglika. Nad możliwością wykorzystania broni biologicznej pracowali również Brytyjczycy, przeprowadzili m.in. próbny atak bombami wąglikowymi. Prace podjęły również USA, badano zastosowanie dżumy, cholery, gorączki Q i innych drobnoustrojów.

Po zakończeniu ery → z i m n e j w o j n y [t. 4] bioterroryzm stał się międzynarodowym problemem. Pojawiały się informacje, że terroryści chcą zgromadzić → b r o ń c h e m i c z n ą i biologiczną. Groźby dotyczące wykorzystania broni biologicznej pojawiały się także ze strony kryminalistów oraz sekt religijnych. W 2001 r. po ataku na World Trade Center doszło do licznych ataków bioterrorystycznych z użyciem laseczek wąglika, rozesłano listy do instytucji rządowych oraz mediów. W wyniku tych ataków zmarło w USA 5 osób, a 32 tys. zostało poddanych profilaktycznej terapii ciprofloksacyną.

W związku z zagrożeniem atakiem bioterrorystycznym podejmowane są prace dotyczące zakazu wykorzystywania broni biologicznej. Kluczowym dokumentem dotyczącym nieproliferacji broni biologicznej jest Konwencja o zakazie prowadzenia badań, produkcji i gromadzenia zapasów broni bakteriologicznej (biologicznej) i toksycznej oraz o ich zniszczeniu sporządzona w Moskwie, Londynie i Waszyngtonie dnia 10 kwietnia 1972 r., tzw. Konwencja o zakazie broni biologicznej i toksynowej (Biological and Toxin Weapons Convention, BTWC). Mimo to w wielu krajach są prowadzone badania nad użyciem czynników biologicznych jako środków militarnych.

Żaneta Mrożek

Y. Alexander, M. Hoenig, *Superterroryzm biologiczny, chemiczny i nuklearny*, tłum. R. Stiller, Bellona, Warszawa 2001; K. Alibek, *Biohazard*, Avon, New York 1999; M. Binczycka-Anholcer, A. Imiołek, *Bioterroryzm jako jedna z form współczesnego terroryzmu*, „Hygeia Public Health" 2011, nr 3 (46); K. Chomiczewski, J. Kocik, M.T. Szkoda, *Bioterroryzm. Zasady postępowania lekarskiego*, Wydawnictwo Lekarskie PZWL, Warszawa 2002; M.R. Grey, K.R. Spaeth, *The Bioterrorism Sourcebook*, The McGraw-Hill Companies, New York 2006; P. Kępka, *Bioterroryzm. Polska wobec użycia broni biologicznej*, Difin, Warszawa 2009; K. Langbein, Ch. Skalnik, I. Smolek, *Bioterroryzm*, tłum. M. Chudzik, Muza, Warszawa 2003; K. Liedel, P. Piasecka, *Jak przetrwać w dobie zagrożeń terrorystycznych? Elementy edukacji antyterrorystycznej*, Wydawnictwo Trio, Collegium Civitas, Warszawa 2008; B. Michailiuk, *Broń biologiczna i bioterroryzm*, „Zeszyty Naukowe AON" 2016, nr 1 (102); tenże, *Broń biologiczna jako zagrożenie bezpieczeństwa państwa*, AON, Warszawa 2015; tenże, *Broń biologiczna*, AON, Warszawa 2004; T. Płusa, *Współczesne zagrożenie patogenami biologicznymi*, Wydawnictwo Medpress, Warszawa 2015; M. Prusakowski, *Bioterror: jak nie dać się zabić*, Wydawnictwo Tower Press, Gdańsk 2001; J.R. Ryan, *Biosecurity and Bioterrorism: Containing and Preventing Biological Threats*, Elsevier, Amsterdam 2016; W. Szot, *Trwałość bezpieczeństwa międzynarodowego w obliczu współczesnego bioterroryzmu*, Drukarnia Pijarów, Kraków 2008; M. Upson, *Handbook of Bioterrorism*, Foster Academics, US 2015; S. Wasiuta, *Broń biologiczna*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; M. Żuber, *Broń masowego rażenia w działalności terrorystycznej*, Difin, Warszawa 2015.

BITWA – akcja militarna na dużą skalę, działania wojenne między 2 stronami lub większą liczbą sił zbrojnych, które są ze sobą w stanie → w o j n y [t. 4] (konfliktu zbrojnego), zderzenie bojowe formacji wojskowych w celu osiągnięcia znaczących rezultatów militarno-politycznych. Ogólnie rzecz biorąc, bitwa to zaangażowanie wojskowe, określone pod względem czasu trwania, obszaru i zaangażowania sił. Bitwę można przeprowadzić poprzez atak lub operację obronną, w której obie strony starają się doprowadzić do klęski siły przeciwnika i utrzymać lub przejąć ważne obszary i fortyfikacje.

Na przestrzeni dziejów do XIX w. armie jako formacje – w porównaniu z nowoczesnymi – były nieliczne, zdecydowane walki toczyły się na ograniczonych przestrzeniach i często wynik jednej bitwy przesądzał nie tylko o losach armii, lecz także o dalszej historii i losach państwa. Nazwa bitwy zwykle pochodziła od miejsca, w którym ta się odbywała.

Definicja bitwy jako pojęcia w naukach wojskowych zmieniała się wraz ze zmianami w organizacji i technologiach sił zbrojnych. Angielski historyk wojskowości J. Keegan zaproponował jedną z najbardziej zbliżonych do realiów i klarownych definicji bitwy jako „czegoś, co dzieje się między dwiema armiami, prowadząc do moralnego, a następnie fizycznego rozpadu jednej z nich".

W czasie II wojny światowej bitwa oznaczała walkę znaczących grup strategicznych na ważnym kierunku strategicznym lub teatrze działań. Decydującą siłą w tych bitwach były formacje frontowe i grupy armii.

We współczesnych realiach termin „bitwa" używany jest jako określenie zbiorcze wielu bitew wykorzystywanych do osiągnięcia celów wojskowych w ramach jednej dużej operacji lub kilku, przykładem może być bitwa pod Kurskiem (1943).

Znaczące wydarzenia militarne, w wyniku których zadecydowano o losach kampanii wojennych, a czasem wojen, nazywane są bitwami generalnymi. Ich czas trwania mógł sięgać kilku miesięcy, a rozciągłość geograficzna dziesiątek i setek kilometrów. Gdy czas trwania bitwy jest dłuższy niż tydzień, używany jest termin „operacja". Starcie z ograniczonym zaangażowaniem między siłami i bez zdecydowanych rezultatów jest czasami nazywane potyczką.

Wiele starć militarnych jest zbyt małych, aby mogły zostać nazwane bitwami, dlatego używa się względem nich określeń takich jak „akcja", „potyczka", „nalot" czy „ofensywny patrol". Walki te zwykle toczą się w ramach właściwej bitwy i chociaż mają określone cele, nie zawsze są decydujące. Tak np. po bitwie pod Waterloo niektórzy brytyjscy oficerowie wątpili, czy wydarzenia, które miały miejsce tego dnia, zasługiwały na tytuł „bitwy", czy też były zwykłą „akcją".

Bitwy różnią się między sobą pod względem skali i znaczenia, często odgrywają decydującą rolę w wojnie. Liczba walczących jest bardzo zróżnicowana i może wahać się od 2 oddziałów do bitew na poziomie armii, w których biorą udział setki tysięcy

jednostek. Wojna zazwyczaj składa się z wielu bitew. Bitwy mogą być planowane lub wymuszane przez jedną stronę, kiedy przeciwna strona już nie jest w stanie wycofać się z owej walki.

Idealnym celem bitwy jest osiągnięcie decydującego punktu, jakim jest zwycięstwo, ale strategia i różne okoliczności, które mogą się pojawić, często zmuszają strony do kompromisu. Zwycięstwo w bitwie zostaje osiągnięte, gdy jedna z walczących stron zmusza drugą do poddania się, przeciwnik zostaje rozproszony, zmuszony do ucieczki lub staje się nieskuteczny militarnie do kontynuowania walk, pozbawiony zdolności do kontynuowania działań wojennych. Jednak bitwa może także zakończyć się pyrrusowym zwycięstwem, które kończy się faworyzowaniem strony „przegrywającej". Bitwa może również przerodzić się w impas, nie prowadzi wówczas do decydującego wyniku dla żadnej ze stron. Jeśli żaden cel bitwy nie zostanie osiągnięty, wynik uważa się za remis.

W starożytności i średniowieczu, a także we współczesnych czasach aż do XX w. bitwy z reguły odbywały się na zwartym terytorium, otwartym terenie, którym mogły być pola lub w niektórych przypadkach zamarznięte jeziora, zwykle nie trwały dłużej niż kilka dni. Miejsca bitew na długo pozostawały w pamięci ludu, często stawiano na nich pomniki, odczuwano z nimi szczególny związek emocjonalny.

Do XIX w. przeważająca liczba bitew była krótkotrwała, większość z nich trwała tylko kilka godzin, jak np. bitwa pod Grunwaldem (1410) czy bitwa pod Preston (1648). Natomiast bitwa pod Lipskiem, stoczona między wojskami francuskimi pod przywództwem N. Bonapartego a wojskami koalicji antyfrancuskiej (złożonej z Austrii, Prus, Rosji i Szwecji), znana też jako „bitwa narodów", trwała 3 dni (16–19 października 1813). Wynikało to głównie z trudności w zaopatrzeniu armii na polu bitwy lub prowadzeniu operacji nocnych.

Typowym sposobem przedłużenia bitwy było zastosowanie technik oblężniczych. Ulepszenie transportu oraz ewolucja działań wojennych w okopach, przypominających oblężenia podczas I wojny światowej w XX w., wydłużyły czas trwania bitew do kilku dni, tygodni, a nawet miesięcy. Stworzyło to wymóg rotacji jednostek, aby zapobiec zmęczeniu podczas walki, przy czym → ż o ł n i e r z e [t. 4] nie powinni byli pozostawać w obszarze działań bojowych dłużej niż miesiąc.

W historii wojskowości termin „bitwa" jest nadużywany w odniesieniu do walki na niemal każdą skalę, zwłaszcza przez siły strategiczne z udziałem setek tysięcy żołnierzy, które mogą brać udział albo w jednej bitwie (bitwa pod Lipskiem), albo w operacji (bitwa pod Kurskiem).

Przestrzeń, jaką zajmuje bitwa, zależy od zasięgu broni walczących. Bitwa w szerszym znaczeniu może trwać długo i toczyć się na dużym obszarze, jak w przypadku bitwy o Anglię czy bitwy o Atlantyk, która trwała od 3 września 1939 r. do kapitulacji Niemiec w maju 1945 r. Aż do pojawienia się artylerii i samolotów bitwy toczyły się między 2 obozami w zasięgu wzroku. Głębokość pola bitwy wzrosła w nowoczesnej

wojnie, a jednostki wsparcia pozostały na tyłach (zasoby, → a r t y l e r i a, jednostki medyczne itp.).

Bitwy na ogół składają się z wielu pojedynczych bitew, a walczący są świadomi tylko ograniczonej części wydarzeń. Żołnierz piechoty może nie wiedzieć, czy bierze udział w mniejszej bitwie czy w dużej ofensywie, może nie mieć możliwości przewidywania przyszłego przebiegu bitwy.

Bitwy można toczyć na lądzie, na morzu i w powietrzu. Bitwy morskie rozgrywały się już przed V w. p.n.e. Bitwy powietrzne były znacznie mniej powszechne ze względu na ich późną koncepcję, najbardziej znaczącą była bitwa o Anglię w 1940 r. Od II wojny światowej bitwy lądowe i morskie opierają się na wsparciu z powietrza. Podczas bitwy o Midway (4–7 czerwca 1942) między okrętami japońskimi a amerykańskimi na Oceanie Spokojnym 5 lotniskowców zostało zatopionych bez bezpośredniego kontaktu między flotami.

Typy bitew można wyróżnić ze względu na zaangażowane siły:

- Potyczka – bitwa z premedytacją, w której obaj przeciwnicy spotykają się na polu bitwy bez przygotowania ataku lub obrony.
- Bitwa na wyczerpanie – ma na celu wyrządzenie wrogowi większych strat. Wiele bitew I wojny światowej było celowo lub nieumyślnie bitwami na wyczerpanie.
- Przełamanie – głównym celem jest zniszczenie obrony przeciwnika poprzez odsłonięcie flanek, które pozostają na wrażliwej pozycji, a tym samym mogą zostać zniszczone.
- Okrążenie – niemiecki Blitzkrieg – jest praktycznie tym samym, co bitwa na większą skalę, ale przełamuje lukę między liniami wroga, aby przemknąć się przez nie szybko do przodu.
- Otoczenie – obejmuje atak na jedną lub obie flanki. Klasycznym przykładem jest bitwa pod Kannami (216 p.n.e.).
- Unicestwienie – to bitwa, w której pokonane siły zostają zniszczone na polu bitwy, tak jak to miało miejsce w przypadku floty francuskiej w bitwie nad Nilem.
- Decydująca bitwa – ma szczególne znaczenie, ponieważ albo kończy działania wojenne, jak w bitwie pod Hastings (14 października 1066), która była decydującym starciem w inwazji Normanów na Anglię, albo wyznacza decydujący moment między rywalami, jak w bitwie pod Stalingradem (23 sierpnia 1942–2 lutego 1943). Decydująca bitwa ma ogromny wpływ zarówno na poziomie politycznym, jak i wojskowym, może bowiem zmienić układ sił i granice między krajami. Bitwy są zwykle hybrydami różnych typów wymienionych powyżej.

Bitwa na otwartej przestrzeni i po ustawieniu przeciwnych stron jest również nazywana bitwą polową. Bitwa o ufortyfikowany punkt jest często określana jako oblężenie (np. oblężenie Orleanu, 1428–1429). Bitwa, w której jedna strona zaskakuje drugą, nazywana jest zasadzką. Bitwa, w której jedno zgrupowanie otacza drugie i atakuje ze wszystkich stron, jest znana jako kocioł (np. kocioł pod Falaise w czasie

II wojny światowej). Istotne dla typu bitew są również rozmaite warunki geograficzne w walkach lądowych, powietrznych, morskich i podwodnych. W bitwach lądowych wyróżnia się walki górskie, walki w dżungli i walki w lesie, a także walki w terenie miejskim.

Na rozwój bitwy i jej wynik wpływają różne czynniki:

- Liczba żołnierzy, dowódców każdej armii i zalety wynikające z ukształtowania terenu należą do najważniejszych czynników.
- Morale. Bitwy znane z historii pokazały, że nastawienie i morale żołnierzy są często ważniejsze niż liczebność. O jakości armii decyduje stan umysłu, który będzie zależał od ducha żołnierzy, wyposażenia i wyszkolenia, jakie przeszli. Jednostka, która szarżuje bez żadnej dyscypliny, ale z wysokim morale, może wyjść zwycięsko z konfrontacji.
- Teren, na którym rozgrywają się bitwy. Zajmowanie wyżyn było główną taktyką w niezliczonych bitwach. Armia, która utrzymuje wysoki poziom, zmusza wroga do wspinania się i tym samym wyczerpania. Fizycznie łatwiej jest też zaatakować z pozycji wysokiej niż z pozycji niskiej. Chociaż czynnik ten stracił na znaczeniu we współczesnej wojnie wraz z pojawieniem się samolotów i dronów, teren może nadal mieć kluczowe znaczenie dla kamuflażu, zwłaszcza w wojnie partyzanckiej.
- Dowódcy również odgrywają decydującą rolę podczas walki: Hannibal, Juliusz Cezar, Chalid ibn al-Walid, Subutai i Bonaparte byli zdolnymi generałami, a ich armie czasami odnosiły legendarne zwycięstwa. Armia mogąca zaufać rozkazom przywódcy, przekonana o dążeniu do sukcesu, niezmiennie ma wyższe morale niż armia, która wątpi w każdy rozkaz kierującego nią wodza. Na przykład Brytyjczycy w morskiej bitwie pod Trafalgarem (21 października 1805) przypisali swój sukces reputacji słynnego admirała Lorda Nelsona.
- Uzbrojenie i wyposażenie. W niektórych przypadkach zwykła broń używana w niekonwencjonalny sposób okazała się korzystna. Tak np. szwajcarscy pikinierzy (jedna z formacji wojskowych z przełomu XV i XVI w. będąca pierwszą nowoczesną piechotą tamtej epoki) odnieśli wiele zwycięstw dzięki umiejętności przekształcenia tradycyjnej broni defensywnej w ofensywną. Wykorzystanie nowoczesnej broni może również stać się czynnikiem decydującym. Wiele razy armie odniosły zwycięstwo dzięki bardziej zaawansowanej broni niż ta, którą dysponowali ich przeciwnicy. Spektakularnym przykładem jest bitwa pod Omdurmanem (2 września 1898) pomiędzy wojskami brytyjskimi i egipskimi a powstańcami sudańskimi. Podczas trwającej kilka godzin bitwy wojska brytyjsko-egipskie dzięki nowoczesnemu uzbrojeniu i lepszemu wyszkoleniu prawie bez strat własnych zniszczyły wielokrotnie liczniejsze oddziały mahdystów.
- Dyscyplina żołnierzy. Zdyscyplinowane wojska mają często większe znaczenie niż uzbrojenie. Tak np. w bitwie pod Alezją (52 p.n.e.), pomiędzy oblegającymi galijskie miasto Alezja wojskami rzymskimi a siłami zbuntowanych Galów, Rzymianie,

chociaż mieli znacznie mniej wojska, zwyciężyli dzięki doskonałej dyscyplinie i wyszkoleniu.

- Strategia. Wojny i kampanie militarne opierają się na strategii, podczas gdy bitwy są fazami, w których stosuje się taktykę, toczą się na poziomie planowania i realizacji zwanym mobilnością operacyjną. Niemiecki strateg C. von Clausewitz stwierdził, że „wykorzystanie bitew […] dla osiągnięcia celu wojny" było istotą strategii. Brytyjski historyk wojskowości Keegan był zdania, że początki i wyniki bitew rzadko można ocenić dokładnie, „rzadko kiedy możemy tak prosto podsumować przyczyny i konsekwencje bitwy".

Praktycznie każda duża bitwa ma skutki i wpływy na poziomie politycznym, określając przebieg wojny oraz powojennego rozwoju. Decydująca bitwa może zmienić równowagę sił w regionie lub granice między krajami. Kiedy jeden z przeciwników wygrywa decydującą bitwę, może doprowadzić do kapitulacji wroga, zmusić go do poddania się interesom zwycięzcy albo przez zrzeczenie się terytorium, albo przez zmianę polityki międzynarodowej na korzyść zwycięzcy.

Bitwy w wojnach domowych zadecydowały o losie monarchów i frakcji politycznych. Przykład tego można widzieć w Wojnie Dwóch Róż (wojna domowa tocząca się w Anglii w latach 1455–1485) i powstaniu jakobickim (powstanie w Szkocji w latach 1745–1746). Warto też zwrócić uwagę na to, jak bitwy mogą wpłynąć na kontynuację lub zakończenie wojny. Przykładem tego jest bitwa o Inczon (15 października 1950) w trakcie wojny koreańskiej, która zakończyła się decydującym i strategicznym zwycięstwem międzynarodowych sił ONZ.

Zwykle nazwa bitwy, chociaż pole bitwy może rozciągać się na kilka kilometrów kwadratowych, pochodzi od miejsca, w którym się toczyła, od nazwy miasta, lasu lub rzeki. Czasami bitwy mogą być nazwane na podstawie daty ich stoczenia. W średniowieczu uważano za bardzo ważne, aby wybierać odpowiednie nazwy bitew, tak aby kronikarze mogli je uwiecznić. Niektóre nazwy geograficzne stały się historycznym synonimem toczonych w danym miejscu bitew, np. Pearl Harbor (7 grudnia 1941, japoński nalot na amerykańskie bazy floty i lotnictwa w Pearl Harbor na Hawajach), Alamo (starcie zbrojne podczas długiej walki o niepodległość Teksasu, która rozpoczęła się w październiku 1835 r.) czy bitwa pod Waterloo (18 czerwca 1815), uważana za jedną z najważniejszych bitew świata; była ostatnią bitwą Napoleona, którego klęska przypieczętowała postanowienia kongresu wiedeńskiego. Zwycięskie mocarstwa wprowadziły nowy ład, który miał panować w Europie przez następne stulecie.

Operacje wojskowe, które kończą się bitwą, z reguły mają nazwy kodowe, niekoniecznie muszą być one związane z rodzajem lub lokalizacją bitew. Niektóre z tych operacji, które zakończyły się bitwą, nadały jej jednak swoją nazwę kodową, np. operacja Market Garden – największa operacja powietrznodesantowa II wojny światowej, przeprowadzona przez aliantów we wrześniu 1944 r. na terytorium okupowanej Holandii,

która miała przynieść spektakularny sukces aliantom, a zamieniła się w krwawą klęskę. Podobnie operacja Rolling Thunder trwająca od 2 marca 1965 do 31 października 1968 r., która była jedną z największych i najkosztowniejszych w historii lotnictwa USA. Przez niemal 4 lata próbowano zmusić do uległości Wietnam Północny, zrzucając nań więcej bomb niż na III Rzeszę czy Japonię. Amerykanie popełnili jednak szereg błędów, które doprowadziły do drastycznego wzrostu kosztów tej wojny. Kiedy pole bitwy jest miejscem więcej niż jednej bitwy w tym samym konflikcie, nazwy są rozróżniane według liczby porządkowej, np. I i II bitwa nad Bull Run. Pierwsza bitwa została stoczona 21 lipca 1861 r., druga miała miejsce pod koniec sierpnia 1862 r. w czasach wojny secesyjnej (1861–1865) i okazała się wielką katastrofą dla sił Unii oraz punktem zwrotnym w tej wojnie. Ekstremalnym przypadkiem jest 12 bitew nad Isonzo (1915–1917) – stoczonych między Włochami a Austro-Węgrami podczas I wojny światowej.

Niektóre bitwy zostały nazwane na podstawie porozumienia historyków wojskowości w celu uporządkowania i rozróżnienia danych okresów walk. Tak np. po I wojnie światowej utworzono British Battles Nomenclature Committee w celu ustalenia standardowych nazw wszystkich bitew i działań pomocniczych.

Dawne pola bitew głęboko wpisały się w zbiorową pamięć narodów, których dotyczyły (np. bitwa pod Verdun w 1916 r. i bitwa pod Stalingradem w 1942 r.), służą one jako miejsce pamięci i tożsamości niezależnie od zwycięstwa lub porażki. Aż do II wojny światowej często tylko zwycięzcy stawiali na polu bitwy heroiczne pomniki, jeśli pola te znajdowały się w ich strefie wpływów. Od tamtej pory pomniki coraz częściej postrzegane są jako miejsca pojednania.

Sergiusz Wasiuta

C. Clausewitz, *O wojnie*, tłum. A. Cichowicz, L.W. Koc, Wydawnictwo Mireki, Kraków 2010; A. Czupryczyński, *Myślenie operacyjne w sztuce wojennej*, AON, Warszawa 2006; S. Drumowicz, *Aktualność klasycznych zasad walki Clausewitza we współczesnej sztuce wojennej*, „Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej" 2012, nr 1; T.N. Dupuy, *Understanding War: History and Theory of Combat*, Leo Cooper, London 1992; *Działania taktyczne wojsk lądowych*, Z. Ścibiorek (red.), AON, Warszawa 1995; D.M. Glantz, C.E. Vuono, *Soviet Military Operational Art: In Pursuit of Deep Battle*, Frank Cass, London 1991; J. Keegan, *The Face of Battle: A Study of Agincourt, Waterloo and the Somme*, Penguin Books, London 2011; S. Koziej, *Podstawy sztuki wojennej*, AON, Warszawa 1992; tenże, *Teoria sztuki wojennej*, Bellona, Warszawa 2011; R. Kuźniar, *Polityka i siła. Studia strategiczne – zarys problematyki*, Wydawnictwo Naukowe Scholar, Warszawa 2006; E. Ludendorff, *Wojna totalna*, tłum. F. Schoener, Wydawnictwo MON, Warszawa 1959; S. Mossor, *Sztuka wojenna w warunkach nowoczesnej wojny*, Wydawnictwo MON, Warszawa 1986; K. Nożko, *Zagadnienia współczesnej sztuki wojennej*, Wydawnictwo MON, Warszawa 1973; A. Polak, *Sztuka wojenna: kontekst teoretyczny i praktyczny*, „Zeszyty Naukowe AON" 2013, nr 3 (92); S.D. Sagan, *The Face of Battle without the Rules of War: Lessons from Red Horse & the Battle of the Little Bighorn*, „Daedalus" 2017, no. 146 (1); F. Skibiński, *Rozważania o sztuce wojennej*, AON, Warszawa 1991; *Współczesna wiedza wojskowa*, C. Czarnogórski (red.), Wydawnictwo MON, Warszawa 1972; L. Wyszczelski, *Historia myśli wojskowej*,

Bellona, Warszawa 2000; P. Zera, *Carl von Clausewitz*. *Filozofia wojny i nowoczesna strategia*, Histmag.org (dostęp 20.10.2020).

BITWA POWIETRZNO-MORSKA (AirSea Battle, ASB) – doktryna (koncepcja) operacyjna sił zbrojnych USA opracowana przez wpływowy amerykański think tank Center for Strategic and Budgetary Assessments (CSBA). W 2010 r. ośrodek ten opublikował 2 raporty: *Why Air-Sea Battle* oraz *Air-Sea Battle: A Point of Departure Operational Concept*. W 2012 r. ukazał się zaś dokument Pentagonu *Joint Operational Access Concept* (JOAC), w którym przedstawione zostały założenia systemu A2/AD (→ a n t y d o s t ę p o w e z d o l n o ś c i) i koncepcja → b i t w y powietrzno-morskiej. Obserwując rosnące zdolności Chin w izolowaniu pola walki na zachodnim Pacyfiku, pracownicy CSBA zaproponowali przyjęcie przez Departament Obrony USA nowej koncepcji operacyjnej, przygotowującej amerykańskie siły zbrojne do konfrontacji militarnej z Chińską Armią Ludowo-Wyzwoleńczą (PLA). Koncepcja ASB składa się z kilku charakterystycznych elementów.

- Pierwszy dotyczy obszaru prowadzenia → w o j n y [t. 4]. W przeciwieństwie do nizin Europy Środkowej, które miały stać się teatrem działań wojennych w czasie → z i m n e j w o j n y [t. 4] czy pustyń Kuwejtu i Iraku, na których realizowane były operacje Pustynna Burza w 1991 r. i Iracka Wolność w 2003 r., w przypadku ASB miejscem konfrontacji miałby być olbrzymi obszar zachodniego Pacyfiku. Stawia to przed armią amerykańską poważne wyzwania logistyczne związane ze strategicznym transportem wojsk w rejon konfliktu oraz ciągłym utrzymaniem dostaw zaopatrzenia. Ze względu na brak możliwości prowadzenia lądowej operacji militarnej na terenie Chińskiej Republiki Ludowej (ChRL) wojna ma się rozstrzygnąć na morzach i w powietrzu. Kluczowe znaczenie będą miały 2 łańcuchy wysp stanowiące oś strategiczną ekspansji chińskiej strefy wpływów. Pierwszy z nich biegnie od Wysp Japońskich przez wyspy Riukiu, Tajwan, Filipiny i Borneo. Drugi rozciąga się od Wysp Ogasawara (dawniej Wyspy Bonin) na południe, obejmując Mariany, Guam, Karoliny oraz zachodnią część Morza Filipińskiego. Koncepcja zakłada konieczność obrony amerykańskich sojuszników – głównie Japonii – oraz utrzymanie kontroli nad szlakami handlowymi, takimi jak cieśnina Malakka. Jak podkreśla J. Bartosiak w opracowaniach poświęconych ASB, dla amerykańskich planistów bardzo trudna będzie obrona Tajwanu i Korei Południowej, ze względu na chińską przewagę ilościową.
- Drugą cechą charakterystyczną ASB jest asymetria sił. Wojsko amerykańskie na zachodnim Pacyfiku rozlokowane jest w kilkunastu → b a z a c h w o j s k o w y c h. Są one położone na izolowanych wyspach, tym samym są bardzo trudne do obrony, a także znajdują się w zasięgu chińskiej broni rakietowej. Z drugiej strony chińska armia w 2012 r. posiadała w regionie 27 baz lotniczych, z których może razić cele na Tajwanie, a mobilne wyrzutnie pocisków balistycznych mogą

korzystać z głębi strategicznej Chin kontynentalnych, przez co stają się celami bardzo trudnymi do zniszczenia. Ponadto USA dysponują tylko kilkoma centrami logistycznymi w regionie, z czego największym jest baza wojskowa na wyspie Guam. Mając na uwadze powyższe, wybuch konfliktu zbrojnego między USA a ChRL będzie się wiązał z asymetrią sił na niekorzyść USA.

- Trzecim elementem ASB jest oparcie przez Chiny obrony własnej strefy wpływów na zdolnościach antydostępowych (A2/AD). Pekin rozwija własne zdolności antydostępowe od lat 80. XX w. W ich skład wchodzą balistyczne rakiety przeciwokrętowe, systemy obrony powietrznej i przeciwrakietowej, zdolności do prowadzenia → c y b e r w o j n y i operacji szpiegowskich w → c y b e r p r z e s t r z e n i, broń antysatelitarna, zdolności do prowadzenia wojny podwodnej czy nowe generacje samolotów załogowych oraz bezzałogowe statki powietrzne. Przykładami systemów obrony powietrznej i przeciwrakietowej są m.in.: HQ-7 o zasięgu 12 km, HQ-9 o zasięgu 100 km, HQ-15 o zasięgu 45 km, HQ-16 o zasięgu 40 km, HQ-17 o zasięgu 12 km czy HQ-18 o zasięgu 100 km. W 2002 r. Chiny posiadały 350 pocisków balistycznych krótkiego zasięgu wymierzonych w Tajwan, natomiast ich liczba w 2012 r. wzrosła do 1,1 tys. Dotychczasowy rozwój zdolności antydostępowych oraz perspektywa ich dalszego wzmacniania wskazują, że dzięki nim chińscy planiści zamierzają wygrać wojnę z USA.
- Czwartą cechą charakterystyczną ASB jest pozbawienie strony amerykańskiej tzw. sanktuariów, czyli miejsc, w których bazy wojskowe, porty morskie, lotniska i centra logistyczne znajdują się poza zasięgiem broni rakietowej, lotnictwa oraz → a r t y l e r i i przeciwnika. Od czasów II wojny światowej amerykańskie → w o j s k a l ą d o w e [t. 4], siły powietrzne oraz marynarka wojenna przyzwyczajone były do prowadzenia operacji wojskowych opartych na sanktuariach. Miejsca te spełniały funkcję punktów przeładunkowych, miejsc przegrupowania wojsk, w nich zlokalizowane były magazyny z amunicją i surowcami naturalnymi. Przykładami amerykańskich sanktuariów były do tej pory m.in. baza marynarki wojennej na wyspie Diego Garcia na Oceanie Indyjskim, baza marynarki wojennej na wyspie Guam, baza sił powietrznych Thule na Grenlandii czy baza sił powietrznych Lajes na Oceania Atlantyckim. W czasie bitwy powietrzno-morskiej między USA a ChRL Amerykanie stracą komfort posiadania bezpiecznych sanktuariów zarówno w domenie fizycznej, jak i wirtualnej. W domenie fizycznej bazy wojskowe w Korei Południowej, Japonii i na wyspie Guam znajdą się w promieniu rażenia pocisków balistycznych DF-11, DF-15, DF-21, DF-4, samolotów JH-7, H-6 czy pocisków przeciwokrętowych C-803. W domenie wirtualnej zniszczone mogą zostać amerykańskie satelity rozpoznawcze i komunikacyjne, co zakłóci tym samym funkcjonowanie systemów C2 (ang. *command and control*), ISR (ang. *intelligence, surveillance and reconnaissance*) oraz możliwości użycia broni precyzyjnej (ang. *precision-guided munition*, PGM).

Zdaniem autorów wspomnianych wcześniej dokumentów jednym z pierwszych posunięć strony chińskiej w czasie konfrontacji będzie użycie broni antysatelitarnej i cybernetycznej. W razie użycia broni cybernetycznej celem ataku będą amerykańskie systemy C2, radary znajdujące się na zachodnim Pacyfiku, jak również wszystkie naziemne i powietrzne obiekty tworzące obraz świadomości sytuacyjnej. Drugą formą ataku będą rakiety mające na celu zniszczenie sanktuariów. Szczególnym → z a g r o ż e n i e m [t. 4] dla strony amerykańskiej jest rakieta balistyczna DF-21D, nazywana „zabójcą lotniskowców". DF-21D znacząco zmienia potencjał militarny obu stron w tym obszarze geograficznym, ponieważ naraża na zniszczenie lotniskowe już w pierwszej fazie konfliktu. Zmasowany atak na amerykańskie bazy wojskowe, bazy wojskowe ich sojuszników oraz → o k r ę t y w o j e n n e [t. 3] będzie miał na celu doprowadzenie do „wypchnięcia" operacyjnego sił zbrojnych USA z regionu, a następnie zablokowanie podejść do teatru wojennego. Doprowadzi to do utraty inicjatywy strategicznej i operacyjnej przez USA. Chiński atak rakietowy ma również doprowadzić do maksymalnych strat osobowych i sprzętowych w siłach zbrojnych USA na zachodnim Pacyfiku, stawiając tym samym amerykańską → o p i n i ę p u b l i c z n ą [t. 3] i administrację rządową przed trudnym wyborem między kontynuowaniem wojny, wiążącym się z kolejnymi ofiarami i rosnącymi kosztami, a zaakceptowaniem porażki i zmianą globalnego układu sił. Atutem USA jest z kolei dominacja pod względem liczby okrętów podwodnych. Poza tym, jak podkreślają autorzy koncepcji, wojska USA w pierwszych dniach bitwy powietrzno-morskiej skupią się na „oślepieniu" dowództw chińskiej armii w ramach „nowoczesnej bitwy zwiadowczej", niszczą satelity oraz radary przeciwnika. Następnie po zwycięskim starciu lotniczym nad Japonią przejdą do eliminacji potencjału chińskiej floty, aby ostatecznie przystąpić do → b l o k a d y m o r s k i e j Państwa Środka.

Koncepcja bitwy powietrzno-morskiej ma zarówno licznych zwolenników, jak i przeciwników. Zwolennicy podkreślają, że jest „drogowskazem" opisującym, jak pokonać nie tylko PLA, ale także doprowadzić do upadku Komunistycznej Partii Chin. Elita polityczna Pekinu z kolei, zdając sobie sprawę z możliwych konsekwencji konfliktu z USA, unika agresywnej polityki w obszarze zachodniego Pacyfiku. Przeciwnicy – tacy jak wykładowca National Defense University i były płk Piechoty Morskiej USA T.X. Hammes – ostrzegają, że koncepcja może doprowadzić do eskalacji wojny z Chinami, w skrajnym wypadku zakończonej wymianą ciosów atomowych. Ponadto jej treść może nie sprawdzić się w praktyce. Zniszczenie amerykańskich satelitów oraz → c y b e r a t a k i na systemy komunikacji wojskowej doprowadzą do przejęcia inicjatywy przez PLA, a ciężko będzie ją odzyskać na kolejnych etapach wojny. Polowanie na mobilne chińskie wyrzutnie rakiet balistycznych również może zakończyć się niepowodzeniem, podobnie jak zakończyło się niepowodzeniem polowanie na irackie wyrzutnie typu SCUD w czasie operacji Pustynna Burza. Alternatywą dla ASB ma być koncepcja „kontroli na morzu" (ang. *offshore control*) oraz „blokowania na odległość"

(ang. *distant blockading*). Zmniejsza ona ryzyko eskalacji konfliktu poprzez rezygnację z uderzeń na cele położone w kontynentalnych Chinach. Rezygnuje również z prowadzenia walki w domenach szczególnie wrażliwych, czyli cyberprzestrzeni i przestrzeni kosmicznej. Państwo Środka ma zostać pokonane w blokadzie morskiej za pomocą niewielkich oddziałów piechoty morskiej dysponujących możliwością ataków przy użyciu broni precyzyjnej.

Niezależnie od sporów toczonych między zwolennikami a przeciwnikami ASB, od 2014 r. w amerykańskich środowiskach wojskowych zauważalny jest spadek zainteresowania jej założeniami. Miejsce koncepcji bitwy powietrzno-morskiej zajęła w 2015 r. koncepcja → b i t w y w ie lo o bsza r o w ej (*multi-domain battle*, MDB) oraz tzw. trzecia strategia offsetowa. Pierwsza z nich opisuje możliwość prowadzenia operacji wojskowych we wszystkich 5 domenach (lądowej, powietrznej, morskiej, kosmicznej i cyberprzestrzeni) przez samodzielne oddziały i pododdziały sił zbrojnych USA z dala od kontynentalnego terytorium USA. Druga opisuje długofalowy plan modernizacji technicznej amerykańskiej armii polegający na zwiększeniu przewag technologicznych w obszarze wojskowości oraz przygotowanie USA do wojny z symetrycznym przeciwnikiem, takim jak Rosja i Chiny.

Tomasz Wójtowicz

J. Bartosiak, *Koncepcja operacyjna wojny powietrzno-morskiej na zachodnim Pacyfiku*, Fundacja Republikańska, Warszawa 2012; tenże, *Pacyfik i Euroazja. O wojnie*, Wydawnictwo Jacek Bartosiak, Warszawa 2016; tenże, *Ucieczka do przodu. Przyszłość modernizacji technicznej Sił Zbrojnych Stanów Zjednoczonych*, JacekBartosiak.pl (dostep 12.12.2019); A.F. Krepinevich, *Why Air-Sea Battle?*, Center for Strategic and Budgetary Assessments, Washington 2010; S.-F. Ou, *China's A2AD and Its Geographic Perspective*, „Asia-Pacific Research Forum" 2014; G. Raymond, *What's displacing Air Sea Battle in US military planning?*, 1.10.2015, EastAsiaForum.org (dostęp 12.12.2019); E. Slavin, *Analysts: Air-Sea Battle Concept carriers risks in possible conflict with China*, 28.09.2014, Stripes. com (dostęp 12.12.2019); J. van Tol, M. Gunzinger, A. Krepinevich, J. Thomas, *AirSea Battle. A Point-of-Departure Operational Concept*, Center for Strategic and Budgetary Assessments, Washington 2010; T. Wójtowicz, *Doktryny operacyjne*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018.

BITWA WIELOOBSZAROWA (*multi-domain battle*, MDB) – doktryna (koncepcja) operacyjna sił zbrojnych USA opracowana przez U.S. Army Training and Doctrine Command (TRADOC) w 2017 r., opisująca przebieg możliwej konfrontacji militarnej poza granicami USA z przeciwnikiem dysponującym zdolnościami antydostępowymi (→ a n t y d o s t ę p o w e z d o l n o ś c i) (A2/D2) oraz rolę i znaczenie poszczególnych rodzajów sił zbrojnych w tym starciu. Bitwa wieloobszarowa jest określana również jako połączona doktryna (ang. *joint doctrine*) lub jako koncepcja przedstawiająca zbiór czynników operacyjnych (czas i przestrzeń prowadzenia operacji, środowisko działań wojska, siła, cel, koncentracja sił, swoboda działania) w obliczu potencjalnego

konfliktu militarnego z Chińską Republiką Ludową lub Federacją Rosyjską. Koncepcja bitwy wieloobszarowej została opisana w kilku dokumentach sił zbrojnych USA: *Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025–2040* wydanym przez TRADOC w 2017 r., w podręczniku polowym *FM 3-0 Operations* z tego samego roku czy w białej księdze TRADOC *Multi-Domain Battle: Combined Arms for the 21st Century*.

Początki koncepcji pojawiły się w 2015 r., kiedy podsekretarz obrony USA B. Work wygłosił na U.S. Army War College krytyczne przemówienie dotyczące przygotowań sił zbrojnych USA do współczesnych i przyszłych → z a g r o ż e ń m i l i t a r n y c h [t. 4]. Jego zdaniem potencjalni przeciwnicy USA będą posiadali zdolności wojskowe do zakwestionowania dominacji USA w wielu domenach (obszarach). Odpowiedzią na te obserwacje powinno być przygotowanie wojska do konfrontacji z przeciwnikiem dysponującym amunicją precyzyjną, systemami świadomości pola walki i inną zaawansowaną technologią. Powinno nią być również opracowanie koncepcji przypominającej AirLand Battle z lat 80. XX w. Na konieczność i przyczyny opracowania koncepcji MDB zwrócił uwagę także gen. D. Perkins – były dowódca TRADOC. Jego zdaniem wynikają one z kilku powodów.

- Po pierwsze w czasie → z i m n e j w o j n y [t. 4] USA przygotowywały swoje siły zbrojne do konfrontacji z przeciwnikiem, jakim była armia ZSRR. Obecnie USA muszą być przygotowane do prowadzenia operacji militarnych z przeciwnikiem dysponującym wojskami konwencjonalnymi, ale także z ugrupowaniami terrorystycznymi czy państwami upadłymi.
- Po drugie w latach 90. XX w. dominacja wojskowa USA na świecie była niepodważalna w każdym z obszarów (domen) – na lądzie, w powietrzu, na wodach, w przestrzeni kosmicznej i → c y b e r p r z e s t r z e n i. Obecnie – mając na uwadze możliwości prowadzenia przez Chiny operacji wojskowych na obszarze zachodniego Pacyfiku oraz zaangażowanie Rosji w konflikt zbrojny w Ukrainie i w Syrii – należy spodziewać się, że w przyszłych → w o j n a c h [t. 4] dominacja amerykańska może być podważona we wszystkich obszarach (domenach).
- Po trzecie zaangażowanie polityczne i wojskowe USA na świecie wymusza utrzymanie sił zbrojnych w różnych miejscach, często oddalonych od siebie. W przypadku konfrontacji militarnej może dojść do sytuacji, w której oddziały amerykańskie będą walczyły w osamotnieniu, bez wsparcia, z odciętymi liniami zaopatrzenia. Powoduje to konieczność przygotowania sił zbrojnych do prowadzenia operacji militarnych w warunkach dużej samodzielności, wystarczalności oraz warunkuje potrzebę umiejętności współdziałania przez poszczególne oddziały we wszystkich domenach (obszarach). Koncepcja MDB zakłada w związku z tym powstanie nowych oddziałów określonych jako I2CEWS (Intelligence, Information, Cyber, Electronic Warfare & Space; → w y w i a d [t. 4], → w a l k a i n f o r m a c y j n a [t. 4], walka w cyberprzestrzeni, → w a l k a e l e k t r o n i c z n a [t. 4],

działania w przestrzeni kosmicznej), mających zdolności do prowadzenia operacji w kilku domenach (obszarach) jednocześnie.

Czynnikiem wprowadzającym zmiany w charakterze konfliktów zbrojnych są uwarunkowania związane z poszczególnymi obszarami (domenami), a także samo określenie i wyszczególnienie przestrzeni bitewnych. Do tradycyjnych obszarów prowadzenia działań zbrojnych – lądu, obszarów wodnych i powietrza – doszły 2 „nowe" domeny – przestrzeń kosmiczna i cyberprzestrzeń. Sama domena definiowana jest jako „obszar wyszczególniony ze względu na określone cechy fizyczne bądź wirtualne". Szczególną uwagę poświęcono nowym domenom. Przestrzeń kosmiczna charakteryzowana jest jako mająca unikalny zestaw uwarunkowań fizycznych, powodujący, że operowanie w niej jest w największym stopniu uzależnione od wytworów techniki, cechuje się przy tym stosunkowo małą elastycznością (np. poruszanie się po określanych trajektoriach orbitalnych).

Co więcej, w ramach bitwy wielodomenowej przestrzeń kosmiczna traci status sanktuarium, gdzie obecne były tylko systemy wsparcia operacji militarnych prowadzonych w pozostałych obszarach, i staje się kolejną przestrzenią bitewną w pełnym tego słowa znaczeniu. Zakłada się możliwość prowadzenia działań ofensywnych i defensywnych w przestrzeni kosmicznej, w tym działań związanych z fizycznym niszczeniem aktywów przeciwnika. Z kolei cyberprzestrzeń jest domeną wyłącznie wirtualną, w całości będącą wytworem człowieka. Infrastruktura fizyczna służy tu jako system „ścieżek" pozwalających na przepływ → i n f o r m a c j i [t. 2]. Informacja, która zgodnie z założeniami → i n f o r m a c y j n e j r e w o l u c j i w s p r a w a c h w o j s k o w y c h [t. 2] miała zwiększyć świadomość sytuacyjną i rozwiać „mgłę wojny", dotychczas zawsze towarzyszącą działaniom zbrojnym, przyczyniła się paradoksalnie do pojawienia się nowego wyzwania, określanego jako „cyfrowa mgła wojny". Wymusza ona przygotowanie do działania w warunkach informacji niepełnej, sprzecznej lub fałszywej, po części właśnie z powodu operacji prowadzonych przez przeciwnika w cyberprzestrzeni. Szczególna uwaga zwrócona na „nowe" domeny wynika z 2 uwarunkowań – po pierwsze system militarny USA jest w największym stopniu uzależniony od przestrzeni kosmicznej oraz cyberprzestrzeni, także ze względu na dotychczasową niekwestionowaną dominację technologiczną USA w tych obszarach, po drugie zaś dominacja militarna USA może być właśnie w tych domenach najłatwiej zakwestionowana.

Za koncepcją domen bitewnych kryje się też założenie, że najlepszym sposobem na skuteczne porażenie jednostek przeciwnika jest zaatakowanie ich z obszaru innej domeny (np. atak lotniczy na jednostki lądowe). W ramach „rzeczywistości multidomenowej" prawda ta jest nadal aktualna, lecz skala wyzwań znacznie się zwiększyła, gdyż → z a g r o ż e n i e m [t. 4] stał się symultaniczny atak z wykorzystaniem kilku odmiennych domen, np. atak z wykorzystaniem pocisków rakietowych (balistycznych lub manewrujących) połączony z atakiem hakerskim oraz zakłóceniem łączności i nawigacji satelitarnej. Odpowiedzią ma być pełna integracja „nowych" domen w proces

planowania i prowadzenia operacji militarnych. Siły zbrojne USA prowadzą bowiem działania militarne w przestrzeni kosmicznej i cyberprzestrzeni od kilkudziesięciu lat, lecz skala ich zintegrowania z działaniami w pozostałych domenach zgodnie z koncepcją „połączoności" czy „spoistości" (ang. *jointness*) okazuje się niewystarczająca.

Pewne elementy koncepcji bitwy wieloobszarowej pojawiły się we wcześniejszych amerykańskich doktrynach operacyjnych. Opublikowana w 2012 r. *Capstone Concept for Joint Operations* wprowadziła ideę synergii międzydomenowej, rozumianej jako sumowane możliwości w ramach rozmaitych domen, co prowadzić ma do wzajemnego wzmocnienia efektywności i kompensacji słabości. *Army Operation Concept* z 2014 r. postrzegała rolę U.S. Army (Wojsk Lądowych USA) jako wkład w realizację operacji połączonych, prowadzonych w różnych domenach i z rozmaitymi partnerami, w nieznanym, niepewnym i nieustannie zmieniającym się środowisku. *U.S. Marine Corps Operation Concept* z 2016 r. zwracała z kolei uwagę na działania Korpusu Piechoty Morskiej w środowisku, gdzie przeciwnik próbuje osiągnąć cele militarne bez przekraczania progu otwartego konfliktu, z wykorzystaniem różnorodnych mechanizmów wywierania presji w ramach poszczególnych domen.

Zgodnie z założeniami koncepcji oddziały amerykańskie biorące udział w operacjach militarnych mają być podzielone na Wieloobszarowe Grupy Zadaniowe (Multi-Domain Task Force), a ich liczebność ma być zmniejszona z 4 tys. do 1,5 tys. → ż o ł n i e r z y [t. 4]. Ma to wpłynąć na ich większą mobilność oraz ograniczyć straty w przypadku ataku rakietowego przeciwnika. Obszar, na którym prowadzona będzie operacja, zostanie podzielony na kilka stref: obszar głębokiego pola walki, obszar głębokiego manewru, bliski obszar oraz obszar wsparcia. Głębokie pole walki oznacza miejsce znajdujące się poza możliwością ruchu → w o j s k l ą d o w y c h [t. 4] (zmechanizowanych/pancernych). Może nim być terytorium państwa sojusznika lub agresora. Aktywne będą w jego granicach oddziały zajmujące się prowadzeniem operacji specjalnych, walki w cyberprzestrzeni oraz walki elektronicznej. Ograniczenie dotyczące wykorzystania ciężkiego sprzętu wojsk lądowych może wynikać z zapisów prawa humanitarnego, uwarunkowań politycznych lub umów dwustronnych. Obszar głębokiego manewru jest miejscem kluczowym ze względu na rozstrzygnięcie konfliktu. W jego granicach ma dojść do decydującego starcia z przeciwnikiem. Użyty zostanie ciężki sprzęt wojsk lądowych, a dowódcy będą mieli możliwość projekcji siły w większym zakresie niż w obszarze głębokiego pola walki. W obszarze bliskim będą toczyć się bezpośrednie działania wojenne. Celem wojsk będzie utrzymanie danego terytorium, odzyskanie utraconego lub przygotowanie miejsca do przeprowadzenia głębokiego manewru. Obszar wsparcia jest natomiast przestrzenią stanowiącą zaplecze pola walki. Znajdą się na nim linie komunikacyjne, → b a z y w o j s k o w e, lotniska i bazy dowodzenia. Wojska amerykańskie będą miały w tym miejscu największą swobodę działania. Zagrożeniem okażą się jednak siły specjalne przeciwnika, → c y b e r a t a k i, efekty prowadzonej → w o j n y i n f o r m a c y j n e j [t. 4]

oraz lokalni sympatycy wroga. Scenariusze przedstawiające obraz możliwego konfliktu zakładają, że zaangażowanie USA będzie wynikało z potrzeby wsparcia sojusznika. Atak na przeciwnika rozpocznie się od operacji w cyberprzestrzeni, na cele takie jak systemy dowodzenia i inne elementy → i n f r a s t r u k t u r y k r y t y c z n e j [t. 2]. Dalej nastąpi atak rakietowy wymierzony w systemy obrony przeciwlotniczej, bazy lotnicze i wyrzutnie typu ziemia–ziemia. Efektem operacji przeprowadzonych w cyberprzestrzeni oraz ataku rakietowego powinno być przełamanie zdolności A2/AD. Po nim nastąpi atak wojsk powietrzno-desantowych i piechoty morskiej, które przeprowadzą głęboki manewr za linią frontu, przecinając tym samym linie komunikacyjne przeciwnika. Ostatnim etapem konfliktu będzie ofensywa wojsk lądowych (zmechanizowanych i pancernych), które wyeliminują pozostałe jednostki wroga zlokalizowane na obszarze państwa sojusznika.

Koncepcja bitwy wieloobszarowej wyróżnia 3 kluczowe komponenty.

Pierwszym z nich jest tzw. *force posture* (z ang. stan sił). W jego ramach zwraca się szczególną uwagę na siły ekspedycyjne oraz na wysuniętą obecność. Stanowią one punkt oparcia w newralgicznych z geostrategicznego punktu widzenia regionach (→ g e o s t r a t e g i a [t. 2]), są wsparciem dla sojuszników i partnerów, tworzą wyłom w „bastionach antydostępowych" przeciwników. Drugi komponent to *resilient formations* (z ang. odporne ugrupowania, dosł. elastyczne formacje), zdolne do funkcjonowania w obliczu przeciwdziałania ze strony zaawansowanego technologicznie przeciwnika. Jednostki mają mieć możliwość prowadzenia walki w sposób częściowo niezależny, także w sytuacji przerwania linii zaopatrzeniowych oraz naruszenia elementów systemu dowodzenia i kontroli. Grupy bojowe mają być mniejsze i bardziej rozproszone, a przez to bardziej manewrowe i lepiej predestynowane do stosowania różnorodnych, obejmujących wszystkie domeny, technik maskowania. Trzecim komponentem jest konwergencja (ang. *convergence*) określana jako zdolność do integrowania możliwości w poprzek obszarów, środowisk i funkcji w czasie i przestrzeni, z myślą o osiągnięciu określonego celu. Konwergencja ma sięgać głębiej niż znane dotychczas działania połączone, gdyż ma łączyć organizacje o odmiennym charakterze (w ramach tzw. *interorganizational capabilities*, zdolności międzyorganizacyjnych), uwzględniając nie tylko elementy sił zbrojnych, własnych i sojuszniczych, ale także inne agendy rządu federalnego, organizacje międzynarodowe i pozarządowe, firmy sektora prywatnego, a także organizacje lokalne i plemienne, w zależności od uwarunkowań geostrategicznych. Celem konwergencji jest kreowanie fizycznych, wirtualnych i kognitywnych „okien możliwości" (ang. *window of opportunity*), które będą wykorzystywane przez Multi-Domain Task Force do osiągnięcia przewagi.

Działania podejmowane w ramach koncepcji bitwy wieloobszarowej mają być użyteczne nie tylko w fazie konfliktu, ale także w tzw. fazie zero, czyli w okresie definiowanym przez Narodową Strategię Bezpieczeństwa USA z 2018 r. jako rywalizacja (ang. *competition*). Obejmuje ona szarą strefę pomiędzy pokojem a wojną,

z założeniem, że dla wielu potencjalnych przeciwników USA (w tym dla Rosji, Chin, Korei Północnej czy Iranu) pokój jest kontynuacją wojny przy użyciu innych środków, co stanowi swoiste odwrócenie głośnej definicji C. von Clausewitza. Państwa te, reprezentując odmienną od zachodniej tradycję prowadzenia wojny, chętnie odwołują się do takich metod, jak działania hybrydowe, ataki hakerskie, → c y b e r s z p i e g o s t w o , zakłócenia łączności i nawigacji satelitarnej czy → d e z i n f o r m a c j a [t. 2] z wykorzystaniem → m e d i ó w s p o ł e c z n o ś c i o w y c h [t. 3]. W ramach fazy przygotowawczej jednostki Multi-Domain Task Force powinny podejmować zarówno działania takie jak aktywne testowanie systemów radioelektronicznych przeciwnika przez prowokowanie ich z wykorzystaniem własnych emisji, jak i manewry jednostek w przestrzeni fizycznej, zakłócenia systemów przeciwnika, defensywne i ofensywne działania w cyberprzestrzeni, w tym włamywanie się do nieprzyjacielskich baz danych.

Rozwiązania zaproponowane w koncepcji bitwy wieloobszarowej porównywane są do rozwiązań zastosowanych w czasie I wojny światowej przez państwa Ententy, rozwiązań zastosowanych przez wojska amerykańskie w czasie bitwy o Guadalcanal oraz wojny o Falklandy w 1982 r. W obliczu trudności w przełamaniu niemieckich linii obronnych państwa Ententy powołały do życia nowe oddziały na poziomie korpusu określane jako Counter-Battery Office, których zadaniem było prowadzenie płytkiego wywiadu, rozpoznania osobowego oraz lotniczego celem wykrycia niemieckich baterii i wyeliminowania ich ogniem → a r t y l e r i i w pierwszym etapie bitwy. Wprowadzone zostały również do użycia czołgi, torujące drogę natarcia oddziałom piechoty, jak i ochraniające je przez ogniem broni maszynowej przeciwnika. Rozwój zdolności prowadzenia wojny pozycyjnej można w tym przypadku porównać do współczesnych zdolności antydostępowych, natomiast powstanie oddziałów Counter-Battery Office do I2CEWS. W czasie bitwy o Guadalcanal strona amerykańska w pierwszym etapie operacji zdecydowała się na zajęcie japońskiego lotniska przez oddziały piechoty morskiej, a następnie do rozbudowy zdolności antydostępowych mających na celu odparcie ataku przeciwnika. Utrzymanie lotniska i odparcie japońskich natarć pozwoliło następnie Amerykanom na oczyszczenie wyspy z resztek oddziałów wroga. W przypadku wojny o Falklandy marynarka brytyjska w pierwszej kolejności odizolowała Falklandy, wykorzystując w tym celu broń przeciwlotniczą, okręty nawodne i podwodne. Dzięki skutecznemu zastosowaniu zdolności antydostępowych doszło do zatopienia argentyńskiego → o k r ę t u w o j e n n e g o [t. 3] oraz udanego rajdu brytyjskich komandosów na bazę sił powietrznych.

Koncepcja bitwy wieloobszarowej ma zarówno przeciwników, jak i zwolenników. Do zwolenników zaliczają się przede wszystkim jej twórcy oraz środowisko wojskowych związanych z TRADOC. Przeciwnicy – tacy jak emerytowany płk D. Johnson, płk M. Pietrucha, kpt. A.J. Shattuck, J. Bott, J. Gallagher, J. Huber i J. Powers – wskazują szereg jej mankamentów. Jednym z nich jest przypisywanie koncepcji

rewolucyjnego charakteru. Zdaniem części specjalistów nie wprowadza ona rozwiązań, które nie byłyby znane w historii wojskowości. Przykładem są Ateńczycy, którzy już w starożytności używali → m a r y n a r k i w o j e n n e j [t. 3] w taki sposób, aby uzyskać przewagę na lądzie. Ponadto autorzy MDB pominęli problem reformy instytucjonalnej sił zbrojnych USA. Zwraca się także uwagę na przypisywanie zbyt dużej roli Wojskom Lądowym USA, które miałyby penetrować obszary A2/AD nieprzyjaciela. Tymczasem U.S. Army nie ma wystarczających możliwości w tym zakresie, a bez odpowiedniego wsparcia innych rodzajów sił zbrojnych, przede wszystkim sił powietrznych, ich zdolność do przetrwania i realizowania zadań stoi pod znakiem zapytania (m.in. kwestionuje się odporność Multi-Domain Task Force na przeciwdziałanie przeciwnika bez zapewnienia → p a n o w a n i a w p o w i e t r z u [t. 3]).

Od 2018 r. w siłach zbrojnych USA obserwuje się ewolucję koncepcji bitwy wieloobszarowej w kierunku koncepcji operacji wieloobszarowych (ang. *multi-domain operations*). W 2018 r. ukazał się dokument TRADOC *The U.S. Army in Multi-Domain Operations 2028*. Jak podkreślił gen. E. Wesley, dyrektor Army Capabilities Integration Center, koncepcja operacji wieloobszarowej jest rozbudowaną wersją MDB. Po pierwsze zawiera ona znacznie więcej szczegółów opisujących to, jak prowadzić operacje w wielu domenach. Po drugie MDB należy traktować jako „hipotezę" przedstawiającą przyszłe teatry działań wojennych i wyzwania stojące przed siłami zbrojnymi USA. Koncepcją operacyjną stała się MDO, oparta na danych, eksperymentach, ćwiczeniach i analizach. Jednymi z pierwszych ćwiczeń, które stały się podstawą do dalszych prac nad MDO, były Joint Warfighting Assessment 18, które odbyły się wiosną 2018 r. w Grafenwöhr i Hohenfels w Niemczech. Wzięło w nich udział 6,8 tys. żołnierzy z 10 państw. Kolejnymi ćwiczeniami były manewry Joint Warfighting Assessment 19 przeprowadzone na Pacyfiku. Joint Warfighting Assessment 20 ponownie zaplanowano w Europie.

Rafał Kopeć, Tomasz Wójtowicz

Field Manual 3-0: Operations, Headquarters Department of the Army, Washington, DC, 6 December 2017; J. Judson, *From Multi-Domain Battle to Multi-Domain Operations: Army Evolves its Guiding Concept*, 9.10.2018, DefenseNews.com (dostęp 20.12.2019); R. Kopeć, T. Wójtowicz, *Bitwa wieloobszarowa*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; S. Marr, *Stability In Multi-Domain Battle*, U.S. Army Peacekeeping and Stability Operations Institute, United States Army War College, Carlisle 2018; *Multi-Domain Battle: Combined Arms for the 21st Century*, TRADOC, 24 February 2017; *Multi-Domain Battle: Evolution of Combined Arms for the 21st Century. 2025–2040*, TRADOC 2017; D. Perkins, *Multi-Domain Battle: Driving Change to Win in the Future*, „Military Review", July–August 2017; *The U.S. Army in Multi-Domain Operations 2028*, TRADOC 2018; K.M. Woods, T.C. Greenwood, *Multidomain Battle: Time for a Campaign of Joint Experimentation*, „Joint Force Quarterly" 2018, no. 88; T. Wójtowicz, D. Król, *Multi-Domain Battle: New Doctrine of the United States Armed Forces*, „Zeszyty Naukowe Akademii Sztuki Wojennej" 2018, nr 3 (112).

BIURO BEZPIECZEŃSTWA NARODOWEGO RP (BBN) – urząd państwowy utworzony na podstawie art. 11 Ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej z 21 listopada 1967 r. Przy pomocy tego urzędu Prezydent RP realizuje zadania w zakresie → b e z p i e c z e ń s t w a .

Do zakresu zadań BBN należy:

- realizacja zadań powierzonych przez Prezydenta RP w obszarze bezpieczeństwa i obronności;
- inicjowanie koncepcji i planów struktur organizacyjnych oraz funkcjonowania zintegrowanego systemu kierowania bezpieczeństwem państwa, udział w ich przygotowaniu i nadzór nad nim;
- monitorowanie, analiza i przygotowywanie ocen oraz wniosków dla Prezydenta RP w zakresie kształtowania się strategicznych warunków bezpieczeństwa państwa;
- opracowywanie i opiniowanie koncepcji, dyrektyw, planów i programów w zakresie bezpieczeństwa państwa w ramach kompetencji Prezydenta RP oraz nadzór nad ich realizacją;
- monitorowanie i analiza bieżącej działalności → S i ł Z b r o j n y c h R P [t. 4] w ramach zwierzchnictwa Prezydenta RP nad Siłami Zbrojnymi, w aspekcie oceny i opiniowania perspektywicznych programów ich rozwoju i użycia w ramach planów operacyjnych;
- współpraca z organami władzy publicznej i organizacjami społecznymi w zakresie problematyki bezpieczeństwa i obronności państwa;
- monitorowanie, ocena i opiniowanie bieżącej działalności organów władzy publicznej i innych struktur państwa w zakresie bezpieczeństwa pozamilitarnego (zob. → p o z a m i l i t a r n e p r z y g o t o w a n i e o b r o n n e p a ń s t w a [t. 3]), a w jego ramach → b e z p i e c z e ń s t w a p u b l i c z n e g o i społeczno-gospodarczego oraz przygotowywanie wniosków dla Prezydenta RP;
- opracowywanie i opiniowanie, z upoważnienia Prezydenta RP, projektów aktów prawnych i normatywnych w dziedzinie bezpieczeństwa państwa;
- organizacyjne i merytoryczne przygotowanie posiedzeń Rady Bezpieczeństwa Narodowego oraz pełnienie obowiązków sekretariatu tej Rady.

Działalnością BBN kieruje szef Biura w randze sekretarza stanu, przy pomocy swojego zastępcy. Strukturę organizacyjną BBN (na styczeń 2021 r.) stanowią: Gabinet Szefa Biura, Departament Analiz Strategicznych, Departament Zwierzchnictwa nad Siłami Zbrojnymi, Departament Prawa i Bezpieczeństwa Pozamilitarnego oraz Pion Pełnomocnika ds. ochrony → in f o r m a c j i n i e j a w n y c h [t. 2].

Do podstawowych zadań Departamentu Analiz Strategicznych należy:

- monitorowanie warunków → b e z p i e c z e ń s t w a m i ę d z y n a r o d o w e g o i narodowego RP w ujęciu strategicznym w aspekcie szans, wyzwań, ryzyka i → z a g r o ż e ń [t. 4] dla bezpieczeństwa Polski;

- przygotowywanie średnio i długoterminowych raportów dotyczących syntezy i prognoz w zakresie bezpieczeństwa międzynarodowego i narodowego RP;
- analiza i ocena → s t r a t e g i i [t. 4] sojuszników i ich praktyki operacyjnej pod kątem potrzeb państwa;
- inicjowanie i udział w Strategicznych Przeglądach Bezpieczeństwa Narodowego oraz pracach nad Strategią Bezpieczeństwa Narodowego;
- analiza i opiniowanie projektów dokumentów zatwierdzanych przez Prezydenta RP, takich jak Strategia Bezpieczeństwa Narodowego czy Polityczno-Strategiczna Dyrektywa Obronna RP;
- nadzorowanie realizacji zadań wynikających z dokumentów strategicznych wydawanych lub zatwierdzanych przez Prezydenta RP, wyciąganie wniosków i składanie propozycji w zakresie ich realizacji;
- współpraca z organami władzy publicznej w zakresie strategii i polityki → b e z p i e c z e ń s t w a n a r o d o w e g o;
- merytoryczne przygotowanie posiedzeń → R a d y B e z p i e c z e ń s t w a N a r o d o w e g o [t. 3];
- przygotowanie wizyt i spotkań szefa i zastępcy szefa BBN w kraju i za granicą;
- współpraca z krajowymi i zagranicznymi instytucjami analitycznymi i naukowo-badawczymi w zakresie bezpieczeństwa międzynarodowego i narodowego;
- monitorowanie problematyki bezpieczeństwa międzynarodowego i narodowego w mediach i wydawnictwach fachowych.

Strukturę Departamentu Analiz Strategicznych stanowią:

- Wydział Bezpieczeństwa Narodowego;
- Wydział Bezpieczeństwa Sojuszniczego;
- Wydział Współpracy Międzynarodowej.

Do zadań Departamentu Zwierzchnictwa nad Siłami Zbrojnymi należy:

- merytoryczne i organizacyjne przygotowanie warunków kadrowych, organizacyjno-technicznych i operacyjnych do sprawowania zwierzchnictwa Prezydenta RP nad Siłami Zbrojnymi;
- monitorowanie funkcjonowania Sił Zbrojnych oraz przygotowywanie raportów dla Prezydenta RP i szefa BBN;
- analiza i przygotowywanie wniosków oraz propozycji w zakresie transformacji Sił Zbrojnych;
- przygotowywanie opinii dotyczących głównych kierunków rozwoju Sił Zbrojnych RP w aspekcie przygotowań do obrony kraju;
- przygotowywanie opinii w zakresie:
  - mianowania szefa Sztabu Generalnego WP, Dowódcy Generalnego Rodzajów Sił Zbrojnych, szefa Inspektoratu Wsparcia Sił Zbrojnych, Dowódcy Operacyjnego Rodzajów Sił Zbrojnych oraz Naczelnego Dowódcy Sił Zbrojnych,
  - mianowania → ż o ł n i e r z y [t. 4] na pierwszy stopień oficerski,

  - mianowania na stopnie oficerskie generałów, admirałów,
  - nadawania orderów i odznaczeń żołnierzom i pracownikom wojska;
- opiniowanie wniosków dotyczących użycia Sił Zbrojnych na terytorium RP oraz poza jej granicami;
- monitorowanie, analiza i ocena udziału Sił Zbrojnych RP w operacjach międzynarodowych oraz współpracy obronnej z innymi państwami i organizacjami międzynarodowymi;
- współdziałanie z organami władzy publicznej oraz organizacjami społecznymi działającymi na rzecz obronności państwa i promocji patriotyzmu;
- organizowanie uroczystości państwowych i wojskowych oraz wizyt z udziałem Prezydenta RP, szefa Biura lub jego zastępcy w instytucjach, jednostkach organizacyjnych oraz jednostkach wojskowych w kraju i za granicą;
- merytoryczne przygotowywanie posiedzeń Rady Bezpieczeństwa Narodowego w zakresie zwierzchnictwa Prezydenta RP nad Siłami Zbrojnymi.

Strukturę Departamentu Zwierzchnictwa nad Siłami Zbrojnymi stanowią:

- Zespół Analiz Wojskowych;
- Zespół Zwierzchnictwa Operacyjnego;
- Zespół Zwierzchnictwa Organizacyjnego.

Do zadań Departamentu Prawa i Bezpieczeństwa Pozamilitarnego należy:

- przygotowywanie projektów aktów normatywnych i innych aktów prawnych w ramach wykonania inicjatyw legislacyjnych Prezydenta RP;
- merytoryczne przygotowywanie posiedzeń Rady Bezpieczeństwa Narodowego w zakresie bezpieczeństwa pozamilitarnego oraz w zakresie prawnym;
- reprezentowanie Biura w pracach legislacyjnych nad projektami aktów normatywnych i innych aktów prawnych;
- opiniowanie pod względem prawnym i uzgadnianie z pozostałymi komórkami organizacyjnymi Biura projektów aktów normatywnych i innych aktów prawnych dotyczących bezpieczeństwa narodowego;
- opracowywanie opinii prawnych;
- zapewnienie obsługi prawnej Biura;
- opiniowanie wniosków w zakresie mianowania na pierwszy stopień oficerski i na stopnie generalskie funkcjonariuszy służb;
- monitorowanie, analiza i ocena bezpieczeństwa i porządku publicznego oraz działalności służb specjalnych, głównie: → Agencji Wywiadu, →Agencji Bezpieczeństwa Wewnętrznego, → Centralnego Biura Antykorupcyjnego, → Służby Wywiadu Wojskowego [t. 4], → Służby Kontrwywiadu Wojskowego [t. 4], → Służby Ochrony Państwa [t. 4], Służby Więziennej, Straży Granicznej, → Państwowej Straży Pożarnej [t. 3], → Policji [t. 3];

- monitorowanie i pozyskiwanie informacji oraz ocena i analiza stanu bezpieczeństwa energetycznego państwa;
- monitorowanie i pozyskiwanie informacji w zakresie → bezpieczeństwa ekonomicznego państwa;
- monitorowanie i pozyskiwanie informacji oraz ocena i analiza bezpieczeństwa społecznego państwa pod względem demografii, migracji, rynku pracy, polityki prorodzinnej i edukacji;
- udział w przygotowywaniu koncepcji strategicznej oraz zadań struktur państwa w pozamilitarnych dziedzinach bezpieczeństwa narodowego, takich jak: bezpieczeństwo publiczne, zdrowotne, informacyjne, społeczne, ekonomiczne, gospodarcze;
- monitorowanie i bieżąca ocena funkcjonowania systemu kierowania bezpieczeństwem narodowym;
- udział w organizacji funkcjonowania zintegrowanego systemu kierowania bezpieczeństwem narodowym w czasie pokoju, → kryzysu [t. 2] i → wojny [t. 4];
- współdziałanie z Kancelarią Prezydenta RP, Ministerstwem Spraw Wewnętrznych i Ministerstwem Obrony Narodowej w przygotowywaniu stanowisk kierowania Prezydenta RP;
- opiniowanie planów krajowych ćwiczeń systemu obronnego państwa;
- organizacyjno-merytoryczne przygotowanie udziału Prezydenta RP i szefa Biura w ćwiczeniach → systemu bezpieczeństwa narodowego [t. 4], w tym → zarządzania kryzysowego [t. 4].

Strukturę Departamentu Prawa i Bezpieczeństwa Pozamilitarnego stanowią:

- Wydział Prawa Bezpieczeństwa Narodowego;
- Wydział Systemu Kierowania Bezpieczeństwem Narodowym;
- Wydział Bezpieczeństwa Pozamilitarnego.

Do najważniejszych zadań Gabinetu Szefa BBN należy:

- koordynowanie i organizowanie pracy szefa Biura, zastępcy szefa Biura oraz zespołów powoływanych przez szefa Biura;
- przygotowywanie krajowych i zagranicznych wizyt szefa i zastępcy szefa Biura oraz wizyt delegacji zagranicznych na zaproszenie szefa Biura;
- organizacyjna obsługa posiedzeń Rady Bezpieczeństwa Narodowego;
- organizowanie konferencji, narad i spotkań oraz ich obsługa techniczna;
- organizowanie kontaktów szefa Biura i zastępców szefa Biura z instytucjami krajowymi i zagranicznymi;
- obsługa logistyczna wyjazdów krajowych i zagranicznych pracowników Biura;
- współpraca z odpowiednimi jednostkami organów administracji publicznej w zakresie działania Biura;
- opracowywanie projektu budżetu Biura oraz nadzór nad jego realizacją;
- współpraca ze środkami masowego przekazu;
- organizowanie i prowadzenie działalności wydawniczej Biura;

- obsługa prawna w zakresie bieżącej działalności Biura, w szczególności w odniesieniu ds. pracowniczych, zamówień publicznych i finansów publicznych.

Marek Pietrzyk

Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Biuro Bezpieczeństwa Narodowego, Warszawa 2013; M. Pietrzyk, *Biuro Bezpieczeństwa Narodowego*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; Strategia rozwoju systemu bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2022, przyjęta uchwałą Rady Ministrów z dnia 9 kwietnia 2013 r.; Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej, Dz. U. 1967, nr 44, poz. 220; Zarządzenie nr 2 Prezydenta Rzeczypospolitej Polskiej z dnia 11 sierpnia 2010 r. w sprawie organizacji oraz zakresu działania Biura Bezpieczeństwa Narodowego; Zarządzenie nr 1 Prezydenta Rzeczypospolitej Polskiej z 30 stycznia 2012 r. zmieniające zarządzenie w sprawie organizacji oraz zakresu działania Biura Bezpieczeństwa Narodowego; R. Zięba, J. Zając, *Budowa zintegrowanego systemu bezpieczeństwa narodowego Polski. Ekspertyza*, Warszawa 2010.

BIURO INFORMACJI I PRASY NATO – jest komórką organizacyjną Sojuszu Północnoatlantyckiego odpowiedzialną za rozpowszechnianie → i n f o r m a c j i [t. 2] o działalności Sojuszu w mediach oraz organizację wsparcia informacyjnego dla rządów państw członkowskich NATO.

Strukturę Biura Informacji i Prasy tworzą:

- Służba Prasy i Mediów;
- Służba Informacyjna, podzielona na:
  - Sekcję Planowania i Produkcji;
  - Sekcję Stosunków z Państwami Członkowskimi;
  - Sekcję Kontaktów Zewnętrznych i Relacji z Państwami Partnerskimi;
- Służba Biblioteczna i Dokumentacyjna;
- Biblioteka Mediów;
- Sekcja Kolportażu.

Biuro prowadzi Centrum Informacji i Dokumentacji w Kijowie. Dyrektor ds. informacji i prasy jest przewodniczącym Komitetu Informacji i Kontaktów Kulturalnych. Rzecznik prasowy oraz Służba Prasy i Mediów wydają oficjalne oświadczenia w imieniu Sojuszu i sekretarza generalnego, a także przygotowują materiały i oświadczenia uzupełniające dla dziennikarzy. Służba Prasy i Mediów przygotowuje akredytacje dla dziennikarzy, wydaje pisemne komunikaty i przemówienia sekretarza generalnego, a także opracowuje codzienny przegląd prasy i serwis wycinków prasowych dla pracowników kwatery głównej w Brukseli.

Biuro prasy i mediów organizuje przekazywane przez media wywiady z sekretarzem generalnym i innymi osobistościami → N A T O [t. 3] oraz zapewnia wsparcie techniczne umożliwiające transmisje radiowe i telewizyjne.

Biuro Informacji i Prasy pomaga rządom państw członkowskich i partnerskich szerzyć rzetelną wiedzę o roli i polityce NATO poprzez realizację różnorodnych

programów i działań. Działalność ta odbywa się z wykorzystaniem periodycznych i nieperiodycznych publikacji, materiałów wideo, fotografii i wystaw, wizyt grupowych, konferencji, seminariów oraz stypendiów badawczych.

Biuro utrzymuje bliskie kontakty z władzami narodowymi odpowiedzialnymi za informowanie publiczne oraz organizacjami pozarządowymi, a także podejmuje działania zmierzające do wyjaśniania celów i osiągnięć Sojuszu → opinii publicznej [t. 3] w państwach członkowskich. Ponadto organizuje i sponsoruje liczne programy międzynarodowe z udziałem obywateli państw członkowskich.

W porozumieniu z państwami partnerskimi podejmuje także działania informacyjne zmierzające do upowszechniania wiedzy i zrozumienia działań Sojuszu w państwach reprezentowanych w Radzie Partnerstwa Euroatlantyckiego oraz Grupie Współpracy Śródziemnomorskiej.

Marek Pietrzyk

M. Filipiak, *Służby prasowo-informacyjne w wybranych armiach świata*, Biuro Prasy i Informacji MON, Warszawa 1996; NATO, *Vademecum NATO*, tłum. R. Brzeski, Bellona, Warszawa 1999; M. Pietrzyk, *Biuro Prasy i Informacji NATO*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; M. Rimanelli, *The A to Z of NATO and Other International Security Organizations*, Scarecrow Press, Toronto 2009.

BLOKADA MORSKA – jedna z metod walki morskiej, stara forma działań wojennych albo polityczno-ekonomiczna forma wojny, która często może mieć nieoczekiwane skutki polityczne.

W historii narody morskie wykorzystywały blokady morskie, aby zniszczyć gospodarkę przeciwników. Jednak wpływ blokady na historię został przeceniony. W całej historii blokada była częścią militarnego sukcesu, ale nigdy – głównym kluczem do zwycięstwa. Najbardziej udane blokady umożliwiły powodzenie kampanii lądowych, ale same nie wygrałyby wojen.

Według polskich badaczy M. Ilnickiego i A. Makowskiego:

> jest to kompleks stosowanych przez siły morskie strony wojującej środków przemocy, które uniemożliwiają przeciwnikowi korzystanie z portów własnych lub okupowanych, baz morskich, wybrzeża i przyległych wód morskich w celu prowadzenia żeglugi i innych kontaktów między państwami.

Autorzy publikacji *Międzynarodowe prawo humanitarne konfliktów zbrojnych* podkreślają:

> są to działania podjęte przez jedną z walczących stron, mające na celu powstrzymanie wszelkich statków morskich i powietrznych od dotarcia do portu, lądu, lądowiska znajdującego się na terytorium okupowanym.

Celem blokady jest uniemożliwienie transportu dóbr i ludzi z wrogiego terytorium lub na to terytorium.

Blokada wojenna nie jest metodą, która może być stosowana dowolnie. Pierwsze regulacje odnoszące się do tej kwestii można odnaleźć w deklaracji paryskiej z 1856 r., kolejne w deklaracji londyńskiej z 1909 r. Całościowe ujęcie zagadnienia blokady stało się przedmiotem wnikliwych badań zakończonych obradami ekspertów prawa międzynarodowego w Tulonie w 1990 r. W toku dyskusji określono szereg wymagań dotyczących blokady, mianowicie:

- efektywność – blokada, która nie jest efektywna, a zwłaszcza tzw. blokada papierowa (tylko zadeklarowana, a nie faktycznie sprawowana), nie może być uznana za legalną;
- bezstronność – blokada powinna być stosowana do statków wszystkich państw;
- notyfikacja ustanowienia wszystkim państwom faktu wprowadzenia blokady;
- notyfikacja wszelkich zmian dotyczących blokady;
- wymóg, aby blokada dotyczyła jedynie wybrzeża należącego do wroga lub terytorium okupowanego;
- zakaz ustanawiania blokady, jeżeli jej celem jest pozbawienie → l u d n o ś c i c y w i l n e j [t. 3] dóbr niezbędnych do przeżycia lub jeżeli szkody poniesione przez ludność cywilną będą wyższe niż spodziewana korzyść wojskowa.

Nie można również zapomnieć o określeniu skutków naruszenia blokady. Statki powietrzne lub morskie naruszające blokadę w sytuacji, gdy nie poddają się zatrzymaniu, po ostrzeżeniu mogą być zatrzymane lub zaatakowane.

Blokada może mieć negatywne konsekwencje dla ludności znajdującej się na odciętym obszarze. Głodzenie ludności jako metoda walki jest zabroniona I protokołem dodatkowym. W konsekwencji przy realizowaniu blokady działania mające na celu niesienie pomocy ludności muszą być dozwolone. Działania takie mogą być nadzorowane bądź przez mocarstwa tzw. opiekuńcze, bądź przez bezstronną organizację, taką jak np. Międzynarodowy Komitet Czerwonego Krzyża.

Blokada może być również rozpatrywana w świetle działań ONZ. Na podstawie rozdziału VII Karty Narodów Zjednoczonych może być zastosowane embargo, którego częścią jest ustanowienie blokady. ONZ nie ma własnych sił zbrojnych mogących efektywnie wykonywać blokadę, należy więc przyjąć, że powyższe zasady będą wiążące w stosunku do państw, które blokadę taką realizują.

Piotr Łubiński

M. Ilnicki, A. Makowski, *Blokada morska – jej istota i aspekty prawnomiędzynarodowe*, „Wojskowy Przegląd Prawniczy" 1992, nr 1/2; ciż, *Wojna na morzu we współczesnym prawie międzynarodowym*, Wydawnictwo Adam Marszałek, Warszawa–Toruń 1996; M. Ilnicki, A. Makowski, S. Pejas, *Wojna minowa na morzu*, Wydawnictwo Adam Marszałek, Toruń 1998; A. Makowski, *Siły morskie współczesnego państwa*, Gdynia 2000; *Międzynarodowe prawo humanitarne konfliktów zbrojnych*, Z. Falkowski, M. Marcinko (red.), Wojskowe Centrum Edukacji Obywatelskiej, Warszawa 2014; *Podstawy działań taktycznych*, L. Elak (red.), AON, Warszawa 2014; D. Szkołuda, *Doświadczenia z operacji ekspedycyjnych w aspekcie przyszłych działań taktycznych*, [w:] *Teoria i praktyka taktyki w XXI wieku*, W. Więcek, L. Elak (red.),

AON, Warszawa 2016; *Wyzwania i perspektywy ewolucji taktyki w świetle konfliktów lokalnych XXI wieku*, L. Elak, A. Michalak, W. Więcek, (red.), Akademia Sztuki Wojennej, Warszawa 2016.

BLOKADA ZBROJNA (ang. *military blockade*) – jest znana i stosowana od tysięcy lat. Obecnie to jedna z form konfliktu zbrojnego. Nazywana jest też blokadą militarną i blokadą wojenną.

W XXI w. mimo ogromnych przemian w prowadzeniu działań zbrojnych nadal niezwykle ważne jest dostarczanie walczącym oddziałom m.in. uzbrojenia, żywności i innych środków, które są niezbędne do walki. Stąd rola długotrwałego izolowania przy pomocy wojska państwa (albo sojuszu państw czy organizacji aspirującej do miana państwa) części (rzadziej całości) terytorium kontrolowanego przez przeciwnika. Zastosowanie blokady zbrojnej generuje duże straty bojowe, zaplanowana skala operacji musi więc odpowiadać możliwościom. Do warunków skuteczności blokady zbrojnej w danym rejonie zaliczane jest posiadanie przez stronę blokującą odpowiedniej przewagi taktycznej i strategicznej.

Blokada zbrojna prowadzona jest zasadniczo w formie działań blokadowych. Te ostatnie można zdefiniować jako zbiór działań zmierzających do izolowania danego obszaru. Można je podzielić na 2 rodzaje. Najważniejsze jest ciągłe, systematyczne, wykorzystujące taktyczne właściwości terenu walk oddziaływanie na siły zbrojne przeciwnika. Ma to uniemożliwić mu przerwanie blokady. Okresowo te oddziaływania wymagają wsparcia skoordynowanymi, w większym stopniu aktywnymi akcjami. Pozwalają one na przeprowadzenie ataków na siły przeciwnika oraz zatrzymanie jego ofensywy.

Kierowanie blokadą zbrojną wymaga wysokiego stopnia kontroli operacyjnej i szybkiego dostosowania się do przeciwblokujących działań przeciwnika. Aby utrzymać inicjatywę, strona blokująca musi elastycznie dostosowywać m.in. cele i kierunek blokady, zasięg i tempo operacji oraz skład używanych sił. Częstotliwość operacji oraz szczegóły działań systematycznych w ramach blokady są zależne od sytuacji. Przy blokadzie większych sił strona blokująca często rozmieszcza swe siły w kilku liniach. Przede wszystkim muszą one uwzględniać możliwości własne oraz szybkość, siłę i kierunek podchodzenia sił przeciwnika do blokady. Przykładem może być wykorzystanie odwodów i oddziałów desantowo-szturmowych do utrzymania przewagi na kierunku natarcia głównych sił przeciwnika. Stąd słusznie podnoszone jest przez D. Szkołudę bardzo duże znaczenie w XXI w. dobrego rozpoznania dla prowadzenia skutecznych działań blokadowych. Jak nie bez racji wskazują specjaliści chińscy, konieczne jest także odpowiednie wsparcie wywiadowcze, logistyczne i inżynieryjne. W tego typu konflikcie zbrojnym zaangażowane mogą być państwa oraz organizacje niemające (przynajmniej na razie) takiego charakteru. Nieprzypadkowo Szkołuda zaliczył blokowanie do typowych form taktyki działań asymetrycznych skierowanych przeciw wojskom regularnym państwa. Zważywszy na specyfikę lokalną, szczególnie

wielu państw afrykańskich, nie można wykluczyć sytuacji, w której i strona blokująca, i blokowana nie będą na arenie międzynarodowej traktowane jako państwa. Aby za pomocą blokady zbrojnej ograniczyć, a najlepiej odciąć przeciwnika od kontaktów wojskowych i gospodarczych ze światem zewnętrznym, przerywa się (lub dezorganizuje) jego szeroko pojętą komunikację wojskową i cywilną. Zastosowanie omawianego typu konfliktu zbrojnego doraźnie ma pomóc państwom blokującym w utrzymaniu już posiadanej pozycji wojskowej.

Blokada zbrojna ma uniemożliwić przeciwnikowi m.in.:

- wycofanie sił z izolowanego obszaru, np. w celu ich udziału w walnej → b i t w i e ;
- przysłanie dodatkowych pododdziałów;
- wykorzystanie danego obszaru i jego infrastruktury jako bazy wypadowej (np. dzięki wykorzystaniu przywiezionych drogą lotniczą jednostek powietrzno-desantowych) oraz jako narzędzia do blokowania przebiegających w pobliżu szlaków komunikacyjnych.

Cele długofalowe danej blokady zbrojnej zależą od jej znaczenia wojskowego. Najważniejsze są blokady strategiczne. Mają doprowadzić do walnej bitwy zakończonej klęską osłabionego przeciwnika i jego kapitulacją lub uzyskaniem oczekiwanych przez stronę blokującą ustępstw. Natomiast zastosowanie blokady operacyjnej ma na celu odizolowanie dużego zgrupowania przeciwnika. Jej celem jest uniemożliwienie wykorzystania takiej jednostki wojskowej w głównej bitwie lub uniemożliwienie jej swobody działań w takim stopniu, by w perspektywie zmusić do kapitulacji. Współcześnie najczęściej stosowana jest blokada taktyczna. Ma odizolować niewielkie zgrupowania przeciwnika od sił głównych – pozbawić je możliwości działania oraz wykorzystania w walce przez przeciwnika.

Oddziały te zajmują z reguły niewielki rejon, ale bronią np. bardzo dobrze przygotowanej do obrony bazy, systemu bunkrów, lotniska czy fortu. Blokada twierdzy z zamiarem jej zdobycia jest niekiedy uznawana za rodzaj oblężenia. Dla porządku należy odnotować, że niektórzy badacze blokadę taktyczną utożsamiają z blokadą zbrojną, pomijając istnienie blokad strategicznych i operacyjnych. Inni przeciwnie – za synonim blokady zbrojnej uznają blokadę strategiczną.

W zależności od możliwości państwa blokującego (lub koalicji państw) oraz uwarunkowań geograficznych blokada zbrojna może obejmować równocześnie blokadę lądową, powietrzną i morską lub tylko niektóre z nich. Najczęściej najważniejszym (lub jedynym) jej elementem jest blokada lądowa. Oznacza to okrążenie i zablokowanie określonego terenu przy pomocy operujących na lądzie sił zbrojnych. Jest ona niekiedy utożsamiana z blokadą jako taką (oczywiście w sensie wojskowym). Bardzo duży wpływ na przebieg działań w ramach blokady lądowej będzie miał otwarty lub zamknięty charakter blokowanego regionu (np. równina, kotlina górska). Znaczenie ma także np. stan infrastruktury komunikacyjnej i poziom zalesienia. Ułatwieniem

może być odpowiednie wykorzystanie terenu, np. lesisto-jeziornego. Jako przykład można wskazać prace ziemne i fortyfikacyjne na tych → r u b i e ż a c h [t. 3] terenowych, które zamykają przeciwnikowi odpowiednie do natarcia kierunki.

Przebieg działań blokadowych jest w dużej mierze zależny od położenia geograficznego blokowanego rejonu, nie tylko dlatego, że może się on znajdować blisko lub daleko od państwa blokującego. Blokada bliska oznacza pozostawienie sił zbrojnych w pobliżu sił blokowanych w celu skuteczniejszego działania. Blokada bliska i daleka mają najpełniejsze zastosowanie w → b l o k a d z i e m o r s k i e j .

Z kolei blokada powietrzna obejmuje odizolowanie blokowanego obszaru komunikacji powietrznej. Związana jest ona głównie z monitorowaniem zakazu lotów, inspekcją niezidentyfikowanych samolotów oraz operacjami bojowymi. Warunkiem jej skuteczności jest znaczna przewaga w powietrzu uzyskana przez niszczenie samolotów przeciwnika (jeśli w rejonie takimi środkami dysponuje) oraz blokowanie kontrolowanych przez niego np. baz powietrznych i lotnisk. Stosowana jest głównie w połączeniu z blokadą lądową i/lub morską. Przykładem mogą być operacje powietrzno-lądowe, wg. M. Huzarskiego obejmujące wspólne działania sił lądowych z formacjami desantowo-szturmowymi.

Blokada lotnicza ma wyraźnie bardziej pasywny charakter od izolacji lotniczej. Jak wskazują badacze chińskiej myśli wojskowej, nie zmienia to jednak tego, że w ramach jednej z najbardziej znanych blokad lotniczych zniszczono ok. 1,2 tys. samolotów przeciwnika.

Aby na określonym obszarze izolowanie sił przeciwnika osiągnęło cel, konieczne jest zadbanie o bardzo dużą szczelność blokady zbrojnej. Jak wskazuje Szkołuda, w XXI w. nadal bardzo ważna jest kontrola nad głównymi szlakami komunikacyjnymi. W omawianym kontekście szczelność jest utożsamiana ze skutecznością. Mierzy się ją liczebnością oddziałów przeciwnika i ich uzbrojenia, którym za pomocą działań blokadowych uniemożliwiono przedarcie się przez rubież blokady (w tym zniszczonych).

W wypadku, gdy działania blokadowe nie są wystarczająco skuteczne, do osiągnięcia celów stosuje się blokadę zbrojną częściową. Jak słusznie zauważono, pojęcie to jednak możemy zastosować wtedy, gdy stronie blokującej udało się w poważnym stopniu utrudnić przeciwnikowi dokonanie zmiany sytuacji operacyjnej na blokowanym obszarze. W wypadku części blokad do osiągnięcia tego celu wystarczy uniemożliwienie opuszczenia omawianego obszaru przez 30% całości blokowanych sił i środków.

K. Tokarczyk i S. Szwagrzyk wskazują na możliwość upowszechnienia się w XXI w. prób odcięcia blokowanego przeciwnika od ewentualnego zaplecza społecznego w tym rejonie. Ich zdaniem może być tu stosowane zarówno zastraszenie → l u d n o ś c i c y w i l n e j [t. 3] przez blokujące wojsko, jak i próby przekonania mieszkańców o bezowocności starań sił blokowanych i/lub pozyskanie ich dla strony blokującej – chcąc pozyskać ludność, niekiedy strona blokująca na swój koszt wysyła pomoc humanitarną. Nic dziwnego. Przy blokadzie częściowej poparcie ludności

dla strony blokowanej np. w rejonach górskich może przedłużyć trwanie konfliktu zbrojnego w rejonie kraju o wiele lat. Utrata cywilnego zaplecza przy stałej militarnej przewadze strony blokującej radykalnie zwiększa możliwość załamania ducha oporu w okrążonych oddziałach.

W zależności od możliwości stron walczących blokadzie zbrojnej może towarzyszyć blokada ekonomiczna i blokada informacyjna.

Nieprzypadkowo wojskowi specjaliści chińscy podkreślają wagę sprzyjającego dla strony blokującej otoczenia międzynarodowego. Aby była skuteczna, blokada zbrojna musi być powszechna. Musi mieć zastosowanie nie tylko do środków transportu stron danego konfliktu zbrojnego, ale także do wszystkich państw neutralnych. Dlatego też zgodnie z prawem międzynarodowym blokadę strategiczną czasem ogłasza się oficjalnie razem z planowanym czasem obowiązywania. Jak wykazuje praktyka, jest ona różnie interpretowana przez ustawodawstwo poszczególnych państw.

Poparcie międzynarodowe pozwala także na uzyskanie akceptacji (lub obojętności) ze strony wielu państw neutralnych dla trudnego losu ludności cywilnej na obszarze blokowanym. Blokada powoduje bowiem straty wśród ludności cywilnej wynikające z niedostatku żywności, lekarstw itp. Są one nieuchronne, jeśli blokowany, często zniszczony walkami, obszar nie jest pod tym względem samowystarczalny. Dostarczenie żywności przez bezstronne organizacje humanitarne musi być uzgodnione ze stronami walczącymi. Państwo blokujące ma także prawo do kontroli nad sposobem rozprowadzenia pomocy.

Los cywilów może wywołać presję ze strony wielu organizacji międzynarodowych. W tej materii skuteczność protestów międzynarodowych jest różna.

Stosowanie blokady powoduje także inne problemy związane z ludnością cywilną. Szczególnie dotyczy to państw, których władze podpisały porozumienia międzynarodowe dotyczące konfliktów zbrojnych niemające jeszcze charakteru powszechnie obowiązujących. Komplikuje to np. zastosowanie przez stronę blokującą pól minowych. Co prawda większość państw ratyfikowała zakaz stosowania min przeciwpiechotnych, ale stronami analizowanego rodzaju konfliktu zbrojnego mogą być np. państwa, które takiej ratyfikacji nie dokonały albo organizacje, które nie mają uznania międzynarodowego. W tym ostatnim przypadku zasady prawa humanitarnego nie obowiązują, gdyż z reguły takie konflikty zbrojne nie mają charakteru międzynarodowego. Rozważania te mają wymiar jak najbardziej praktyczny, gdyż w XXI w. obie te grupy są nadreprezentowane w obszarach konfliktów zbrojnych. Warto tu podkreślić, że obowiązek stosowania ratyfikowanych dokumentów prawa międzynarodowego nie jest związany ze stosowaniem wzajemności przez drugą stronę konfliktu zbrojnego. W praktyce często jednak wiele reguł prawa międzynarodowego jest stosowanych przez obie strony omawianego typu konfliktu zbrojnego. Przedłużająca się blokada zbrojna sprawia też inny problem. Rubież blokady przechodząca przez ziemie uprawne koliduje z prawem własności uprawiających je rolników. Może odciąć w tym rejonie dostęp do wody dla części gospodarstw.

W przypadku przedłużającej się blokady może zajść konieczność dokonania wysiedleń ludności z obszarów sąsiadujących z rubieżą blokady. Ich skala może być różna. Jeśli konflikt ma charakter międzynarodowy, a strona blokująca ratyfikowała odpowiednie dokumenty prawa humanitarnego, to jest zobowiązana zapewnić podlegającym przemieszczeniom osobom cywilnym m.in. odpowiednie warunki transportu do miejsca czasowego pobytu, a w nowym miejscu zamieszkania zadowalający poziom wyżywienia, → b e z p i e c z e ń s t w a, opieki lekarskiej i higieny. Obecna ewolucja sztuki wojennej wskazuje jednak, że wysiedlenia ludności cywilnej w czasie blokad zbrojnych w XXI w. zapewne będą stosowane wyraźnie rzadziej niż w XX w.

Tomasz Skrzyński

R. Cliff i in., *Shaking the Heavens and Splitting the Earth. Chinese Air Force Employment Concepts in the 21st Century*, RAND Corporation, Santa Monica–Arlington–Pittsburgh 2011; A. Dziewulska, S*ztuka rozwiązywania konfliktu zbrojnego. Teoria i praktyka oddziaływania na współczesne konflikty*, Bellona, Warszawa 2007; S. Koziej, *Teoria sztuki wojennej*, Bellona, Warszawa 2011; *Międzynarodowe prawo humanitarne konfliktów zbrojnych*, Z. Falkowski, M. Marcinko (red.), Wojskowe Centrum Edukacji Obywatelskiej, Warszawa 2014; *Podstawy działań taktycznych*, L. Elak (red.), AON, Warszawa 2014; D. Szkołuda, *Doświadczenia z operacji ekspedycyjnych w aspekcie przyszłych działań taktycznych*, [w:] *Teoria i praktyka taktyki w XXI wieku*, W. Więcek, L. Elak (red.), AON, Warszawa 2016; K. Tokarczyk, S. Szwagrzyk, *Wyzwania i perspektywy ewolucji taktyki w świetle konfliktów lokalnych XXI wieku*, [w:] *Wyzwania i perspektywy ewolucji taktyki w świetle konfliktów lokalnych XXI wieku*, L. Elak, A. Michalak, W. Więcek (red.), Akademia Sztuki Wojennej, Warszawa 2016; A. Wietoszka, A. Truskowski*, Lotnictwo w operacji połączonej*, „Przegląd Sił Zbrojnych" 2018, nr 5.

BOTNET – sieć współpracujących ze sobą, zdalnie kontrolowanych i zainfekowanych → z ł o ś l i w y m o p r o g r a m o w a n i e m [t. 4] komputerów. Służy m.in. do rozsyłania spamu, rozprzestrzeniania złośliwego oprogramowania oraz działań o charakterze przestępczym na masową skalę. Bot i komputer-zombie to określenia urządzenia, które wchodzi w skład botnetu. Bot, którego nazwa pochodzi od słowa „robot", nie zawsze musi mieć pejoratywne znaczenie. Jego działanie opiera się na sztucznej inteligencji. Bardzo często boty tworzone są po to, by wykonywać proste i powtarzalne zadania, wyręczając w tym człowieka. Większość botów nie jest szkodliwa i odgrywa kluczową rolę w rozwoju internetu, by wspomnieć np. czatboty, czyli automatycznych asystentów obsługujących klientów online.

Historia botów sięga końca lat 80. XX w. To wtedy pojawiła się usługa sieciowa – Internet Relay Chat (IRC), która pozwoliła na rozmowę tekstową z innym użytkownikiem sieci w czasie rzeczywistym. Pierwsze boty zapewniały użytkownikom IRC zautomatyzowane usługi, a także znajdowały się na kanale po to, by nie mógł on zostać zamknięty z powodu braku aktywności. Stopniowo zaczęły pojawiać się boty indeksujące, których celem jest zbieranie danych wykorzystywanych do tworzenia indeksów stron internetowych. Pierwszym botem używanym do indeksowania stron

internetowych był WebCrawler, utworzony w 1994 r. Po raz pierwszy został użyty przez America Online (AOL) w 1995 r.

Boty wykorzystywane są także przez cyberprzestępców, np. do kradzieży danych osobowych.

Botnety zaczęły pojawiać się w latach 90. XX w. Pierwszy botnet, który zyskał rozgłos, został stworzony przez K.K. Smitha w 2000 r. Botnet wysłał 1,25 mln wiadomości typu e-mail – w celu oszustw phishingowych (zob. → p h i s h i n g [t. 3]) – w nieco ponad rok. Miał na celu zebranie poufnych → i n f o r m a c j i [t. 2], np. numerów kart kredytowych.

W 2000 r. pojawił się GTbot (Global Threat Bot) – fałszywy program kliencki, zdolny do przeprowadzania pierwszych ataków typu „odmowy usługi". W kolejnych latach twórcy botnetów mogli wykorzystywać zainfekowane maszyny do przeprowadzania różnych ataków, np. typu → r a n s o m w a r e [t. 3].

Botmaster to osoba kierująca zainfekowanymi komputerami typu „zombie", wykonującymi zautomatyzowane operacje, których celem jest przeważnie osiągnięcie korzyści majątkowych. Do zainfekowania złośliwym oprogramowaniem służą często kampanie phishingowe oraz rozsyłanie spamu. Botnet jest ukryty przed właściwym użytkownikiem sprzętu, nieświadomym tego, że jego urządzeniem steruje zupełnie inna osoba. Botnet złożony jest zazwyczaj z setek tysięcy urządzeń, rozproszonych po świecie, które stanowią kluczowy element infrastruktury informatycznej internetu.

Botnet przejmuje kontrolę nad hostem komputerowym, by następnie wykonywać działania takie jak np.:

- inwigilacja,
- rozsyłanie niechcianej korespondencji,
- sabotaż,
- pozyskiwanie danych osobowych,
- ataki typu DDoS (ang. *distributed denial of service*),
- kradzież danych o charakterze wrażliwym,
- uzyskanie korzyści majątkowej w sposób niezgodny z prawem,
- pozyskanie adresu IP poprzez wykorzystanie zainfekowanego komputera do aktywności w internecie niezgodnej z prawem,
- ataki na inne systemy teleinformatyczne.

Botnety są powszechnie używane, a sieci urządzeń, które je tworzą, stają się obecnie coraz większe. Botnety są także sprzedawane przez cyberprzestępców i wykorzystywane wiele razy. Wykrycie, że dane urządzenie jest botem, okazuje się niełatwe. Infekcję można rozpoznać po m.in.: nadmiernym użyciu łącza sieciowego, wiadomościach pochodzących od nieznanych osób, zwiększonej aktywności dysku twardego oraz braku dostępności typowych funkcji systemu.

Przykłady botnetów wykorzystywanych przez cyberprzestępców:

- Storm, 2007 r. – zainfekował ok. 50 mln komputerów z zainstalowanym systemem operacyjnym Microsoft Windows i był wykorzystywany do wielu cyberprzestępstw;
- Grum, 2008 r. – botnet spamowy specjalizujący się w wiadomościach farmaceutycznych; w 2009 r. wysyłał blisko 40 mld wiadomości dziennie, czyli 18% spamu na świecie;
- Mariposa, 2008 r. – hiszpański botnet, jego działanie koncentrowało się na udostępnianiu cyberprzestępcom numerów kart kredytowych i haseł do kont na stronach usług finansowych, co pozwoliło na kradzież milionów USD od nieświadomych użytkowników;
- Cutwail, 2009 r. – botnet wysyłał ok. 74 mld wiadomości typu spam dziennie. Do dziś pozostaje botnetem „do wynajęcia" w podziemiu komputerowym;
- Mirai, 2016 r. – pierwszy duży botnet infekujący urządzenia IoT (ang. *Internet of Things*); w szczytowym momencie robak zainfekował ponad 600 tys. urządzeń. W wyniku ataku DDoS doprowadził do wyłączenia większej części internetu na wschodnim wybrzeżu USA;
- Avalanche, 2016 r. – → E u r o p o l wraz z europejskimi ekspertami rozbili jedną z największych międzynarodowych organizacji → c y b e r p r z e s t ę p c z y c h ; wykorzystywała ona komputery-zombie, których liczba sięgała ponad 500 tys. „Avalanche" istniał co najmniej od 2009 r. Cyberprzestępcy z Ukrainy, Niemiec i innych krajów zarobili dzięki wykorzystaniu botnetu kilkaset milionów euro.

Agnieszka Warchoł

A. Adamski, *Botnety jako zagadnienie prawnokryminologistyczne na tle doświadczeń amerykańskich*, „Prokuratura i Prawo" 2013, nr 11; IBM Security, *The Inside Story on Botnets. How Threat Actors Exploit Networks of Infected Computers to Commit Cybercrime*, IBM.com (dostęp 20.02.2020); T. Knecht, *A Brief History of Bots and How They've Shaped the Internet Today*, Abusix.com (dostęp 20.02.2020); A. Kura, *Zagrożenia dla bezpieczeństwa informacyjnego państwa u progu XXI wieku*, Wydawnictwo Sztafeta, Stalowa Wola 2016; T. Pączkowski, *Słownik cyberbezpieczeństwa*, Szkoła Policji w Katowicach, Katowice 2017; M. Siwicki, *Cyberprzestępczość*, Wydawnictwo C.H.Beck, Warszawa 2013; A. Warchoł, *Botnet*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019.

BRICS (do 2010 r. BRIC) – związek 5 państw: Brazylii, Rosji, Indii, Chin, Republiki Południowej Afryki, grupa największych pod względem powierzchni i liczby ludności krajów rozwijających się. Od 2006 r. odbywały się nieformalne spotkania przedstawicieli tych państw, a także spotkania na szczeblu ministrów spraw zagranicznych, ministrów finansów i innych. Od 2009 r. rządy tych krajów spotykają się corocznie na oficjalnych szczytach. XIV szczyt BRICS odbył się 24 czerwca 2022 r. w Chinach, a ostatni – XV – w sierpniu 2023 r. w Republice Południowej Afryki.

Termin BRIC został pierwotnie opracowany w kontekście strategii inwestycji zagranicznych. Wprowadził go prezes Goldman Sachs Asset Management, Jim O'Neill, w tekście z 2001 r. *Building Better Global Economic BRICs*. Kolejność liter w akronimie jest taka sama jak w angielskim słowie *bricks*, które oznacza 'cegiełki'. Termin ten jest używany wobec grupy krajów, których rozwój w dużej mierze zapewni przyszły wzrost światowej gospodarki, a szczególnie rynków giełdowych.

W pierwszym raporcie z 2003 r. (*Dreaming with BRIC: The Path to 2050*), który wydał Goldman Sachs, zauważono, że po zakończeniu → z i m n e j w o j n y [t. 4], a nawet wcześniej, rządy BRIC zainicjowały reformy gospodarcze lub polityczne, aby włączyć swoje kraje do globalnego systemu gospodarczego. Od 2003 r. Brazylia, Rosja, Indie i Chiny zmodernizowały swoje systemy polityczne, aby w pełni uczestniczyć w globalnym kapitalizmie. By osiągnąć konkurencyjność na rynku światowym, kraje te kładły nacisk na edukację, inwestycje zagraniczne, krajową konsumpcję i krajową przedsiębiorczość. Według badań Indie mają największy potencjał wzrostu spośród 4 krajów BRIC w ciągu najbliższych 30–50 lat. Głównym powodem takiego stanu rzeczy jest to, że obniżenie wieku produkcyjnego ludności Indii i Brazylii nastąpi później niż w Rosji i Chinach. Raport zwraca również uwagę na główną nieefektywność energetyczną Indii. Wspomina o niedostatecznej reprezentacji gospodarek krajów BRIC na światowych rynkach kapitałowych. Wskazuje także na ogromną populację tych krajów, podczas gdy poziom dochodu na mieszkańca pozostaje znacznie poniżej normy w porównaniu z nowoczesnymi krajami uprzemysłowionymi. Zjawisko to wpłynie na rynki światowe, ponieważ międzynarodowe korporacje będą próbowały wykorzystać ogromny potencjał rynków BRIC przez np. produkcję znacznie tańszych samochodów i innych towarów przemysłowych dostępnych dla konsumentów w krajach BRIC zamiast luksusowych modeli, które obecnie przynoszą duże zyski w branży motoryzacyjnej. Indie i Chiny już zaczęły zaznaczać swoją obecność w sektorach usług i produkcji na arenie światowej.

Podkreślano, że Chiny i Indie mogą ostatecznie stać się dominującymi światowymi dostawcami towarów przemysłowych i usług, podczas gdy Brazylia i Rosja zawładną rynkiem dostaw surowców. Współpraca w ramach BRIC jest więc logicznym krokiem, ponieważ Brazylia i Rosja stają się dostawcami dla Indii i Chin.

Pierwotnie państwa BRIC zostały zidentyfikowane w celu podkreślenia możliwości inwestycyjnych i nie były zrzeszone w formalnej organizacji międzyrządowej. Raport przygotowany przez instytucję Goldman Sachs nie przewidział zaistnienia koordynacji polityk gospodarczych między krajami grupy. Ponadto nie spodziewano się, że państwa te utworzą blok gospodarczy lub oficjalne stowarzyszenie na wzór Unii Europejskiej. Z biegiem czasu pojawiły się jednak oznaki, że wspomniane 4 kraje dążą do powołania klubu politycznego lub „związku", a tym samym przekształcenia swojej rosnącej potęgi gospodarczej ku większemu wpływowi geopolitycznemu. Od 2009 r. w coraz większym stopniu formują się w spójny

blok geopolityczny, a ich rządy spotykają się rokrocznie na szczytach i koordynują politykę wielostronną. Początkowym celem grupy państw było ustanowienie sprawiedliwego, demokratycznego i wielobiegunowego porządku światowego, ale wraz z wejściem do grupy Republiki Południowej Afryki i zmianą nazwy na BRICS stowarzyszenie to stopniowo przekształciło się w organizację polityczną w tradycyjnym rozumieniu. Raport stwierdza, że Rosja, utrzymując dominację na europejskim rynku energii, będzie nadal borykać się z problemami ekonomicznymi w związku z dalszym zmniejszaniem się liczby ludności. Zdaniem O'Neilla Rosja raczej nie zasługuje na miejsce w tym klubie ze względu na niskie tempo wzrostu. Opinię tę podzielają także profesor Uniwersytetu Nowojorskiego Nouriel Roubini oraz prezes firmy konsultingowej

Eurasia Group Ian Bremmer. Analityk firmy badawczej w dziedzinie makroekonomii Capital Economics, Roger Bootle, uważa, że Rosja została przyjęta do BRIC ze względu na fakt, że dzięki niej nazwa tej grupy stała się rozpoznawalna. Ekonomista zauważa, że gospodarka Rosji bardzo różni się od gospodarek Indii, Chin i Brazylii. W Rosji, w przeciwieństwie do wymienionych krajów, przyczyną wzrostu PKB nie była transformacja gospodarki, ale splot czynników niezależnych od państwa. Wśród tych ostatnich Bootle wymienia wzrost cen surowców, przede wszystkim ropy. Zdaniem analityka gospodarka Rosji jest wciąż archaiczna. Społeczeństwo rosyjskie jest skorumpowane, a demografia wykazuje negatywne tendencje.

O'Neill wyraził zdziwienie, gdy Republika Południowej Afryki przystąpiła do BRIC, ponieważ gospodarka RPA stanowi zaledwie 1/4 gospodarki Rosji (słabszego ekonomicznie kraju BRIC). Uważał, że to państwo ma potencjał, ale nie spodziewał się szybkiej akcesji Republiki Południowej Afryki. Południowoafrykański ekonomista Martin Davies argumentował, że decyzja o zaproszeniu RPA nie miała ekonomicznego sensu, ale była czysto politycznym posunięciem w ramach chińskiej strategii rozszerzenia obecności w Afryce i zwiększenia wpływów globalnych. Obecność państwa afrykańskiego ma duże znaczenie geopolityczne, gdyż w ten sposób BRICS uzyskało obecność na 4 głównych kontynentach, co pozwala mu szybciej zwiększać swoje wpływy i poszerzać możliwości handlowe.

Duża powierzchnia i duża populacja krajów BRICS umożliwiają ich szybki rozwój, a według szacunków instytucji Goldman Sachs do 2050 r. ich gospodarki łącznie mogą przebić połączone gospodarki najbogatszych współczesnych krajów rozwiniętych (G7). Raport szacował, że potencjał gospodarczy Brazylii, Rosji, Indii i Chin jest taki, że mogą one stać się 4 dominującymi systemami gospodarczymi, a ich łączny produkt krajowy brutto (PKB) wyniesie 15,435 mld dolarów. Te kraje należą do największych i najszybciej rozwijających się rynków wschodzących.

Łączna powierzchnia krajów BRICS wynosi 39 746 220 km^2, a całkowitą populację szacuje się na ok. 3,21 mld ludzi, co stanowi ok. 26,7% powierzchni lądowej świata i ok. 43% światowej populacji. Czterech z pięciu członków grupy należy do

dziesięciu największych krajów świata pod względem liczby ludności, powierzchni i PKB.

Członkowie grupy BRICS byli wielokrotnie określani jako najszybciej rozwijające się duże kraje. Ich korzystną pozycję zapewnia zarówno rozwijająca się gospodarka, jak i duża ilość surowców ważnych z punktu widzenia gospodarki światowej:

- Brazylia jest 8. gospodarką świata pod względem PKB, bogatą w produkty rolne;
- Rosja była 6. gospodarką na świecie pod względem PKB, krajem największych rezerw surowców mineralnych, o największym terytorium na świecie, jedną z dwóch największych potęg jądrowych na świecie;
- Indie to 3. gospodarka świata pod względem PKB, ma tanie zasoby intelektualne, to największa populacja świata;
- Chiny to 1. gospodarka na świecie pod względem PKB i 1. eksporter na świecie, właściciel jednej z największych na świecie rezerw walutowych; ma tanie zasoby siły roboczej, jeden z dwóch krajów na świecie o populacji ponad 1 mld ludzi;
- Republika Południowej Afryki stanowi 32. gospodarkę świata pod względem PKB, ma zróżnicowane zasoby naturalne.

Wysoka liczba ludności krajów BRICS determinuje ich tanią siłę roboczą oraz relatywnie wysokie stopy wzrostu gospodarczego. Przewiduje się, że wzrost gospodarczy tych krajów przekształci się w przyszłości we wpływy polityczne, co doprowadzi do powstania nowej elity gospodarczej i zmniejszy wpływy „złotego miliarda".

W kręgach politycznych i eksperckich toczy się dyskusja nad rozszerzeniem formatu BRICS do BRICS+, rozumianej jako struktura, która uzupełniałaby współpracę między 5 głównymi członkami za pomocą szerszego kręgu tworzonego przez każdego z jej członków w ramach odpowiednich regionalnych bloków i organizacji integracyjnych. W czerwcu 2017 r. na spotkanie BRICS w chińskim mieście Fuzhou zaproszono do dialogu w formacie BRICS+ przedstawicieli Indonezji, Malezji, Filipin, Kambodży, Egiptu, Nigerii, Etiopii, Kenii, Argentyny, Chile, Meksyku i innych państw ze względu na ich regionalne wpływy, potencjał gospodarczy, wielkość terytorium i liczbę ludności.

Państwa BRICS są uważane za głównego rywala bloku → Grupy Siedmiu (G 7) [t. 5]. Ogłaszają konkurencyjne inicjatywy, takie jak Nowy Bank Rozwoju (The New Development Bank, NDB), Porozumienie w sprawie rezerw warunkowych (Contingent Reserve Arrangement, CRA), system płatności BRICS i koszyk rezerw walutowych BRICS. InicjatywyNDB i CRA, stanowiące obecnie architekturę finansową BRICS, zostały ustanowione w traktacie z 2014 r.

Od 2022 r. grupa dąży do rozszerzenia członkostwa, a kilka krajów rozwijających się wyraziło zainteresowanie dołączeniem do niej: 19 maja 2022 r. chiński minister spraw zagranicznych Wang Yi zaproponował rozszerzenie grupy BRICS, a 27 czerwca Argentyna i Iran złożyły wniosek o przystąpienie do BRICS. Stosunki między Iranem, Chinami i Rosją ociepliły się, ponieważ wszystkie 3 rządy szukają nowych sojuszników przeciwko rosnącej opozycji Zachodu. Arabia Saudyjska, Turcja i Egipt

również wyraziły zainteresowanie przystąpieniem do BRICS, ale nie złożyły jeszcze oficjalnych wniosków. Nie ma formalnego procesu aplikacyjnego dołączenia do BRICS, ale każdy rząd musi uzyskać jednomyślne poparcie wszystkich członków BRICS, aby otrzymać zaproszenie do grupy.

W związku z → w o j n ą [t. 4] Rosji przeciwko Ukrainie grupa BRICS potencjalnie może stanowić dla Rosji pewną poduszkę bezpieczeństwa, zwłaszcza że państwa te chętnie przyjmą rosyjskie surowce energetyczne, szczególnie ropę. W Indiach import rosyjskiej ropy w 2022 r. znacznie wzrósł i jest równy 1/5 importu ropy do Indii. Rosja nie zamierza jednak ograniczać współpracy z BRICS wyłącznie do eksportu surowców. Władimir Putin zaproponował kooperację w zakresie wymiany → i n f o r m a c j i [t. 2] w sektorze finansowym (alternatywa wobec zachodniego SWIFT), a nawet stworzenie nowej waluty rezerwowej opartej na koszyku walut państw należących do grupy. Rosja chciałaby również, by jej system płatności MIR (alternatywa wobec VISA / Mastercard) rozszerzył się na inne kraje chętne do jego przyjęcia. Trzeba podkreślić również, że do → s a n k c j i p r z e c i w k o F e d e r a c j i R o s y j s k i e j nie przyłączyły się właściwie żadne państwa nienależące do szeroko pojętego Zachodu. Przykładowo, wśród państw Azji do sankcji dołączyły tylko Korea Południowa, Japonia i Tajwan, czyli kraje, które mentalnie i strukturalnie należą do Zachodu.

Sergiusz Wasiuta

P.N. Batista Jr., *The BRICS and the Financing Mechanisms They Created. Progressand Shortcomings*, Anthem Press, London 2021; P.R. Carmody, *The Rise of BRICS in Africa. The Geopolitics of South-South Relations*, Zed Books, London 2013; K. Chun, *The BRICs Superpower Challenge. Foreign and Security Policy Analysis*, Ashgate Publishing, Farnham 2013; *Handbook of BRICS and Emerging Economies*, F. Comim, P.B. Anand, S. Fennell (eds.), Oxford University Press, Oxford 2021; Joint Site OfMinistries Of Foreign Affairs Of Brics Member States, http://infobrics.org/ (dostęp 15.04.2023); P. Kugiel, *Znaczenie grupy BRICS po rosyjskiej inwazji na Ukrainę*, 15.06.2022, „Biuletyn PISM" 2022, nr 99 (2518), https://www.pism.pl/publikacje/znaczenie-grupy-brics-po-rosyjskiej-inwazji-na-ukraine (dostęp 17.04.2023); C. Majaski, *Brazil, Russia, India and China (BRIC) Definition in Investing*, 17.05.2022, https://www. investopedia.com/terms/b/bric.asp (dostęp 15.04.2023); J. O'Neill, *Building Better Global Economic BRICs*, „Global Economics Paper", 30 November 2001, no. 66, http:// www.goldmansachs.com/our-thinking/archive/archive-pdfs/build-better-brics.pdf (dostęp 11.03.2023); O. Stuenkel, *The BRICS and the Future of Global Order*, Lexington Books, Lanham, Maryland 2015; *The International Political Economy of the BRICS*,Li Xing (ed.), Taylor & Francis, Oxfordshire 2019; D. Wilson, R. Purushothaman, *Dreaming with BRICs: The Path to 2050*, Goldman Sachs 2003, https://www.goldmansachs.com/intelligence/archive/brics-dream.html (dostęp 30.06.2023); *Who's Who: Bric Leaders Take Their Place at the Top Table*, https://www.ft.com/content/d31392b289ca-11dd-8371-0000779fd18c?nclick_check=1 (dostęp 11.03.2023); Ye Xie, *Goldman's BRIC Era Ends as Fund Folds After Years of Losses*, 8.11.2015, https://www.bloomberg. com/news/articles/2015-11-08/goldman-s-bric-era-ends-as-fund-closes-after-yearsof-losses?leadSource=uverify%20wall (dostęp 15.04.2023); J. Zajączkowski, *BRIC dziesięć lat później, czyli anty-Zachód w rozsypce*, „Rocznik Strategiczny" 2013/2014, t. 19, https://wnpism.uw.edu.pl/wp-content/uploads/2020/06/17_2014.pdf (dostęp 2.04.2023); *Россию включили в БРИКС ради буквы „Р", – экономист*, 15.07.2013, http://economics.lb.ua/business/2013/07/15/212892_rossiyu_vklyuchili_briks_radi_ bukvi.html (dostęp 11.03.2023).

BROŃ ANTYSATELITARNA – inaczej: broń przeciwsatelitarna (ang. *Anti-Satellite Weapon*, ASAT), urządzenie przeznaczone do neutralizacji (niszczenia, uszkadzania lub trwałego zakłócania działania) celów znajdujących się na orbicie. Definicję broni antysatelitarnej można rozszerzyć w celu ujęcia oddziaływania na inne elementy systemów satelitarnych (oprócz satelitów, w skład systemu satelitarnego wchodzą infrastruktura naziemna oraz łącze), a także aby objąć nią oddziaływania niedestrukcyjne lub sytuujące się na granicy między oddziaływaniami destrukcyjnymi a niedestrukcyjnymi (w pewnych przypadkach wyznaczenie tej granicy może być problematyczne).

Zasadniczy podział broni antysatelitarnej opiera się na kryterium obszaru stacjonowania i sposobu osiągnięcia rejonu ataku. W związku z tym możemy mówić o 2 rodzajach broni:

- broń wystrzeliwana z Ziemi i niszcząca obiekty w kosmosie, bez umieszczenia efektora na orbicie okołoziemskiej (tzw. broń bezpośredniego wznoszenia, ang. *direct ascent*). Składa się ona z rakiety nośnej wynoszącej ponad atmosferę, na trajektorię zbieżną z celem, tzw. interceptor (efektor, element przechwytujący), wyposażony w układ naprowadzania oraz w system sterowania. Taka broń pozwala na zastosowanie stosunkowo słabych rakiet nośnych, gdyż muszą one tylko osiągnąć odpowiednią wysokość, nie są natomiast obarczone wymogiem osiągnięcia prędkości koniecznej do umieszczenia obiektu na orbicie. Warto zauważyć, że trudno w takim układzie skonstruować broń pozwalającą na rażenie celów na orbitach geosynchronicznych. Analogicznie skomplikowane okazuje się – ze względu na wysokość – umieszczenie satelity bezpośrednio na takiej orbicie (dlatego stosuje się pośrednie orbity transferowe).
- broń koorbitalna (ang. *co-orbital*), umieszczona na orbicie okołoziemskiej i stamtąd oddziałująca na inne obiekty w przestrzeni kosmicznej. Taka broń może zostać umieszczona na orbicie przecinającej orbitę celu, ewentualnie na tej samej płaszczyźnie orbitalnej (tak określa się też niekiedy każdą broń antysatelitarną wymagającą umieszczenia obiektu przechwytującego na orbicie okołoziemskiej – albo na tej samej, albo na innej płaszczyźnie orbitalnej w stosunku do celu). Teoretycznie do działań antysatelitarnych można zastosować każdego satelitę dysponującego zdolnością manewrowania, co powoduje potencjalne problemy weryfikacyjne w razie ewentualnego wprowadzenia traktatu zakazującego tego rodzaju broni. Ta możliwość jest także źródłem obaw w sytuacji, gdy inne państwa dysponują satelitami, które mogą zbliżać się do innych obiektów. Broń koorbitalna może podążać za celem w niewielkiej odległości (broń śledząca), w dużej odległości (co wymaga forsownych manewrów dla zbliżenia się do celu), rozważa się także tzw. broń pasożytniczą (ang. *parasitic ASAT*) – łączącą się z celem na podobieństwo pasożytniczych gatunków zwierząt i niszczącą go w odpowiednim momencie. Ta metoda wydaje się jednak zbyt kuriozalna, żeby stanowić realne rozwiązanie, a → i n f o r m a c j e [t. 2] o rzekomym rozwijaniu jej przez Chiny rozpowszechniała

hongkońska gazeta Sing Tao, powołująca się na anonimowe źródło. Broń orbitalna może być wystrzeliwana bezpośrednio przed atakiem (radzieckie systemy tego typu, mające wykonać zaledwie kilka obrotów orbitalnych przed przypuszczeniem ataku) lub znacznie wcześniej. Tę drugą kategorię określa się niezbyt precyzyjnie mianem kosmicznych min.

Ze względu na sposób oddziaływania stosuje się następujący podział broni antysatelitarnej:

- Broń kinetyczna (ang. *hit-to-kill*), wykorzystująca energię kinetyczną, czyli energię obiektu w ruchu. Działanie tej broni polega na doprowadzeniu do kolizji 2 obiektów przy dużej prędkości (chodzi o względną prędkość jednego obiektu w relacji do drugiego). W wyniku zderzenia powstaje znacząca liczba kosmicznych odpadków, określanych anglojęzycznym terminem *debris* lub rosyjskojęzycznym *musor* (мусор). W polskim piśmiennictwie te obiekty określa się jako kosmiczne śmieci, szczątki, odpadki lub kosmiczny gruz. Same kosmiczne odpadki to „wszystkie wytworzone przez człowieka obiekty znajdujące się na orbitach wokół Ziemi, które nie służą już do praktycznych celów". Broń kinetyczna to najbardziej dynamicznie rozwijana kategoria broni antysatelitarnej. Do ataku z jej wykorzystaniem można użyć obiektów umieszczonych na orbicie. Umożliwia to szybkie ataki bez oczekiwania, aż cel znajdzie się w zasięgu rażenia. Ten sposób może być bardziej użyteczny także w realizacji skoordynowanego ataku na wiele satelitów. Wymaga to jednak posiadania całej konstelacji satelitów przechwytujących, rozmieszczonych na orbitach okołoziemskich. Zastosowanie kinetycznej broni *direct ascent* przekłada się z kolei na mniejsze wyzwanie technologiczne.

Broń kinetyczną można podzielić na kierowaną, czyli wymagającą systemu naprowadzania, oraz na niekierowaną. Kinetyczna broń kierowana to główna tendencja rozwoju broni antysatelitarnej. W końcowej fazie ataku wykorzystuje się zazwyczaj naprowadzanie optyczne. Z myślą o broni niekierowanej mówimy o koncepcji zakładającej rozrzucenie elementów rażących na drodze satelity. Taki sposób wymaga częściowego naprowadzania – posiadania systemu śledzącego tor lotu celu oraz śledzącego i korygującego rakietę, która posłużyć ma do wyniesienia elementów rażących. Ta metoda może być atrakcyjna dla krajów dysponujących rozwiniętą technikę w zakresie rakiet nośnych lub balistycznych, lecz przy tym mających braki w sferze technologii potrzebnych do budowy układu końcowego naprowadzania interceptora. Ze względu na mniejszą precyzję trzeba się jednak liczyć z niższą skutecznością takiej metody ataku. Świadectwem możliwości w tym zakresie jest konieczność wykonania przez Międzynarodową Stację Kosmiczną manewru Pre-Determined Debris Avoidance Maneuver (PDAM), aby nie zderzyć się z osłoną obiektywu chińskiego satelity szpiegowskiego Yaogang 12 (Object 39372). Można sobie wyobrazić, że taki element zostaje „zgubiony" nie przypadkiem, lecz celowo.

- Broń wykorzystująca głowice wybuchowe: konwencjonalne oraz nuklearne. W przypadku eksplozji nuklearnej możemy wyróżnić 3 sposoby niszczącego oddziaływania na satelity: bezpośrednie skutki wybuchu, wpływ impulsu elektromagnetycznego oraz oddziaływanie pośrednie przez tzw. pompowanie radiacji w pasmach Van Allena przez protony i elektrony emitowane w czasie eksplozji. Zwłaszcza to ostatnie oddziaływanie może mieć charakter długotrwały. Po teście Starfish Prime przeprowadzonym w 1962 r. i polegającym na eksplozji nuklearnej na wysokości 400 km, niszczące działania na satelity miało miejsce jeszcze 7 miesięcy po wybuchu, a wpływ na pasma Van Allena notowano do 1970 r. Długotrwała radiacja powstała wskutek wybuchu nuklearnego może być bardzo szkodliwa dla sztucznych satelitów, ponadto charakteryzuje się ogromnym zasięgiem. Szacuje się, że w przypadku eksplozji głowicy o mocy 1 megatony w przestrzeni kosmicznej, satelita niewyposażony w specjalne osłony może zostać porażony nawet z odległości 20–30 tys. km.

Trudno wyobrazić sobie przeprowadzenie tego typu ataku przez państwo, które dysponuje znaczącą własną infrastrukturą w przestrzeni kosmicznej, gdyż byłby on niemożliwy do precyzyjnego ukierunkowania. Mógłby być jednak dogodnym sposobem oddziaływania dla pozostałych państw, mających jednak głowice nuklearne oraz rakiety, nawet o względnie niewielkich możliwościach (w przypadku rakiet balistycznych pułap odpowiada przeciętnie połowie zasięgu, więc do wyniesienia głowicy na niskie orbity okołoziemskie (od ok. 150 do 800–1000 km) wystarczy rakieta o zasięgu 300–2000 km). Oczywiście, takie działanie może być uznane za prowokacyjne oraz eskalujące, ale zdecydowanie okaże się mniej prowokacyjne i eskalujące niż atak nuklearny na obiekt na Ziemi, zwłaszcza że zapewne nie pociągnie za sobą żadnych ofiar w ludziach.

- Broń wiązkowa (ang. *directed energy weapons*), wykorzystująca źródła kierowanej energii. Do tej kategorii zaliczamy m.in. broń laserową oraz mikrofalową. Przestrzeń pozaziemska jest środowiskiem sprzyjającym wykorzystaniu broni działającej z wykorzystaniem propagacji fal elektromagnetycznych (radiowych lub świetlnych), gdyż pozwala na ich transmisję na duże odległości przy stosunkowo niewielkim wydatku energetycznym. Potencjalną zaletą broni wiązkowej jest możliwość niszczenia satelitów bez tworzenia ogromnej liczby kosmicznych szczątków. Użycie broni laserowej może prowadzić do czasowego i odwracalnego zakłócenia układu optycznego satelity (ang. *dazzling* – oślepianie) albo do nieodwracalnego zniszczenia satelity. Niszczący promień lasera może zostać skierowany na układ optyczny, jeśli satelita takowy posiada (tzw. blinding – trwałe oślepienie), na zasadniczą strukturę satelity lub na jego elementy (szczególnie podatne na zniszczenie są panele słoneczne). Lasery mające na celu oślepianie systemów optycznych mają stosunkowo niewielkie wymagania odnośnie do mocy, działanie niszczące wymaga natomiast większych mocy. Szacunki mówią, że w celu

uszkodzenia wrażliwych elementów satelity (np. paneli słonecznych) należy dostarczyć energię między 10 a kilkudziesięcioma dżulami na centymetr kwadratowy, natomiast dla wywołania natychmiastowego „brutalnego" efektu niszczącego w stosunku do zasadniczej struktury satelity wymagana energia będzie już wynosić ok. 1 tys. dżuli na centymetr kwadratowy. Ta druga wartość jest podobna jak w przypadku rakiet balistycznych. Jeśli jednak ograniczymy się do uszkodzenia satelity, będzie to wymagało wielokrotnie mniejszej mocy, co z kolei oznacza, że taki efekt można osiągnąć ze znacznie większego dystansu. Z kolei linia podziału między odwracalnym a nieodwracalnym porażeniem układu optycznego satelity może być trudna do ustalenia, ponieważ wiele czynników (np. zakłócenia atmosfery) przyczynia się do finalnego efektu. Dlatego predykcja dokładnych zniszczeń wskutek działania broni laserowej może być trudna.

Lasery należą do dwóch kategorii: laserów pracy ciągłej, emitujących promieniowanie o stałym natężeniu, oraz laserów impulsowych, emitujących impulsy światła zdolne do dostarczania bardzo wysokiej energii, ale przez krótki czas. Broń laserowa może być umieszczona na Ziemi lub w kosmosie. To drugie rozwiązanie pozwala uniknąć zakłóceń promienia w atmosferze – promienie laserowe ulegają pochłanianiu, rozpraszaniu i załamywaniu się pod wpływem czynników atmosferycznych (mgła, chmury, deszcz, śnieg, ruchy mas powietrza, zanieczyszczenia). Przykładowo: dla lasera zdolnego do emisji wiązki o średnicy wynoszącej 0,5 m w odległości 1 tys. km od źródła w sytuacji braku wpływu atmosfery ta średnica w przypadku typowych zakłóceń atmosferycznych będzie wynosiła aż 7 m. Tak duży wzrost rozbieżności wiązki oznacza aż 180-krotny spadek możliwości doprowadzania ciepła do opromieniowanej powierzchni. Umieszczenie laserów w przestrzeni kosmicznej wymaga jednak przezwyciężenia technicznych ograniczeń związanych z koniecznością uzyskania dużych mocy przy użyciu stosunkowo lekkich urządzeń. Pośrednim rozwiązaniem jest umieszczenie lasera na pokładzie samolotu, dzięki czemu operuje on ponad najbardziej gęstymi warstwami atmosfery. Porażenie strukturalne satelity na orbicie geostacjonarnej laserem umieszczonym na Ziemi lub na niskiej orbicie nie jest przy obecnych możliwościach technicznych wykonalne. Przyczyną jest zbyt duża odległość. Broń laserowa może razić cele na znacznych odległościach, ale nie – na dowolnych: skupienie wiązki staje się niewystarczające (mówimy tu o odległości ponad 35 tys. km). Pewnym ograniczeniem broni laserowej jest fakt, że może ona działać tylko w linii wzroku (ang. *line-of-sight*).

Z kolei broń mikrofalowa (ang. *high-powered microwaves attacks*, HPM) wykorzystuje mikrofale, czyli fale elektromagnetyczne o długości mniejszej niż fale radiowe, ale większej niż fale światła widzialnego.Mikrofale są stosowane m.in. w radiolokacji i w komunikacji radiowej. Broń mikrofalowa może być zlokalizowana w kosmosie lub na Ziemi, jednak w tym drugim przypadku użyteczność ograniczają odległość oraz zakłócenia w atmosferze. Tego typu broń oddziałuje na elektronikę czasowo – powoduje zakłócenia (ang. *jamming*), lub trwale, co jednak wymaga zastosowania wielokrotnie

większej mocy sygnału. W porównaniu do wiązki lasera skupienie wiązki mikrofalowej jest znacznie mniejsze, gdyż długość fali jest tysiące razy większa niż w przypadku światła optycznego. Co prawda, technologie konieczne do realizacji ataków HPM ze skutkiem permanentnym istnieją, ale rzeczywista skuteczność takiej broni jest trudna do oszacowania.

Analiza sposobów oddziaływania broni antysatelitarnej pozwala przeprowadzić kolejną klasyfikację na broń niedestrukcyjną, czyli unieszkodliwiającą satelity czasowo (np. zakłócanie lub oślepianie), oraz na broń trwale niszczącą satelitę. Działania niedestrukcyjne mogą być realizowane z wykorzystaniem systemów → w a l k i r a d i o e l e k t r o n i c z n e j [t. 4]. Istnieją 2 zasadnicze metody – zakłócenia sygnałów oraz wysyłanie fałszywych sygnałów (ang. *spoofing*). Granica między działaniem destrukcyjnym a niedestrukcyjnym może w pewnych przypadkach być nieoczywista, gdyż pewne techniki zakłócania czy oślepiania mogą skutkować fizycznymi zniszczeniami. Środki niedestrukcyjne mogą być bardziej użyteczne, gdyż są mniej prowokacyjne i nie powodują zanieczyszczenia kosmosu odpadkami. Dodatkowo mogą zostać zastosowane w sposób bardziej skryty,co powoduje trudność w atrybucji źródła ataku. Dlatego są szczególnie predestynowane do wykorzystania poniżej progu otwartego → k o n f l i k t u z b r o j n e g o .

Kolejna klasyfikacja dotyczy celu ataku. Oddziaływanie antysatelitarne może być skierowane na poszczególne elementy systemów satelitarnych: na samego satelitę, na infrastrukturę naziemną, czyli urządzenia otrzymujące lub wysyłające sygnał do satelity, lub na ów sygnał (łącze).Hipotetycznym sposobem ataku trzeciego rodzaju, ukierunkowanego na sygnał łączący satelitę i stację naziemną, może być próba przejęcia kontroli nad satelitą (ang. *hacking*). Trudno sobie jednak wyobrazić testowanie tego sposobu ataku w warunkach pokojowych. Sam atak na transmisję związane z aktywnością satelitów może odbywać się we wszystkich fazach „życia" satelity: testowania przed wystrzeleniem, wynoszenia na orbitę, fazy aktywnej związanej z funkcjonowaniem na orbicie, deorbitacji.

Kolejny podział wyróżnia broń działającą w sposób otwarty oraz w sposób skryty. Ta druga kategoria rozwija się wobec coraz powszechniejszego postrzegania ataku na satelity jako aktu → w o j n y [t. 4] i obejmuje przed wszystkim różne rodzaje oddziaływania tymczasowego. Należy również wyróżnić kategorię pośrednią – broń przeprowadzającą atak w sposób otwarty, ale rozmieszczoną tak, żeby ukryć jej przeznaczenie. Chodzi przede wszystkim o ukrycie przeznaczenia broni antysatelitarnej rozmieszczonej na orbicie okołoziemskiej. Jest to łatwiejsze, jeśli system został umieszczony na innej orbicie niż cel – może być wtedy zidentyfikowany jako satelita o innym przeznaczeniu. Jeśli obiekt jest stosunkowo niewielki i nie manewruje samodzielnie, może nawet zostać potraktowany jako kosmiczny śmieć. Ukryciu broni antysatelitarnej może sprzyjać wyniesienie jej na orbitę razem z innymi satelitami i oficjalne zgłoszenie tylko „jawnych" satelitów. Ostatnią metodą ukrycia

broni antysatelitarnej jest wystrzelenie jej w sposób skryty. Tej metodzie sprzyja wystrzelenie rakiety nośnej metodami nietypowymi, np. z wykorzystaniem samolotu do wstępnego wyniesienia rakiety zamiast klasycznego startu z kosmodromu.

Jeżeli kategorię broni antysatelitarnej rozszerzymy na kategorię działań antysatelitarnych, które mogą być definiowane jako każdy obiekt lub proces mający możliwości w zakresie niszczenia satelitów lub uczynienia ich nieoperacyjnymi, wyróżnimy działania aktywne oraz pasywne. W tej drugiej kategorii mieszczą się ukrywanie, przemieszczanie i maskowanie aktywów, co do których chcemy, aby pozostały nierozpoznane z kosmosu. Ta kategoria dotyczy więc przede wszystkim działań ukierunkowanychna satelity rozpoznawcze.

Rafał Kopeć

M. Czajkowski, *Anti-Satellite Weapons: A Political Dimension*, „Safety and Defense" 2021, vol. 7, iss. 1; T. Harrison, K. Johnson, J. Moye, M. Young, *Space Threat Assessment 2021*, Center for Strategic & International Studies, Washington 2021; D. Housen-Couriel, *Cybersecurity and Anti-Satellite Capabilities (ASAT). New Threats and New Legal Responses*, „Journal of Law and Cyber Warfare" 2015, vol. 4, iss. 3; R. Kopeć, *Broń antysatelitarna. U progu drugiego etapu militaryzacji kosmosu*, „Politeja" 2018, nr 53/2; M.E. O'Hanlon, *Neither Star Wars nor Sanctuary. Constraining the Military Uses of Space*, Brookings Institution Press, Washington 2004.

BROŃ BIOLOGICZNA (ang. *biological weapons*) – rodzaj → b r o n i m a s o w e g o r a ż e n i a, której ładunkiem bojowym są mikroorganizmy patogenne (np. laseczki wąglika), wirusy (np. wirus ospy prawdziwej), niektóre rodzaje bakterii, grzybów i pasożytów lub toksyny pochodzenia biologicznego (np. botulina, rycyna). Broń ta może być używana do zakażenia ludzi, zwierząt i roślin, a także wykorzystana przeciwko niektórym rodzajom amunicji, sprzętu wojskowego i broni.

Broń biologiczna charakteryzuje się:

- stosunkowo niewielkimi kosztami produkcji – duża część drobnoustrojów potencjalnie użytecznych w broni biologicznej wywołuje choroby wśród zwierząt (laseczka wąglika, pałeczka dżumy i in.);
- dużą skutecznością – drobnoustroje i toksyny są w szczególny sposób preparowane (np. przez modyfikacje genetyczne), aby zwiększyć zdolność do przetrwania w środowisku, wirulencję, śmiertelność, lekooporność;
- słabą wykrywalnością w początkowym etapie ataku oraz możliwością preparowania w szczególny sposób (np. przez modyfikacje genetyczne), aby zwiększyć śmiertelność lub zdolność do przetrwania w środowisku.

Patogeniczność niektórych z tych czynników biologicznych może wynikać z toksycznych substancji, które same wytwarzają. Same toksyny mogą być czasami wydzielone w czystej postaci i używane jako broń. W tym przypadku osiągają one cele ze względu nie na zakażenie, a toksyczność, dlatego należą również do → b r o n i c h e m i c z n e j, nawet jeśli w treści Konwencji o zakazie broni biologicznej

zostały określone jako broń biologiczna. Mikroorganizmy nie są jedynymi formami życia, które mogą wytwarzać toksyny, mogą je wytwarzać wszystkie żywe organizmy. Od 2010 r. roczniki Sztokholmskiego Międzynarodowego Instytutu Badań nad Pokojem SIPRI (Stockholm International Peace Research Institute) zawierają oddzielny rozdział, który jest poświęcony problemom zmniejszenia → z a g r o ż e ń b e z p i e c z e ń s t w a [t. 4] od materiałów chemicznych i biologicznych.

Broni biologicznej używano już w starożytności i była początkowo prosta, gdyż wykorzystywano wszelkie dostępne naturalne środki do zgładzenia przeciwnika. Pierwsze wzmianki na temat użycia broni o charakterze biologicznym pochodzą z VI w. p.n.e., kiedy Asyryjczycy zatruwali studnie sporyszem w celu skażenia żywności swoich wrogów. Z kolei Rzymianie zatruwali wodę pitną swoich wrogów, wrzucając do źródeł padlinę. Tę metodę stosowano zresztą jeszcze w latach 1861–1865 podczas amerykańskiej → w o j n y [t. 4] secesyjnej. Znane są przykłady powszechnego zatruwania strzał toksynami pochodzenia biologicznego oraz podrzucania jadowitych węży na wrogie statki (praktyka Hannibala), a w Chinach podrzucania pszczół nieprzyjaciołom. W rozumieniu ścisłym definicji broni biologicznej, tj. z pominięciem jadów, typowym przykładem z okresu starożytności jest polityka Aleksandra Macedońskiego, który porzucał w czasie wycofywania się z pól bitewnych zwłoki koni i → ż o ł n i e r z y [t. 4] zmarłych na choroby zakaźne. Uznaje się, że po raz pierwszy broni biologicznej użyli w 1346 r. Tatarzy, gdy zaatakowali Kaffę (dzisiejsza Teodozja, Krym), a po nieudanym oblężeniu na teren fortu katapultowali ciała zmarłych na dżumę, co spowodowało rozprzestrzenienie się epidemii w całej Europie.

Do XIX w. stosowanie broni biologicznej ograniczało się do prymitywnej metody zarażania wroga aktualnie grasującą i naturalnie występującą chorobą. Później naukowcy, wśród których czołową pozycję zajmował niemiecki bakteriolog R. Koch, wyizolowali i wyhodowali niektóre bakterie i drobnoustroje. Patogeny i toksyny ostrych chorób epidemicznych o krótkim okresie inkubacji (dżuma, cholera, wąglik), których produkcja rozpoczęła się w latach 20. ubiegłego wieku, zostały przetestowane przez Japończyków na dziesiątkach tysięcy schwytanych Chińczyków podczas II wojny światowej.

Oprócz Japonii także inne państwa kontynuowały badania nad bronią biologiczną, w tym Kanada, Wielka Brytania, Francja, USA i ZSRR. W Wielkiej Brytanii Departament Badań Mikrobiologicznych został utworzony w 1947 r. i rozbudowany w 1951 r., prowadzono w nim badania nad opracowaniem nowych czynników biologicznych i projektowaniem broni. W 1957 r. rząd brytyjski postanowił zrezygnować z ofensywnych badań wojny biologicznej i zniszczyć zgromadzone zapasy. W tym czasie nacisk położono na dalszy rozwój badań nad obroną biologiczną.

Intensywny rozwój broni biologicznej miał miejsce w okresie → z i m n e j w o j n y [t. 4] (przede wszystkim w ZSRR, w którym próbowano np. wykorzystać wirus Ebola). W Zagorsku, mieście oddalonym o 70 km od Moskwy, powstało wojskowe

centrum badań nad bronią biologiczną. W latach 50. prowadzono tam badania nad szeregiem różnych drobnoustrojów. Od 1974 r. Sowieci prowadzili badania nad bronią biologiczną w Swierdłowsku. Kompleks „Biopreparat" działał pod przykrywką komercyjnych badań biotechnologicznych, nieoficjalnie eksperci pracowali nad doskonaleniem broni biologicznej. Raporty dotyczące badań ofensywnych ZSRR wielokrotnie pojawiały się w latach 60. i 70. XX w., chociaż oficjalnie ZSRR twierdził, że nie posiada żadnej broni biologicznej ani chemicznej. Broń biologiczna i jej komponenty są tańsze i niekiedy skuteczniejsze od broni jądrowej lub broni chemicznej. Oprócz bezpośrednich strat ludzkich broń biologiczna przynosi inny znaczący skutek – może wywołać panikę na dużą skalę. Szkodliwe działanie broni biologicznej oparte jest na wykorzystaniu właściwości głównie chorobotwórczych patogenów i toksycznych produktów ich życia. Po przedostaniu się do organizmu człowieka lub zwierzęcia w bardzo małych ilościach patogenne drobnoustroje i ich toksyczne produkty prowadzą do bardzo poważnych chorób, które kończą się w przypadku braku natychmiastowej reakcji długotrwałym leczeniem lub śmiercią. Uderzające działanie broni biologicznej nie objawia się natychmiast, ale po pewnym czasie (po okresie inkubacji). Zależy to od rodzaju i ilości zarazków lub toksyn, które są uwięzione w ciele, a także stanu fizycznego osoby. Najczęściej okres inkubacji trwa 2–5 dni. W tym czasie ludzie zachowują zdolność do pracy. Niektóre choroby powodowane przez wirusy (ospa, dżuma) mogą być następnie przekazywane zdrowym osobom drogą kropelkową, przenoszone przez owady lub rozprzestrzeniane innymi drogami. Broń biologiczna ma silny wpływ psychologiczny na ludzi.

Z badań przeprowadzonych przez → Ś w i a t o w ą O r g a n i z a c j ę Z d r o w i a [t. 4] (World Health Organization, WHO) jeszcze w 1970 r. wynika, że rozpylenie z samolotu 50 kg zarodników wąglika nad terenem zamieszkałym przez 5 mln osób doprowadzić może do zachorowania 250 tys., z których 100 tys. umrze. Cechami środków biologicznych warunkującymi ich skuteczność są: wysoka śmiertelność (np. w przypadku wąglika ok. 80%, gorączki krwotocznej Ebola ok. 76%); łatwość uzyskania i produkcji masowej; mała masa cząsteczek ułatwiająca dyspersję (1–5 mm) w formie aerozolu; możliwość zakażenia przez kontakt bezpośredni; brak skutecznego leczenia; brak szczepionki.

Nowoczesne środki transportu i nowe technologie przenoszenia dużej liczby osób lub towarów drogą powietrzną, lądową i morską znacząco zintensyfikowały procesy rozprzestrzeniania się infekcji i ich wektorów w niemal wszystkich krajach. Ekspansja w międzynarodowym handlu i przepływ osób między kontynentami zwiększają prawdopodobieństwo rozprzestrzeniania się chorób zakaźnych, zwłaszcza w przypadku krótkiego okresu inkubacji i transmisji w powietrzu. Nawet najmniejsza epidemia będzie znacznie bardziej skuteczna niż jakakolwiek dobrze zaplanowana i przeprowadzona operacja wojskowa. Do rozsiewu patogenów mogą być wykorzystywane: aerozole biologiczne (np. w celu wprowadzenia patogenów do wentylacji i klimatyzacji);

naturalni przenosiciele zarazków (zakażone owady, szczury itp.); zanieczyszczona woda i żywność (→ t e r r o r y z m [t. 4] hipermarketowy); podrzucone i wysyłane zakażone przedmioty i przesyłki.

Mnogość sposobów przenoszenia utrudnia przeciwdziałanie, a także odnajdywanie źródła pochodzenia zakażenia. Drogą wtargnięcia chorobotwórczego patogenu mogą być m.in. drogi oddechowe, skóra i przewód pokarmowy. Drobnoustroje chorobotwórcze w razie wystąpienia ataku bioterrorystycznego mogą być rozprzestrzeniane za pomocą wiatru. W razie rozpylenia w postaci aerozolu są w stanie przenosić się na duże odległości. Zarazkami mogą być zakażeni także nosiciele (np. wszy, pchły, myszy, szczury), z których chorobotwórcze drobnoustroje przemieszczają się bezpośrednio na ludzi lub wodę i żywność.

Obecnie największym → z a g r o ż e n i e m [t. 4] ze strony broni biologicznej jest łatwość produkcji nowych toksyn roślinnych i bakteryjnych do celów zbrodniczych; są one wytwarzane technikami biologii molekularnej, które oddziałują na cechy genetyczne organizmów. Zmiany w środowisku naturalnym ułatwiają rozpylanie oraz zwiększają zdolność wnikania i namnażania się patogenów w zainfekowanych organizmach. Tak np. jesienią 2001 r. po ataku na World Trade Center w USA doszło do licznych ataków bioterrorystycznych z wykorzystaniem laseczek wąglika. Rozesłano wówczas przesyłki pocztowe do ważnych instytucji rządowych i mediów skażone przetrwalnikami wąglika (tzw. listy wąglikowe). U 10 osób zakażonych rozpoznano postać płucną wąglika, a u 11 postać skórną. Spośród chorych na postać płucną zmarły 4 osoby. Wydarzenia te spotęgowały ogromną panikę wśród → o p i n i i p u b l i c z n e j [t. 3]. Nowa forma → b i o t e r r o r y z m u zastosowana na oczach całego świata otworzyła nowy rozdział w wieloletniej historii wojen biologicznych, stawiając społeczeństwa w obliczu niezwykłego zagrożenia na progu III tysiąclecia.

W 1925 r., zgodnie z protokołem genewskim, użycie broni biologicznej w trakcie działań wojennych zostało zabronione. Jednak Włochy, Francja, Niemcy i ZSRR nadal przeprowadzały badania nad tego rodzaju bronią. Pierwszy światowy dokument regulujący stosowanie broni masowego rażenia został podpisany w maju 1972 r. Konwencja o zakazie stosowania broni biologicznej nie tylko zabroniła użycia broni biologicznej w czasie wojny, ale także zakazała prac nad nią, produkcji, gromadzenia zapasów, nabywania, przechowywania, przekazywania i używania broni biologicznej przez kogokolwiek. Sam dokument nie rozwiązał problemu, gdyż postanowienia konwencji były łamane od początku przez ZSRR, który przez wiele lat prowadził utajoną, nielegalną działalność. Trudno również przypuszczać, aby terroryści uszanowali postanowienia międzynarodowej konwencji. Ponadto w przeciwieństwie do konwencji o broni chemicznej w traktacie brakuje procedur weryfikacji i zgodności, nie ma też organu wdrażającego, który monitorowałby przestrzeganie przepisów. Kongres USA uchwalił ustawę antyterrorystyczną o broni biologicznej w 1989 r. w celu wdrożenia konwencji.

Państwa, które podpisały konwencję, formalnie dokonały przeglądu funkcjonowania broni biologicznej podczas pięcioletnich konferencji rewizyjnych, które odbyły się w latach 1980, 1986, 1991, 1996, 2001/2002, 2006, 2011 i 2016. Podczas tych konferencji państwa potwierdziły, że zakres konwencji rozciąga się na nowe osiągnięcia naukowe i technologiczne, a także zainicjowały wymianę danych budujących zaufanie w celu zwiększenia przejrzystości i wzmocnienia konwencji.

Broń biologiczna jest znacznie tańsza niż → b r o ń n u k l e a r n a i chemiczna, stosunkowo niewielka ilość czynnika biologicznego może spowodować względnie dużą liczbę zgonów – podobnie do broni nuklearnej. Nie wymaga skomplikowanych systemów dostarczania, a jej łatwość produkcji rośnie wraz z postępem nauki. Biorąc pod uwagę względną przystępność cenową, skuteczność i elastyczność, broń biologiczna jest coraz częściej uważana za atrakcyjną opcję przez podmioty niepaństwowe, co sprawia, że bioterroryzm to jedno z głównych zagrożeń związanych z tego rodzaju bronią. Zastosowanie środków biologicznych w celu wymuszenia wyeliminowania uprawy narkotyków jest promowane przez USA, zwłaszcza w Kolumbii.

Gwałtowny rozwój biologii syntetycznej podniósł ryzyko dotyczące nowej generacji broni biologicznej, jak wynika z najnowszego amerykańskiego raportu. Postępy w tej dziedzinie oznaczają, że naukowcy mają teraz możliwość odtwarzania niebezpiecznych wirusów od zera, mogą także uczynić szkodliwe bakterie bardziej śmiercionośnymi albo modyfikować drobnoustroje, aby wydzielały śmiertelne toksyny po wejściu do organizmu. Te 3 scenariusze zostały wskazane jako zagrożenie najbardziej niepokojące w opublikowanym przez Narodową Akademię Nauk USA (National Academy of Sciences, NAS) raporcie z 2018 r. Opisano w nim, w jaki sposób biologia syntetyczna, która daje naukowcom precyzyjne narzędzia do manipulowania żywymi organizmami, „poprawia i rozszerza" możliwości tworzenia broni biologicznej.

Raport z 2019 r. przygotowany przez naukowców z Uniwersytetu w Cambridge (Centre for the Study of Existential Risk, CSER) zwraca uwagę na fakt, że znalezienie się broni biologicznej w niepowołanych rękach może spowodować rozwój patogenów i toksyn, które rozprzestrzeniałyby się w powietrzu, żywności i zbiornikach wodnych, stanowiąc tym samym śmiertelne zagrożenie dla człowieka. Technologia staje się coraz bardziej wyrafinowana, a koszty coraz niższe, co wpływa na zwiększanie zdolności broni do wyrządzania szkód. Autorzy ostrzegli, że konsekwencje zbudowania inteligentnej broni biologicznej, która byłaby w stanie samodzielnie siać spustoszenie, mogłyby być katastrofalne.

W ciągu następnej dekady 2 trendy będą dominować w dziedzinie bezpieczeństwa biologicznego, kształtując zarówno szanse, jak i zagrożenia. Pierwszym z nich jest uprzemysłowienie, ponieważ biotechnologia staje się globalnie ważną bazą produkcyjną i siłą ekonomiczną. Drugim jest personalizacja, ponieważ coraz więcej osób może wykorzystać nauki biologiczne do własnych celów. Istotny wpływ będą miały

zasady i przepisy regulujące tę dziedzinę. Bezpieczeństwo będzie również głównym problemem, ponieważ żadne laboratorium nie jest całkowicie wolne od wypadków; niezbędne jest zmniejszenie ryzyka dla pracowników laboratoriów i społeczeństwa, ustanowienie protokołów, stosowanie sprzętu ochronnego i podniesienie politycznego profilu bezpieczeństwa biologicznego.

Aby sprostać → w y z w a n i u b e z p i e c z e ń s t w a [t. 4] biologicznego, konieczne będzie również posiadanie systemów opieki zdrowotnej, które mogą szybko reagować na epidemie.

Pandemie są tak stare jak ludzkość, ale w dzisiejszym, połączonym świecie jesteśmy bardziej narażeni niż kiedykolwiek. Wzrost zdolności i rozprzestrzeniania się biotechnologii stwarza nowe zagrożenia, od przypadkowego uwolnienia do celowego niewłaściwego użycia.

Sergiusz Wasiuta

Y. Alexander, M. Hoenig, *Superterroryzm biologiczny, chemiczny i nuklearny*, tłum. R. Stiller, Bellona, Warszawa 2001; D. Avery, *Pathogens for War: Biological Weapons, Canadian Life Scientists, and North American Biodefence*, University of Toronto Press, Toronto 2013; M. Binczycka-Anholcer, A. Imiołek, *Bioterroryzm jako jedna z form współczesnego terroryzmu*, „Hygeia Public Health" 2011, nr 3; *Bioterroryzm – zagrożenia, przeciwdziałanie*, Ośrodek Prawa Europejskiego, Warszawa 2003; S. Chauhan, *Biological Weapons*, APH, New Delhi 2004; CSER, *Managing Global Catastrophic Risks. Part 1: Understand*, 13.08.2019, CSER.ac.uk (dostęp 10.02.2020); J. Guzy, *Broń biologiczna – charakterystyka i zagrożenia*, „Biuletyn Stowarzyszenia Higieny i Lecznictwa" 2001, nr 4; D. Harmon, *Chemical and Biological Weapons: Agents of War and Terror*, The Rosen Publishing Group, New York 2009; J. Kalenik, *Bioterroryzm – zagrożenie XXI wieku*, Centralny Ośrodek Szkolenia Straży Granicznej, Koszalin 2003; P. Kępka, *Bioterroryzm. Polska wobec użycia broni biologicznej*, Difin, Warszawa 2009; K. Langbein, C. Skalnik, XI. Smolek, *Bioterroryzm*, tłum. M. Chudzik, Muza, Warszawa 2003; B. Michailiuk, *Broń biologiczna i bioterroryzm*, „Zeszyty Naukowe AON" 2016, nr 1 (102); tenże, *Broń biologiczna jako zagrożenie bezpieczeństwa państwa*, AON, Warszawa 2015; tenże, *Broń biologiczna*, AON, Warszawa 2004; S.K. Prasad, *Biological Weapons*, Discovery Publishing House, New Delhi 2009; I. Sample, *Synthetic Biology Raises Risk of New Bioweapons, US Report Warns*, 19.06.2018, TheGuardian.com (dostęp 10.02.2020); G.C. Satpathy, *Biological Weapons and Terrorism*, Gyan Publishing House, Delhi 2004; M. Stojek, *Współczesne zagrożenia bronią biologiczną – bioterroryzm*, „Medycyna Ogólna" 2008, nr 2; S. Wasiuta, *Broń biologiczna*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; K. Zieliński i in., *Patologia obrażeń i schorzeń wywołanych współczesną bronią w działaniach wojennych i terrorystycznych*, MON, Warszawa–Bydgoszcz 2010; Л.А. Фёдоров, *Советское биологическое оружие: История, экология, политика*, МСоЭС, Москва 2005.

BROŃ CHEMICZNA (BCH) – broń, w której podstawowym czynnikiem rażącym jest związek chemiczny o właściwościach toksycznych. Oprócz samego czynnika rażącego (bojowego środka trującego, BST), termin BCh obejmuje urządzenia i sposoby jego przenoszenia na polu walki. Wyróżniamy:

- bojowe środki trujące (głównie gazy lub ciecze lotne);
- bojowe środki pomocnicze:

- zapalające,
- defolianty – substancje chemiczne powodujące zrzucanie liści przez rośliny, stosowane w celach wojskowych z uwagi na użyteczność w zakresie odsłaniania obiektów ukrytych wśród roślinności,
- lakrymatory – środki drażniące błony śluzowe rogówki i spojówki oka, stosowane głównie przez służby porządku publicznego.

Należy zaznaczyć, że zaliczenie bojowych środków pomocniczych w obręb BCh jest przedmiotem kontrowersji. BCh w ścisłym znaczeniu tego terminu to broń, której działanie jest skutkiem toksycznych właściwości związków chemicznych, czyli bojowych środków trujących, a nie np. spalania czy wybuchowego rozkładu substancji chemicznej jak w przypadku środków zapalających (takie działanie jest wszakże typowe dla wielu rodzajów broni konwencjonalnej). Druga kontrowersja związana ze środkami pomocniczymi odnosi się do konwencji o broni chemicznej z 1993 r., która wyłączyła gazy łzawiące, o ile nie są wykorzystywane jako środki walki, z obrębu BCh.

W ramach BCh mieszczą się:

- środki walki – toksyczne środki chemiczne, których działanie rażące polega głównie na biochemicznym oddziaływaniu bojowych środków trujących ze składnikami żywego organizmu, czego następstwem są porażenia stanu osobowego prowadzące do utraty zdolności bojowej;
- środki przenoszenia, tj:
  - amunicja i urządzenia zaprojektowane do spowodowania śmierci lub szkody poprzez toksyczne właściwości środków chemicznych,
  - sprzęt zaprojektowany do użycia w bezpośrednim związku ze stosowaniem amunicji i urządzeń.

Cechą charakterystyczną BCh jest śmiertelne lub szkodliwe działanie na organizmy żywe. Zatrucie żywego organizmu następuje poprzez wniknięcie bojowego środka trującego do jego wnętrza. Drogami przenikania (wrotami skażenia) mogą być: układ oddechowy, skóra, błony śluzowe, przewód pokarmowy, otwarte rany. Działanie BCh polega na reakcji chemicznej ze składnikami żywego organizmu, w której wyniku dochodzi do zaburzenia niektórych procesów biochemicznych.

Biorąc pod uwagę mechanizm toksycznego działania, bojowe środki trujące możemy podzielić na kilka kategorii. Należą do nich środki:

- drażniące,
- parzące (nekrozujące),
- duszące,
- paralityczno-drgawkowe,
- psychotoksyczne,
- ogólnotrujące.

Niektóre bojowe środki trujące charakteryzują się kompleksowym działaniem toksycznym, łączącym kilka kategorii.

Biorąc pod uwagę właściwości bojowe (użytkowe) BST, możemy podzielić je na:
- uśmiercające (letalne),
- obezwładniające (powodujące przejściową niezdolność do działania),
- nękające (utrudniające prowadzenie działań).

Inne kryteria podziału BCh to czas działania w terenie (materiały nietrwałe – lotne; materiały trwałe – zdolne do skażenia danego terenu) oraz czas, po którym występują objawy działania danego środka (środki szybkodziałające, np. cyjanowodór; środki wolnodziałające, np. fosgen). Pierwsze udokumentowane użycie BCh miało miejsce ok. 600 r. p.n.e. podczas oblężenia miasta Kyrra w Grecji. Atakujący zatruli wodę korzeniem ciemiernika białego. Był to więc atak z pogranicza wykorzystania BCh i → b r o n i b i o l o g i c z n e j (w pewnych przypadkach ustalenie precyzyjnej linii podziału między tymi rodzajami broni jest utrudnione). Nowoczesne zastosowanie BCh datuje się od I wojny światowej.

Pierwszy atak chemiczny przeprowadzony został przez wojska francuskie w sierpniu 1914 r. (zastosowano granaty z bromoacetonem, wystrzeliwane z karabinów), natomiast pierwszy skuteczny atak chemiczny miał miejsce 22 kwietnia 1915 r. pod Ypres. Użycie przez wojska niemieckie chloru spowodowało porażenie ok. 5 tys. osób. W okresie międzywojennym BCh zastosowali Brytyjczycy przeciwko bolszewikom (1919), ZSRR w czasie tłumienia powstania tambowskiego (1921), Hiszpanie przeciwko rebeliantom w Maroku (1922–1927), Włosi podczas walk w Abisynii (1936) oraz Japończycy w Chinach (1938–1939).

W czasie II wojny światowej użycie BCh na polu walki ograniczyło się do chińsko-japońskiego teatru działań (od 1937 do co najmniej 1942 r.). Podczas → w o j n y [t. 4] w Wietnamie wojska amerykańskie stosowały substancje chemiczne w 2 celach. Pierwszym z nich było niszczenie roślin (ogołacanie drzew z liści w celu pozbawienia partyzantów możliwości ukrywania się w dżungli oraz niszczenie upraw ryżu), drugim działanie obezwładniające (nieletalne). Kwestia uznania takich działań za stosowanie BCh jest kontrowersyjna.

BCh stosowana była podczas wojny iracko-irańskiej. Na skalę masową BCh używała strona iracka, a w znacznie mniejszym stopniu Iran. Irak zastosował również BCh podczas tłumienia powstania kurdyjskiego. Wykorzystano ją także w czasie → w o j n y d o m o w e j [t. 4] w Syrii. Najpoważniejszy atak gazowy miał miejsce 21 sierpnia 2013 r. w Ghucie. W raporcie inspektorów ONZ nie wskazano jednak jednoznacznie jego sprawców. W 2015 r. podczas walk w pobliżu Irbilu w Iraku dżihadyści (→ d ż i h a d [t. 2]) z → P a ń s t w a I s l a m s k i e g o [t. 3] przypuszczalnie użyli iperytu przeciwko bojownikom kurdyjskim. BCh stosowana była także do przeprowadzenia ataków terrorystycznych. Najpoważniejszy atak miał miejsce 20 marca 1995 r., kiedy sekta Aum Shinrikyō zaatakowała tokijskie metro przy użyciu sarinu, co spowodowało śmierć 12 osób i poważne zatrucia u blisko 6 tys.

Rafał Kopeć

F. Brown, *Chemical Weapons. A Study in Restraints*, Routledge, New York 2005; E. Croddy, C. Perez-Armendariz, J. Hart, *Broń chemiczna i biologiczna – raport dla obywatela*, tłum. Z. Witkiewicz i in., Wydawnictwa Naukowo-Techniczne, Warszawa 2003; P. Durys, *Broń chemiczna. Działania na rzecz zakazu i eliminacji*, AON, Warszawa 2009; L. Konopski, *Historia broni chemicznej*, Bellona, Warszawa 2009; R. Kopeć, *Broń chemiczna*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; tenże, *Broń chemiczna – historia i perspektywy zastosowania we współczesnych konfliktach zbrojnych*, [w:] *Bezpieczeństwo w nowych czasach*, Z. Kwiasowski, K. Pabis-Cisowska, M. Pietrzyk (red.), Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2016; T. Kubaczyk, *Broń chemiczna i biologiczna we współczesnym świecie*, AON, Warszawa 2016; D. Michalski, A. Kowalewska, *Broń chemiczna jako narzędzie terroru*, [w:] *Terroryzm wobec środowiska potencjalnym zagrożeniem współczesnych czasów – wybrane zagadnienia*, E. Zębek, N. Kulbacka-Burakiewicz (red.), Kortowski Przegląd Prawniczy Monografie, Olsztyn 2017.

BROŃ EKOLOGICZNA / BROŃ BIOSFERYCZNA (ang. *ecological weapon*) – jeden z rodzajów → b r o n i g e o f i z y c z n e j, która polega na zastosowaniu na dużą skalę chemiczno-biologicznego, termicznego lub mechanicznego uszkodzenia krytycznych elementów środowiska naturalnego wroga. Z punktu widzenia specjalistów wojskowych środowisko naturalne przeciwnika należy traktować w całości, uwzględniając biosferę, technosferę i → i n f o s f e r ę [t. 2]. Broń ekologiczna pierwotnie przeznaczona była do uderzenia w kluczowe segmenty biosfery, zasoby której są ograniczone, nie zawsze odnawialne, a mają zasadnicze znaczenie dla przetrwania człowieka jako gatunku. W takim ujęciu broń ekologiczna należy do kategorii broni masowej zagłady i jest często uważana za jedną z najbardziej niebezpiecznych broni. Charakterystyczne konsekwencje zastosowania broni ekologicznej to niszczenie lasów, upraw rolniczych i pastwisk, zanieczyszczenie powietrza, wody i gleby. Skutki wykorzystania broni ekologicznej mogą mieć nieodwracalny charakter: w wyniku wyniszczenia lasów zmniejsza się populacja flory i fauny, zmienia się tryb wodny, intensyfikuje się erozja żyznej gleby, co może prowadzić do niepożądanej zmiany lokalnego klimatu.

Należy podkreślić, że termin „broń ekologiczna" oznacza broń stworzoną specjalnie do niszczenia przyrody. Właśnie przeznaczenie i charakter wpływu na cel odróżniają ją od innych rodzajów broni. Broń ekologiczna jest stworzona w celu bezpośredniego działania na elementy środowiska naturalnego, by je zniszczyć lub naruszyć mechanizm interakcji z innymi komponentami środowiska. Na człowieka taka broń oddziałuje z reguły pośrednio, poprzez zniszczenie środowiska naturalnego. Zwykłe rodzaje broni i sprzętu wojskowego lub → b r o n i m a s o w e g o r a ż e n i a przeznaczone są przede wszystkim do niszczenia człowieka i technosfery. Środowisko przy wykorzystaniu takiej broni jest niszczone jako cel poboczny (np. w przypadku użycia broni jądrowej).

Za symboliczną datę pojawienia się broni ekologicznej można uznać 30 listopada 1961 r., gdy prezydent USA J.F. Kennedy podjął decyzję o wykorzystywaniu na szeroką skalę fitotoksycznych preparatów i innych środków niszczenia środowiska

naturalnego w trakcie operacji wojskowych w Indochinach. Specjalnie zaprojektowana operacja Ranch Hand została ukierunkowana na zniszczenie środowiska naturalnego. Jej celem było zniszczenie zasobów naturalnych półwyspu, co osiągnięto przez zastosowanie standardowych i niestandardowych, specjalnie zaprojektowanych rodzajów broni ekologicznej i sprzętu wojskowego.

Amerykańskie siły zbrojne w czasie działań bojowych w Azji Południowo-Wschodniej w latach 60. XX w. wykorzystywały broń ekologiczną, stosowano herbicydy i defolianty w lasach i na gruntach ornych, próbując pozbawić Wietkong żywności i osłony roślinności. Rozpylono ponad 100 tys. ton herbicydów i defoliantów do niszczenia roślinności wzdłuż dróg, kanałów i linii przesyłowych w celu ułatwienia prowadzenia zwiadu lotniczego, fotografowania terenu, niszczenia różnego rodzaju broni znajdującej się w lasach. W rezultacie skażono ok. 43% ogólnej powierzchni gruntów rolnych w Wietnamie Południowym i 44% powierzchni lasów. Wszystkie użyte środki okazały się toksyczne dla ludzi i zwierząt, w wyniku czego ponad 7 mln ludzi zmuszonych zostało opuścić obszary stosowania broni ekologicznej. Wynikiem jej użycia było uwilgotnienie gruntów rolnych i wylesienie dużych obszarów, co spowodowało naruszenie naturalnej równowagi ekosystemów.

Można wyodrębnić określone kierunki tworzenia różnych rodzajów broni ekologicznej, mających odmienne źródła energii i mechanizmy oddziaływania na środowisko, ale wspólny cel – naruszenie równowagi ekologicznej. Do takich kierunków zaliczamy m.in.:

- generowanie klęsk żywiołowych (wywoływanie trzęsień ziemi, lawin i osuwisk, zmian przepływu rzek, wywołanie niszczących huraganów i burz z nadaniem ich trajektoriom określonego kierunku, powodzi, tajfunów, sztuczne tworzenie tsunami itp.);
- inicjowanie zjawisk fizycznych (pobudzanie aktywności wulkanicznej, lawin, silnych opadów lub ich znacznego zmniejszenia przez wysiew w chmurach odczynników chemicznych);
- lokalne zmiany klimatu (np. tworzenie dziur ozonowych);
- modyfikacja warunków pogodowych;
- zniszczenie źródeł (a nawet rezerw) zasobów naturalnych;
- tworzenie nowych sposobów niszczenia flory i fauny.

Często jednak nawet najprostsze sposoby wpływania na naturę wykorzystywane w konflikcie zbrojnym mogą mieć bardzo negatywny wpływ na pozycję jednej z przeciwnych stron. Na przykład Irak używał broni ekologicznej podczas ośmioletniej → w o j n y [t. 4] z Iranem: zmienił bieg rzek i podpalił obszary bagienne, aby stworzyć bariery dla wojsk irańskich. Podpalanie szybów naftowych, przeprowadzone w 1991 r. przez wojska irackie podczas I wojny w Zatoce Perskiej, oprócz ogromnego zniszczenia środowiska naturalnego doprowadziło do zniszczenia wcześniej kwitnącej gospodarki Kuwejtu.

Od ok. 1986 r. w sowieckich tekstach wojskowych pojawiają się odniesienia do „broni ekologicznej", wskazała na nie I. Kass, pracownik National War College w Waszyngtonie, zwracając także uwagę na wydanie w 1989 r. 399-stronicowego podręcznika *Obrona przed bronią masowego rażenia* w języku rosyjskim, którego 100 tys. egzemplarzy trafiło do wykorzystania przez wojsko radzieckie jako materiał referencyjny. W tej książce gen. W. Miasnikow napisał, że możliwe jest „wykorzystanie niszczycielskich sił występujących w naturze do celów wojskowych", mianowicie powodzi i zanieczyszczeń, które zakłócają nawigację, uniemożliwiają nawadnianie i zaburzają działanie rozmaitych hydrostruktur, a także tworzą przeszkody w rzekach, kanałach i innych zbiornikach wodnych.

Istnieje wiele historycznych precedensów dotyczących wykorzystania środowiska jako broni. Na przykład w 1938 r. podczas II wojny chińsko-japońskiej wojska pod rządami Czang Kaj-szeka wysadziły w powietrze groble powstrzymujące Huang He (Rzekę Żółtą) w Huayankou w prowincji Henan w celu powstrzymania nadciągających wojsk japońskich. Spowodowało to zalanie obszaru obejmującego 54 tys. km² i śmierć 500–900 tys. osób. Kolejne 11 mln pozostało bez jedzenia i schronienia. Groblа została naprawiona z pomocą Amerykanów w 1947 r.

Sporządzony w 1977 r. protokół pierwszy dodatkowy do Konwencji genewskich z 12 sierpnia 1949 r., dotyczący ochrony ofiar międzynarodowych konfliktów zbrojnych w art. 35 podkreśla:

> Zabronione jest stosowanie metod i środków prowadzenia wojny, których celem jest wywoływanie rozległych, długotrwałych i poważnych szkód w środowisku naturalnym lub po których można oczekiwać, że takie szkody wywołają.

Analizując konflikty takie jak I wojna w Zatoce Perskiej, należy wskazać, że ani USA, ani Irak nie ratyfikowały tego protokołu.

Posiadanie broni ekologicznej sprawi, że właśnie ona będzie w XXI w. potężnym czynnikiem → z a g r o ż e ń [t. 4] geopolitycznych i pozwoli w warunkach zwiększonego zużycia zasobów naturalnych (bez stosowania bezpośredniej → p r z e m o c y [t. 3]) dość pewnie kontrolować najbogatsze źródła zasobów naturalnych, a także zarządzać procesami biosferycznymi na rozległych obszarach.

Sergiusz Wasiuta

W.A. Buckingham, *Office of Air Force History*, United States Air Force, Washington 1982; S. Bull, *Encyclopedia of Military Technology and Innovation*, Greenwood Press, Westport 2004; *Ecological Risks Associated with the Destruction of Chemical Weapons: Proceedings of the NATO ARW on Ecological Risks Associated with the Destruction of Chemical Weapons*, V.M. Kolodkin, W. Ruck (eds.), Springer, New York 2006; M.C. Fitzgerald, *Weapons Based on New Physical Principles*, [w:] *Managing the Revolution in Military Affairs*, R. Matthews, J. Treddenick (eds.), Springer, New York 2001; G.E. Machlis, T. Hanson, *Warfare Ecology*, „BioScience" 2008, vol. 58, no. 8; Protokoły dodatkowe do Konwencji genewskich z 12 sierpnia 1949 r., dotyczący ochrony ofiar międzynarodowych konfliktów zbrojnych (Protokół I) oraz dotyczący ochrony ofiar niemiędzynarodowych konfliktów zbrojnych (Protokół II),

sporządzone w Genewie dnia 8 czerwca 1977 r., Dz. U. 1992, nr 41, poz. 175; J.P. Robinson, *The Effects of Weapons on Ecosystems*, Elsevier, Springer, 2013; D. Vallero, *Biomedical Ethics for Engineers: Ethics and Decision Making in Biomedical and Biosystem Engineering*, Academic Press, New York 2011; A. Vayda, *War in Ecological Perspective: Persistence, Change, and Adaptive Processes in Three Oceanian Societies*, Springer, New York 2012; *Warfare Ecology: A New Synthesis for Peace and Security*, G.E. Machlis (ed.), Springer, New York 2011; S. Wasiuta, *Broń ekologiczna*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; A. Westing, *Ecological Effects of Military Defoliation on the Forests of South Vietnam*, „BioScience" 1971, vol. 21, no. 17; A.L. Young, *The History, Use, Disposition and Environmental Fate of Agent Orange*, Springer, New York 2009; В.А. Лисичкин, Л.А. Шелепин, *Экологическое оружие*, [w:] *Глобальная империя Зла. Новая геополитическая расстановка сил*, Крымский мост-9Д, Москва 2001; Г.П. Маскин, Т.М.Волкова, *Нелетальные виды оружия*, Варб, Минск 1996; Г.П. Маскин, Т.М. Волкова, *Новые виды оружия*, Мввиу, Минск 1994; Г.П. Маскин, Т.М. Волкова, *Современное оружие на новых физических принципах*, ВАРБ, Минск 1998; Д. Рогозин, *Экологическая борьба в войне*, [w:] *Война и мир в терминах и определениях*, Д. Рогозин (ред.), Вече, Москва 2016; В.И. Слипченко, *Войны шестого поколения*, Вече, Москва 2002; Г.С. Черных, А.С. Старостин, *Оружие на новых физических принципах, проблемы защиты населения и территорий от его поражающих факторов*, „Стратегия гражданской защиты: проблемы и исследования" 2015, Т. 5, № 2; *Экологический энциклопедический словарь*, Главная редакция Молдавской советской энциклопедии, И.И. Дедю, Кишинев 1989.

BROŃ DEMOGRAFICZNA – broń „D" (ang. *Demographic Bombing*) ewentualnie: broń masowej migracji (ang. *Weapon of Mass Migration*), → t a k t y k a wykorzystania dużej grupy cywilów (również przemieszczających się – strumień migracyjny), świadomych lub nieświadomych nadanej im funkcji, jako broni do osiągnięcia celów strategicznych poprzez doprowadzenie do zmian w strukturze demograficznej zaatakowanego aktora, prowadzących do wytworzenia niepokojów wewnętrznych, → w o j n y d o m o w e j [t. 4], obniżenia wartości sojuszniczej, zmniejszenia potencjału obronnego, → w o j n y i n f o r m a c y j n e j [t. 4], a także – do trwałej zmiany tożsamości kulturowej.

Sam termin jeszcze nie przyjął się powszechnie w nauce. Jednym z pierwszych przypadków użycia takiego sformułowania były słowa wypowiedziane przez profesor Marthę Minow z Harvard Law School's, dotyczące → k r y z y s u [t. 2] w Kosowie z 1999 r.: „istota wojny się zmieniła, teraz emigranci są wojną".

Wykorzystanie zjawisk demograficznych możemy rozpatrywać w kilku podstawowych wymiarach.

1. **Zaborczość** – klasa zdarzeń, obejmująca zarówno migracje w celu przywłaszczenia terytorium lub mienia, jak i eliminacja innej grupy lub grup uważanych jako → z a g r o ż e n i e [t. 4] dla etnopolitycznej lub ekonomicznej dominacji sprawców (jest to element czystki etnicznej).

Przykłady: „Zielony Marsz" króla Maroka Hassana II z 1975 r. na sporne terytoria Sahary Hiszpańskiej, → l u d o b ó j s t w o [t. 2] jazydów w Iraku.

2. **Wydalanie** – przesiedlenia podejmowane albo w celu umocnienia wewnętrznej polityki poprzez wydalanie dysydentów politycznych i innych wewnętrznych przeciwników (banicja), albo do wywołania problemu, a nawet dążenie do destabilizacji drugiego aktora.

   Przykłady: wydalenie rodziny Brutusa z Rzymu, przesiedlenie Kartagińczyków, wspieranie przez Rosję migracji muzułmanów do Europy,konflikt w Rwandzie.
3. **Zmilitaryzowanie** – zwykle w trakcie aktywnego konfliktu, w celu: uzyskania przewagi militarnej nad przeciwnikiem – poprzez zakłócenie lub zniszczenie procesu dowodzenia, logistyki lub zdolności manewrowania (dostępność polityczna teatru działań), jak również wzmacnianie własnej struktury siłowej poprzez nabywanie dodatkowej (czasem przymusowo) siły roboczej zasobów.

   Przykłady: przesiedlenia ludności pochodzenia niemieckiego w czasie II wojny światowej w głąb ZSRR, przesiedlenia ludności arabskiej z regionu działań Kurdów w Syrii.
4. **Przymus** – klasa zdarzeń, w których jako narzędzie polityki zagranicznej wykorzystuje się (rzeczywiste lub zagrożone) wpływy – w celu wywołania (lub zapobieżenia) zmianom w zachowaniu politycznym lub uzyskania korzyści od aktora dotkniętego odpływem lub przypływem ludności, często dzięki wojnie informacyjnej.

   Przykłady: zezwolenie na migracje na terytorium Unii Europejskiej przez Turcję, zatrzymanie fali migracyjnej za zgodę UE na wzmacniający się autorytaryzm i na zaangażowanie Turcji w Syrii.
5. → **P i ą t a k o l u m n a** [t. 3] odnosi się do długoterminowej → s t r a t e g i i [t. 4], w której agresor wysyła migrantów na terytorium docelowe (lub pozyskuje już znajdujących się tam migrantów), aby zdestabilizować sytuację lub przejąć kontrolę. Agresor może wykorzystać również swoich sympatyków lub grupy etniczne bądź religijne znajdujące się na terytorium aktora, często powiązane z agresorem.

   Przykłady: Chińczycy na Tajwanie, Rosjanie na Krymie, potencjalnie Rosjanie w państwach bałtyckich.
6. **Ekonomiczny** – aktor wykorzystuje napływ lub odpływ migrantóww celu uzyskania korzyści ekonomicznych.

   Przykłady: pracownicy wysyłani przez Koreę Północną do pracy zagranicą, import siły roboczej do państw Zatoki Perskiej, wymuszenie przez Turcję pomocy ekonomicznej w zamian za uszczelnienie granic.
7. **Polityczny** – szereg działań mających na celu wykorzystanie narzędzi charakterystycznych dla polityki wewnętrznej do destabilizacji podmiotu zewnętrznego poprzez zastąpienie go w jego prerogatywach, np. nadawanie obywatelstwa innego niż dotychczasowe zewzględu na miejsce zamieszkania.

   Przykłady: uznanie separatystycznych republik przez Rosję na terenie Gruzji (Osetia Południowa). Nadanie obywatelstwa rosyjskiego mieszkańcom Krymu i Donbasu.

Poszczególne taktyki mogą być łączone: przykładem jest działalność Rosji, która od wielu lat wykorzystuje zjawiska demograficzne w wymiarze politycznym w celu kontroli, a następnie – destabilizacji wewnętrznej innego podmiotu. Jednym z przykładów było prowadzenie polityki dobrosąsiedztwa (do 2010 r.) wobec Ukrainy: chodziło o utrzymywanie przyjaznych stosunków między państwami, rozwój więzi kulturowych oraz społecznych. Nadanie obywatelstwa Federacji Rosyjskiej mieszkańcom Krymu i wschodniej części Ukrainy wynikało z ich tożsamości politycznej i kulturowej. Większość ludności potwierdzała swoją przynależność do narodu rosyjskiego. W 2014 r. Rosja rozpoczęła agresywne działania na Krymie, a później – w Donbasie, pod pretekstem okazania wsparcia oraz ochrony swoim obywatelom, co doprowadziło do → a n e ks j i [t. 1] półwyspu i do wojny we wschodniej części Ukrainy. Rosja, poprzez wykorzystanie potencjału demograficznego, osiągnęła swoje cele polityczne i wzmocniła wpływy na terytorium innego państwa, które nadal w stanie kryzysu, co blokuje ewentualną integrację ze strukturami Zachodu.

Wywołanie migracji z myślą o celach strategicznych może nastąpić w wyniku mniej lub bardziej subtelnych metod. Możemy wyróżnić następujące sposoby:

1. Działania militarne wymierzone w → l u d n o ś ć c y w i l n ą [t. 2] (działania bezpośrednie).
2. Działania militarne niewymierzone bezpośrednio w ludność cywilną (pogarszająca się sytuacja humanitarna w rejonie działań militarnych).
3. Działania ekologiczne (wprowadzanie zmian w środowisku danej ludności, np. budowa zapory wodnej czy „trudne sąsiedztwo" uzyskiwane przez budowę uciążliwej infrastruktury czy zasiedlanie innymi grupami etnicznymi/religijnymi/ekonomicznymi).
4. Działania ekonomiczne – celowe zubożanie ludności (np. przez dodatkowe daniny) lub stosowanie zachęt finansowych (np. zapewnienie logistyki).
5. → D e z i n f o r m a c j a [t. 1] i → p r o p a g a n d a [t. 3].

Wykorzystanie ludności cywilnej w konflikcie nie jest – oczywiście – nowym zjawiskiem. Miało ono wiele płaszczyzn, np. zmuszanie do służby wojskowej (w regionie Wielkich Jezior Afrykańskich), rozmieszczanie jako żywe tarcze (działania ISIS w Iraku i Syrii), wykorzystywanie do tworzenia logistycznych przeszkód (np. w Kosowie i Sudanie). Były również wykorzystywane jako narzędzia propagandowe w celu wywołania międzynarodowej sympatii i poparcia (w tym – przez wszystkie strony konfliktów w Bośni). Specyfika broni „D" polega na jej wykorzystaniu w konflikcie asymetrycznym, przy czym niekoniecznie sednem jest rywalizacja między podmiotem niepaństwowym a państwowym, po taką broń może sięgać państwo posiadające znaczny potencjał militarny, ale nie na tyle duży, żeby przez konkurenta było postrzegane za podmiot wiarygodny w polityce → o d s t r a s z a n i a [t. 3] militarnego, lub sam agresor zdaje sobie sprawę ze swoich słabości i jest zmuszony do działania poniżej progu → w o j n y [t. 4]. Połączenie kwestii militarnych, społecznych, ekonomicznych

i informacyjnych czyni broń „D" szczególnie użyteczną w → w o j n i e h y b r y d o w e j [t. 4]. Wykorzystanie → l u d n o ś c i c y w i l n e j [t. 3], w tym – grup społecznych, do destabilizacji odpowiada też założeniom rosyjskiej koncepcji → w o j e n b u n t o w n i c z y c h [t. 4]. Ludność, która stała się narzędziem działania w charakterze broni, postrzega państwo ją wykorzystujące jako sojusznika i z reguły nie jest świadoma pełnionej funkcji.

Stosowanie broni „D" może być celowe i zaaranżowane przez aktywne działania własne (np. militarne) lub pasywne (np. zaniechanie kontroli granic). Aktorami mogą być zarówno podmioty państwowe, jak i niepaństwowe (np. organizacje terrorystyczne). Podmioty państwowe mogą wykorzystywać taką broń przede wszystkim do osłabienia gospodarki państwa przyjmującego, do wywołania niepokojów społecznych, ale przede wszystkim do utraty kontroli nad granicami – co jest jednym z podstawowych zadań sił zbrojnych. Użycie środków militarnych wobec takiego strumienia jest natomiast nieakceptowane przez znaczną część → o p i n i i p u b l i c z n e j [t. 3], zwłaszcza przy jednoczesnej → w a l c e i n f o r m a c y j n e j [t. 4], i może prowadzić do kompromitacji państwa wobec sojuszników, kierujących się podobnymi wartościami. Natomiast zastosowanie środków niewystarczających do powstrzymania strumienia migracyjnego może prowadzić do kompromitacji służb granicznych jako niezdolnych do obrony granic oraz skutkować wprowadzeniem chaosu w państwie atakowanym. Zatem po taką broń raczej sięgnie aktor niedemokratyczny wobec aktora demokratycznego – jest to szczególnie pomocna broń w → w o j n a c h c z w a r t e j g e n e r a c j i [t. 4]. Przykładem takich działań może być operacja sprowadzania, a następnie dostarczania migrantów przez służby białoruskie na granicę z Polską i z innymi krajami UE (2021). Agresor w ten sposób wymusza zmianę → r e ż i m u [t. 3] prawnego (Polska wprowadziła stan wyjątkowy), co może być wykorzystane w polityce wewnętrznej do przedstawienia Polski jako sąsiada agresywnego. Z jednej strony – powstały → k r y z y s h u m a n i t a r n y [t. 2] na granicy konsoliduje zwolenników rządu, daje większą swobodę na działania służbom specjalnym (wykorzystujących poczucie zagrożenia), a z drugiej – dyskredytuje rząd w oczach zwolenników opozycji, chociażby przez podważanie zaufania do służb mundurowych. Tym samym polska scena polityczna dzieli się jeszcze bardziej, co przekłada się na osłabienia państwo. Drugim ważnym aspektem jest towarzysząca wojna informacyjna: część społeczeństwa ulega presji medialnej i zaczyna proces migracyjny postrzegać jako → z a g r o ż e n i e c y w i l i z a c y j n e czy społeczne. Może to wpływać na wzmocnienie postaw ksenofobicznych i nacjonalistycznych. Taki manewr zastosowała Rosja po 2015 r. Federacja Rosyjska we wrześniu 2015 r. rozpoczęła interwencję militarną w Syrii. Oficjalną przyczyną była działalność → P a ń s t w a I s l a m s k i e g o [t. 3] (ISIS). W rzeczywistości walki toczono głównie w Idlib i Latakki, opanowanych przez inne ugrupowania rebelianckie (głównie sojuszu Dżabath al-Fateh – zwalczającego ISIS). Prowadzono szereg działań militarnych z wykorzystaniem

→ a r t y l e r i i [t. 1] i lotnictwa, często te ataki były skierowane w ludność cywilną. Wywołało to olbrzymią falę migracyjną z Syrii przez Turcję, która nie była zainteresowana powstrzymaniem tejże. Wywołało to liczne obawy w Europie i przysporzyło znacznej popularności partiom o retoryce antyimigranckiej i antyislamskiej. Te partie często korzystały ze wsparcia dezinformacyjnego służb rosyjskich, a nawet pomocy finansowej. Wśród partii, które podjęły taką retorykę, a nierzadko – współpracę finansową, możemy wymienić: Alternatywa dla Niemiec / Alternative für Deutschland (Niemcy), Front Narodowy (Francja), Liga Północna (Włochy), Fidesz (Węgry), Szwedzcy Demokraci (Szwecja), Partia Wolnościowa (Austria) oraz Prawo i Sprawiedliwość (zwłaszcza w samorządowej kampanii wyborczej z 2018 r.). Co ważne, wszystkie te partie są eurosceptyczne, co prawdopodobnie jest ważnym walorem dla Rosji, która postrzega UE jako przeciwnika.

Strumień migracyjny może również być wykorzystywany jako swoista osłona do swobodnego przepływu terrorystów i infiltracji przeciwnika. Służby specjalne ISIS – tzw. *emni* lub *Amniyat* – za jedno ze swoich zadań uważały „wysyłanie i rozmieszczanie szpiegów i rekruterów w innych krajach, w tym przy wykorzystaniu emigrantów syryjskich". Przykładowo: Marokańczyk Mourad T., ujęty w Polsce, udawał nieletniego uchodźcę z Syrii (taki status otrzymał w Austrii), był łącznikiem komórki ISIS odpowiedzialnej za zamachy w Brukseli (2016). Jeden z autorów tego zamachu dostał się na terytorium Unii Europejskiej w październiku przez Grecję, był nawet w ośrodku dla emigrantów na wyspie Lesbos. Zamachowiec z Paryża (2015) mieszkał w ośrodku dla azylantów w Recklinghausen w Niemczech, figurował pod 4 różnymi nazwiskami, złożył wniosek o → a z y l . Żaden z tych ludzi nie był w rzeczywistości emigrantem uciekającym przed wojną, tylko – bojownikiem ISIS.

Pojęcie broni „D" jest bardzo kontrowersyjne. Po pierwsze – trudno o naukową weryfikację: takie działania są na ogół wynikiem działalności służb specjalnych, zatem często wnioskowanie oparte jest o metodę ekstrapolacji. Po drugie – kontrowersja jest widoczna także na poziomie semantycznym: mówienie o ludziach jako o broni to pewna dehumanizacja, co może budzić wątpliwości natury etycznej.

Przemysław Mazur, Anna Netreba

A. Antczak-Barzan, Z. Śliwa, R. Zaniewski, *Wojna XXI wieku: początki wojny „trzeciej fali"*, Vizja Press & IT, Warszawa 2016; K.M. Greenhill, *Strategic Engineered Migration as a Weapon of War*, „Civil Wars" 2008, vol. 10, iss. 1; P. Pawliczek, J. Pawłowski, *Zagrożenia asymetryczne*, Akademia Obrony Narodowej, Warszawa 2003; W. Repetowicz, *Broń „D" jako zagrożenie asymetryczne*, „Kwartalnik Towarzystwa Wiedzy Obronnej" 2018, nr 1–2; T. Snyder, *Droga do niewolności. Rosja, Europa, Ameryka*, Wydawnictwo Znak, Kraków 2019; I. Sobczak, M. Wyrzykowska-Antkiewicz, *Demografia i bezpieczeństwo społeczne krajów Unii Europejskiej*, CeDeWu, Warszawa 2013; L. Sykulski, *Rosyjska koncepcja wojen buntowniczych Jewgienja Messnera*, „Przegląd Geopolityczny" 2015, nr 11; O. Wasiuta, S. Wasiuta, *Wojna hybrydowa Rosji przeciwko Ukrainie*, Arkana, Kraków 2018; K. Załęski, *Współczesne migracje ekonomiczne czy broń demograficzna*

celowo użyta przeciwko Europie?, „Kwartalnik Bellona" 2016, nr 1; В. Портніков, *Демографічна зброя: навіщо РФ заселяє Крим росіянами, Волинь. Правда*, https://pravda.volyn.ua/ demohrafichna-zbroia-navishcho-rf-zaseliaie-krym-rosiianamy/?fbclid=IwAR2Sc0TqwhOXAOnfmapeleXVcNpWmIRjAs1CFrlbXyn kPaVSWp7t3SASXc (dostęp 15.10.2021).

BROŃ ENTOMOLOGICZNA (ang. *entomological warfare*) – wykorzystanie owadów lub innych bezkręgowców do bezpośrednich ataków lub jako wektory przenoszenia czynnika biologicznego, takiego jak dżuma lub cholera. Idea takiego wykorzystania owadów istniała od czasów starożytnych i była badana oraz stosowana przez różne kraje przez wiele stuleci, ale dopiero w XX w. zaczęto aktywnie wykorzystywać ją do tworzenia broni.

Owady mają 3 główne zastosowania w działaniach wojennych:

- zarażanie owadów śmiercionośnym wirusem lub bakterią, a następnie rozpraszanie ich nad obszarami docelowymi; owady te działają jak wektory, infekują każdą osobę lub zwierzę poprzez ukąszenia;
- bezpośredni atak owadów w celu niszczenia roślin rolniczych, by pozbawić wroga źródeł pożywienia; w tym wypadku owady niekoniecznie są zarażone, ale powinny stanowić → z a g r o ż e n i e [t. 4] dla rolnictwa;
- użycie niezakażonych owadów takich jak pszczoły lub osy do bezpośredniego ataku na przeciwników.

W historii było wiele przypadków, w których →wojny [t. 4] toczono z wykorzystaniem → b r o n i b i o l o g i c z n e j : wirusy, bakterie i grzyby odegrały dużą rolę w rozpowszechnianiu i wywoływaniu chorób. Jednym z przykładów może być przenoszona przez pchły epidemia dżumy z XIV w., znana jako czarna śmierć, która ostatecznie doprowadziła do śmierci 30–60% populacji Europy. Epidemia ta była prawdopodobnie pierwszą wywołaną na skutek ataku biologicznego – Tatarzy pod przywództwem Dżanibega mieli katapultować na teren oblężonej Kaffy (dzisiejszej Teodozji) zwłoki zakażonych, skąd później dżuma rozprzestrzeniła się po Europie.

„Granaty" ze skorpionów to jeden z najstarszych precedensów wykorzystania broni entomologicznej, pochodzący sprzed ok. 2 tys. lat. Cesarz rzymski Septymiusz Sewer w kampanii przeciwko Mezopotamii został zmuszony do zatrzymania się przed twierdzą Khatra, otoczoną murami obronnymi. Zamiast dokonać szturmu, Rzymianie zaczęli zbierać jadowite skorpiony i miotać nimi w stronę obrońców. Jest mało prawdopodobne, aby pokonano w ten sposób wielu wojowników Khatry, zadziałało to jednak jako atak psychologiczny, który zmusił fortecę do poddania się.

Ule pszczele były używane jako improwizowane bomby także przez Rzymian, a następnie przez wiele innych ludów od starożytności do naszych czasów. Na przykład podczas II wojny włosko-abisyńskiej (1935– 1936) partyzanci z Etiopii potrafili walczyć z pomocą pszczół przeciwko włoskim czołgom.

Według J. Lockwooda, autora książki *Six-Legged Soldiers: Using Insects as Weapons of War*, najwcześniejszym użyciem owadów jako broni było prawdopodobnie

użycie pszczół. Pszczoły lub ich gniazda wrzucano do jaskiń i innych schronów, aby zmusić wroga do wyjścia na otwartą przestrzeń.

Świat nie doświadczył na wielką skalę wykorzystania broni entomologicznej aż do II wojny światowej. Japońskie ataki w Chinach były jedynym potwierdzonym użyciem broni biologicznej lub entomologicznej podczas tej wojny – wykorzystano wtedy stonkę ziemniaczaną. W trakcie wojny i po jej zakończeniu także inne państwa rozpoczęły własne programy badań nad bronią entomologiczną.

Japonia była jedynym krajem, który rozwinął i szeroko wykorzystywał broń entomologiczną podczas II wojny światowej, prawie wyłącznie na terytorium Chin. Japońska Jednostka 731 stosowała zarażone dżumą pchły i muchy przenoszące cholerę, aby zarażać chińską populację. Japońska armia rozproszyła owady, rozpryskując je z nisko lecących samolotów i zrzucając bomby wypełnione mieszanką owadów. Fala epidemii, która powstała w wyniku tych działań, kosztowała życia prawie 500 tys. Chińczyków.

Niemcy w czasie II wojny światowej również prowadzili badania nad możliwościami wykorzystania owadów w walce entomologicznej. Głównym celem programu tego kraju była masowa produkcja i dystrybucja nad terytorium przeciwnika stonki ziemniaczanej (*Lepinotarsa decemlineata*), skierowanej na źródła żywności wroga. Testy przeprowadzono na południe od Frankfurtu nad Menem, gdzie wypuszczono 54 tys. owadów. Stonka ziemniaczana jako broń entomologiczna ma na celu zniszczenie źródeł żywności wroga. Nie ma dokładnych danych na temat wykorzystania stonki ziemniaczanej jako broni w innych krajach. Oprócz stonki ziemniaczanej nazistowskie Niemcy planowały również wykorzystanie komarów przenoszących malarię przeciwko swoim wrogom. Testy przeprowadzono na więźniach obozów koncentracyjnych.

Zainteresowanie nazistowskimi eksperymentami z bronią biologiczną nadal nie maleje. Wiadomo, że wiele instytucji Trzeciej Rzeszy działało w celu ochrony przed potencjalnymi atakami biologicznymi. Możliwe, że naziści przekroczyli cienką linię, która odróżnia → o c h r o n ę l u d n o ś c i [t. 3] od rozwoju broni ofensywnej. K. Reinhardt, badacz z Uniwersytetu Eberharda Karola w Tybindze, odkrył dokumenty archiwalne i w 2013 r. opublikował artykuł w czasopiśmie „Endeavour", w którym podał dowody na to, że w obozie koncentracyjnym Dachau podczas II wojny światowej były przeprowadzane eksperymenty z użyciem komarów przenoszących malarię.

W 1942 r. z inicjatywy G. Himmlera powstał Instytut Entomologiczny Waffen-SS; jego głównym celem była walka z epidemią tyfusu, który wśród więźniów obozów koncentracyjnych wykorzystywanych jako niewolników w przedsiębiorstwach wojskowo-przemysłowych roznosiły wszy. Na czele instytutu stał biolog E. May, zagorzały nazista. W 1943 r. May otrzymał fundusze na program rozwoju pestycydów chroniących uprawy na polach Rzeszy, na wypadek gdyby alianci spróbowali je zniszczyć, wysyłając owady.

W związku z tym powierzono mu zadanie „zbadania właściwości owadów szkodliwych dla ludzi, aby ustalić ich praktyczne zastosowanie i wzmocnić ochronę przed nimi".

Ze znalezionych dokumentów wiadomo, że May badał komary rodzaju *Anopheles*, aby ustalić, czy alianci mogliby je wykorzystać do ataku biologicznego na Trzecią Rzeszę. To, czy May rzeczywiście pracował nad bronią entomologiczną, wymaga potwierdzenia. Pod koniec wojny wiele ważnych dokumentów zostało zniszczonych przez administrację niemiecką i sowiecką, dlatego nie wiadomo, jaką skalę nazistowski program broni biologicznej faktycznie osiągnął.

Wśród aliantów Kanada pierwsza podjęła próbę opracowania broni opartej na owadach-wektorach. Po zapoznaniu się z rozwojem wykorzystania pcheł jako broni przez Japonię Kanada, a następnie USA i Francja rozpoczęły prace w tym kierunku. Podobnie jak w Niemczech, program Francji był przede wszystkim ukierunkowany na wykorzystanie stonki ziemniaczanej w celu zniszczenia żywności wroga.

W ZSRR laboratoria wojskowe prowadziły efektywne badania nad bronią entomologiczną mającą na celu zniszczenie upraw rolnych i zwierząt przeciwnika. Sowieci opracowali techniki wykorzystywania kleszczy do transmisji patogenów zwierzęcych. Znana jest również praca nad zastosowaniem kleszczy atakujących ptaki w celu zakażenia kurcząt pasożytem *Chlamydophila psittaci*. Ponadto radzieccy inżynierowie opracowali metody zautomatyzowanej masowej hodowli owadów, zdolnej do wypuszczania milionów pasożytniczych owadów dziennie.

USA podczas → z i m n e j w o j n y [t. 4] badały potencjał wykorzystania owadów jako broni. Opracowano plany utworzenia centrum, które mogłoby miesięcznie wyprodukować 100 mln komarów zarażonych żółtą gorączką. Wojskowi testowali również zdolność kąszenia niezainfekowanych komarów, wypuszczając je nad miastami USA. W maju 1955 r. ponad 300 tys. niezainfekowanych *Aedes aegypti*, potencjalnych przenośników żółtej gorączki, zostało zrzuconych z samolotu w bombach nad stanem Georgia w celu ustalenia, czy komary zrzucone z samolotów mogą przeżyć i kąsać ludzi. Ogółem do badań wyhodowano ok. miliona samic komarów. Testy te były znane pod nazwą operacji Big Buzz. USA wykorzystywały również badania broni entomologicznej w sytuacjach niewojennych. W latach 90. XX w. rząd USA sfinansował za 6,5 mln USD program badań i uprawy gąsienic przeznaczonych do zrzucania na plantacje koki w Peru w ramach wojny z narkotykami. W 2002 r. pojawiła się → i n f o r m a c j a [t. 2] o pracach laboratorium badawczego w Fort Detrick nad owadami-wektorami przenoszącymi wirusa, który miał zainfekować mak lekarski w ramach walki z produkcją opium.

Konwencja z 1972 r. o zakazie broni biologicznej i toksycznej (Biological and Toxin Weapons Convention, BWC) nie wymienia wprost owadów, chociaż tekst wskazuje bezpośrednio wektory biologiczne. Artykuł 1 konwencji zakazuje „rozwoju, produkcji, magazynowania lub nabywania […] broni, sprzętu i środków dostarczania przeznaczonych do użycia takich środków we wrogich celach lub podczas konfliktów zbrojnych". Zgodnie z tekstem BWC stosowanie wektorów opartych na owadach jest zabronione przez tę konwencję. Jednak kwestia ta jest mniej jasna w odniesieniu do

stosowania niezakażonych owadów, które można wykorzystać przeciwko rolniczym uprawom.

Na szczęście dla nas żyjących w czasach współczesnych broń entomologiczna należy już do przeszłości, gdyż dysponujemy znacznie ulepszonymi środkami zwalczania szkodników niż kiedyś.

Olga Wasiuta

B.J. Bernstein, *The Birth of the U.S. Biological Warfare Program*, „Scientific American" 1987, no. 6; F.N. Chaudhry i in., *Insects as Biological Weapons*, „Journal of Bioterrorism & Biodefense" 2017, vol. 9, iss. 1; E. Geissler, *Biological Warfare Activities in Germany, 1923–45*, [w:] *Biological Warfare from the Middle Ages to 1945*, E. Geissler, J. Moon, E. van Courtland (eds.), Oxford University Press, New York 1999; R. Harris, J. Paxman, *A Higher Form of Killing: The Secret Story of Chemical and Biological Warfare*, Hill and Wang, New York 1982; S. Harris, *The Japanese Biological Warfare Program: An Overview*, [w:] *Biological Warfare from the Middle Ages to 1945*, E. Geissler, J. Moon, E. van Courtland (eds.), Oxford University Press, New York 1999; O. Lepick, *French Activities Related to Biological Warfare, 1919–1945*, [w:] *Biological Warfare from the Middle Ages to 1945*, E. Geissler, J. Moon, E. van Courtland (eds.), Oxford University Press, New York 1999; J.A. Lockwood, *Entomological Warfare: History of the Use of Insects as Weapons of War*, „Bulletin of the Entomological Society of America" 1987, vol. 33, no. 2; tenże, *Insects as Weapons of War, Terror, and Torture*, „Annual Review of Entomology" 2012, no. 57; tenże, *Locust: The Devastating Rise and Mysterious Disappearance of the Insect that Shaped the American Frontier*, Basic Books, New York 2004; tenże, *Six-Legged Soldiers: Using Insects as Weapons of War*, Oxford University Press, New York 2008; *Medical Aspects of Chemical and Biological Warfare*, F. Sidell, E. Takafuji, D. Franz (eds.), Borden Institute, Walter Reed Army Medical Center, Washington 1997; SIPRI, *The Problem of Chemical and Biological Warfare*, t. 2: *CB Weapons Today*, Almkvist and Wiksell, Stockholm 1973; O. Wasiuta, *Broń entomologiczna*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; А. Марцулевич, *Биохимическое оружие древности*, Litres, Москва 2018.

BROŃ GENETYCZNA – inaczej biogenetyczna, niekiedy broń etniczna – rodzaj → b r o n i b i o l o g i c z n e j przeznaczonej do wyrządzenia szkody lub selektywnego niszczenia populacji wg rasowych, etnicznych, płciowych lub innych genetycznych cech. Jest to jeden z rodzajów broni biologicznej zabronionej przez protokół genewski z 1925 r. Opracowywanie, produkcja i gromadzenie zapasów tego rodzaju broni jest zabronione przez Konwencję o broni biologicznej z 1972 r.

Działalność broni genetycznej opiera się przede wszystkim na zniszczeniu albo porażeniu wybranej części populacji, np. mężczyzn jako potencjalnych → ż o ł n i e r z y [t. 4] lub niektórych narodów jako całości, przez sztucznie wyhodowane patogenne mikroorganizmy. Patogenny efekt jest celowo zwiększony. Leki, które istniały przed stworzeniem któregokolwiek z rodzajów broni genetycznej, są wobec nich nieskuteczne.

Broń genetyczna to sztucznie stworzone szczepy bakterii i wirusów, zmodyfikowane za pomocą technologii inżynierii genetycznej w taki sposób, że mogą wywoływać negatywne zmiany w organizmie człowieka. Broń genetyczna działa w zależności od płci, wieku i różnych cech antropologicznych, które można zidentyfikować poprzez

analizę struktury DNA. Inżynieria genetyczna umożliwia także tworzenie kopii DNA – wszystkie eksperymenty klonowania oparte są na tej zasadzie, co wywołuje największe kontrowersje i sprzeciw ze strony społeczeństw i Kościoła.

Broni biologicznych używano od zawsze, a historia broni genetycznej jest nierozerwalnie związana z historią broni bakteriologicznej. W czasach średniowiecza i wcześniej armie zatruwały wodę i żywność, przez mury obronne przerzucano martwe zwierzęta, by wywoływać epidemie w obleganych twierdzach. Współcześnie jednak pojawiła się możliwość wyprodukowania jakościowo nowej broni – takiej, która korzystałaby z zaawansowanego rozwoju biologii molekularnej i pozwoliłaby razić selektywnie ludzi o określonej budowie DNA, atakowałaby tylko określone rasy ludzkie. Pierwsze wzmianki w prasie na temat nowych broni pojawiły się w 1970 r. w artykule pt. *Ethnic Weapons* (*Bronie etniczne*), opublikowanym w czasopiśmie „Military Review" przez C. Larsona, szwedzkiego genetyka z Uniwersytetu w Lund. Larson rozważał możliwości militarnego wykorzystania różnic między rasami, takich np. jak nietolerowanie laktozy przez organizmy Azjatów. Fakt, że żadna populacja nie jest homogeniczna, a zastosowanie tego rodzaju broni wobec wroga spowodowałoby również szkody po stronie napastnika, dla strategów wojskowych wydawał się nie mieć dużego znaczenia. Różnic między poszczególnymi grupami etnicznymi, które mogłyby zostać potencjalnie wykorzystane przy wytwarzaniu broni etnicznej, choć wiele, acz nieczęsto można o nich usłyszeć w mediach. Na przykład pewne nacje europejskie są z powodów biologicznych nieco bardziej odporne na zarażenie wirusem HIV niż inne.

Idea nowej broni polega na tym, by zidentyfikować geny odróżniające nacje, a następnie wytworzyć bakterie lub wirusy atakujące ludzi w sposób wybiórczy, w zależności od budowy ich DNA. Wiele → i n f o r m a c j i [t. 2] ze świata nauki świadczy o tym, że teoretycznie zadanie takie jest możliwe do wykonania, praktycznie zaś być może zostało już w jakiejś mierze zrealizowane. Pierwsze badania tego rodzaju prowadzone były przez białych w Republice Południowej Afryki czasów apartheidu. Planowano wtedy wytworzenie mikrobów, które reagowałyby na kolor skóry ofiar, jako sposób ich rozprzestrzeniania rozważano zaś dodawanie określonych substancji do piwa, kukurydzy, a nawet do szczepionek. Eksperymenty z RPA miały na celu przetestowanie substancji, która powodowałaby wyłączenie niektórych genów, co miało prowadzić do ciężkich chorób i w konsekwencji redukcji niechcianej populacji. Według relacji naocznych świadków w specjalnych laboratoriach, pod pozorem eksperymentów medycznych, ludzi o ciemnym kolorze skóry karmiono zanieczyszczoną kukurydzą i oferowano im piwo, do którego dodawano substancje mające eliminować konkretne geny. Jak wynika z dostępnych informacji, program testowy został zatrzymany, bo okazało się, że ze względu na niejednorodność genetyczną nowa broń zagrażała również białym. Istniało po prostu realne ryzyko, że zabójca genów wymknie się spod kontroli i zacznie zabijać wszystkich.

Można oczywiście wierzyć w to, że nikt poza RPA nie prowadził takich eksperymentów, ale niestety fakty pozwalają sądzić inaczej. Tak np. w 1997 r. sekretarz obrony USA W. Cohen odniósł się do koncepcji → z a g r o ż e n i a [t. 4] etnicznego jako potencjalnego ryzyka. W 1998 r. eksperci od broni biologicznej uważali broń genetyczną za wiarygodną i byli przekonani, że ZSRR przeprowadzał pewne badania nad wpływem różnych substancji na ludzkie geny. Niektórzy twierdzą, że dowodem na stosowanie broni genetycznej była dziwna epidemia SARS, która wybuchła w Chinach w listopadzie 2002 r. W jej wyniku śmierć poniosło 813 osób, w tym 770 Chińczyków. Wirus powodował objawy przypominające zapalenie płuc, ale żaden ze znanych leków nie pomagał. Do dziś nie jest jasne pochodzenie wirusa. Mimo że rozprzestrzenił się na cały świat, stanowił zagrożenie głównie dla Chińczyków. Może to stanowić dowód tego, że był to jakiś rodzaj testu udoskonalonej broni wymierzonej w jedną grupę etniczną.

W 2004 r. „The Guardian" poinformował, że British Medical Association (BMA) uznało badania nad bronią biologiczną zaprojektowaną z myślą o pewnych grupach etnicznych za możliwość zyskania istotnej wiedzy, podkreślono jednak, że postępy w nauce dotyczące spraw takich jak „leczenie Alzheimera i innych wyniszczających chorób mogą być wykorzystywane również do celów złośliwych". Według specjalistów krajami najbardziej skłonnymi, by zajmować się tego rodzaju badaniami, są Japonia i Chiny – ze względu na stosunkowo łatwe wykrycie różnic genetycznych między rasą żółtą a pozostałymi, ale też ze względów, które można by określić jako kulturowe. Profesor B. Lee z Black Hawk College w Moline (Illinois, USA), autor kilku książek na temat AIDS i epidemiologii, uważa, że obecnie możliwe jest wytwarzanie broni genetycznej, która atakować będzie nie tylko różne populacje etniczne, ale wręcz konkretne osoby. Aby to zrobić, należałoby poznać dokładnie kod genetyczny danej osoby, a potem na podstawie tych danych przygotować odpowiednio bakterie albo wirusy.

Jeśli ta śmiercionośna biotechnologiczna broń jest rozwijana od lat, należy się spodziewać znacznego postępu w zakresie jej skuteczności.

Mimo że oficjalnie obowiązujące konwencje międzynarodowe zabraniają prac nad tego typu „genetycznymi bombami", to wielu ekspertów uważa, że badania są prowadzone do dzisiaj, ale kamuflowane jako eksperymenty medyczne.

Przełomowe może być odkrycie amerykańskich naukowców, którzy już w 1998 r. udowodnili, że można dokonać sztucznej ingerencji w łańcuch RNA, wprowadzając go do ciała człowieka. Cząsteczka ta może niszczyć predefiniowane kombinacje genów. Innymi słowy możliwe byłoby wręcz wyłączenie procesów życiowych ewentualnych ofiar. Zabójcza cząsteczka po znalezieniu się w organizmie mogłaby dopisywać lub zmieniać części kodu genetycznego, co prowadziłoby do powstawania raka, cukrzycy czy innych nieuleczalnych chorób. Oficjalnie badania są prowadzone po to, aby leczyć te choroby, jeśli jednak ich wyniki zostałyby wykorzystane do stworzenia broni, technologia taka pozwalałaby zabijać części populacji ludzkiej w sposób wręcz niezauważalny.

W maju 2007 r. rosyjska gazeta „Kommiersant" poinformowała, że rosyjski rząd zakazał wszelkiego eksportu ludzkich biopróbek. Powodem wprowadzenia zakazu miał być tajny raport FSB o trwającym rozwoju „genetycznej broni biologicznej", skierowanej przeciwko rosyjskiej populacji przez zachodnie instytucje. W raporcie wspomniano o Harwardzkiej Szkole Zdrowia Publicznego, Amerykańskim Międzynarodowym Sojuszu Zdrowia (The American International Health Alliance), Departamencie Biotechnologii Medycznej, Wydziale Sprawiedliwości oraz Wydziale Zasobów Naturalnych Departamentu Sprawiedliwości USA, Instytucie Genetyki i Biotechnologii oraz Agencji Stanów Zjednoczonych ds. Rozwoju Międzynarodowego (U.S. Agency for International Development).

Dotąd nie zanotowano w świecie prób użycia zaawansowanej broni genetycznej, jednak jest to coraz bardziej realne. W 2016 r. magazyn „Foreign Policy" zasugerował możliwość użycia wirusa jako etnicznej broni biologicznej, która mogłaby wysterylizować genetycznie powiązaną populację etniczną. Ludzkość dysponuje już bowiem technologią, która takie działania umożliwia. Już dziś jest wykorzystywana w nauce i biznesie do celów handlowych. Ponadto rozwija się w błyskawicznym tempie i jest coraz tańsza. R. Kessler, autor książki *In the President's Secret Service* (*W tajnej służbie prezydenta*), twierdzi, że żołnierze marynarki chroniący prezydenta USA starannie zbierają pościel, szklanki i wszystkie przedmioty, których dotykał. Są potem sterylizowane lub niszczone. Chodzi o to, aby materiał genetyczny nie wpadł w ręce niepowołanych osób. Poprzez pobranie tylko jednej komórki prezydenta można by bowiem wyhodować wirusa, który zaatakuje tylko jego. Dyrektor Wywiadu Narodowego USA J. Clapper w corocznym raporcie na temat ocen zagrożenia dla ludzkości technologią inżynierii genetycznej CRISPR, pozwalającej na manipulację genomem, podkreślił, że w razie nieprawidłowego wykorzystania może ona stać się czymś podobnym do → b r o n i m a s o w e g o r a ż e n i a .

Raport z 2019 r. przygotowany przez naukowców z Uniwersytetu w Cambridge (Centre for the Study of Existential Risk, CSER) zwraca uwagę na fakt, że już niebawem powstanie broń biologiczna, która dzięki analizie ludzkiego DNA będzie oddziaływać jedynie na osoby z określonej grupy etnicznej. W związku z tym eksperci wzywają decydentów politycznych do „ochrony swoich obywateli" i przygotowania się na potencjalne niszczycielskie pandemie, wywołane przez nowe rodzaje broni biologicznej. Naukowcy twierdzą, że światowe rządy nie przygotowały się na futurystyczną broń opartą na zaawansowanych technologiach takich jak sztuczna inteligencja i manipulacja genetyczna.

Znana z wielu zaawansowanych projektów militarnych amerykańska agencja rządowa DARPA (Defense Advanced Research Projects Agency) zainwestowała 100 mln USD w technologie genetyczne, która pozwalają zniszczyć dany gatunek zwierząt. Tym razem na cel wzięto komary, które przenoszą malarię. Oczekuje się, że nowa technologia będzie w stanie zniszczyć nie tylko owady, ale także ssaki – zwłaszcza

gryzonie. Eksperci z ONZ obawiają się jednak wykorzystania tej technologii jako broni. Istnieje bowiem ryzyko, że zostanie zastosowana do stworzenia broni genetycznej, która może być użyta w warunkach bojowych, co stwarza zagrożenie również dla ludzi. Broń genetyczna, jeśli faktycznie powstanie, może stanowić poważne zagrożenie. Jak dotąd nie było jeszcze takiego wynalazku, którego nie próbowano zmilitaryzować.

Wiele organizacji na całym świecie zaangażowanych jest obecnie w dziedzinie identyfikacji wyróżniających się genów. Dziś znane jest np. ok. 50 ludzkich grup etnicznych, które można odróżnić na poziomie genetycznym. Oznacza to, że jeśli broń genetyczna znajdzie się w rękach terrorystów, cała grupa etniczna może być zagrożona. BMA ostrzega, że przy użyciu broni genetycznej możliwe jest zniszczenie nawet małych grup w obrębie większych grup etnicznych. Rzeczywistość tworzenia broni genetycznych została otwarcie stwierdzona przez ekspertów BMA twierdzących, że:

> w następnym dziesięcioleciu będzie można stworzyć genetyczną broń masowego rażenia, a gwałtownie postępujący rozwój genetyki może w nadchodzących latach spowodować bezprecedensowe czystki etniczne.

Broń taka pozwoli w dowolnie wybranym czasie – od kilku godzin do dziesięcioleci – systematycznie niszczyć całe ludzkie populacje, postępując wg określonego klucza cech genetycznych, bez obawy przed ewentualnym odwetem.

Sergiusz Wasiuta

R. Abadie, K. Heaney, *We Can Wipe an Entire Culture: Fears and Promises of DNA Biobanking Among Native Americans*, „Dialectical Anthropology" 2015, no. 3; *Amerykańska armia rozwija broń genetyczną. Eksperci ostrzegają przed konsekwencjami*, 6.12.2017, AlexJones.pl (dostęp 10.02.2020); P. Anderson, G. Bokor, *Bioterrorism: Pathogens as Weapons*, „Journal of Pharmacy Practice" 2012, no. 5; S.M. Block, *The New Terror: Facing the Threat of Biological and Chemical Weapons*, Hoover Institution Press, Stanford 1999; S. Cary, *The Tipping Point: Biological Terrorism*, „Journal of Strategic Security" 2009, no. 3; O. Cenciarelli, S. Rea, M. Carestia, *Bioweapons and Bioterrorism: A Review of History and Biological Agents*, „Defence S&T Tech. Bull" 2013, no. 2; CSER, *Managing Global Catastrophic Risks. Part 1: Understand*, 13.08.2019, CSER.ac.uk (dostęp 10.02.2020); A. Garreffa, *Future Bioweapons Designed to Kill ONLY People of a Particular Race*, 15.08.2019, TweakTown.com (dostęp 10.02.2020); J. Kalenik, *Bioterroryzm – zagrożenie XXI wieku*, Centralny Ośrodek Szkolenia Straży Granicznej, Koszalin 2003; S. Knapton, *World Must Prepare for Biological Weapons that Target Ethnic Groups Based on Genetics, Says Cambridge University*, 13.08.2019, Telegraph.com (dostęp 10.02.2020); G.D. Koblentz, *From Biodefense to Biosecurity: The Obama Administration's Strategy for Countering Biological Threats*, „International Affairs" 2012, no. 1; K. Langbein, C. Skalnik, I. Smolek, *Bioterroryzm*, tłum. M. Chudzik, Muza, Warszawa 2003; Ch. Muanya, *Bioweapons Designed to Kill Only People of Particular Race*, 20.08.2019, TheGuardian.com (dostęp 10.02.2020); L. Parker, *Bioterrorism and Intelligence*, „Global Security Studies" 2013, vol. 4, no. 3; D. Robitzsk, *Future Bioweapons Could Kill People with Specific DNA*, 14.08.2019, Futurism.com (dostęp 10.02.2020); I. Sample, *Synthetic Biology Raises Risk of New Bioweapons, US Report Warns*, 19.06.2018, TheGuardian.com (dostęp 10.02.2020); S. Wasiuta, *Broń genetyczna*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; *W trzeciej wojnie światowej pojawi się broń genetyczna zabijająca konkretne nacje?*, 10.09.2019, Interia.pl (dostęp 10.02.2020).

BROŃ GEOFIZYCZNA (ang. *geophysical weapons*) – zbiór różnych narzędzi, które pozwalają w celach wojskowych wykorzystywać niszczycielskie działania natury poprzez ingerencję w fizyczne właściwości lub procesy zachodzące w atmosferze, hydrosferze i litosferze Ziemi; użycie tego rodzaju broni może polegać np. na wywołaniu destrukcyjnych trzęsień ziemi poprzez detonacje ładunków nuklearnych w miejscach napięcia tektonicznego. Zastosowanie broni geofizycznej opiera się na celowej modyfikacji w obszarze klimatu czy pogody, jonosfery, magnetosfery, systemu płyt tektonicznych w celu spowodowania fizycznych, ekonomicznych i psychospołecznych zniszczeń w obrębie danego celu geofizycznego lub populacji, w ramach wojny strategicznej lub taktycznej.

Broń geofizyczna dzieli się w zależności od rodzaju dotkniętych jej działaniem sfer na:

- tektoniczną (sejsmiczną, litosferyczną, geologiczną) – wywołującą trzęsienia ziemi, erupcje wulkanów, przesunięcia płyt litosferycznych;
- atmosferyczną (meteorologiczną, klimatyczną) – wywołującą zmiany temperatury, huraganowe wiatry, zniszczenie warstwy ozonowej, pożary;
- hydrosferyczną – wywołującą tsunami, powodzie na dużych obszarach, pękanie pokrywy lodowej, burze śnieżne, grad, oblodzenie, mgłę;
- orientacyjną – wywołującą zmianę położenia Ziemi w przestrzeni, jej prędkości obrotowej;
- uderzeniową – wywołującą uderzenie asteroidy wprowadzonej na pożądaną orbitę (zniszczenia może spowodować także sztuczny masywny obiekt wprowadzony na orbitę).

Za pomocą broni geofizycznej możliwe będzie wpływanie na atmosferę, niszczenie systemu łączności, przesyłanie energii, powodowanie samodetonacji amunicji oraz manipulowanie ludzkimi umysłami. Badania obejmują m.in. eksperymenty z zastosowaniem impulsowych wiązek energii do spalania lub podgrzewania ograniczonego obszaru jonosfery. Skutkiem takiego działania może być modyfikacja pogody, wywołanie burz, powodzi, tornad, cyklonów, susz itp.

W 1996 r. w artykule w „The New York Times" opisującym broń geofizyczną podkreślono, że oznaczałaby ona działania z wykorzystaniem inżynierii środowiska mające na celu zmianę przepływu powietrza i wody, aby zniszczyć jedną stronę konfliktu, a przynieść korzyści drugiej. Najbardziej elementarnym rodzajem takich działań jest wywoływanie krótkotrwałych opadów w celach wojskowych. Broń geofizyczna może być w stanie zatopić rozległe kontynentalne obszary przybrzeżne, zamienić żyzne obszary w pustynie, a może nawet radykalnie zmienić cały światowy klimat. Jak zaznaczono w artykule:

> Każdy poważny akt inżynierii środowiska niesie za sobą znaczne ryzyko, ponieważ zawsze towarzyszy mu duży potencjał niezamierzonych efektów ubocznych, powodujących nieoczekiwane zmiany, które mogą zaszkodzić – a nawet zniszczyć – niektóre obszary świata.

Niszczycielski wpływ wielu naturalnych zjawisk opiera się na ich potężnej energii. Ingerencja w procesy geofizyczne w obszarach narażonych na wstrząsy sejsmiczne może wywołać sztuczne trzęsienia ziemi. Podobnie, oddziałując na procesy zachodzące w niższych warstwach atmosfery, można spowodować silny deszcz, grad czy wywołać mgłę. Tworzenie barier na rzekach i kanałach może wywoływać powodzie, zaburzać działanie nawigacji, a nawet przyczynić się do zniszczenia hydrosystemów. Badana jest również możliwość zmiany temperatury powietrza poprzez rozpylanie substancji pochłaniających energię promieniowania słonecznego. Zniszczenie danego fragmentu warstwy ozonowej w atmosferze umożliwia skierowanie promieniowania kosmicznego i promieniowania ultrafioletowego Słońca na obszary zajmowane przez wroga. Do oddziaływania na procesy naturalne wykorzystuje się substancje chemiczne takie jak jodek srebra, karbamid, kwas węglowy, proszek węglowy, związki bromu, fluoru. Możliwe jest stosowanie potężnych generatorów promieniowania elektromagnetycznego, generatorów ciepła i innych środków technicznych. To, że duże eksplozje mogą powodować powstanie dużych i niszczących fal, znane było od dawna, np. tsunami powstałe po erupcji Krakatau w 1883 r. było odpowiedzialne za przynajmniej 36 tys. ofiar śmiertelnych. Wiedziano także, że sztuczne eksplozje mogą spowodować powstanie fal, np. eksplozja statku z bronią na kanale La Manche w 1915 r. wywołała niewielką falę pływową, zaobserwowaną u wybrzeży Wielkiej Brytanii. W czasie II wojny światowej amerykański oficer U.S. Navy E.A. Gibson zauważył, że wyburzanie raf koralowych ładunkami wybuchowymi czasami powodowało znaczne fale, co podsunęło mu pomysł na stworzenie „bomby tsunami". W czerwcu 1944 r. prowadzono tajny program amerykańsko-nowozelandzki pod kryptonimem Projekt Seal, kierowany przez prof. T. Leecha, którego zadaniem było opracowanie takiej właśnie bomby, będącej w stanie wywołać sztuczną falę tsunami.

W ramach projektu w latach 1944–1945 w okolicach Nowej Kaledonii w Melanezjii i w pobliżu półwyspu Whangaparaoa w Nowej Zelandii przeprowadzono ok. 3,7 tys. próbnych wybuchów. W trakcie eksperymentów udało się wytworzyć fale sięgające wysokości ok. 10 m. Obliczenia wskazywały jednak, że do wywołania tsunami o wielkości równej naturalnemu zjawisku tego typu potrzebne byłoby ok. 2 mln kg materiałów wybuchowych.

Rządy USA i Wielkiej Brytanii sądziły, że „bomba tsunami" może być realną alternatywą dla powstającej wówczas w ramach Programu Manhattan bomby atomowej. Ostatecznie projekt zakończono w 1945 r., w 1947 r. Leech otrzymał zaś Order Imperium Brytyjskiego za prace nad rozwojem tej broni. Koncepcję uznano za wykonalną, ale sama broń nigdy nie została w pełni opracowana ani wykorzystana.

Już po zakończeniu programu w Nowej Zelandii kontynuowano niezależne badania nad „bombą tsunami", które ostatecznie zakończono w latach 50. Istnieją przypuszczenia, że podobne badania prowadzono w ZSRR w czasach → z i m n e j w o j n y [t. 4] z myślą o ataku na południowe regiony Wielkiej Brytanii i Holandii.

Oficjalnie projekt Seal został odtajniony dopiero w 1999 r. W 1968 r. U.S. Navy, po ponownym wykonaniu obliczeń, wyraziła wątpliwości co do realnej możliwości stworzenia sztucznego tsunami nawet z zastosowaniem eksplozji ładunków atomowych.

Środki, za pomocą których stymulowane są czynniki geofizyczne, mogą być różne, ale energia wydatkowana przez te środki jest zawsze znacznie mniejsza niż energia uwalniana przez siły natury, powstała w wyniku naturalnych procesów geofizycznych.

N. Tesla stwierdził, że mały oscylator mechaniczny napędzany parą, z którym odkrywca eksperymentował w 1898 r., przyniósł efekty podobne do trzęsienia ziemi, ale próba nigdy nie została przez niego powtórzona. Jako broń tektoniczna mogą zostać wykorzystane dowolne środki powodujące wibracje skorupy ziemskiej: eksplozje, specjalnie montowane w wybranych miejscach wibratory sejsmiczne, a także wstrzykiwanie dużej ilości płynu w miejscu naprężenia tektonicznego. Największy na świecie wibrator sejsmiczny CVO-100 został zbudowany w 1999 r. na poligonie doświadczalnym w pobliżu miasta Babushkin w Buriacji, opracowany przez naukowców z Syberyjskiego Oddziału Rosyjskiej Akademii Nauk. Współczesne wibratory sejsmiczne są zbyt małe, aby można ich było użyć jako broni tektonicznej. Pompowanie płynu do zbiorników i wykopalisk w obszarach nisko położonych i niestabilnych może prowadzić do poważnych trzęsień ziemi. Na przykład napełnienie zbiornika Kariba w Afryce wodą spowodowało, że obszar ten stał się aktywny sejsmicznie. Podziemna eksplozja również może spowodować potężne trzęsienie ziemi. Prace nad takimi eksplozjami zainicjował Pentagon w połowie lat 70. XX w.

Głównym celem broni tektonicznej jest uwolnienie potencjalnej energii Ziemi, skierowanie jej przeciw wrogowi i spowodowanie maksymalnych zniszczeń. Aby go osiągnąć, można zastosować:

- podziemne i podwodne eksplozje jądrowe lub wybuchy chemicznych materiałów wybuchowych;
- eksplozje na szelfie kontynentalnym lub na wodach przybrzeżnych;
- wibratory sejsmiczne w wyrobiskach podziemnych lub studniach wypełnionych wodą;
- sztuczna zmiana trajektorii upadku asteroidów.

Konwencja z 1978 r. o zakazie używania technicznych środków oddziaływania na środowisko w celach militarnych lub jakichkolwiek innych celach wrogich jest traktatem międzynarodowym, ratyfikowanym przez 75 państw i podpisanym przez kolejne 17, zabraniającym stosowania technik modyfikacji środowiska w celu wywołania trzęsień ziemi i tsunami oraz innych zjawisk pogodowych.

W kwietniu 2002 r. Tbilisi nawiedziło trzęsienie ziemi o sile blisko 6 stopni w skali Richtera. Po tych wydarzeniach lider Partii Zielonych Gruzji G. Gachechiladze stwierdził, że wstrząsy zostały sztucznie wywołane przez rosyjskich wojskowych za pomocą znajdującej się w Abchazji stacji Esherskoy pełniącej funkcje monitoringu sejsmicznego. W laboratorium sejsmicznym Eschera w czasach sowieckich pracowano nad

stworzeniem broni tektonicznej, w latach 70. w Azji Środkowej wojskowi, wykorzystując tę broń, wywołali trzęsienie ziemi o sile 7 stopni w skali Richtera. Odnosząc się do źródeł rosyjskich, Gachechiladze podkreślił, że Esherskaya Sejsmologiczna Laboratoria nadal jest jednym z najbardziej tajnych obiektów i podlega bezpośrednio Sztabowi Generalnemu Sił Zbrojnych Rosji.

W 2005 r. tomski oddział Federalnej Służby ds. Własności Intelektualnej, Patentów i Znaków Towarowych wydał naukowcom z Irkucka patent na „Sposób zarządzania reżimem przemieszczeń we fragmentach sejsmicznie aktywnych tektonicznych błędów skorupy ziemskiej". W mediach ten patent został natychmiast nazwany „patentem na broń tektoniczną". Zaprojektowano go jednak w celu zapewnienia → b e z p i e c z e ń s t w a sejsmicznego w miejscach o największej gęstości zaludnienia i obiektów niebezpiecznych dla środowiska, na placach budowy oraz podczas projektowania szczególnie ważnych projektów budowlanych. Według naukowców jednak, opierając się na monitorowaniu wewnętrznego rytmu Ziemi, można ustalić czas i miejsce sztucznego trzęsienia ziemi, znacznie zwiększając jego siłę i towarzyszące mu efekty.

Jak pisała w książce o broni tektonicznej inżynier kompleksów rakiet kosmicznych J. Kobrinovich, praca nad bronią tektoniczną w USA i ZSRR rozpoczęła się niemal w tym samym czasie – od połowy lat 70. XX w. Jednak w prasie otwartej praktycznie nie było → i n f o r m a c j i [t. 2] o tych projektach. Podstawą naukową badań nad tą bronią w ZSRR był ściśle tajny sowiecki program Merkury-18 (НИР № 2М 08614ПК) – zadanie techniczne w bardziej ogólnym tajnym programie Wulkan, którego wykonawcą został wybrany Instytut Geologii Akademii Nauk ZSRR w Azerbejdżanie (Baku). Celem programów było opracowanie broni tektonicznej, która mogłaby wywołać trzęsienia ziemi z wykorzystaniem słabych pól sejsmicznych i transferu energii eksplozji z dużej odległości, manipulując elektromagnetyzmem. Program Merkury rozpoczęto w 1987 r., przeprowadzono 3 testy w Kirgistanie, a ostatni test w ramach programu Wulkan miał miejsce w 1992 r. (jego wyniki wpadły w ręce japońskiej rezydentury).

Warto w tym kontekście przedstawić fragmenty książki *Sto wielkich tajemnic XXwieku*:

- W listopadzie 1987 r., zgodnie z zamkniętym postanowieniem Komitetu Centralnego KPZR i Rady Ministrów ZSRR, rozpoczęto opracowywanie projektu stworzenia broni tektonicznej o nazwie kodowej Merkury.
- Uzbecka osada Gazli w 1976 i 1984 r. przetrwała niszczycielskie trzęsienie ziemi i za każdym razem pokrywały się one w czasie z wybuchami nuklearnymi w Semipałatyńsku.
- Ładunek nuklearny eksploduje w wybranym miejscu, a fale rozprzestrzeniają się pod ziemią.
- Podziemnej eksplozji jądrowej o niskiej mocy przypisuje się rolę czynnika uruchamiającego trzęsienie ziemi.

- Po trzęsieniu ziemi w Spitaku (4–7 grudnia 1988 r., Armenia) zwolniono wielu pracowników w związku z nieudanym zakończeniem eksperymentu (w wyniku trzęsienia ziemi zginęło wtedy od 25 do 50 tys. osób). W przeciwieństwie do innych niszczycielskich trzęsień ziemi skoordynowane badania mające na celu zrozumienie okoliczności i warunków, które doprowadziły do rozległych szkód spowodowanych tym trzęsieniem ziemi, nie zostały jeszcze odpowiednio zbadane.

Skalę programu Merkury-18 można zrozumieć, analizując listę 22 instytucji badawczych biorących udział w tym projekcie. W rezultacie, zgodnie z raportem kierownika programu I. Kerimova, na początku lat 90. XX w. skumulowane teoretyczne i eksperymentalne materiały pozwoliły opracować spowodowanie trzęsienia ziemi jakiejkolwiek mocy z odległości tysięcy kilometrów od sztucznych stref sejsmicznych i na obszarach, gdzie trzęsienia ziemi nie było od wieków. Trudno sobie wyobrazić, czym skończyłyby się destrukcyjne eksperymenty prof. Kerimova, gdyby ZSRR się nie rozpadł, a program Merkury-18 nie został zamknięty z powodu ogromnych wydatków.

Taka broń, bez względu na to, czy istnieje, czy też nie, budzi obawy. Sekretarz obrony USA W.S. Cohen, omawiając niebezpieczeństwa związane z fałszywymi → z a g r o ż e n i a m i [t. 4], powiedział 28 kwietnia 1997 r. na konferencji w sprawie → t e r r o r y z m u [t. 4], → b r o n i m a s o w e g o r a ż e n i a i → s t r a t e g i i [t.4] USA z nimi związanej: „Inni angażują się nawet w terroryzm typu ekologicznego, dzięki któremu mogą zmieniać klimat, uruchamiać zdalnie trzęsienia ziemi i wulkany dzięki falom elektromagnetycznym".

Po wystąpieniu naturalnych zjawisk tektonicznych, takich jak trzęsienie ziemi na Haiti z 2010 r. czy w Japonii w 2011 r., często pojawiają się → t e o r i e s p i s k o w e [t. 4], zwykle dotyczące sił zbrojnych USA i Federacji Rosyjskiej, chociaż nie ma dowodów na ich poparcie. Po trzęsieniu ziemi na Haiti szeroko informowano, że według zarzutów ówczesnego prezydenta Wenezueli H. Cháveza zostało ono wywołane amerykańskimi testami broni tektonicznej. Gazeta „Komsomolskaja Prawda" z Moskwy poinformowała 30 maja 1992 r. na pierwszej stronie, że „broń geofizyczna lub tektoniczna została faktycznie opracowana w ZSRR pomimo konwencji ONZ", ale Ministerstwo Obrony FR kategorycznie odrzuciło te doniesienia.

W USA podobnymi badaniami zajmuje się HAARP (High Frequency Active Auroral Research Program). To naukowe przedsięwzięcie mające na celu badanie jonosfery i procesów w niej zachodzących, które ma służyć usprawnieniu systemów komunikacji i nadzoru elektronicznego do celów cywilnych oraz obronnych. HAARP bada bezprzewodowe przesyłanie energii i fal elektromagnetycznych w kontekście zrozumienia, symulowania i kontroli procesów zachodzących w jonosferze.

W styczniu 1999 r. UE opisała HAARP jako projekt o znaczeniu globalnym i przyjęła rezolucję wzywającą do uzyskania dodatkowych informacji na temat zagrożeń dla zdrowia i środowiska z nim związanych. Rezolucja UE uznała HAARP – ze względu na jego dalekosiężny wpływ na środowisko – za globalny problem i wezwała do

zbadania jego prawnych, ekologicznych i etycznych konsekwencji przez niezależny organ międzynarodowy przed kontynuowaniem badań i testów. USA zignorowały jednak rezolucję. Urzędnicy HAARP poinformowali, że fale radiowe transmitowane w ramach programu nie są absorbowane ani w troposferze, ani w stratosferze, czyli sferach związanych z pogodą na Ziemi. Z uwagi na to, że nie zachodzi tego typu interakcja, nie ma sposobu, by kontrolować pogodę.

W 1998 r. płk S. Lunew, najwyższy rangą rosyjski szpieg wojskowy, który uciekł na Zachód, opublikował wspomnienia pt. *Through the Eyes of the Enemy* (*Oczami wroga*). W książce stwierdził, że Rosja ma tajną broń geofizyczną, która może wywoływać trzęsienia ziemi i burze. Kilka tygodni po tsunami, które spustoszyło Japonię w marcu 2011 r., rosyjski polityk i były kandydat na prezydenta W. Żyrinowski (lider partii LDPR) powiedział, że „Rosja ma broń [geofizyczną] zdolną zniszczyć całe kontynenty w kilka minut".

Również USA eksperymentują z bronią geofizyczną. W artykule z października 2018 r. F. Bucks, były amerykański tłumacz wojskowy, który pisze dla kanadyjskiej grupy medialnej Global Research, ujawnił, że amerykańskie wojsko ma zdolność wywoływania tsunami i może również powodować trzęsienia ziemi i huragany.

Według sztokholmskiego SIPRI (Stockholm International Peace Research Institute) tematyka broni tektonicznej jest ściśle utajniona, ale badania aktywnie prowadzone są w USA, Chinach, Japonii, Izraelu i Brazylii. Żadne z tych państw nie przyznaje jednak, że posiada broń tektoniczną. Oskarżenia o rozwój i używanie takiej broni od czasu do czasu słyszymy z ust polityków. Meksyk, Peru, Chile, Kuba, Iran i inne kraje wielokrotnie oskarżały USA, ZSRR i Chiny o wywoływanie trzęsień ziemi na ich terytoriach, ale nigdy nie przedstawiono żadnych dowodów.

Olga Wasiuta

B. Bartosik, D. Stępień, *Wojna geofizyczna*, „Wojska Lądowe" 2006, nr 2; S. Bayda, *Interrelations of Changes of Space and He-lio-Geophysical Factors and the Number of Victims after Catastrophic Earthquakes*, [w:] *Proceedings of the International Disaster and Risk Conference (IDRC Davos 2008), August 25–29 2008. Extended Abstracts*, W.J. Ammann (ed.), Global Risk Forum GRF, Davos 2008; J.P. Caves Jr., W. Seth Carus, *The Future of Weapons of Mass Destruction: Their Nature and Role in 2030*, National Defense University Press, Washington 2014; B. Iwanicka, *Broń geofizyczna*, „Przegląd Obrony Cywilnej" 1982, nr 11; J. Jeziorna, *Broń geofizyczna przyszłością terrorystów*, „Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa" 2010, nr 3; M. Kalinowski, *Z archiwów zimnej wojny: broń geofizyczna – krok w stronę wojny totalnej*, „Głos Weterana i Rezerwisty" 2000, nr 10; T. Kasperek, W. Zacharewicz, *Broń geofizyczna i inne nowe rodzaje broni masowego rażenia*, Akademia Marynarki Wojennej im. Bohaterów Westerplatte, Gdynia 2000; S. Lunev, *Through the Eyes of the Enemy: The Autobiography of Stanislav Lunev*, Regnery Publishing, Washington 1998; J.E. Smith, *HAARP – broń ostateczna*, tłum. K. Kurek, Amber, Warszawa 2004; J.E. Smith, *HAARP: The Ultimate Weapon of the Conspiracy*, Adventures Unlimited Press, Kempton 2002; J.J. Schultz, *Detecting Buried Firearms Using Multiple Geophysical Technologies*, NCJRS, 2009; O. Wasiuta, *Broń geofizyczna*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; J. Wiśnicki, *Broń geofizyczna orężem XXI wieku*, „Przegląd

Wojsk Lądowych" 2010, nr 2; В.В. Адушкин, А.А. Спивак, М.Г. Дубиня, *Сейсмические явления, наведенные подземным ядерным взрывом*, [w:] *Наведенная сейсмичность*, Наука, Москва 1994; С. Айвазян, *К 20-летию Геофизической Войны, развязанной Кремлевскими убийцами*, „Мецамор" 2008, № 14; М.Ю. Андреева, В.Н. Патрикеев, *Создание модели зон возможных очагов землетрясений для территорий, расположенных вблизи зон беньофа*, „Геодинамика и тектонофизика" 2012, Т. 3, № 1; С.Е. Байда, *Исследование частотновременных и пространственно-волновых закономерностей возникновения землетрясений, аварий электроснабжения и авиакатастроф*, [w:] *Труды 53-й научной конференции МФТИ «Современные проблемы фундаментальных и прикладных наук».* 3. *Аэрофизика и космические исследования*, Т. 2, МФТИ, Москва–Долгопрудный 2010; С.Е. Байда, *Мегакатастрофы, как стратегическое и тактическое оружие войн нового поколения, возможность их прогнозирования и предупреждения*, „Технологии гражданской безопасности" 2010, Т. 7, № 1–2; Ю.В. Баранов, *Анализ геофизических полей для выделения зон возможных очагов землетрясений восточной окраины восточно-европейской платформы*, „Вестник Пермского университета. Геология" 2016, № 4; *Землетрясения и микросейсмичность в задачах современной геодинамики восточно-европейской платформы*, К. 2: *Микросейсмичность*, Н.В. Шарова, А.А. Маловичко, Ю.К. Щукина (ред.), *Карельский научный центр*, Петрозаводск 2007; Н. Непомнящий, *100 великих загадок XX века*, ЛитРес, Москва 2010; А.В. Николаев, *Инициирование землетрясений подземными ядерными взрывами*, „Вестн. РАН" 1993, Т. 36, № 2; А.В. Николаев, Г.М. Верещагина, *Об инициировании землетрясений подземными ядерными ззрывами*, „ДАН" 1991, Т. 319, № 2; А.В. Николаев, Г.М. Верещагина, *Об инициировании землетрясений землетрясениями*, „Докл. АН СССР" 1991, Т. 318, № 2; С.И. Рыбников, *Влияние запусков крупнейших ракетных комплексов на образование сильных землетрясений*, [w:] *Наведенная сейсмичность*, Наука, Москва 1994; Л.В. Сорокин, *Инициирование землетрясений сейсмическими волнами*, „Вестник Российского университета дружбы народов" 2005, № 1; И.Э. Сулейменов, *Воздействие на процессы в атмосфере и проблематика геофизических вооружений*, Казахский Национальный Университет Им. АльФараби, Алматы 2007; Г.М. Сухарев, *Землетрясения, вызванные техногенными процессами*, „Изв. вузов. Нефть и газ" 1976, № 5; М. Штейнберг, *Удар из глубин земли*, „Военное обозрение", № 3.

BROŃ HIPERSONICZNA – inaczej broń hiperdźwiękowa – broń zdolna do lotu z prędkością powyżej 5 Ma (5-krotność prędkości dźwięku, określanej liczbą Macha, od nazwiska austriackiego fizyka E. Macha). Prędkość 5 Ma to ok. 6125 km/h, zależnie od wysokości. Dla porównania najszybszy używany operacyjnie samolot, czyli SR-71 Blackbird, osiągał prędkość ok. 3,5 Ma. Obecnie prawie wszystkie rodzaje broni działają poniżej obszaru prędkości hiperdźwiękowych – jedynym wyjątkiem są rakiety balistyczne.

Sam termin został po raz pierwszy użyty w 1946 r. przez inżyniera Caltechu (California Institute of Technology) Hsue-shen Tsiena, późniejszego twórcę chińskiego programu rakietowego i kosmicznego. Prędkości od 0,8 Ma do 1,2 Ma określane są jako okołodźwiękowe (ang. *transonic*) – gdyż krytyczne zjawiska nie następują dokładnie w momencie przekraczania bariery dźwięku, ale zaczynają się nieco wcześniej i kończą później, gdy opływ staje się typowo naddźwiękowy. Prędkości od 1,2 Ma do 5 Ma to prędkości ponaddźwiękowe (ang. *supersonic*), a powyżej 5 Ma hiperdźwiękowe (ang. *hipersonic*). W ramach tego ostatniego zakresu prędkości wyróżnia się jeszcze

2 podzakresy – wysokie prędkości hiperdźwiękowe (ang. *high hipersonic*) powyżej 10 Ma oraz prędkości ultradźwiękowe (ang. *ultrasonic*) powyżej 25 Ma (nie należy ich jednak utożsamiać z prędkością rozchodzenia się ultradźwięków). Prędkości powyżej 25 Ma osiągają jednak tylko statki kosmiczne. W przypadku broni hipersonicznej ważne jest to, że mówimy o osiąganiu prędkości powyżej 5 Ma w atmosferze, a nie w przestrzeni kosmicznej.

W przypadku prędkości hiperdźwiękowych nie ma dokładnej bariery, takiej jak bariera dźwięku, ale wartość 5 Ma nie jest ustalona zupełnie arbitralnie. Lot hipersoniczny jest bardzo różny od lotu z mniejszymi prędkościami. Występują tu zjawiska fizyczne niespotykane przy niższych prędkościach. Mają one dominujący wpływ na możliwość takiego lotu, znacznie silniejszy niż zjawiska typowo aerodynamiczne, dominujące przy niższych prędkościach. Najważniejszym z tych czynników jest ciepło. Przy prędkościach hipersonicznych ciepło pochodzi nie tylko od tarcia powietrza na powierzchni płatowca, ale przede wszystkim – i to jest zasadnicza różnica – od kompresji powietrza, która pojawia się przy prędkościach okołodźwiękowych, a przy przekroczeniu progu prędkości hiperdźwiękowych staje się tak duża, że powietrze przekształca się w rozgrzaną plazmę.

O wojskowym wykorzystaniu prędkości hipersonicznej Niemcy myśleli już w 1938 r. Powstała wtedy koncepcja samolotu Silbervogel autorstwa E. Sängera, przeznaczonego do bombardowania USA. Miał on charakteryzować się szczególnym profilem lotu, a duży zasięg miał wynikać z powtarzającego się manewru ślizgania się po powierzchni atmosfery (odbijania się od niej) przy prędkości hiperdźwiękowej. Ówczesny stan techniki nie pozwalał jednak na realizację tego projektu.

Pierwszy lot hiperdźwiękowy miał miejsce w 1949 r. Wykonała go amerykańska dwustopniowa rakieta Bumper, złożona z niemieckiej rakiety V2 służącej za pierwszy stopień oraz zmodyfikowanej rakiety WAC Corporal pełniącej funkcję drugiego stopnia rakiety. W teście przeprowadzonym 24 lutego 1949 r. rakieta wzniosła się po trajektorii suborbitalnej na wysokość 389 km, a w czasie powrotu do atmosfery drugi stopień osiągnął prędkość przekraczającą 8000 km/h.

W latach 50. XX w. okazało się, że osiąganie prędkości z zakresu hiperdźwiękowego jest kluczowe dla budowy międzykontynentalnych rakiet balistycznych oraz statków kosmicznych. Szczególnie ważny był moment powrotu do atmosfery, zarówno statków kosmicznych (kapsuł kosmicznych, szczególnie załogowych), jak i tzw. pojazdów powrotnych (ang. *reentry vehicle*) rakiet balistycznych, zawierających głowice bojowe. Opracowano jednak nowe materiały, które pozwoliły na ochronę przed nagrzewaniem, a nawet technologie pozwalające do pewnego stopnia na sterowanie pojazdem powrotnym (szczególnie istotne w przypadku bojowych rakiet balistycznych, w mniejszym stopniu dla kapsuł kosmicznych). Kontrolowany lot hipersoniczny udało się zrealizować wraz z powstaniem badawczego samolotu rakietowego X-15, który wykonał pierwszy lot w 1959 r. Rozpędzał się on z użyciem silnika rakietowego

po oddzieleniu od samolotu nosiciela i kontynuował lot jak szybowiec, cały czas zachowując możliwość sterowania. Najwyższy osiągnięty pułap to 108 km. W 1967 r. samolot osiągnął prędkość 6,7 Ma (7274 km/h) na wysokości 31,12 km. Jest to nadal najszybszy lot załogowy poza rakietami i promami kosmicznymi.

W latach 1957–1963 Amerykanie rozwijali program samolotu kosmicznego X-20 Dyna-Soar. Miał to być samolot kosmiczny zdolny do lotu w atmosferze i do wchodzenia na orbitę. Co ciekawe, w celu realizacji długodystansowego lotu nieorbitalnego X-20 miał wykonywać ślizg przez górne warstwy atmosfery w locie pod niewielkim kątem, zamiast zanurzyć się atmosferze – miał mieć zdolność odbijania się jak kaczka puszczona na wodzie. W uproszczeniu powtarzał więc koncepcję samolotu Silbervogel. Budowa pierwszego prototypu nie została jednak ukończona, gdyż uznano za bardziej perspektywiczne statki kosmiczne oparte na rakietach nośnych i kapsułach załogowych. Podobny projekt nieco później był rozwijany w ZSRR – samolot kosmiczny MiG-105 wykonał 8 lotów testowych, ale bez wchodzenia w przestrzeń kosmiczną i osiągania znacznych prędkości.

Kolejne eksperymentalne konstrukcje związane były z rozwojem programów promów kosmicznych. W USA konstrukcje takie jak bezzałogowy X-23 PRIME i załogowe X-24A i X-24B przeznaczone były przede wszystkim do testowania koncepcji kadłuba nośnego (ang. *lifting body*). W ZSRR w ramach programu Buran w latach 80. XX w. testowano bezzałogowe BOR-4 (zmniejszona wersja MiG-a-105) oraz BOR-5 (wersja docelowego promu Buran w skali 1:8). Eksperymenty te ostatecznie doprowadziły do zbudowania 5 wahadłowców w ramach amerykańskiego programu STS (Space Transportation System) oraz radzieckiego wahadłowca Buran (odbył zaledwie 1 lot bezzałogowy). Tymczasem spokrewnione z rakietami nośnymi rakiety balistyczne zdominowały militarny wymiar broni dużych prędkości.

Wyróżniamy 3 drogi dojścia do prędkości hiperdźwiękowych:

- Klasyczne rakiety balistyczne. Gdy rakiety (lub ich głowice) wracają do atmosfery, rozwijają prędkość hiperdźwiękową. Przykładowo głowice międzykontynentalnych pocisków balistycznych na wysokości ok. 90 km rozwijają prędkości w granicach 7 km/s, czyli ok. 24 Ma. W związku z tym muszą one wytrzymać temperaturę ok. 11 tys. stopni Celsjusza, ale przez stosunkowo krótki czas. Gdy głowica rakiety balistycznej wchodzi do atmosfery, kontrola nad nią (możliwość sterowania) jest bardzo niewielka. Oznacza to, że broń leci generalnie po z góry zdefiniowanej trajektorii. Tego typu broń jest dobrze znana od wielu dekad i silnie umocowana w aktualnym systemie równowagi strategicznej.
- Broń typu HGV (Hipersonic Glide Vehicle), inaczej określana jako Boost Glide Vehicle. Konstrukcje HGV to głowice szybujące. Rozpędzane są one za pomocą silnika nosiciela (zasadniczo są to rakiety balistyczne, ale możliwy jest też sposób analogiczny, jak w przypadku X-15), a potem kontynuują lot szybujący z prędkością hiperdźwiękowa, ew. ze ślizgiem po atmosferze jak samolot Dyna-Soar.

Głowica więc nie porusza się po czystej trajektorii balistycznej, ale zaczyna manewrować, używając siły nośnej pochodzącej z powietrza. Jeśli nosicielem jest międzykontynentalna rakieta balistyczna, to na wysokości ok. 90 km głowica HGV może osiągać prędkości nawet 20–25 Ma, lecz potem prędkość spada. Spada ona tym bardziej, im niższy jest pułap i im profil lotu jest bardziej zbliżony do horyzontalnego. Ostatnia faza lotu może odbywać się z prędkością ok. 5 Ma. Sumaryczna trajektoria jest znacznie odmienna od trajektorii pocisku balistycznego o porównywalnym zasięgu – apogeum i znaczna część lotu wypadają wyraźnie niżej, a trajektoria może być w pewnym stopniu zmienna. Głowica ma bowiem większe możliwości sterowania w porównaniu z klasyczną głowicą pocisku balistycznego. Wszystko to ma utrudnić wykrycie, śledzenia i zniszczenie takiej głowicy przez systemy antyrakietowe (→a n t y ra k iet o w e sys t em y).

- Broń HCV (Hipersonic Cruise Vehicle), czyli hiperdźwiękowe pociski manewrujące. Broń HCV zakłada wykorzystanie napędu na całym torze lotu. Ciąg silnika musi być wystarczający, by utrzymać określoną prędkość i wysokość. Pociski HCV zupełnie nie poruszają się po trajektorii balistycznej. Są ciągle napędzane, więc mogą utrzymywać długodystansowy lot poziomy. Co więcej, na całym torze lotu zapewniona jest możliwość manewrowania, w stopniu daleko większym niż w pozostałych kategoriach broni hipersonicznej. W najbardziej zaawansowanych koncepcjach zakłada się przy tym dodatkowo możliwość lotu hiperdźwiękowego na bardzo niskiej wysokości, podobnie jak to jest w przypadku obecnie stosowanych rakiet manewrujących, poruszających się jednak z prędkościami poddźwiękowymi (np. Tomahawk, Kalibr) lub naddźwiękowymi, ale w granicach 2,5 Ma (przede wszystkim wybrane typy rakiet przeciwokrętowych, jak radziecki P-700 Granit czy rosyjski P-800 Oniks).

Broń hipersoniczna HGV i HCV rozwijana jest przede wszystkim w 3 państwach: Rosji, Chinach i USA. Kilka konstrukcji zostało zadeklarowanych jako operacyjne, chociaż → i n f o r m a c j e [t. 2] o ich rzeczywistym statusie są trudne do zweryfikowania, czy to z uwagi na otoczkę tajności zaawansowanych typów uzbrojenia, czy też z powodu kampanii dezinformacyjnych. Pozostałe konstrukcje znajdują się w różnych fazach rozwoju: prototypów, demonstratorów technologii lub nawet koncepcji. Poniżej przedstawiono wybrane konstrukcje rozwijane w poszczególnych państwach.

Systemy rosyjskie:

- Kindżał – oficjalnie wprowadzony do uzbrojenia jako rakietowy system hipersoniczny w 2018 r. Kompleks składa się z nosiciela – samolotu MiG-31K i rakiety H-47M2. Definicyjnie mieści się w kategorii broni hipersonicznej, ale nie jest ani pociskiem manewrującym, ani głowicą szybującą. Kindżał jest lotniczym wariantem pocisku aerobalistycznego Iskander. Oznacza to, że jest przede wszystkim rakietą balistyczną, ale dysponującą dużymi jak na tego typu konstrukcję zdolnościami do manewrowania. Szacunkowa prędkość rakiety to 7–10 Ma, a deklarowany

zasięg to 2 tys. km (nie wiadomo jednak, czy chodzi tylko o zasięg rakiety, czy też zasięg całego kompleksu, czyli promień działania nosiciela i zasięg rakiety).

- Awangard – system typu HGV, zadeklarowany jako operacyjny w grudniu 2019 r. Jest to system o charakterze strategicznym, składający się z międzykontynentalnego pocisku balistycznego UR-100NUTTH i hiperdźwiękowej głowicy szybującej Ju-71 z pojedynczą głowicą nuklearną. Dokładny profil ataku jest nieznany, chociaż Rosjanie deklarują, że głowica porusza się w gęstych warstwach atmosfery z prędkością ponad 20 Ma, manewrując w kierunku i wysokości. Być może do roli nosiciela głowicy zostaną przystosowane inne typy rosyjskich pocisków balistycznych, w tym nowa, ciężka rakieta RS-28 Sarmat.
- 3M22 Cyrkon – pocisk typu HGV, mający być wystrzeliwany z pokładów okrętów nawodnych i podwodnych, samolotów bombowych Tu-160M oraz wyrzutni naziemnych. Wyposażony w silnik strumieniowy z naddźwiękową komorą spalania pocisk manewrujący ma przenosić głowicę konwencjonalną lub nuklearną, dysponować zasięgiem ok. 400 km (docelowo ma to być nawet 1 tys. km) i osiągać prędkość ok. 5–6 Ma. Profil lotu zakłada wzniesienie się na wysokość 40 km i stopniowe obniżanie wysokości, tak by końcowa faza ataku przebiegała na wysokości 10–15 m. System prawdopodobnie przystosowany będzie do atakowania okrętów i celów lądowych. Cyrkon znajduje się przypuszczalnie w końcowej fazie testów.

Systemy chińskie:

- DF-17 – system typu HGV, zadeklarowany jako operacyjny podczas parady wojskowej w Pekinie 1 października 2019 r. Składa się on z rakiety balistycznej pełniącej funkcję nosiciela (prawdopodobnie rakieta DF-16 o zasięgu szacowanym na 800–1400 km) oraz głowicy szybującej, znanej wcześniej pod oznaczeniami DF-ZF oraz WU-14. System prawdopodobnie może być przystosowany zarówno do przenoszenia głowicy nuklearnej (głowica szybująca służyć ma efektywnej penetracji systemów przeciwrakietowych), jak i konwencjonalnej. W tej drugiej aranżacji będzie wykorzystywany do precyzyjnych uderzeń na ważne cele w skali operacyjnej, a być może także w roli systemu przeciwokrętowego.
- Starry Sky 2 (Xing Kong 2) – pocisk typu HCV. Podczas testu w sierpniu 2018 r. osiągnął, wg chińskich deklaracji, prędkość rzędu 5,5 Ma na wysokości ok. 30 km. Stopień zaawansowania projektu nie jest znany, prawdopodobnie jest to demonstrator technologii.

Systemy amerykańskie:

- Szereg programów badawczych, ukierunkowanych na rozwijanie technologii przydatnych do budowy broni hipersonicznej. Wymienić tu należy takie programy jak Hypersonic Test Vehicle HTV-2, Advanced Hypersonic Weapon (AHW), Hypersonic International Flight Research and Experimentation (HIFiRE – realizowany wspólnie z australijską agencją Defence and Science Technology) oraz Boeing X-51 Waverider (zbudowany w ramach programu Hypersonic Technology

HyTech). Ten ostatni odbywał testy w latach 2010–2013, a w czasie testu przeprowadzonego 1 maja 2013 r. utrzymał prędkość powyżej 5 Ma przez 210 sekund (cały lot trwał ponad 6 min), co jest najdłuższym lotem hipersonicznym przy użyciu silnika przelotowego (pobierającego powietrze z atmosfery, w przeciwieństwie do silnika rakietowego). X-51 napędzany jest typowym dla systemów typu HCV silnikiem strumieniowym z naddźwiękową komorą spalania (tzw. scramjet, od ang. *Supersonic Combustion Ramjet*). Podobnym napędem dysponował wcześniejszy aparat X-43, zbudowany w ramach programu Hyper-X, który 16 listopada 2004 r. osiągnął na krótko prędkość 9,6 Ma, co do dzisiaj jest rekordem prędkości dla samolotów. Kwestia zastosowań bojowych była rozwijana w ramach parasolowego programu Prompt Global Strike, zakładającego budowę broni zdolnej do konwencjonalnego uderzenia w cele na całym świecie w ciągu godziny od wystrzelenia z terytorium USA. Miało to umożliwić atakowanie celów w tzw. państwach zbójeckich z mniejszym ryzykiem rozpętania globalnego konfliktu, gdyż trajektoria takich pocisków jest zupełnie inna niż w przypadku międzykontynentalnych rakiet balistycznych, które niejako z definicji traktowane są jako nosiciele głowic nuklearnych.

- AGM-183A ARRW (Air-Launched Rapid Responce Weapon) – broń hipersoniczna przenoszona przez bombowiec strategiczny B-52. Informacje na temat tej broni są bardzo skromne, poinformowano jedynie o testach przeprowadzonych w czerwcu 2019 r., ale prawdopodobnie obejmowały one jedynie loty w podwieszeniu, bez oddzielenia się od nosiciela. ARRW wywodzić się ma z programu Tactical Boost Glide, co oznaczałoby, że jest to broń typu HGV. Prawdopodobnie system zawierał będzie również przyspieszacz rakietowy, który rozpędzi głowicę do odpowiedniej prędkości po oddzieleniu od lecącego stosunkowo wolno samolotu. Pojawiły się informacje o planowanym wprowadzeniu AGM-183A do służby w 2022 r., ale trudno zweryfikować wiarygodność tych deklaracji.
- HCSW (Hypersonic Conventional Strike Weapon) – broń hipersoniczna wystrzeliwana z samolotów, zapewne – podobnie jak ARRW – typu HGV. Obie konstrukcje rozwija Lockheed Martin i obie mają wejść do służby w 2022 r. Prawdopodobnie broń krótszego zasięgu niż ARRW, stosunkowo nieskomplikowana technologicznie, możliwa do produkcji w dużej serii.
- IRCPS (Intermediate Range Conventional Prompt Strike Weapon System) – system HGV średniego zasięgu, przeznaczony do przenoszenia głowic konwencjonalnych. Lockheed Martin realizuje równolegle 2 kontrakty na broń tej klasy, dla U.S. Army i dla U.S. Navy – ten drugi prawdopodobnie przeznaczony do wystrzeliwania z pokładów okrętów podwodnych.
- LRHW (Long-Range Hypersonic Weapon) – system HGV dalekiego zasięgu, integrujący wspólną dla różnych systemów głowicę szybującą (Common Hypersonic Glide Body) oraz nowy pocisk rakietowy dalekiego zasięgu wystrzeliwany z mobilnych wyrzutni lądowych.

- HAWC (Hypersonic Air-breathing Weapon Concept) – pocisk typu HCV z silnikiem typu scramjet, rozwijany pod egidą agencji DARPA (Defense Advanced Research Projects Agency) przez 2 konkurujące zespoły: Lockheed Martin oraz współpracujące firmy Raytheon i Northrop Grumman. Pocisk ma być przenoszony przez samoloty i wyposażony w dodatkowy przyspieszacz rakietowy rozpędzający go do prędkości, przy której działać może silnik strumieniowy. Ze względu na zastosowanie bardzo zaawansowanych technologii planowany termin wprowadzenia broni do służby jest bardziej odległy niż w przypadku poprzednich programów.

Spośród programów realizowanych w innych państwach warto wspomnieć o indyjskim demonstratorze technologii HSTDV (Hypersonic Technology Demonstrator Vehicle) z napędem scramjet, który odbył pierwszy lot 12 czerwca 2019 r.

Broń hipersoniczna staje się jednym z kluczowych elementów obecnego wyścigu zbrojeń. Padają deklaracje o jej ogromnym znaczeniu, jak wypowiedź z grudnia 2018 r. M. Gryffina, zastępcy amerykańskiego sekretarza obrony ds. badań i rozwoju, kiedy stwierdził on, że broń hipersoniczna może być czynnikiem zmieniającym reguły gry. Wprowadzane jednak obecnie systemy klasy HGV nie zmieniają w sposób zasadniczy sytuacji strategicznej, chociaż niewątpliwie dodają nowe możliwości do arsenału → o d s t r a s z a n i a [t. 3]. Wydaje się, że klasyczne pociski balistyczne dysponują wystarczającymi możliwościami przełamywania obrony przeciwrakietowej oraz przeprowadzania precyzyjnych ataków, tak że broń hipersoniczna tego szczebla stanowi przede wszystkim element dywersyfikacji możliwości, nie wprowadza zmiany jakościowej. Nieco większe znaczenie może mieć broń HGV o charakterze operacyjnym, przenosząca głowice konwencjonalne. Może ona stanowić użyteczne narzędzie przełamywania zdolności antydostępowych (→ a n t y d o s t ę p o w e z d o l n o ś c i) przeciwnika. Prawdziwym przełomem będzie jednak dopiero wprowadzenie broni typu HCV, zwłaszcza niskolecących hiperdźwiękowych pocisków manewrujących. Kombinacja dużej prędkości, niewielkiej wysokości lotu, nieprzewidywalności trajektorii i zdolności do manewrowania może spowodować, że obecnie istniejące systemy antyrakietowe okażą się wobec takiej broni nieefektywne. Wymusi to nowe podejście do kwestii zwalczania środków napadu powietrznego, prawdopodobnie oparte częściowo (przede wszystkim w zakresie sensorów, w mniejszym stopniu efektorów) na systemach rozmieszczonych w przestrzeni kosmicznej. Perspektywa wprowadzenia tego rodzaju broni hipersonicznej do służby operacyjnej wydaje się jednak stosunkowo odległa.

Rafał Kopeć

J.M. Acton, *Hypersonic Boost-Glide Weapons*, „Science & Global Security" 2015, vol. 23, iss. 3; M. Czajkowski, *Hypersonic Missiles – A Political Multipurpose Weapon*, „Analiza Zakładu Bezpieczeństwa Narodowego UJ" 2019, nr 4 (43); M. Dąbrowski, *Hipersoniczny wyścig potęg*, 20.04.2019, Defence24.pl (dostęp 15.01.2020); K.M. Sayler, *Hypersonic Weapons: Background and Issues for Congress*, Congressional Research Service, Washington 2019; T. Schütz,

Technology and Strategy: Hypersonic Weapon Systems Will Decrease Global Strategic Stability – and Current Control Regimes Won't Do, „Deutsche Gesellschaft für Auswärtige Politik" 2019, nr 4; M.E. White, W.R. Price, *Affordable Hypersonic Missiles for Long-Range Precision Strike*, „Johns Hopkins APL Technical Digest" 1999, vol. 20, no. 3; D. Wilkening, *Hypersonic Weapons and Strategic Stability*, „Survival – Global Politics and Strategy" 2019, vol. 61, iss. 5; B. Zohuri i in., *New Weapon of Tomorrow's Battlefield Driven by Hypersonic Velocity*, „Journal of Energy and Power Engineering" 2019, vol. 13.

BROŃ KLIMATYCZNA / BROŃ METEOROLOGICZNA (ang. *climate weapon*) – hipotetyczna → b r o ń m a s o w e g o r a ż e n i a , której głównym czynnikiem niszczącym są różne zjawiska naturalne lub klimatyczne wywoływane poprzez zamierzoną ingerencję w środowisko w celu zniszczenia gospodarki poszczególnych krajów lub pojedynczego państwa za pomocą wpływu na zasoby naturalne, pogodę i klimat danego terytorium, państwa czy kontynentu. Wykorzystywane w tym celu mogą być różne technologie, sztucznie spowodowane katastrofy technogenne, które powodują katastrofy ekologiczne, a tym samym tworzą problemy gospodarcze. Należą do nich tornada, tajfuny, ulewy. Ponadto ten rodzaj broni jest w stanie zmienić ogólny klimat na określonym terytorium, powodując suszę, zamarzanie lub erozję gleby, a także sztucznie generować katastrofy technologiczne, które mogą wywoływać → k r y z y s y [t. 2] gospodarcze i polityczne. Jest to jedna z odmian → b r o n i g e o f i z y c z n e j . Atmosferyczna broń geofizyczna dzieli się na 3 typy: meteorologiczny (huragany, tajfuny, tornada), ozonowy (bezpośrednie niszczące działanie promieniowania ultrafioletowego Słońca na organizmy żywe) i klimatyczny (broń zmniejszająca produktywność rolniczą wojskowego lub geopolitycznego przeciwnika).

Kwestia istnienia broni klimatycznej jest nierozstrzygnięta. Oficjalnie żaden kraj na świecie nie przyznał otwarcie, że posiada taką broń. Najbardziej zaawansowane w tej dziedzinie są USA i Rosja, w przypadku tej drugiej prace w tym obszarze zostały spowolnione (z powodu rozpadu ZSRR). Broń klimatyczna obejmuje zestaw narzędzi, które mogą wpływać na atmosferę, hydrosferę i geosferę Ziemi, powodując katastroficzne wydarzenia na określonym obszarze planety.

Wykorzystywanie zjawisk naturalnych i klimatu przeciwko wrogowi jest odwiecznym marzeniem wojskowych. Skierować huragan na przeciwnika, zniszczyć plony w wrogim kraju, a tym samym spowodować głód, ulewne deszcze i zniszczyć całą infrastrukturę transportową wroga – takie możliwości nie mogły nie wzbudzić zainteresowania strategów.

W naszych czasach człowiek zyskał niespotykaną moc: rozdzielił atom, poleciał w kosmos, dotarł do dna oceanu. Dowiedzieliśmy się znacznie więcej o klimacie: teraz wiemy, dlaczego występują susze i powodzie, dlaczego pada deszcz i sypie śnieg, jak rodzą się huragany. Ale nawet obecnie nie jesteśmy w stanie w sposób pewny wpłynąć na globalny klimat. To bardzo złożony system, w którym oddziałują niezliczone czynniki. Aktywność słoneczna, procesy zachodzące w jonosferze, ziemskie pole

magnetyczne, oceany, czynnik antropogeniczny – to tylko niewielka część sił, które mogą determinować klimat naszej planety. Nawet nie rozumiejąc do końca wszystkich mechanizmów, które składają się na klimat, człowiek próbuje go kontrolować.

Pierwsze eksperymenty związane z celową zmianą klimatu i zarządzaniem pogodą rozpoczęły się w 2. poł. XX w. Początkowo nauczono się sztucznie wywoływać tworzenie się chmur i mgły. Badania w tym obszarze były prowadzone w wielu krajach, w tym w ZSRR. Nieco później dowiedziano się, jak doprowadzić do opadów deszczu, rozpraszać chmury, aby uzyskać słoneczną pogodę, transformować zwykłe chmury w deszczowe czy zapobiegać opadom gradu. Takie rezultaty można uzyskać, rozpraszając w chmurach – za pomocą samolotów lub pocisków – drobne cząstki pewnych substancji chemicznych, które w zależności od składu albo nie pozwalają parze wodnej na skroplenie, albo tworzą centrum kondensacji, co prowadzi do tworzenia się kropelek wody; podobnie przebiega zmiana gradu w zwykły deszcz.

Początkowo badania były prowadzone w czysto pokojowych celach, wkrótce jednak podobne technologie zaczęli opracowywać wojskowi. W XX w. wykonywano np. eksperymenty nad zmianą gęstości mas powietrza poprzez ich jonizację, rozpylanie aerozoli (np. jodku srebra) lub jego schłodzenie (aerozole suchego lodu czy propanu). Jonizację mas powietrza przeprowadza się za pomocą wyładowań elektromagnetycznych dużej mocy (w instalacjach rosyjskich) i poprzez oddziaływanie na chmury za pomocą fal radiowych wysokiej częstotliwości (w instalacjach amerykańskich). Zmiany pogody następują na ściśle określonym obszarze: w rejonie rozpylonych aerozoli, w zasięgu urządzeń wyładowczych, systemów kierunkowych anten mikrofalowych lub promieni dział laserowych.

Najbardziej znana jest operacja pod kryptonimem „Popeye", przeprowadzona podczas konfliktu w Wietnamie, której celem było znaczne zwiększenie ilości opadów deszczu w tej części Wietnamu, wzdłuż której przebiegał Szlak Ho Chi Minha, system tras zaopatrzenia wietnamskiego. Amerykańskie służby meteorologiczne w 1966 r. rozpoczęły zasiew chmur nad szlakiem, wywołały gigantyczne deszcze, wydłużyły sezon deszczowy i zwiększyły intensywność opadów trzykrotnie. Leśne drogi zmieniły się w bagna, linie komunikacyjne wroga zostały zerwane. Ponadto na wiele lat poważnie zaburzyło to naturalną równowagę, ale pomimo ogromnych kosztów finansowych operacji rzeczywiste zyski w walce były niewielkie. Opisana technologia rozpraszania chmur deszczowych narodziła się już w 1946 r. w laboratoriach firmy General Electric. Tam odkryto działanie procesu, który nazwano zasiewaniem chmur.

Mniej więcej w tym samym czasie amerykańscy naukowcy próbowali kontrolować huragany. W południowych stanach USA huragany są prawdziwą katastrofą. Dążąc jednak do pozornie tak szlachetnego celu, naukowcy badali również możliwość wysłania huraganu do innych krajów. W tym celu słynny matematyk J. von Neumann współpracował z amerykańskim departamentem wojskowym.

Te i inne eksperymenty na przyrodzie doprowadziły do wniosku, że przede wszystkim cierpi na nich ludzkość jako całość. W 1978 r. weszła w życie Konwencja o zakazie używania technicznych środków oddziaływania na środowisko w celach militarnych lub jakichkolwiek innych celach wrogich – dotycząca np. sztucznej stymulacji trzęsień ziemi, topnienia lodu polarnego i zmian klimatu. Przyjęcie tej konwencji na forum ONZ zapobiega negatywnemu wpływaniu na modyfikację środowiska naturalnego przez nowe rodzaje broni. Było to następstwem wojny wietnamskiej, podczas której masowo stosowano defolianty i inne środki chemiczne niszczące roślinność tropikalną i uprawy w strefie działań wojennych.

Wszystkie kraje, które podpisały tę konwencję, były zobowiązane „nie szkodzić innym państwom, zmieniając lub kontrolując wszelkie procesy pogodowe na Ziemi, w tym jej hydrosferę i atmosferę". Zdaniem wielu ekspertów tajne prace nad stworzeniem absolutnej broni masowego rażenia nadal trwają.

Między ZSRR a USA została także podpisana umowa o przerwaniu opracowywania rozwiązań z zastosowaniem militarnym w tej sferze, lecz mimo to nadal kontynuowano badania. Niedawno odtajnione dokumenty świadczą o tym, że w latach 70. XX w. USA i ZSRR weszły w bezprecedensowy klimatyczny wyścig zbrojeń. Z dokumentów archiwum brytyjskiego rządu wynika, że oba supermocarstwa posądzały się nawzajem o przygotowania do „wojny klimatycznej". Zarówno USA, jak i ZSRR prowadziły tajne programy wojskowe kierowania klimatem na globalną skalę.

Zgodnie z → i n f o r m a c j a m i [t. 2] ONZ w ciągu ostatnich 25 lat liczba sytuacji nadzwyczajnych spowodowanych przez pogodę – takich jak lawiny, cyklony, wybuchy wulkanów, trzęsienia ziemi, susze, powodzie i huragany – potroiła się, a my wciąż nie znamy ich prawdziwych przyczyn. Dlatego wojskowi i naukowcy z wielu krajów dyskutują na temat różnych sposobów kontroli pogody. Tak np. huragan Katrina w sierpniu 2005 r. był jednym z 30 najbardziej morderczych huraganów, jakie kiedykolwiek nawiedziły USA, spowodował ogromne zniszczenia, zginęło prawie 2 tys. osób, ponad milion ludzi ewakuowano. Powódź spowodowana silnymi deszczami w południowo-wschodniej części Chin w czerwcu 2011 r. doprowadziła do ewakuacji ponad 2,4 mln osób. Zniszczone zostały drogi, mosty i tysiące domów, zalane zostało 5,2 tys. ha ziem uprawnych, powódź dotknęła 11 miast. W kontekście Polski należy zauważyć, że tak dynamicznych zmian pogody o tak katastrofalnych skutkach jak w ostatnich latach jeszcze nie było. 9,8 mln m^3 powalonych i połamanych drzew, 79,7 tys. ha uszkodzonych lasów, w tym 39,2 tys. ha do całkowitego odnowienia – to skutek tylko tych nawałnic, które w nocy z 11 na 12 sierpnia 2017 r. spustoszyły lasy w kilkudziesięciu nadleśnictwach, głównie na Pomorzu i Kujawach. Także w innych krajach huragany i powodzie poczyniły nie mniejsze szkody. Nie trzeba być zwolennikiem → t e o r i i s p i s k o w y c h [t. 4], żeby zastanowić się nad przyczyną takiego natężenia tych niebezpiecznych zjawisk. Niektórzy twierdzą, że mogą one być skutkiem programu testów broni klimatycznej, a huragany Harvey, Irma i Jose, które

gwałtownie uderzyły na karaibskie wyspy wiosną 2018 r., są w rzeczywistości wynikiem projektów geoinżynieryjnych „stworzonych przez człowieka", ale tego zapewne się nie dowiemy, ponieważ wszystkie programy wojskowe są ściśle tajne.

Chiny zapowiedziały przeprowadzenie największego w historii ludzkości eksperymentu związanego z modyfikacją pogody. Chcą wywoływać opady deszczu w jednym z najbardziej suchych miejsc na świecie. ChRL ogłosiła zamiar zmiany Wyżyny Tybetańskiej w żyzną krainę, ale żeby móc to zrobić, trzeba najpierw sprawić, aby na jednym z najbardziej suchych miejsc na Ziemi zaczął padać deszcz. Dlatego też planuje się rozmieścić na obszarze o powierzchni 1,5 mln km2, pięciokrotnie większym od Polski, specjalne komory spalania paliwa stałego, w których ma być produkowany jodek srebra. Projekty geoinżynieryjne mogą doprowadzić do katastrofy, ponieważ nie jest jasne, jak może się zachować ziemska atmosfera, gdy będziemy za pomocą substancji chemicznych próbować zmieniać pogodę lub klimat.

Jak podkreślają specjaliści geolodzy, technologia pozwala dziś na zatrzymanie albo na wywołanie deszczu. ZSRR pracował nad stworzeniem sztucznej mgły, usuwaniem naturalnej mgły i zapobieganiem wczesnym przymrozkom w ramach celów wojskowych. W ten sposób każdego roku zapewniano dobrą pogodę na placu Czerwonym w Moskwie podczas wojskowych defilad. Laboratoria opracowały specjalny rodzaj sztucznego lodu, którego zadaniem było kondensować parę wodną w pożądanych na niebie miejscach – tak odciągano znad placu Czerwonego chmury i kierowano deszcz na inne rejony miasta. W tym celu samoloty rozpylają kryształy srebra azotowego nad deszczowymi chmurami w celu zapewnienia słonecznej pogody.

Pionierem badań nad procesami elektromagnetycznymi w jonosferze na początku XX w. był słynny naukowiec N. Tesla. Warto przypomnieć popularną hipotezę, wg której słynny meteoryt tunguski z 1908 r., którego tajemnica wciąż nie jest odkryta, był eksperymentem Tesli – w jego rezultacie niewielka część energii jonosfery, zmieniona w rezonans przekaźnikami naukowca, została uwolniona nad tajgą syberyjską. Badania wynalazcy wciąż są owiane tajemnicą. Po jego śmierci archiwum naukowe zostało skonfiskowane przez FBI i utajnione. Pomysły Tesli wywarły ogromny wpływ na amerykańskiego fizyka dra B. Eastlunda – ów badacz ostatecznie zarejestrował patent na wynalazek, który mógłby zostać wykorzystany do zmiany pogody, zakłócania komunikacji na całym świecie i do odbicia ataku rakietowego.

Od 1960 r. wiele krajów zaczęło budowę elektrowni podobnych do nadajników Tesli – z wykorzystaniem nowoczesnych technologii, jednak znacznie bardziej wydajnych. Zakres ich stosowania jest oficjalnie uznawany za badania jonosfery. Najbardziej znanym obiektem w tym obszarze jest stacja HAARP (ang. High Frequency Active Auroral Research Program) – naukowe przedsięwzięcie mające na celu zbadanie właściwości i zachowania jonosfery. Amerykańskie eksperymenty w oficjalnej wersji dotyczą wpływu pola elektromagnetycznego na pogodę. Celem projektu jest – jak podkreślają jego twórcy – zrozumienie, stymulowanie i kontrola procesów zachodzących

w jonosferze, które mogą mieć wpływ na działanie systemów komunikacji i nadzoru elektronicznego.

Stacja HAARP na Alasce może stymulować uwalnianie energii wewnętrznej jonosfery, co może mieć wpływ na pogodę i klimat w wybranych regionach świata, otwierając drogę do wojen klimatycznych. Została zbudowana w 1997 r. Nie jest to jednak jedyny projekt tego typu; są jeszcze EISCAT i SPEAR w Norwegii oraz stacja HIPAS – także na Alasce. W 2001 r. została wybudowana 5. stacja projektu HAARP na Grenlandii, jej moc wynosi 11 tys. kW i dziś jest ona najpotężniejsza. Wszystkie 5 stacji projektu HAARP znajduje się w pobliżu północnego bieguna magnetycznego Ziemi, gdzie odbywa się przeniesienie strumienia energii naładowanych cząstek i plazmy emitowanych przez słońce w jonosferę. To znaczy, że stacje HAARP znajdują się tam, gdzie mogą być najbardziej efektywne procesy zarządzania w jonosferze. Wpływając na jonosferę, stacje HAARP są w stanie kontrolować pogodę i klimat na całej półkuli północnej. Od 2002 r., kiedy projekt HAARP zaczął być realizowany w pełnej skali, gwałtownie wzrosła liczba anomalnych zjawisk pogodowych na półkuli północnej.

W ZSRR w latach 1960–1970 również zbudowano stacje do badania jonosfery, podobne do HAARP. Dziś wiemy o 4, znajdują się one na terytorium Rosji, Ukrainy i w Tadżykistanie, są to: stacja Sura – 150 km od Niżnego Nowogrodu (Rosja), stacja w Murmańsku (Rosja), stacja w pobliżu Charkowa (Ukraina), stacja w pobliżu Duszanbe (Tadżykistan). Nie wiadomo, czy działają one obecnie, sądząc jednak po publikacjach, stacja Sura należąca do Narodowego Instytutu Badań Radiofizycznych (NIRFI) działa. Zajmuje ona obszar 9 ha, na którym w równych odległościach stoją szeregi 144 nadszarpniętych zębem czasu 20-metrowych anten. Obiekt oddano do użytku w 1981 r.

W XXI w. ludzka cywilizacja stała się najpotężniejszym czynnikiem wpływu na środowisko. Do tej pory, niestety, ten wpływ jest negatywny: bezmyślne, drapieżne wykorzystanie przez człowieka naturalnych zasobów planety, eskalacja badań naukowych w celu tworzenia nowych rodzajów broni – wszystko to prowadzi ludzkość do granicy, za którą cywilizację czekają niszczące wstrząsy i śmierć. Anomalii klimatycznych nie można uznać za konsekwencję jedynie globalnego ocieplenia wynikającego z zanieczyszczenia środowiska i emisji gazów cieplarnianych. Jest zbyt wiele przesłanek pozwalających sądzić o istnieniu technologii zarządzania klimatem w celach wojskowych, funkcjonujących pod przykrywką.

Broń klimatyczna niesie ze sobą poważne → z a g r o ż e n i e [t. 4] dla całej ludzkości dlatego, że ma ogromny zasób energii i może mieć nieprzewidywalne katastrofalne skutki. Na przykład cyklon, który w przyrodzie jest w ciągłym ruchu, ma ogromną moc, porównywalną z kilkudziesięcioma bombami atomowymi i wodorowymi.

Obecnie broń klimatyczna jest w zasięgu, ale do jej użycia – aby wpłynąć na klimat w skali globalnej, na obszarach o powierzchni wielu tysięcy kilometrów kwadratowych – potrzebne są zbyt duże zasoby. Wciąż nie w pełni rozumiemy mechanizmy występowania zjawisk pogodowych, dlatego wynik może być nieprzewidywalny, a kontrolowanie

takiej broni – problematyczne. Użycie broni klimatycznej może spowodować cios w samego agresora lub jego sojuszników i zniszczyć państwa neutralne. Ponadto regularnie prowadzi się obserwacje meteorologiczne, a użycie takiej broni spowodowałoby poważne anomalie pogodowe, które z pewnością nie pozostałyby niezauważone. Reakcja społeczności światowej na takie działania nie różniłaby się od reakcji na → a g r e s j ę nuklearną. Niewątpliwie trwają badania i eksperymenty nad tym rodzajem broni, lecz nadal jest bardzo daleko od stworzenia skutecznej broni klimatycznej.

Jeśli broń klimatyczna (w jakiejś formie) istnieje dzisiaj, jest mało prawdopodobne, że zostanie ona wykorzystana. Jak dotąd nie ma poważnych dowodów na istnienie takiej broni.

Olga Wasiuta

N. Begich, J. Manning, *Angels Don't Play this Haarp. Advances in Tesla Technology*, Earthpulse Press, Washington 1995; D. Degroot, *Never Such Weather Known in These Seas: Climatic Fluctuations and the Anglo-Dutch Wars of the Seventeenth Century, 1652–1674*, „Environment and History" 2014, no. 20; E.M. Freeland, C*hemtrails, HAARP, and the „Full Spectrum Dominance" of Planet Earth*, Feral House, Washington 2014; W.M. Gray, *Weather-modification by Carbon Dust Absorption of Solar Energy*, „Journal of Applied Meteorology" 1976, no. 15; T.J. House i in., *Weather as a Force Multiplier: Owning the Weather in 2025*, A Research Paper Presented To Air Force, 1996; T. Kasperek, W. Zacharewicz, *Obrona przeciwchemiczna okrętu: broń geofizyczna i inne nowe rodzaje broni masowego rażenia*, cz. 2, Akademia Marynarki Wojennej im. Bohaterów Westerplatte, Gdynia 2000; J.E. Smith, *HAARP – broń ostateczna*, tłum. K. Kurek, Amber, Warszawa 2004; tenże, *HAARP: The Ultimate Weapon of the Conspiracy*, Adventures Unlimited Press, Kempton 2002; O. Wasiuta, *Broń klimatyczna*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; В.Л. Правдивцев, *Тайные технологии. Биосферное и геосферное оружие*, Издательство Лаборатория знаний, Москва 2017.

BROŃ MASOWEGO RAŻENIA (BMR); inaczej broń masowej zagłady – to środki walki przeznaczone do rażenia organizmów żywych i sprzętu na znaczną (masową) skalę. W przeciwieństwie do broni konwencjonalnej nie można precyzyjnie określić ich szkodliwego działania w czasie i przestrzeni. Termin ten nie ma ujednoliconego znaczenia w prawie międzynarodowym, chociaż jest stosowany – jednak bez ścisłego zdefiniowania – w wielu traktatach (m.in. Traktat o przestrzeni kosmicznej z 1967 r., Traktat o dnie morza z 1971 r.).

Zazwyczaj przyjmuje się, że do BMR zaliczamy → b r o ń n u k l e a r n ą, →b r o ń b i o l o g i c z n ą, → b r o ń c h e m i c z n ą i → b r o ń r a d i o l o g i c z n ą. Ujęcie takie odnosi się do definicji wypracowanej przez ONZ, zawartej w rezolucji Komisji Zbrojeń Konwencjonalnych z 12 sierpnia 1948 r. Rezolucja nr 32/84 z 1977 r. zatwierdziła tę definicję do stosowania w sferze międzynarodowej dyplomacji. W związku z tym należy ją uznać za najbardziej powszechną w stosunkach międzynarodowych. Precyzyjne wskazanie rodzajów broni należących do BMR pozwala uniknąć kontrowersji związanych z nieostrym pojęciem „masowości" rażenia,

a także z oczywistym faktem, że w pewnych okolicznościach broń konwencjonalna może powodować znacznie większe straty niż BMR. Rodzaje broni traktowane jako BMR zasadniczo różnią się od broni konwencjonalnej za sprawą odmiennych czynników rażenia: w przypadku broni nuklearnej i radiologicznej jest to radiacja (chociaż w przypadku broni nuklearnej występują również inne czynniki rażenia, spotykane także w broni konwencjonalnej, radiacja odróżnia te rodzaje broni od innych), w przypadku broni chemicznej jest to zatrucie organizmu, a w przypadku broni biologicznej – choroby. Broń masowego rażenia funkcjonuje jako osobna kategoria od lat 40. XX w., jednak jej historia jest znacznie dłuższa. Wykorzystanie chemicznych i biologicznych czynników rażenia sięga czasów starożytnych. Dynamiczny rozwój broni masowego rażenia miał miejsce w 1. poł. XX w. Broń chemiczna w nowoczesnej formie pojawiła się na polach bitew podczas I wojny światowej, a nowoczesna broń biologiczna w latach 30. podczas japońskiej → i n w a z j i [t. 2] na Chiny i Mandżurię. Pod koniec II wojny światowej miał miejsce pierwszy test broni nuklearnej oraz jej pierwsze zastosowanie bojowe.

Po raz pierwszy termin broń masowego rażenia zastosowany został prawdopodobnie w grudniu 1937 r. Użył go arcybiskup Canterbury

W.C.G. Lang w orędziu na święta Bożego Narodzenia. Współczesna interpretacja tego pojęcia odnosi się do ang. określenia *atomic weapons and all other major weapons adaptable to mass destruction* (broń atomowa i inne główne rodzaje broni zdolne do spowodowania masowego zniszczenia) użytego w amerykańsko-brytyjsko-kanadyjskiej Deklaracji o bombie atomowej podpisanej 15 grudnia 1945 r. Analogiczne określenie (*weapons adaptable to mass destruction*, broń zdolna do spowodowania masowego zniszczenia) znalazło się w pierwszej rezolucji wydanej przez Zgromadzenie Ogólne ONZ (Rezolucja Zgromadzenia Ogólnego nr 1 z 24 stycznia 1946 r.).

W ciągu kilku następnych lat zamiast określenia *weapons adaptable to mass destruction* upowszechnił się termin *weapons of mass destruction*.

Definicja wypracowana w 1948 r. przez Komisję Zbrojeń Konwencjonalnych (UN Commission on Conventional Armaments – instytucja powołana w 1947 r. pod auspicjami → R a d y B e z p i e c z e ń s t w a O N Z [t. 3]) zawierała właśnie to określenie. Według niej broń masowego rażenia powinna być definiowana jako:

> broń atomowa oddziaływająca za pomocą eksplozji, broń radiologiczna, śmiercionośna broń chemiczna i biologiczna oraz każdy inny rodzaj broni opracowany w przyszłości posiadający charakterystyki porównywalne w zakresie efektu niszczącego do bomby atomowej i innych, wspomnianych wyżej, rodzajów broni.

W zasadzie definicja ta odpowiada postrzeganiu broni masowego rażenia jako broni nuklearnej (w tym przypadku użyto węższego pojęcia – broń atomowa), biologicznej, chemicznej i radiologicznej (NBCR), z ewentualnym rozszerzeniem tego katalogu o inne, powstałe w przyszłości rodzaje broni. Warty podkreślenia jest również fakt, że

broń chemiczna i biologiczna to broń o działaniu śmiercionośnym, co ma znaczenie w kontekście kontrowersji związanych np. z możliwością zaliczenia w poczet broni masowego rażenia środków o działaniu obezwładniającym czy oddziaływających na rośliny. Według przytoczonej definicji tego typu środki nie spełniają kryterium śmiercionośności i nie powinny być traktowane jako BMR.

Prawnomiędzynarodowy reżim regulujący kwestię BMR zakłada albo całkowitą → d e m i l i t a r y z a c j ę [t. 2] obszarów o ogólnym znaczeniu międzynarodowym (a więc wyeliminowanie wszystkich rodzajów broni, w tym BMR), albo odnosi się do poszczególnych rodzajów BMR. System nieproliferacji BMR składa się z traktatów rozbrojeniowych *sensu stricto*, które zakładają rozbrojenie powszechne (obejmujące jak największą grupę państw, a w optymalnym wariancie wszystkie państwa na świecie) oraz całkowite (wszystkie rodzaje broni danego rodzaju oraz wszystkie aktywności z nią związane – badania, produkcja, posiadanie, rozpowszechnianie, nabywanie, stosowanie; dodatkowo nakaz zniszczenia zapasów), a także traktaty w zakresie kontroli zbrojeń, które zakładają nałożenie ograniczeń w zakresie parametrów ilościowych i/lub jakościowych dopuszczalnych arsenałów albo w zakresie określonych aktywności związanych z danym rodzajem broni.

W zakresie BMR funkcjonują 2 traktaty rozbrojeniowe w ścisłym znaczeniu: Konwencja o broni biologicznej z 10 kwietnia 1972 r. oraz Konwencja o broni chemicznej z 13 stycznia 1993 r. Traktaty w zakresie kontroli zbrojeń odnoszące się do BMR podzielić można na 4 grupy. Pierwszą stanowią ograniczenia terytorialne ogólne, czyli wspomniana wcześniej demilitaryzacja obszarów o ogólnym znaczeniu międzynarodowym (Układ w sprawie Antarktydy z 1 grudnia 1959 r., Układ o przestrzeni kosmicznej z 27 stycznia 1967 r., Układ o dnie morza z 11 lutego 1971 r.). Druga grupa to ograniczenia terytorialne regionalne, czyli tworzenie stref wolnych od określonego rodzaju broni, np. stref wolnych od broni nuklearnej. Do trzeciej grupy ograniczeń jakościowych zaliczają się porozumienia zakazujące określonej działalności związanej z danego rodzaju bronią, np. testowania, proliferacji czy stosowania. Czwarta grupa to ograniczenia ilościowe, czyli redukcje zbrojeń, zakładające ograniczenie liczebności danego rodzaju broni lub likwidację pewnych kategorii broni w zakresie danego rodzaju broni.

Broń masowego rażenia ma nie tylko znaczenie militarne, ale także polityczne i normatywne – jej stosowanie uchodzi za przejaw barbarzyństwa i spotyka się z powszechnym potępieniem (jak w przypadku domniemanego stosowania broni chemicznej w czasie → w o j n y [t. 4] w Syrii). Prowadzi to do powstania swoistej linii demarkacyjnej między bronią konwencjonalną a niekonwencjonalną (rozumianą jako broń masowego rażenia). Ta pierwsza uchodzi za zwyczajowo uznane narzędzie prowadzenia konfliktów zbrojnych, druga z kolei traktowana jest przede wszystkim jako środek polityczno-militarnego oddziaływania poprzez → o d s t r a s z a n i e [t. 3]. Oskarżenie o wytwarzanie, posiadanie lub stosowanie broni masowego rażenia często

jest też wykorzystywane jako pretekst do interwencji zbrojnej (czego najlepszym przykładem jest atak na Irak w 2003 r.).

Rafał Kopeć

J. Baylis, M. Smith, *Kontrola broni masowej zagłady*, [w:] *Strategia we współczesnym świecie. Wprowadzenie do studiów strategicznych*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2009; M. Bentley, *Weapons of Mass Destruction and the US Foreign Policy. The Strategic Use of a Concept*, Routledge, New York 2014; T. Jemioło, T. Kubaczyk, M. Preus, *Broń masowego rażenia w świetle prawa międzynarodowego. Wybrane problemy*, AON, Warszawa 2004; R. Kopeć, *Broń masowego rażenia*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; tenże, *Broń masowego rażenia – definiowanie pojęcia*, „Bezpieczeństwo – Teoria i Praktyka" 2014, nr 4; tenże, *Militarne metody zapobiegania proliferacji broni masowego rażenia*, Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2015; J. Pawłowski, *System przeciwdziałania rozprzestrzenianiu broni masowego rażenia*, AON, Warszawa 2008.

BROŃ NIEŚMIERCIONOŚNA (ang. *non-lethal weapon*, NLW) – jeden z rodzajów broni używanych przez współczesne formacje policyjne i siły zbrojne, którego oddziaływanie na człowieka nie powoduje śmierci. Sojusz Północnoatlantycki definiuje broń nieśmiercionośną jako rodzaj broni, który jest jednoznacznie zaprojektowany i rozwijany w celu obezwładnienia lub odpierania ludzi, z niskim prawdopodobieństwem śmiertelności lub trwałego uszkodzenia ciała, lub do unieruchomienia urządzeń, przy minimalnym ich niepożądanym uszkodzeniu lub szkodliwym wpływie na środowisko. Departament Obrony USA przedstawia ją jako broń, urządzenia lub amunicję, które są zaprojektowane i wykorzystywane do obezwładniania siły żywej lub sprzętu wojskowego, z jednoczesnym minimalizowaniem ofiar śmiertelnych, trwałych uszkodzeń ciała, niepożądanych oddziaływań na mienie i środowisko naturalne. Skutki jej użycia w stosunku do ludzi i urządzeń powinny mieć charakter odwracalny.

Obok wielu definicji broni nieśmiercionośnej funkcjonuje również wiele sposobów jej klasyfikacji. Ze względu na obiekt oddziaływania dzieli się ona na broń oddziałującą na człowieka oraz broń przeciwmaterialną. Broń oddziałująca na człowieka ma za zadanie obezwładniać, nie dopuszczać do wchodzenia na określony teren lub do budynków, pacyfikować wzburzony tłum czy zmuszać do opuszczenia budynków, pojazdów itp. Broń oddziałująca na urządzenia techniczne służy m.in. do zatrzymywania i unieruchamiania pojazdów, uniemożliwienia sprawnego działania sprzętu technicznego, uniemożliwienia schronienia się w obiektach lub domach i korzystania z nich czy uniemożliwiania działania urządzeń przemysłowych. Broń nieśmiercionośna oddziałująca na ludzi dzieli się na: działającą na psychikę człowieka (fobie, paniki, apatie) oraz działającą na jego fizjologię (ból, pieczenie, mdłości, wymioty, padaczka, oślepienie, ogłuszenie). Kolejny podział dotyczy zastosowanych w niej technologii oraz zjawisk fizycznych. Polski badacz zajmujący się policyjnym i wojskowym wykorzystywaniem broni nieśmiercionośnej, N. Świętochowski, wyróżnił w tej klasyfikacji

broń mechaniczną i kinetyczną, → b r o ń c h e m i c z n ą, broń elektryczną, broń elektromagnetyczną i broń akustyczną. Raport Wysokiego Komisarza Narodów Zjednoczonych ds. Praw Człowieka (United Nations Human Rights Guidance on Less-Lethal Weapons in Law Enforcement) wymienił natomiast pałki policyjne, ręczne miotacze gazu, gaz łzawiący wystrzeliwany na dużą odległość, broń elektryczną typu taser, pociski kinetyczne (gumowe i plastikowe), broń oślepiającą, armatki wodne oraz broń akustyczną. Do grupy tej niektórzy badacze zaliczają również broń cyfrową (wirusy komputerowe, robaki komputerowe, zob. → z ł o ś l i w e o p r o g r a m o w a n i e [t. 4]), broń oddziałującą na środowisko (modyfikacja pogody, modyfikacja monosferyczna, herbicydy) czy oddziaływanie psychologiczne (→ p r o p a g a n d a [t. 3], →d e z i n f o r m a c j a [t. 2]).

Dynamiczny rozwój broni nieśmiercionośnej przypadł na lata 90. XX w. Jej początków należy jednak szukać w USA w latach 20. i 60. XX w. Jedną z przyczyn pojawienia się policyjnych broni, które nie służyły do zadawania śmierci, były liczne protesty i zamieszki uliczne związane z Free Speech Movement, ruchem antywojennym i ruchami na rzecz praw kobiet. W czasie zamieszek na ulicach amerykańskich miast używany był m.in. gaz drażniący 2-chlorobenzylidenomalononitryl. Oprócz gazu drażniącego formacje policyjne używały również pałek, armatek wodnych oraz amunicji niepenetracyjnej (obezwładniającej). Jednym z pierwszych przykładów użycia amunicji niepenetracyjnej były starcia demonstrantów z → p o l i c j ą [t. 3] w Hongkongu w 1958 r. Używano wówczas pocisków z drewna tekowego, które jednak powodowały poważne obrażenia łącznie z groźbą spowodowania śmierci. Mniejsze obrażenia powodowała amunicja gumowa wprowadzona do użytku w 1970 r. w oddziałach armii brytyjskiej stacjonującej w Irlandii Północnej. Kule z twardej gumy miały 15 cm długości, 3,5 cm średnicy i wagę 140 g. Od pierwszego zastosowania do końca 1974 r. w Irlandii Północnej wystrzelono ponad 55 tys. sztuk tego rodzaju amunicji. W Polsce broń gładkolufowa znalazła się na wyposażeniu policji w 1994 r. Wśród strzelb gładkolufowych znajduje się m.in. Mossberg kal. 12/70, Hatsan Escort kal. 12/70 czy SDASS Imperator kal. 12/70. W 1974 r. opatentowana została jedna z najbardziej znanych obecnie elektrycznych broni nieśmiercionośnych – amerykański taser. Jego pierwsze modele, takie jak TF-1, miały moc 5–7 W, a elektrody wystrzeliwane były za pomocą ładunku prochowego, w związku z tym taser zaliczano do broni palnej. Air-Taser wyposażony w elektrody wystrzeliwane za pomocą sprzężonego powietrza powstał w latach 90. XX w.

W związku z rosnącą liczbą operacji pokojowych organizowanych przez ONZ oraz postępującą w zachodnich społeczeństwach humanizacją → w o j n y [t. 4] broń nieśmiercionośna zaczęła być rozwijana oprócz formacji policyjnych także w siłach zbrojnych. W marcu 1995 r. amerykańska piechota morska wyposażona w broń nieśmiercionośną nadzorowała wycofywanie się 2,5 tys. → ż o ł n i e r z y [t. 4] misji ONZ z Somalii. W 1997 r. Pentagon powołał do życia Joint Nonlethal Weapons

Directorate (JNWD) – jednostkę zajmującą się badaniami i wdrożeniem broni nieśmiercionośnej w siłach zbrojnych USA. Wkrótce po powstaniu budżet JNWD wyniósł ponad 30 mln USD, a do 2004 r. wdrożono ponad 80 technologii opartych na NLW. Przykładami NLW o wojskowym zastosowaniu są m.in.: Long Range Acoustic Device, wykorzystujący dźwięki słyszalne celem pacyfikacji tłumu lub zwalczania → p i r a c t w a m o r s k i e g o [t. 3], Active Denial System umożliwiający rażenie precyzyjnymi falami milimetrowymi człowieka z odległości 1 km, powodujący piekący ból podskórny zmuszający do natychmiastowej ucieczki z pola rażenia, czy bomba E, która za pomocą silnego impulsu elektromagnetycznego może niszczyć urządzenia elektroniczne znajdujące się w promieniu kilkuset metrów od niej.

Tomasz Wójtowicz

T. Czechowicz, T. Głuchowski, *Strzelby gładkolufowe na wyposażeniu policji od 1994 roku*, Szkoła Policji w Katowicach, Zakład Wyszkolenia Specjalnego, Katowice 1994; N. Davison, *The Early History of Non-Lethal Weapons*, University of Bradford, Bradford 2006; D.P. Fidler, *The International Legal Implications of Non-Lethal Weapons*, „Michigan Journal of International Law" 1999, vol. 21, iss. 1; M. Kwiecińska, *Broń nieśmiercionośna w zastosowaniach wojsk*, „Obronność. Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej" 2015, nr 4 (16); NATO, *NATO Policy on Non-Lethal Weapons*, NATO.int (dostęp 23.12.2019); OHCHR, *United Nations Human Rights Guidance on Less-Lethal Weapons in Law Enforcement*, OHCHR, New York–Geneva 2020; N. Świętochowski, *Współczesna broń nieśmiercionośna. Podział i charakterystyka*, „Zeszyty Naukowe WSOWL" 2013, nr 2 (168).

BROŃ NUKLEARNA – rodzaj broni wykorzystującej wewnątrzjądrową energię wydzielaną podczas reakcji łańcuchowej rozszczepienia jąder ciężkich pierwiastków lub reakcji termojądrowej syntezy jąder lekkich pierwiastków. Wspólną cechą obu reakcji jest to, że energia powstaje podczas reakcji zachodzących w jądrach atomów, a nie wskutek oddziaływania elektronów zawartych w otaczających jądro powłokach elektronowych (jak w reakcjach chemicznych).

Pojawienie się broni nuklearnej (a w szczególności termonuklearnej) wymusiło całkowite przewartościowanie strategicznych pryncypiów rządzących zastosowaniem siły zbrojnej w celu realizacji politycznych zamierzeń. Dotychczas naczelną zasadą przyświecającą wojskowemu kierownictwu państwa było wygranie → w o j n y [t. 4]. Pojawienie się broni nuklearnej – z jej bezprecedensowym potencjałem niszczącym – spowodowało, że celem tym stało się uniknięcie wojny. Z tego powodu broń nuklearna jest przede wszystkim środkiem → o d s t r a s z a n i a [t. 3]. Cech odróżniających broń nuklearną od innych rodzajów broni nie da się adekwatnie opisać za pomocą parametrów ilościowych (np. porównania mocy wybuchu). Broń nuklearna nie jest bowiem „bronią jak każda inna, tylko nieco bardziej potężną", żeby przywołać słowa francuskiego stratega A. Beaufre'a. Cechą odróżniającą broń nuklearną od innych rodzajów broni jest bowiem doprowadzenie mocy niszczącej do takiego poziomu, że kryje się za nią już tylko wizja zagłady całej planety. Ta perspektywa, nierozerwalnie związana

z bronią nuklearną, każe postrzegać ją jako zjawisko zupełnie odrębne od innych rodzajów broni – w tym właśnie kryje się jej jakościowa odmienność.

W czasie → z i m n e j w o j n y [t. 4], chociaż pod względem liczebnym dominująca była taktyczna broń nuklearna (przeznaczona do użycia na polu walki – bomby, pociski artyleryjskie, pociski rakietowe o zasięgu do 500 km), kluczowe znaczenie zyskała broń strategiczna. Mocarstwa nuklearne opracowały i wdrożyły tzw. strategiczną triadę nuklearną. Składa się na nią broń nuklearna przenoszona za pomocą 3 głównych środków: międzykontynentalnych rakiet balistycznych bazowania lądowego (ICBM, od ang. *intercontinental ballistic missile*; na potrzeby układów z zakresu kontroli zbrojeń przyjmuje się, że ich zasięg przekracza 5500 km), pocisków balistycznych wystrzeliwanych z pokładów okrętów podwodnych (SLBM, od ang. *submarine-launched ballistic missile*) oraz bombowców strategicznych zdolnych do przenoszenia broni nuklearnej (bomb lub pocisków manewrujących). Koncepcja triady wynikała z potrzeby posiadania potencjału nuklearnego, który nie mógłby być całkowicie wyeliminowany przez niespodziewany atak nuklearny przeciwnika (tzw. atak *counterforce* – wymierzony w potencjał nuklearny). Przetrwanie pierwszego ataku warunkowało zdolność do wykonania ataku odwetowego, zazwyczaj wymierzonego w potencjał demograficzny i gospodarczy przeciwnika (tzw. atak *countervalue* – biorący na cel zasoby stanowiące dla przeciwnika wartość). Takie zdolności były i nadal są fundamentem nuklearnego odstraszania. Oprócz broni strategicznej oraz taktycznej wyróżnić możemy broń substrategiczną – o mniejszym zasięgu i często także mniejszej mocy niż broń strategiczna, ale w przeciwieństwie do broni taktycznej nieprzeznaczoną do zastosowania na polu walki. Kategoria ta została znacznie zredukowana w wyniku podpisania traktatu INF (Treaty on Intermediate-Range Nuclear Forces; Układ o całkowitej likwidacji pocisków pośredniego zasięgu) w 1987 r.

Zjawisko rozprzestrzeniania broni nuklearnej nazywamy proliferacją.

W chwili obecnej (stan na 2021 r.) bronią nuklearną dysponuje 9 państw. Są to (w nawiasie rok pierwszej próby nuklearnej): USA (1945), Rosja (wcześniej ZSRR, 1949), Wielka Brytania (1952), Francja (1960), Chiny (1964), Indie (1974), Pakistan (1998), Korea Północna (2006), Izrael (brak oficjalnej próby nuklearnej). Czasowa zależność między próbą nuklearną a wprowadzeniem broni nuklearnej do służby operacyjnej jest nieoczywista, np. Indie nie rozpoczęły militarnego programu nuklearnego bezpośrednio po próbie w 1974 r. (oficjalnie pokojowej), a Pakistan wprowadził broń nuklearną do służby na ok. dekadę przed oficjalną próbą. Pierwsze 5 państw (USA, Rosja, Wielka Brytania, Francja i Chiny) to tzw. oficjalne państwa nuklearne wg traktatu NPT (Non-Proliferation Treaty, Traktat o nierozprzestrzenianiu broni nuklearnej) z 1968 r., Indie, Pakistan i Izrael nie podpisały go, a Korea Północna wystąpiła z niego w 2003 r. Broń nuklearną miała także Republika Południowej Afryki (wycofała ją podczas transformacji systemowej związanej z odchodzeniem od apartheidu i przystąpiła do NPT jako państwo nienuklearne w 1994 r.) oraz 3 państwa poradzieckie: Ukraina, Białoruś i Kazachstan.

Obecnie żaden akt prawa międzynarodowego nie zakazuje wprost stosowania broni nuklearnej. Jednakże każde użycie broni powinno być zgodne z zasadami prawa międzynarodowego konfliktów zbrojnych, szczególnie z koniecznością → o c h r o n y l u d n o ś c i [t. 3] i obiektów cywilnych oraz z zakazem używania broni niezdolnej do rozróżniania między kombatantami i niekombatantami, a także z zakazem zadawania zbędnych cierpień kombatantom poprzez używanie pewnych rodzajów broni. Istnieją wątpliwości, czy w przypadku broni nuklearnej te warunki mogą być spełnione. Nierozstrzygnięte jednak pozostaje pytanie, czy nielegalne będzie tylko użycie broni nuklearnej niezgodne z przytoczonymi zasadami, czy też takowym będzie każde użycie broni nuklearnej, bo niezdolność do wypełnienia tych warunków wynika z samej istoty broni nuklearnej. Chociaż nie istnieje żaden traktat rozbrojeniowy *sensu stricto* dotyczący broni nuklearnej, funkcjonują traktaty w zakresie kontroli zbrojeń.

Podzielić je można na 4 grupy.

Pierwszą stanowią ograniczenia terytorialne ogólne, czyli → d e m i l i t a r y z a c j a [t. 2] obszarów o ogólnym znaczeniu międzynarodowym (Układ w sprawie Antarktydy z 1 grudnia 1959 r., Układ o przestrzeni kosmicznej z 27 stycznia 1967 r., Układ o dnie morza z 11 lutego 1971 r.). Układ Antarktyczny oraz Układ o dnie morza zakładają wyeliminowanie wszelkich rodzajów broni z danych obszarów, natomiast Układ o przestrzeni kosmicznej stosowanym zakazem obejmuje → b r o ń m a s o w e g o r a ż e n i a . W każdym przypadku oznacza to eliminację z danego obszaru broni nuklearnej.

Druga grupa to ograniczenia terytorialne regionalne, czyli tworzenie stref wolnych od broni nuklearnej. Do tej grupy zalicza się Traktat o zakazie broni jądrowej w Ameryce Łacińskiej i na Karaibach z 14 lutego 1967 r., Traktat o ustanowieniu strefy wolnej od broni nuklearnej na południowym Pacyfiku z 6 sierpnia 1985 r., Traktat o ustanowieniu strefy wolnej od broni nuklearnej w Afryce z 11 kwietnia 1996 r., Traktat o ustanowieniu strefy wolnej od broni nuklearnej w Azji Środkowej z 8 września 2006 r., deklarację z Cartageny z 4 grudnia 1991 r. (Boliwia, Ekwador, Kolumbia, Peru i Wenezuela) dotyczącą wyrzeczenia się wszystkich rodzajów broni masowego rażenia.

Do trzeciej grupy ograniczeń jakościowych należą porozumienia zakazujące określonej działalności związanej z danego rodzaju bronią, np. testowania, proliferacji czy stosowania. W zakresie związanym z bronią nuklearną i energią nuklearną można wyróżnić przede wszystkim wspomniany Układ o nierozprzestrzenianiu broni nuklearnej z 1 lipca 1968 r., zakazujący proliferacji tej broni. Poza tym do grupy tej należą: Układ o zakazie prób z bronią nuklearną w atmosferze, w przestrzeni kosmicznej i pod wodą z 5 sierpnia 1963 r., Układ o ograniczeniu podziemnych prób z bronią nuklearną z 3 lipca 1974 r., Układ o podziemnych eksplozjach nuklearnych w celach pokojowych z 28 maja 1976 r., Konwencja o ochronie fizycznej materiałów nuklearnych i obiektów nuklearnych z 3 marca 1980 r., a także Traktat o całkowitym zakazie prób

z bronią nuklearną z 24 września 1996 r., który jednakże nie wszedł w życie. Pośrednio z bronią nuklearną związane są również Traktat o ograniczeniu systemów obrony przeciwrakietowej z 26 maja 1976 r. (utracił moc obowiązującą 13 czerwca 2002 r., wskutek jednostronnego wypowiedzenia przez USA) oraz Konwencja o zakazie używania technicznych środków oddziaływania na środowisko w celach militarnych lub jakichkolwiek celach wrogich z 18 maja 1977 r.

Czwarta grupa to ograniczenia ilościowe, czyli redukcje zbrojeń, zakładające ograniczenie liczebności danego rodzaju broni lub likwidację pewnych kategorii broni w zakresie danego rodzaju broni. Porozumienia z tej grupy jak dotychczas zawierane były pomiędzy największymi mocarstwami nuklearnymi, czyli USA i ZSRR, a później Rosją. Zaliczyć do nich można: Traktat o redukcji zbrojeń strategicznych SALT I z 26 maja 1972 r., Traktat o redukcji zbrojeń strategicznych SALT II z 18 czerwca 1979 r. (nieratyfikowany), Traktat o likwidacji rakiet pośredniego zasięgu INF z 8 grudnia 1987 r. (utracił moc obowiązującą 2 sierpnia 2019 r., wskutek jednostronnego wypowiedzenia przez USA), Traktat o redukcji i ograniczeniu zbrojeń strategicznych START I z 31 lipca 1991 r. (wygasł 5 grudnia 2009 r.), Traktat o redukcji i ograniczeniu zbrojeń strategicznych START II z 3 stycznia 1993 r. (jednostronnie wypowiedziany przez Rosję 14 czerwca 2002 r.), Traktat o redukcji strategicznych potencjałów ofensywnych SORT z 24 maja 2002 r. (stracił moc obowiązującą 5 lutego 2011 r.), Traktat o redukcji i ograniczeniu zbrojeń strategicznych New START z 8 kwietnia 2010 r. Traktat New START zawarto na 10 lat od momentu wejścia w życie, a w lutym 2021 r. administracja Joe Bidena zgodziła się na wydłużenie na okres 5 lat obowiązywania traktatu ograniczającego strategiczne zbrojenia jądrowe.

Rafał Kopeć

P. Grudziński, *Teologia bomby. Narodziny systemu nuklearnego odstraszania 1939– 1953*, Państwowe Wydawnictwo Naukowe, Warszawa 1988; Ł. Kamieński, *Technologia i wojna przyszłości. Wokół nuklearnej i informacyjnej rewolucji w sprawach wojskowych*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2009; R. Kopeć, *Broń nuklearna*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; tenże, *Strategie nuklearne w okresie pozimnowojennym*, Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2014; R. Rhodes, *Jak powstała bomba atomowa*, Prószyński i S-ka, Warszawa 2000; T.S. Sechser, M. Fuhrmann, *Nuclear Weapons and Coercive Diplomacy*, Cambridge University Press, Cambridge–New York 2017; N. Tannenwald, *The Nuclear Taboo, The United States and the Non-Use of Nuclear Weapon since 1945*, Cambridge University Press, Cambridge 2007.

BROŃ ORBITALNA – broń rażąca cel poprzez umieszczenie satelity z głowicą bojową na orbicie przez rakietę nośną, a następnie poprzez poddanie tego satelity kontrolowanej deorbitacji. Ten rodzaj broni jest szerzej znany pod akronimami **FOBS** (ang. *Fractional Orbital Bombardment System*) oraz **MOBS** (ang. *Multiple Orbital Bombardment System*). Głowica kategorii FOBS przed deorbitacją wykonuje niepełny obrót orbitalny (wchodzi na tzw. orbitę szczątkową), natomiast głowica MOBS wchodzi na pełną orbitę i tam pozostaje: wykonuje więcej niż jeden obrót.

Systemy zaliczane do kategorii FOBS rozwijano w ZSRR w latach 60. XX w. jako metodę przenoszenia strategicznych głowic nuklearnych. Zaletą takiej koncepcji był w zasadzie nieograniczony zasięg. Jednak ważniejsze okazywało się to, że stanowiła ona większe wyzwanie dla rozwijanych wtedy systemów antyrakietowych: głowica zbliżała się na stosunkowo niewielkiej wysokości, po torze zupełnie odmiennym od balistycznego. Radzieccy inżynierowie szacowali, że amerykańskie radary będą w stanie ją wykryć zaledwie 2 minuty przed uderzeniem w cel. Co więcej, głowica mogła uderzyć z każdego kierunku, np. od południa, a to oznaczało, że ominie kluczowe systemy Dowództwa Obrony Północnoamerykańskiej Przestrzeni Powietrznej i Kosmicznej (ang. North American Aerospace Defense Command, NORAD). Zasadniczą niedogodnością była natomiast znacznie mniejsza dokładność w porównaniu do rakiet balistycznych – zagadnienie precyzyjnej deorbitacji było ówcześnie ogromnym wyzwaniem technicznym.

W Związku Radzieckim rozwijano 3 rakiety stanowiące podstawę bronitypu FOBS. Rakietę GR-1 (8K713) rozwijało biuro konstrukcyjne OKB-1 Siergieja Korolowa, rakietę UR-200B (8K83) – biuro OKB-52 Władimira Czołomieja, natomiast rakietę R-36O (8K69) – biuro OKB-586 Michaiła Jangiela. Rozwój rakiety GR-1 oficjalnie rozpoczęto w 1962 r. Trójstopniowa rakieta o masie 117 ton miała za zadanie wynieść na orbitę o wysokości 150 km głowicę nuklearną o mocy 2,2 megatony i masie 1500 kg. Do dalszego rozwoju wybrano jednak w 1965 r. rakietę R-36O. Ze względu na zastosowane paliwo nadawała się ona znacznie lepiej do długotrwałego przechowywania w silosach od GR-1. Ponadto rozwój GR-1 zanotował opóźnienie wywołane problemami z zespołem napędowym. Z kolei rakieta UR-200 we wszystkich wersjach straciła poparcie polityczne po odsunięciu od władzy Nikity Chruszczowa, głównego „mecenasa" Czołomieja. Rakieta R-36O stanowiła jedną z wersji ciężkiej międzykontynentalnej rakiety balistycznej R-36: pozostałe wersje to 8K67 z głowicą termonuklearną dużej mocy oraz 8K67P z trzema głowicami działającymi w systemie MRV (z wspólnym punktem celowania).

Rakietę R-36O testowano w latach 1965–1971. Początkowo system deorbitacji sprawiał ogromne problemy. Po ich rozwiązaniu system uznano za operacyjny 19 listopada 1968 r. Rozmieszczono 18 rakiet w silosach na terenie Bajkonuru, jednak bez zamontowanych głowic nuklearnych, przechowywanych oddzielnie. Jednostka uzyskała gotowość bojową w sierpniu 1969 r.

Głowica orbitująca miała oznaczenie 8F021. Wyposażono ją w system orientacji w przestrzeni, składający się z układu nawigacji inercyjnej oraz wysokościomierza radarowego. System określał moment rozpoczęcia manewru deorbitacji, inicjowanego przez silnik hamujący. Korektę trajektorii realizowano za pomocą 8 silników korekcyjnych.

Systemy typu FOBS okazały się ślepą uliczką w rozwoju radzieckiego strategicznego arsenału rakietowego – ze względu na dynamiczny rozwój konkurencji w postaci

międzykontynentalnych rakiet balistycznych oraz na stopniową utratę głównej zalety w postaci zdolności do przenikania przez obronę antyrakietową. Po pierwsze – radary pozahoryzontalne oraz sensory kosmiczne zdecydowanie lepiej radziły sobie z wykrywaniem broni FOBS, a po drugie – Amerykanie niezbyt kwapili się do rozwoju systemów antyrakietowych, a od 1972 r., na mocy traktatu ABM (ang. Anti-Ballistic Missile Treaty) ich rozwój znacznie ograniczano, w imię zachowania zimnowojennej równowagi strachu.

Broń tego rodzaju wzbudziła pewne kontrowersje podczas negocjacji traktatu o przestrzeni kosmicznej (Outer Space Treaty z 1967 r.). Traktat zakazywał umieszczania w kosmosie, w tym – na orbitach, → b r o n i m a s o w e g o r a ż e n i a [t. 1]. Stany Zjednoczone, chociaż świadome posiadania przez Związek Radziecki broni orbitalnej, uznały, że nie stanowi ona pogwałcenia zapisów traktatu, gdyż głowica nie wykonuje całkowitego obrotu orbitalnego – wykonuje jedynie częściowy. Co więcej, nawet gdyby obrót był całkowity, traktat nie zakazywał testowania orbitalnej broni masowego rażenia, lecz tylko – jej operacyjnego rozmieszczenia (a rakiety R-36O nie miały zamontowanych głowic nuklearnych, lecz były one przechowywane w oddzielnym magazynie). Ta niezwykła spolegliwość Amerykanów wynikała zapewne z przekonania o niewielkim militarnym znaczeniu orbitalnej broni nuklearnej, połączonym z chęcią ustanowienia traktatu kosmicznego i obawą przed jego storpedowaniem z powodu jednego zagadnienia o poślednim znaczeniu. Broń orbitalna została zakazana na mocy amerykańsko-radzieckiego porozumienia o ograniczeniu zbrojeń strategicznych SALT II z 1979 r. Wycofanie istniejących pocisków ze służby w styczniu 1983 r. było elementem realizacji postanowień tego traktatu.

W październiku 2021 r. pojawiły się → i n f o r m a c j e [t. 2] o teście chińskiego systemu FOBS, datowanym na sierpień 2021 tego roku. Informację ujawnił dziennik „Financial Times", natomiast chińskie ministerstwo spraw zagranicznych im zaprzeczyło: stwierdziło, że testowano nie pocisk, lecz statek kosmiczny. Według „Financial Times" testowany system stanowi połączenie broni typu FOBS oraz broni hipersonicznej typu HGV (ang. *Hipersonic Glide Vehicle*). Głowicę bojową ma w nim stanowić właśnie szybowiec hipersoniczny, którego atutem jest zdolność do wykonywania manewrów w celu zmylenia systemów obrony powietrznej. Znacząco utrudniłoby to przechwycenie takiej głowicy, zarówno w porównaniu z rakietami balistycznymi, jak i z klasycznymi głowicami typuFOBS/MOBS, poruszającymi się po względnie przewidywalnej trajektorii.

Rafał Kopeć

S. Buono, *Merely a 'Scrap of Paper'? The Outer Space Treaty in Historical Perspective*, „Diplomacy & Statecraft" 2020, vol. 31, iss. 2; M. Czajkowski, *Obrona przeciwrakietowa w stosunkach międzynarodowych*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2013; T. Rogoway, *China Tested A Fractional Orbital Bombardment System That Uses A Hypersonic Glide Vehicle: Report*, The Drive, https://www.thedrive.com/the-war-zone/42772/china-tested-a-fractional-orbital-bombardment-syste-m-that-uses-a-hypersonic-glide-vehicle-report (dostęp 29.11.2021);

A.A. Siddiqi, *The Soviet Fractional Orbiting Bombardment System (FOBS). A Short Technical History*, „Quest. The History of Spaceflights Quarterly" 2000, vol. 7, iss. 4.

BROŃ RADIOLOGICZNA – broń polegająca na rozpylaniu na danym obszarze pyłu radiacyjnego. Do jej budowy wykorzystać można ok. 200 izotopów promieniotwórczych (radioizotopów, radionuklidów) o wystarczająco długim czasie połowicznego rozpadu. Należą do nich np. stront, cez, kobalt, iryd, pluton, ameryk czy kaliforn.

Broń radiologiczna często jest określana mianem „brudnej bomby". Termin ten – mimo jego medialności – nie jest jednak precyzyjny. Po pierwsze każda → b r o ń n u k l e a r n a jest „brudna", gdyż powoduje skażenie środowiska (z wyjątkiem broni neutronowej, określanej jako „czysta"). Po drugie zastosowanie słowa „bomba" implikuje fakt, że do rozprzestrzenienia pyłu radiacyjnego wykorzystany zostanie ładunek wybuchowy (konwencjonalny). Tymczasem jest to tylko jedna z metod uwolnienia pyłu radiacyjnego. Najprostsza metoda polega na umieszczeniu w danym miejscu otwartego pojemnika z pyłem radioaktywnym. Broń radiacyjna różni się także w zależności od tego, jakie środowisko ma być skażone. Może to być nie tylko powietrze, ale także woda, ziemia, żywność, budynki, roślinność itp.

Broń radiologiczna w najbardziej klasycznej postaci zbudowana jest z pojemnika z materiałem radioaktywnym oraz konwencjonalnego ładunku wybuchowego, wykorzystywanego do rozproszenia materiału radioaktywnego. Jest to tzw. radiologiczne urządzenie rozpraszające (ang. *radiation dispersal device*, RDD). Fala uderzeniowa wybuchu powoduje rozprzestrzenienie pyłu radioaktywnego. Dalsze rozprzestrzenianie zależy od warunków atmosferycznych, m.in. od siły i kierunku wiatru, wilgotności, temperatury.

Broń radiologiczna nie ma w zasadzie praktycznego zastosowania militarnego – trudno przewidzieć skutki ataku, gdyż w dużej mierze zależą od warunków atmosferycznych. Może on zakończyć się porażeniem własnych wojsk. Precyzję ataku da się w pewnym stopniu zwiększyć, używając odmiennego nośnika – np. małego samolotu bezzałogowego do rozprzestrzenienia pyłu na określonym obszarze. Nie zmienia to jednak w zasadniczy sposób tej cechy broni. Broń radiologiczna stanowi przede wszystkim potencjalne narzędzie ataku terrorystycznego. W tym zastosowaniu jej wady nie mają większego znaczenia, co więcej, cechuje się ona wieloma zaletami jako broń obliczona na wywołanie efektu psychologicznego. Zastosowanie broni radiologicznej najprawdopodobniej nie pociągnęłoby za sobą masowych strat (ze względu na stosunkowo niewielki zasięg oddziaływania). Atak taki byłby obliczony na spowodowanie paraliżu aktywności ekonomicznej w strefie skażenia oraz wywołanie paniki. Obawy budzi również konieczność opuszczenia skażonego obszaru – w przypadku ataku z wykorzystaniem niektórych materiałów, np. cezu – nawet na kilkadziesiąt lat. Alternatywą jest niezmiernie skomplikowane i kosztowne usunięcie skutków skażenia pyłem radiacyjnym.

Kwestia możliwości pozyskania przez podmioty pozapaństwowe broni radiologicznej nie jest jednoznacznie rozstrzygnięta. Dostępność elementów towarzyszących (materiały wybuchowe, samolot bezzałogowy) nie stanowi oczywiście żadnego problemu. W ostateczności można posłużyć się zamachowcem samobójcą. Źródłem pozyskiwania materiałów radioaktywnych mogą być np. placówki → o c h r o n y z d r o w i a [t. 3] (aparatura do diagnostyki medycznej), przeciwpożarowe czujniki ostrzegawcze, urządzenia do sterylizacji żywności, sondy do badania szybów naftowych, sygnalizatory oblodzenia w samolotach, miejsca składowania prętów paliwa do reaktorów, uczelnie i ośrodki radiografii. Część z tych źródeł jest dobrze chroniona, część natomiast słabo lub w zasadzie nie jest objęta nadzorem. Dostępności sprzyjają także wysokie koszty utylizacji tego typu urządzeń, które powodują, że mogą one być albo wyrzucane, albo oferowane na sprzedaż zainteresowanym podmiotom.

Największe nasilenie incydentów związanych z nielegalnym handlem materiałami radioaktywnymi miało miejsce w połowie lat 90. XX w. Dotychczas jednak jedynym incydentem związanym z wykorzystaniem broni radiologicznej było zakopanie w moskiewskim parku zasobnika z radioaktywnym cezem-137 przez rebeliantów czeczeńskich w 1995 r. Przywódca Czeczenów S. Basajew poinformował o tym telewizję. Nie była to więc próba ataku radiologicznego, ale komunikat skierowany do władz rosyjskich, świadczący o tym, że separatyści (zob. → s e p a r a t y z m [t. 4]) czeczeńscy dysponują materiałami radioaktywnymi i mogą ich użyć. W 2017 r. pojawiły się → i n f o r m a c j e [t. 2] o wysiłkach → P a ń s t w a I s l a m s k i e g o [t. 3] w kierunku zdobycia materiałów rozszczepialnych potrzebnych do budowy „brudnej bomby". W Mołdawii ujawniono 4 próby przemytu materiałów rozszczepialnych, w tym uranu-235 i cezu-135. W lutym 2016 r. dyrektor Międzynarodowej Agencji Energii Atomowej Y. Amano poinformował, że od 1995 r. doszło do 2800 incydentów związanych ze zniknięciem niebezpiecznych materiałów. Innym potencjalnym sposobem dokonania ataku radiologicznego przez terrorystów jest uderzenie na obiekty wykorzystujące energię nuklearną. Do poważnego incydentu doszło w marcu 2016 r., 2 dni po zamachach terrorystycznych na lotnisko Zaventem i stację metra w Brukseli, dokonanych przez Państwo Islamskie. Zamordowano wtedy strażnika pracującego w belgijskiej elektrowni atomowej i skradziono jego przepustkę. Policyjne dochodzenie ujawniło także, że dyrektor belgijskiego programu badań jądrowych znajdował się pod obserwacją Państwa Islamskiego. W październiku 2016 r. Amano poinformował o → c y b e r a t a k u na elektrownię atomową, który spowodował zakłócenia w jej pracy. Nie ujawnił jednak żadnych szczegółów, w tym czasu ataku i kraju, w którym miał on miejsce.

Rafał Kopeć

J.M. Acton, M.B. Rogers, P. D. Zimmerman, *Beyond the Dirty Bomb: Re-Thinking Radiological Terror*, „Survival: Global Politics and Strategy" 2007, vol. 49, iss. 3; R. Kopeć, *Broń radiologiczna*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.),

Wydawnictwo Libron, Kraków 2018; tenże, *The Threat of Mega-Terrorism: Availability, Inhibitors and Motivations*, „Reality of Politics: Estimates – Comments – Forecasts" 2013, no. 4; W. Liss, *Brudna bomba – mit czy realne zagrożenie*, „Raport – Wojsko Technika Obronność" 2002, nr 7; H. Rosoff, D. Von Winterfeldt, *A Risk and Economic Analysis of Dirty Bomb Attack on the Ports of Los Angeles and Long Beach*, [w:] *Improving Homeland Security Decisions*, A. Abbas, M. Tambe, D. von Winterfeldt (eds.), Cambridge University Press, Cambridge 2017; J. Solarz, *Broń radiologiczna jako środek terroru*, „Kwartalnik Bellona" 2010, nr 1.

BROŃ STRZELECKA – rodzaj broni palnej wykorzystujący amunicję strzelecką, czyli taką, której kaliber na ogół nie przekracza 20 mm (z wyjątkiem wyspecjalizowanych urządzeń, jak granatniki). Broń palna z kolei to urządzenie, które w wyniku działania sprężonych gazów powstających na skutek spalania materiału miotającego jest zdolne do wystrzelenia pocisku lub substancji z lufy bądź elementu zastępującego, a przez to do rażenia celów na odległość.

Obecnie, z wyjątkiem broni historycznej, stosowana jest amunicja zespolona. W naboju zespolonym pocisk, ładunek miotający (prochowy) i spłonka połączone są w całość za pomocą łuski. Wykorzystywany nabój w dużej mierze determinuje cechy broni, stąd jest on podstawą jednej z zasadniczych typologii broni strzeleckiej. Na tej podstawie wyróżniamy 3 zasadnicze kategorie:

- broń strzelającą nabojem pistoletowym (pistolety, pistolety maszynowe);
- broń strzelającą nabojem pośrednim (karabinki automatyczne, ręczne karabinki maszynowe);
- broń strzelającą nabojem karabinowym (karabiny, karabiny maszynowe).

Ponadto występują kategorie uzupełniające wynikające z zastosowania innych rodzajów nabojów, np. rewolwerowych, wielkokalibrowych.

Biorąc pod uwagę stopień automatyzacji broni, wyróżniamy:

- Broń nieautomatyczną, w której czynności związane z przygotowywaniem strzału wykonywane są ręcznie, w tym:
  - jednostrzałową: każdy nabój ładowany jest pojedynczo przed strzałem do lufy lub komory nabojowej;
  - powtarzalną: naboje ładowane są do mechanizmu zasilającego (magazynka), przeładowanie (dosyłanie naboju do komory nabojowej) wykonywane jest ręcznie.
- Broń automatyczną, w przypadku której ręcznie wykonywane są tylko czynności związane z przygotowaniem do oddania pierwszego strzału, a następnie czynności związane z przygotowaniem i oddaniem kolejnych strzałów wykonywane są dzięki energii gazów prochowych. Wyróżnia się tu broń:
  - samopowtarzalną: pełna automatyka przeładowania, ale możliwość prowadzenia tylko ognia pojedynczego (oddanie strzału wymaga dodatkowej czynności strzelca);
  - samoczynną: pełna automatyka przeładowania i oddawania następnych strzałów, możliwość prowadzenia ognia ciągłego. Znaczna część broni samoczynnej

ma również możliwość prowadzenia ognia pojedynczego, co czyni z niej broń samoczynno-samopowtarzalną.

- Broń samoczynną – tradycyjnie określa się jako maszynową, a na współczesnym polu walki pełni ona funkcję broni wsparcia (np. ręczny karabin maszynowy). Z kolei broń samoczynno-samopowtarzalna tradycyjnie określana jest jako automatyczna (np. karabinek automatyczny; warto zaznaczyć, że chodzi tu o węższe znaczenie automatyczności niż w przypadku ogólnego podziału na broń automatyczną i nieautomatyczną) i pełni ona funkcję podstawowej broni indywidualnej → ż o ł n i e r z a [t. 4] piechoty.
- Broń półautomatyczną, w przypadku której część operacji w ramach cyklu pracy broni wykonywana jest z wykorzystaniem energii gazów prochowych, a część ręcznie (nieliczne przykłady broni strzeleckiej, jak karabin przeciwpancerny PTRD).
- Broń napędową, w przypadku której do napędu automatyki wykorzystywana jest wyłącznie energia z zewnętrznego silnika (obecnie przede wszystkim wielolufowe karabiny w układzie Gatlinga).

Działanie broni automatycznej opiera się na jednym z kilku sposobów automatycznej realizacji procesów wchodzących w skład cyklu pracy broni. Pierwszą grupą jest broń działająca na zasadzie odrzutu. Powszechnie stosowanymi zasadami są: odrzut zamka (swobodnego lub półswobodnego) oraz odrzut lufy (krótki i długi). Rzadko spotykaną zasadą działania broni jest odrzut całej broni. Druga grupa to broń działająca na zasadzie narzutu lufy, ale obejmuje ona rzadkie, raczej historyczne typy broni strzeleckiej. Trzecia grupa to broń działająca na zasadzie odprowadzania gazów prochowych z przestrzeni zapociskowej. Oprócz niszowych sposobów realizacji tej zasady (z części wylotowej lufy oraz z dna komory nabojowej) najczęściej spotykanym sposobem jest odprowadzanie gazów prochowych z przewodu lufy. Sposób ten może być realizowany za pośrednictwem układu bez tłoka gazowego oraz z tłokiem gazowym (w tym ostatnim przypadku z długim lub krótkim ruchem tłoka).

Broń strzelecka we współczesnej postaci znana jest od 2 poł. XIX w., kiedy pojawiła się większość rozwiązań określających do chwili obecnej zasadniczy schemat konstrukcyjny broni strzeleckiej. Do rozwiązań tych należą: broń ładowana odtylcowo (1849), nabój w łusce metalowej (1869), nabój elaborowany prochem bezdymnym (1886), broń powtarzalna (1867), magazynek wymienny (1888), broń automatyczna (1882). W okresie II wojny światowej wprowadzono nową kategorię broni, jaką jest karabinek automatyczny na nabój pośredni, będący do czasów współczesnych zasadniczym rodzajem indywidualnego uzbrojenia żołnierza piechoty. Jedną z pierwszych tego rodzaju konstrukcji – i pierwszą powszechnie wykorzystywaną – był niemiecki StG44. Dominującą pozycję w tej kategorii zdobyły 2 rodziny broni – radziecki karabinek AK oraz broń oparta na rozwiązaniach konstrukcyjnych amerykańskiego karabinka AR-15 (m.in. M16, M4).

W latach 80. prowadzono rewolucyjne projekty zmierzające do wzrostu skuteczności broni strzeleckiej, m.in. w ZSRR (projekt Abakan – broń z możliwością wystrzeliwania 2-strzałowej serii z bardzo dużą szybkostrzelnością), w Niemczech (oparty na amunicji bezłuskowej karabinek G11) oraz w USA (program Advanced Combat Rifle, w ramach którego testowano m.in. broń na amunicję strzałkową). Ze względu na koniec → z i m n e j w o j n y [t. 4] projekty te zarzucono, a rozwój broni strzeleckiej poszedł w innym kierunku. Skupiono się nie na rewolucyjnych rozwiązaniach technicznych, ale przede wszystkim na stopniowej poprawie ergonomii broni oraz zwiększeniu jej modułowości. Przykładem tej tendencji są systemy szyn montażowych, które przy okazji ułatwiły powszechne stosowanie celowników optycznych i kolimatorowych, co jest kolejnym trendem rozwojowym broni strzeleckiej, polegającym na zmniejszeniu błędów celowania.

Chociaż broń strzelecka jest niezbędnym wyposażeniem żołnierza i obowiązkowym elementem współczesnych działań zbrojnych, jej bezpośredni wpływ na przebieg walk zazwyczaj nie jest znaczący. Procent strat zadawanych na współczesnym polu walki przez broń strzelecką szacuje się na 10–25, natomiast zasadnicza część strat jest zadawana przez → a r t y l e r i ę. Rośnie za to znaczenie broni strzeleckiej w atakach terrorystycznych. Przy zastosowaniu odpowiedniej taktyki zamachowcy są w stanie zadawać straty, które dotychczas były możliwe przede wszystkim z wykorzystaniem materiałów wybuchowych, a przy tym osiągają odpowiednio silny efekt psychologiczny.

Rafał Kopeć

A. Ciepliński, R. Woźniak, *Encyklopedia współczesnej broni palnej*, WiS, Warszawa 1994; M. Czerwiński, *Broń strzelecka XX i XXI wieku*, Bellona, Warszawa 2016; S. Kochański, *Automatyczna broń strzelecka*, Sigma-NOT, Warszawa 1991; tenże, *Broń strzelecka lat osiemdziesiątych*, Bellona, Warszawa 1991; R. Kopeć, *Broń strzelecka*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; R. Kopeć, K. Kopeć, *Postinstytucjonalna rewolucja przemysłowa na przykładzie prosumpcyjnego modelu produkcji broni strzeleckiej*, [w:] *Przemysł zbrojeniowy. Tendencje, perspektywy, uwarunkowania, innowacje*, R. Kopeć (red.), Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2016; P. Kupidura, R. Woźniak, M. Zahor, *Współczesne karabiny maszynowe*, Bellona, Warszawa 2003.

BRYTYJSKA KRÓLEWSKA MARYNARKA WOJENNA (Royal Navy) – należy do najstarszych sił morskich na świecie. Tylko nieistniejąca już flota austriacka mogłaby się chlubić nieco dłuższą historią, sięgającą 1278 r. Jako stały rodzaj sił zbrojnych Royal Navy istnieje od epoki Tudorów, a po I wojnie światowej była hegemonem na światowych morzach i oceanach. Drugi ze światowych konfliktów zepchnął → m a r y n a r k ę w o j e n n ą [t. 3] imperium brytyjskiego z pierwszego miejsca, które – w zasadzie od → b i t w y [t. 1] pod Midway – należy do US Navy.

Gdy po śmierci Jerzego VI (6 lutego 1952 r.) Elżbieta II obejmowała brytyjski tron, Royal Navy była już znacznie słabsza od → M a r y n a r k i W o j e n n e j

S t a n ó w Z j e d n o c z o n y c h , a jej potencjał niewiele już przewyższał rosnącą w siłę flotę radziecką. Nawet przystąpienie Wielkiej Brytanii do → N A T O [t. 3] i rozpoczęcie → z i m n e j w o j n y [t. 4], co doprowadziło wkrótce do wyścigu zbrojeń między Zachodem a ZSRR, nie było w stanie powstrzymać spadku znaczenia niegdysiejszej „królowej mórz". Oczywiście zdolności operacyjne oraz wyszkolenie kadry floty brytyjskiej nadal pozostawały na wysokim poziomie, czego dowiodła interwencja przeciw Egiptowi (we współdziałaniu z Francją i Izraelem), znana jako operacja Musketeer, z października 1956 r. Trzon sił brytyjskich stanowiła eskadra lotniskowców (HMS Albion, Bulwark, Eagle, Ocean, Theseus) oraz kilka krążowników w eskorcie licznych niszczycieli i fregat. Cele militarne operacji zostały wprawdzie osiągnięte, lecz politycznie zakończyła się ona fiaskiem z racji ostrej reakcji dyplomacji radzieckiej i dwuznacznego stanowiska USA.

Duża liczba stosunkowo nowoczesnych okrętów (w momencie gdy wchodziły do służby tuż po zakończeniu II wojny światowej) i redukcje ilościowe sprawiły, że dla Royal Navy w zasadzie przez cały okres lat 50. minionego stulecia budowano niewiele okrętów. Jeśli chodzi o innowacje w przemyśle okrętowym, to Brytyjczycy zaczęli odstawać nie tylko od Amerykanów, ale także innych sojuszników z NATO, Francuzów, a nawet Włochów. Przykładem takiego stanu rzeczy była budowa krążowników typu Minotaur / Tiger, pod które stępki położono jeszcze pod koniec II wojny światowej. Liczne zmiany planów i koncepcji dotyczących tych okrętów doprowadziły do tego, że ostatecznie wcielono je do służby u progu lat 60. minionego stulecia po niemal 20 latach budowy. Był to niechlubny rekord brytyjskiego przemysłu okrętowego, związany także ze sporami koncepcyjnymi w brytyjskiej admiralicji co do pomysłów na wykorzystanie tych jednostek, z których ostatecznie tylko 3 zasiliły Royal Navy: HMS Lion, Blake i Tiger. Dwa ostatnie zostały przebudowane w połowie lat 60. XX stulecia na krążowniki śmigłowcowe. Dla porównania, w tym samym czasie włoska Marina Militare oddała do służby 3 mniejsze, ale znacznie nowocześniejsze jednostki podobnego przeznaczenia typu Andrea Doria i Vittorio Veneto. Ten wymowny fakt najlepiej świadczy o kondycji Royal Navy w połowie minionego wieku. Wprawdzie planowano budowę w tym okresie nowych krążowników (tzw. *escort cruiser*), co było elementem szerszego programu budowy nowych lotniskowców (CVA 01), ale pozostał on wyłącznie w sferze koncepcyjnej. W ten sposób 3 krążowniki typu Minotaur / Tiger były ostatnimi jednostkami tej klasy służącymi w Royal Navy.

Po części cięcia w finansowaniu budowy okrętów konwencjonalnych spowodowane były przystąpieniem brytyjskiej marynarki wojennej do nuklearnego wyścigu zbrojeń morskich. W 1960 r. królowa Elżbieta II dokonała chrztu wodowanego kadłuba pierwszego brytyjskiego okrętu podwodnego o napędzie nuklearnym HMS Dreadnought. Nazwa tej jednostki, którą wcielono do służby 3 lata później, nie była przypadkowa. Nawiązywała bowiem do okrętu liniowego o tej samej nazwie, który rozpoczął nowy jakościowo wyścig zbrojeń morskich po doświadczeniach bitwy

cuszimskiej, polegający na budowie potężniejszych od dotychczasowych pancerników. Budowa tego okrętu byłaby jednak niemożliwa – co stanowiło swoiste *signum temporis* – bez pomocy amerykańskiej, a konkretnie rzecz ujmując, bez dostarczenia stronie brytyjskiej reaktora atomowego przez Amerykanów. HMS Dreadnought był okrętem napędzanym nuklearnie, ale wyposażony był wyłącznie w uzbrojenie konwencjonalne –6 wyrzutni torped kalibru 533 mm.

Prawdziwa zmiana jakościowa nastąpiła kilka lat później, gdy do służby weszły 4 (z planowanych pierwotnie 5) okręty podwodne o napędzie nuklearnym, uzbrojone w pociski balistyczne typu Polaris. Były to jednostki typu Resolution. Poza czołowym okrętem tej serii pozostałe trzy to: HMS Repulse, Renown i Revenge. Piąta jednostka, dla której planowano nazwę Ramillies, nie została zbudowana. Okręty stanowiły część brytyjskiego systemu odstraszania nuklearnego (uzupełnianego bombowcami strategicznymi Vulcan oraz szturmowymi Jaguar i Buccaneer, dostosowanymi do przenoszenia ładunków jądrowych). Pociski rakietowe średniego zasięgu Blue Streak okazały się zbyt kosztowne i nie uruchomiono ich seryjnej produkcji. Okręty podwodne typu Resolution stanowiły podstawową część brytyjskiego programu Polaris, oficjalnie nazwanego Brytyjskim Systemem Pocisków Balistycznych Marynarki Wojennej. Polaris funkcjonował w latach 1968–1996, stanowił system operacyjny złożony z owych 4 okrętów podwodnych z pociskami balistycznymi typu Resolution, każdy był uzbrojony w 16 pocisków balistycznych Polaris A-3. Pocisk był w stanie przenosić 3 głowice termojądrowe ET317. Ta konfiguracja została później zmodernizowana, aby pomieścić 2 głowice utwardzone przed skutkami promieniowania i jądrowego impulsu elektromagnetycznego. Brytyjski program Polaris został ogłoszony w grudniu 1962 r. po podpisaniu umowy w Nassau między Stanami Zjednoczonymi a Wielką Brytanią. Formalne ramy współpracy stworzyła umowa sprzedaży pocisków Polaris. Budowa okrętów podwodnych rozpoczęła się w 1964 r., a pierwszy patrol okrętu tego typu odbył się w czerwcu 1968 r. Wszystkie 4 jednostki osiągnęły gotowość operacyjną w grudniu 1969 r. Stacjonowały w Clyde Naval Base na zachodnim wybrzeżu Szkocji, kilka mil morskich od Glasgow. Co najmniej 1 okręt podwodny był zawsze na patrolu, aby zapewnić ciągłe odstraszanie na morzu. Ta zasada obowiązuje do dziś na jednostkach zbudowanych w ramach programu Trident.

Powstaniu flotylli okrętów podwodnych strategicznego znaczenia towarzyszyła rozbudowa jednostek o napędzie nuklearnym wyposażonych w uzbrojenie konwencjonalne. Dreadnought był okrętem prototypowym, nie miał bliźniaczych jednostek. Typ Valiant obejmował już 2 okręty(bliźniakiem prototypu był HMS Warspite), stanowiły one konstrukcyjne rozwinięcie Dreadnoughta. Okręty te weszły do służby w latach 1963–1965 i pozostawały w niej przez prawie 30 lat. Uchodziły za udane jednostki w swojej klasie, były chwalone przez załogi i dowodzących nimi oficerów. Kolejnym typem okrętów podwodnych z napędem nuklearnym uzbrojonych konwencjonalnie był

HMS Churchill i 2 bliźniacze jednostki, a mianowicie: HMS Conqueror i Courageous. Oddano je do służby w latach 1967–1970. HMS Conqueror, dowodzony przez kmdr. por. Chrisa Wreforda-Browna, wsławił się podczas → k o n f l i k t u f a l k l a n d z k i e g o zatopieniem argentyńskiego krążownika General Belgrano.

Podwodne zbrojenia nuklearne Royal Navy generowały bardzo wysokie koszty. Budowa okrętów typu Churchill pochłonęła łącznie prawie 85 mln funtów, a jednostek typu Resolution – ok. 40 mln funtów za sztukę. Tak znaczne nakłady na podwodną flotyllę nuklearną nie pozostały bezwpływu na jakość oraz liczbę nawodnych okrętów o konwencjonalnym uzbrojeniu. Dość powiedzieć, że pod koniec lat 50. minionego stulecia pozostające w służbie najnowsze brytyjskie niszczyciele typu Daring projektowano pod koniec II wojny światowej.

Dlatego też projekt nowych, dużych okrętów nawodnych opracowywano niezwykle starannie. Rozważano koncepcję budowy 4 krążowników rakietowych i 8–10 niszczycieli o podobnym (choć mniej licznym) uzbrojeniu. Ostatecznie po wielu pracach studyjnych zdecydowano się na kompromisowy projekt, który przeszedł do historii jako typ County. Jakkolwiek okręty te zostały ostatecznie sklasyfikowane jako niszczyciele (*destroyers*), to pod względem wyporności (ponad 6,2 tys. t) na tle innych ówczesnych jednostek tej klasy (np. amerykańskich Charles F. Adams czy radzieckich Kanin), mających wyporność standardową ok. 3,5 tys. t, były zdecydowanie większe. Otrzymały potężne uzbrojenie artyleryjsko-rakietowe, na które składały się: 4 działa uniwersalne kalibru 114 mm (nawiasem mówiąc, ten kaliber jest podstawowym kalibrem używanym do dziś na dużych okrętach Royal Navy, jak niszczyciele i fregaty), 1 podwójna wyrzutnia rakiet Sea Slug oraz 2 poczwórne wyrzutnie rakiet Sea Cat. Hybrydowy napęd(turbiny parowe i gazowe) miał moc 60 tys. KM i zapewniał prędkość maksymalną 30 węzłów. Okręty miały nad wyraz elegancką sylwetkę, przypominającą duży jacht oceaniczny. Okazały się bardzo udanymi jednostkami, pozostały w służbie do przełomu lat 60. i 70. ubiegłego stulecia.

Planowano budowę 10 okrętów, ostatecznie ukończono 8. W miejsce7 nigdy niewybudowanych niszczycieli typu 82 Royal Navy zamówiła dodatkowo 7 fregat typu Leander.

To okręty tej klasy zastąpiły od lat 60. XX w. niszczyciele w służbie uniwersalnych okrętów eskortowych Jej Królewskiej Mości. Łącznie zbudowano aż 26 jednostek tego typu. Przy standardowej wyporności sięgającej niemal 2,4 tys. t uzbrojono je w dwulufową wieżę dział kalibru 114 mm, na niektórych okrętach zastąpiono ją później wyrzutnią rakiet typu Exocet, 2 działka kalibru 20 mm. Miały także uzbrojenie przeciwpodwodne. Podstawą uzbrojenia przeciwlotniczego były rakiety Sea Cat. Prędkość maksymalna sięgała 28,5 węzła. Cztery jednostki tego typu walczyły w wojnie falklandzkiej (HMS Andromeda, Argonaut, Minerva oraz Penelope). Kolejnym rozwinięciem konstrukcyjnym fregat brytyjskich było 8 jednostek określanych jako Amazon lub typ 21. Budowane były one w latach 1969–1978 i były swoistą

budżetową konstrukcją powstałą pod wpływem narastających cięć w w finansowaniu Royal Navy. Mimo to mogły uchodzić za udane okręty w swojej klasie. Przy zbliżonym (choć zmodyfikowanym) uzbrojeniu w stosunku do poprzedników dysponowały znacznie większą prędkością (w granicach 33 węzłów) i nieporównywalnym z innymi okrętami tej kategorii przyśpieszeniem. Dlatego ich dowódcy określani byli przez kolegów z innych okrętów mianem „chłopców wyścigowców" (*the boy racers*).

Lata 70. XX w. były okresem głębokiego kryzysu gospodarczego i społecznego Zjednoczonego Królestwa. Przezwyciężono go dopiero w następnej dekadzie, w dobie rządów Margaret Thatcher. Jednocześnie dobiegła końca epoka imperialnej Brytanii. Oba te czynniki nie pozostały bez wpływu na kondycję Royal Navy.

Jak już wspomniano, zrezygnowano z budowy dużych lotniskowców uderzeniowych, a rolę pływających lotnisk miały przejąć okręty projektowane początkowo jako krążowniki helikopterowe typu Invincible (oprócz jednostki czołowej były to HMS Illustrious oraz Ark Royal). Ironią losu jest fakt, że projektowano je jako okręty eskortowe lotniskowców z planu CVA 01. Jedynym jasnym punktem w tej wymuszonej redukcji lotnictwa morskiego były samoloty myśliwsko-szturmowe skonstruowane przez British Aerospace, mianowicie odrzutowce pionowego startu i lądowania typu Harrier. Ich morska wersja Harrier GR 7/9 stała się trzonem skrzydła lotniczego na tych okrętach, który doskonale się sprawdził w wojnie falklandzkiej.

Początek rządów konserwatywnych w 1979 r. przyniósł znaczne redukcje we flocie – na pozostałym dużym lotniskowcu floty HMS Ark Royal w 1979 r. po raz ostatni opuszczono banderę. Ówczesny minister obrony w rządzie Żelaznej Damy, John Nott, po zmianie planów dotyczących przyszłości Royal Navy (jeszcze większe redukcje) zamierzał sprzedać prototypowy nowy okręt lotniczy HMS Invincible Australii. On i jego współpracownicy doszli bowiem do wniosku, że na potrzeby marynarki wojennej wystarczą 2 jednostki tego typu. Zadaniem Royal Navy było już tylko utrzymanie dróg komunikacyjnych między Starym a Nowym Światem na wypadek → w o j n y [t. 4] między NATO a ZSRR i jego satelitami z Układu Warszawskiego. Poza tym u islandzkich wybrzeży pozostała eskorta brytyjskich rybaków od czasu słynnych „wojen dorszowych", rozpoczętych w latach 50. minionego wieku, a zakończonych w 1976 r.

Sytuację zdecydowanie zmienił wybuch konfliktu o Falklandy między Londynem a Buenos Aires, zapoczątkowany argentyńską → i n w a z j ą [t. 2] na ten archipelag 2 kwietnia 1982 r. Wprawdzie był on zwycięski dla Wielkiej Brytanii, ale wykazał duże braki jakościowe i ilościowe Royal Navy i zadecydował o zatrzymaniu degradacji brytyjskiej marynarki.

Najważniejszym elementem zmiany w marynarce wojennej, co premier Thatcher uznała za absolutny priorytet, była budowa nowych okrętów podwodnych o napędzie nuklearnym, nosicieli pocisków balistycznych, następców jednostek typu Resolution. W atmosferze wyścigu zbrojeń NATO z ZSRR uzyskała w tej mierze wsparcie od amerykańskiego politycznego partnera i osobistego przyjaciela w jednym – prezydenta

Ronalda Reagana. Już w 1981 r. administracja prezydenta Reagana wyraziła zgodę na udostępnienie Brytyjczykom pocisków balistycznych Trident II najnowszej generacji. Zwycięstwo wyborcze Partii Konserwatywnej w 1983 r. przypieczętowało tę decyzję, gdyż opozycyjna Partia Pracy szermowała podczas kampanii wyborczej hasłem anulowania tego programu. Pierwszy okręt nowej generacji, nosiciel pocisków balistycznych HMS Vanguard, wszedł do służby w 1986 r. Następne bliźniacze okręty wcielono do służby w 1995 r. – HMS Victorious i w 1996 r. – HMS Vigilant, wreszcie ostatni HMS Vengeance podniósł banderę w 1999 r. Wszystkie okręty do dziś pozostają w aktywnej służbie. Planowana jest kolejna wymiana podwodnych nosicieli pocisków balistycznych typu Dreadnought. Dwa z nich są już w budowie, której ukończenie planowane jest u progu lat 30. XXI w.

Kolejną próbą ogniową dla Royal Navy była tzw. I wojna w Zatoce Perskiej (1991 r.), kiedy → R a d a B e z p i e c z e ń s t w a O N Z [t. 3] udzieliła mandatu międzynarodowej koalicji pod egidą USA do interwencji w celu wyzwolenia Kuwejtu spod okupacji irackiej. Na morzu operował wtedy silny zespół skupiony wokół lotniskowca Ark Royal i jego grupy eskortowej złożonej z kilku niszczycieli typu 42 oraz fregat typu 22.

Rozpad Układu Warszawskiego oraz Związku Radzieckiego w 1991 r. nie mógł nie mieć wpływu na politykę obronną Zjednoczonego Królestwa (oraz innych państw Europy Zachodniej). Wprawdzie niemal jednocześnie wybuchł krwawy konflikt na Bałkanach na tle rozpadu Socjalistycznej Federacyjnej Republiki Jugosławii, ale w Londynie, podobnie jak w Brukseli, Bonn czy Paryżu, wierzono w chybioną – jak dowiódł rozwój sytuacji – tezę amerykańskiego politologa i futurysty Francisa Fukuyamy. Ta wizja była jednak dla wielu polityków (także brytyjskich) bardzo wygodna i prowadziła do znacznych cięć wydatków na → o b r o n n o ś ć [t. 5]. Do tego neoliberalna polityka ekonomiczna i powstanie rajów podatkowych prowadziły do sytuacji stałego deficytu w finansach publicznych, nie tylko zresztą w Wielkiej Brytanii, lecz także we wszystkich niemal krajach szeroko rozumianego Zachodu. Konsekwencją były kolejne cięcia wydatków publicznych, przede wszystkim na cele militarne. Sytuacji tej nie zmieniły wydarzenia z 11 września 2001 r. i proklamowana wówczas → „w o j n a z t e r r o r y z m e m" [t. 5]. Więcej nawet – wielu ekspertów wojskowych świata zachodniego wychodziło z założenia, że te asymetryczne działania będą mogły odbywać się przy udziale relatywnie niewielkich sił (zwłaszcza sił specjalnych, w wymiarze zarówno morskim, jak i lądowym). Niemal powszechne stawało się mniemanie, że flotom państw zachodnich pozostanie zwalczanie piractwa, jak w Zatoce Gwinejskiej czy w okolicach tzw. Rogu Afryki.

Większość brytyjskiego establishmentu politycznego (choć nie militarnego) podzielała ten pogląd. Starzejącej się monarchini przyszło patrzeć na to, jak z dawnej korony brytyjskiego imperium wypadają ostatnie perły, np. Hongkong, który w 1997 r. przeszedł pod zwierzchność Chińskiej Republiki Ludowej. Obszar działania Royal

Navy kurczył się coraz bardziej. Do rangi symbolu urasta fakt, że w czasie, kiedy przekazano Hongkong Pekinowi, 11 grudnia 1997 r. po raz ostatni spuszczono banderę na królewskim jachcie HMY Britannia. Dla Elżbiety II była to bardzo bolesna chwila, ponieważ to właśnie ona była matką chrzestną tego okrętu oraz uświetniła swoją obecnością jego dzień wcielenia do służby. Dzisiaj ten symbol świetności drugiej ery elżbietańskiej pełni funkcję muzeum przy nabrzeżu w portowej dzielnicy Leith stolicy Szkocji – Edynburga.

Jakkolwiek we wszystkich państwach UE, licząc od początku XXI stulecia, udział wydatków na obronność systematycznie spadał grubo poniżej 2%, to Zjednoczone Królestwo pozostawało chlubnych wyjątkiem, gdyż jego wkład zawsze plasował się powyżej tego poziomu, a w sytuacji, gdy położenie międzynarodowe się komplikowało, wskaźnik ten przekraczał nawet 2,5%. Tak działo się w latach 2008 i 2014, kiedy to Federacja Rosyjska dokonała → a g r e s j i [t. 1] na Gruzję i Ukrainę. Warto w tym miejscu wspomnieć, że czynnikiem, który nie pozostał bez wpływu na problem brexitu, była niezgoda politycznych, a w jeszcze większym stopniu militarnych elit brytyjskich na politykę swoistego appeasementu wobec Rosji, jaką prowadziła Komisja Europejska orz Niemcy i Francja. Nawet jednak ten fakt nie uchronił Royal Navy przed postępującą atrofią u progu obecnego stulecia.

Gdy w 2005 r. uroczyście obchodzono rocznicę bitwy pod Trafalgarem, największym okrętem uczestniczącym w międzynarodowej paradzie na słynnym kotwicowisku Spithead (28 czerwca) był francuski lotniskowiec Charles de Gaulle. Kiedy 11 marca 2011 r. opuszczono po raz ostatni banderę na lotniskowcu Ark Royal, królewska marynarka wojenna pierwszy raz od prawie 100 lat nie miała w linii okrętu lotniczego. Dopiero ostatnie lata panowania Elżbiety II przyniosły pewne odrodzenie Royal Navy.

Zaostrzająca się sytuacja polityczno-militarna w Europie spowodowana agresywną polityką Federacji Rosyjskiej skłoniła rząd brytyjski po brexicie do zdecydowanego zwiększenia wydatków na obronę. Koniec panowania Elżbiety II będzie się w Royal Navy już zawsze kojarzyć z wcieleniem do służby 2 najnowszych lotniskowców HMS Queen Elizabeth i Prince of Wales. Okręty te, o standardowej wyporności prawie 72 tys. t, są zarazem największymi jednostkami nawodnymi, jakie kiedykolwiek weszły w skład Royal Navy. Grupa lotnicza tych lotniskowców liczy do 36 samolotów myśliwsko-szturmowych F-35B, uzupełnia ją 14 śmigłowców. Moc maszyn tych okrętów wynosi 105 tys. KM, a prędkość maksymalna – 32 węzły.

Specjalnie do eskorty tych potężnych okrętów lotniczych, nim jeszcze weszły one do służby, zaprojektowano i zbudowano 6 niszczycieli typu 45. Są to HMS Daring, Dauntless, Dimond, Dragon, Defender oraz Duncan, wcielane do służby w latach 2009–2013 w tej właśnie kolejności. Są to duże jednostki, standardowo wypierające ponad 7,3 tys. t, czyli mniej więcej tyle samo, co lekkie krążowniki z początku II wojny światowej. Ich głównym zadaniem jest ochrona przeciwlotnicza i przeciwrakietowa

wspomnianych wyżej lotniskowców. Ochrona przeciwpodwodna to zadanie fregat. Obecnie funkcję tę pełnią fregaty typu 23, które od połowy trzeciej dekady obecnego stulecia mają być zastąpione fregatami typu 26. W ostatnich latach panowania Elżbiety II Royal Navy przeszła wyraźny renesans i odzyskała obecnie pierwsze miejsce wśród flot państw europejskich, dystansując tym samym siły morskie Federacji Rosyjskiej (w wymiarze konwencjonalnym) oraz francuską Marine Nationale. Wiele wskazuje na to, że to czołowe miejsce Royal Navy utrzyma w dającej się przewidzieć perspektywie czasowej.

To niezwykły zbieg okoliczności, że koniec panowania Elżbiety II przyniósł jednocześnie odrodzenie Royal Navy we wszystkich aspektach – poczynając od 2 nowych lotniskowców, a kończąc na projektach nowych okrętów nuklearnych. Można postawić tezę, że w dobie zagrożenia ze strony agresywnej polityki rosyjskiej i coraz bardziej dynamicznego rozwoju sił morskich ChRL brytyjska marynarka wojenna jest mocnym ogniwem w systemie obrony świata zachodniego – w ramach zarówno NATO, jak i nowego sojuszu AUKUS.

Anna Kochnowska

D.K. Brown, G. Moore, *Rebuilding the Royal Navy. Warship Design since 1945*, Naval Institute Press, Annapolis 2003; C. Chant, *Air War in the Falklands, 1982*, Osprey Aviation, Oxford 2001; R. Czulda, *Brytyjska doktryna odstraszania nuklearnego 1945–1955*, „Bellona" 2012, nr 4; N. Friedman, *British Destroyers and Frigates. The Second World War and After*, Seaforth, Barnsley 2008; K. Kubiak, *Działania sił morskich po drugiej wojnie światowej. Studia przypadków*, Wydawnictwo „Książka i Wiedza", Warszawa 2007; J. Krzewiński, *Royal Navy 1950–1994*, Wydawnictwo Magnum, Warszawa 1995; J. Stavridis, *Sea Power. The History and Geopolitics of the World Ocean's*, Penguin Press, New York 2017; J. Stöhs, *The Decline of European Naval Forces. Challenges to the Sea Power in an Age of Fiscal Austerity and Political Uncertainty*, Naval Institute Press, Annapolis 2018; B. Wilson, *Empire of the Deep.The Rise and Fall of the British Navy*, Phoenix, London 2014; K. Young, *The Royal Navy's Polaris lobby, 1955–62*, „Journal of Strategic Studies" 2002, vol. 25, no. 3.

BUKARESZTAŃSKA DZIEWIĄTKA (B9) – niesformalizowana platforma konsultacji i dialogu politycznego wysokiego szczebla w dziedzinie stabilności i → b e z p i e c z e ń s t w a [t. 1] Europy Środkowej i Wschodniej, nazywana też formatem bukareszt ańskim. Stanowi ona inicjatywę dyplomatyczną 2 państw – Polski i Rumunii – służącą zacieśnieniu współpracy między państwami zaliczanymi do → w s c h o d n i e j f l a n k i NAT O, koordynacji stanowisk i wymianie poglądów państw regionu w dziedzinie bezpieczeństwa oraz wzmocnieniu siły głosu w ramach szerszej, międzysojuszniczej debaty. To także uzupełnienie współpracy gospodarczej i infrastrukturalnej, realizowanej w ramach Inicjatywy Trójmorza o niezbędny wymiar współpracy polityczno-militarnej państw regionu, pogłębiające w ten sposób solidarność regionalną oraz integrację Europy Środkowej. Współpracę państw regionu w tzw. formacie bukareszt ańskim zainicjowali w 2014 r. prezydenci: Polski – Andrzej Duda oraz Rumunii – Klaus Iohannis. Spotkanie założycielskie odbyło się 4 listopada 2015 r. w Bukareszcie. W tym spotkaniu wzięli udział: prezydent Bułgarii Rosen Plewneliew,

prezydent Estonii Toomas Hendrik Ilves, prezydent Litwy – Dalia Grybauskaitė, prezydent Łotwy – Raimonds Vējonis, prezydent Słowacji Andrej Kiska, prezydent Węgier János Áder, przewodniczący Izby Poselskiej Czech Jan Hamáček oraz Alexander Vershbow, zastępca sekretarza generalnego NATO. Bukareszt ańska Dziewiątka (B9) łączy wiec państwa bałtyckie (Litwa, Łotwa, Estonia), państwa → G r u p y W y s z e h r a d z k i e j [t. 1] (Polska, Słowacja, Czechy, Węgry) oraz państwa Morza Czarnego (Bułgaria i Rumunia). W grupie tej kluczową rolę pełnią Rumunia i Polska jako inicjatorzy B9 oraz państwa o największym potencje demograficznym i militarnym.

Podczas spotkania założycielskiego grupy B9 poruszano zagadnienia szeroko rozumianego bezpieczeństwa Europy Środkowej i Wschodniej oraz kierunków jego ewolucji. Poszczególne państwa zadeklarowały połączenie wysiłków na rzecz zapewnienia – tam, gdzie to konieczne – silnej, wiarygodnej i zrównoważonej obecności wojskowej → N A T O [t. 3] w regionie. Te kraje łączą członkostwo w NATO i UE, bliskość geograficzna, a także podobne doświadczenia historyczne (tę grupę tworzą państwa postkomunistyczne, w tym – byłe republiki radzieckie) oraz poczucie → z a g r o ż e n i a [t. 4] wynikające z niestabilnej sytuacji bezpieczeństwa w ich bliskim sąsiedztwie. Zainicjowanie pogłębionej dyskusji państw wschodniej flanki NATO wynika więc ze świadomości wspólnoty więzi, ze zbieżności potrzeb i interesów, z podobieństw problemów bezpieczeństwa oraz z woli bardziej aktywnego włączenia się tych państw w szerszą debatę na temat dynamicznego otoczenia międzynarodowego i kierunków adaptacji NATO do nowych warunków i wyzwań. Powstanie i funkcjonowanie Bukareszt ańskiej Dziewiątki jest wyrazem jedności i solidarności państw tworzących wschodnią flankę sojuszu, stanowi siłę negocjacyjną zrzeszonych państw w dążeniu do uzgodnienia wspólnoty stanowisk oraz do wypracowania wspólnej płaszczyzny działania na arenie międzynarodowej.

Celem współpracy państw w ramach B9 jest zapewnienie spójnego i zintegrowanego podejścia do obrony wschodniej flanki NATO, a w szerszej perspektywie – zapewnienie stabilności i bezpieczeństwa całego obszaru północnoatlantyckiego. Cele szczegółowe koncentrują się wokół kwestii:

- pogłębienia dialogu i współpracy w dziedzinie bezpieczeństwa państw tworzących wschodnią flankę NATO oraz wzmocnienie siły głosu tych państw w ramach całego Sojuszu Północnoatlantyckiego;
- zapewnienia stabilności i bezpieczeństwa regionu Europy Środkowej i Wschodniej w obliczu → k o n f l i k t u z b r o j n e g o w Ukrainie oraz konsekwentnej presji politycznej i militarnej ze strony Federacji Rosyjskiej. Państwa wschodniej flanki NATO, a zwłaszcza państwa bałtyckie, stanowią wszakże obszar potencjalnego testowania spoistości i determinacji NATO przez Rosję;
- realnego wzmocnienia bezpieczeństwa wschodniej flanki Sojuszu. Chodzi tu o rozbudowę potencjału oraz mechanizmów → o d s t r a s z a n i a [t. 3] i obrony NATO w tej części obszaru traktatowego („od Bałtyku do Morza Czarnego") opartą na:

- efektywnej strukturze dowodzenia NATO, skupionej na regionach;
- wzmocnionej i trwałej obecności wojsk sojuszniczych na wschodniej flance NATO, w tym – sił zbrojnych państw spoza regionu (zapewnienie „silnej, wiarygodnej, zrównoważonej obecności wojskowej" NATO w regionie);
- rozwoju współpracy militarnej państw B9 (podniesienie poziomu gotowości bojowej, zdolności i interoperacyjności sił zbrojnych państw Dziewiątki, wspólne ćwiczenia wojskowe, współpraca przemysłu zbrojeniowego itd.);
- rozbudowie infrastruktury cywilno-wojskowej w regionie Europy Środkowej i Wschodniej (rozwój infrastruktury drogowej i kolejowej, niezbędnej do stacjonowania i szybkiego przemieszczania sił sojuszniczych między Morzem Bałtyckim a Morzem Czarnym);
- zwiększaniu wydatków obronnych oraz modernizację sił zbrojnych państw B9.

Powstanie Bukareszt ańskiej Dziewiątki było spowodowane niekorzystną – z punktu widzenia państw Sojuszu Północnoatlantyckiego – ewolucją sytuacji bezpieczeństwa we wschodnim sąsiedztwie NATO. Polityka rewizjonizmu Federacji Rosyjskiej na obszarze poradzieckim, narastająca na przestrzeni ostatnich lat, unaoczniona interwencjami militarnymi Rosji w Gruzji (2008) i w Ukrainie (2014), skomplikowała stosunki między NATO a Rosją. Coraz bardziej asertywne dążenia Rosji do zatrzymania procesów demokratyzacji i modernizacji państw Europy Wschodniej oraz do odbudowy utraconej pozycji →mocarstwa światowego, równego Zachodowi, prowadziło do pogłębiającej się geostrategicznej rywalizacji mocarstw, do rosnącej niestabilności oraz do obniżonej przewidywalności środowiska międzynarodowego. Świadomość zagrożeń i wyzwań dla → b e z p i e c z e ń s t w a m i ę d z y n a r o d o w e g o [t. 1] w Europie Środkowej i Wschodniej, wynikających z agresywnej polityki Rosji, wywołała uzasadnione zaniepokojenie państw Sojuszu Północnoatlantyckiego położonych w regionie. Stała się także impulsem do powstania Bukareszt ańskiej Dziewiątki, która wyrosła na gruncie wrażliwości na zagrożenia generowane przez Rosję. Państwa założycielskie – Polska i Rumunia – to kraje, które z racji swego położenia i potencjału militarnego odgrywają kluczową rolę w regionie Morza Bałtyckiego oraz Morza Czarnego. W swoich koncepcjach obronnych szczególną uwagę zwracają na rozwój rosyjskich zdolności – militaryzację obwodu kaliningradzkiego oraz Półwyspu Krymskiego – a przy tym podkreślają fundamentalne znaczenie Sojuszu Północnoatlantyckiego oraz strategicznego sojuszu z USA dla zapewnienia bezpieczeństwa. Zabiegają zatem o to aby te podmioty zwiększyły swoją obecność na wschodnich rubieżach Sojuszu. Pozostałe państwa formatu B9 – Czechy, Słowacja, Węgry i Bułgaria – inaczej akcentują swoją politykę bezpieczeństwa. W swoich koncepcjach obronnych w mniejszym stopniu podkreślają zagrożenia ze strony Rosji, a koncentrują się bardziej na zagrożeniach wewnętrznych lub na pochodzących z Bliskiego Wschodu lub Bałkanów Zachodnich.

Regularne spotkania 9 krajów regionu mają na celu wypracowanie wspólnego stanowiska państw wschodniej flanki NATO. W ramach współpracy kraje zobowiązały się do:

- zwiększenia wydatków na obronność,
- modernizacji technicznej sił zbrojnych,
- wypracowania wspólnego stanowiska wobec działań rosyjskich,
- lobbowania na rzecz zwiększenia obecności wojsk sojuszniczych.

Spotkania w tym formacie mają tradycyjną formę dyplomacji wielostronnej, która z kolei odpowiada formule dyplomacji konferencyjnej. W ich trakcie odbywają się sesje plenarne, podczas których są dyskutowane zagadnienia dotyczące szeroko definiowanego bezpieczeństwa państw wschodniej flanki NATO. Obrady kończą się zwykle wspólną deklaracją, podsumowującą ich treść oraz definiującą uzgodnione stanowisko państw Dziewiątki dotyczące najważniejszych kwestii i dalszych kierunków współpracy grupy B9. Na marginesie rokowań wielostronnych w ramach B9 odbywają się także spotkania w formule bilateralnej. Dialog międzynarodowy w formacie bukareszteńskim rozpoczął się na szczeblu prezydentów państw wschodniej flanki NATO. Wymiar prezydencki B9 rozszerzono o wymiar międzyrządowy (ministerialny) oraz o wymiar wielostronnej dyplomacji parlamentarnej. Obecnie spotkania przedstawicieli państw w ramach Bukareszteńskiej Dziewiątki są realizowane są na różnych szczeblach jako:

- spotkania prezydentów,
- konsultacje ministrów spraw zagranicznych,
- spotkania ministrów obrony,
- szczyty parlamentarne,
- konsultacje doradców ds. bezpieczeństwa narodowego,
- spotkania przewodniczących komisji obrony parlamentów grupy B9.

Bukaresztańska Dziewiątka szybko zyskała siłę przebicia jako głos państw, których bezpieczeństwo jest najbardziej osłabiane przez coraz bardziej prowokującą retorykę i siłową postawę Rosji. Potencjał formatu do sygnalizowania własnych priorytetów do omówienia w ramach szczytów NATO okazuje się znaczący. Większość jego krajów aktywnie angażuje się we wspólną obronę – m.in. zwiększa wydatki na obronę i inwestuje w nowe zdolności. Ograniczenia skuteczności państw B9 wynikają głównie z różnic w postrzeganiu zagrożeń. Poszczególne kraje nierównomiernie zobowiązały się do wzmocnienia zdolności → o b r o n y n a r o d o w e j [t. 3], a także wykazały potencjalną niestabilność planów modernizacji i transformacji sił zbrojnych. Szersza współpraca, zarówno polityczna jak i militarna, może jednak złagodzić problemy i wzmocnić głos wschodniej flanki – na rzecz reorganizacji polityki NATO wobec rosnącego zagrożenia rosyjskiego.

Kolejne spotkania Bukaresztańskiej Dziewiątki pokazały, że współpraca poszczególnych jej krajów podąża we właściwym kierunku i daje wymierne efekty

w realizowanej polityce wobec narastających zagrożeń ze strony Federacji Rosyjskiej. Do 2021 r. odbyły się 4 spotkania w formacie bukaresztańskim: 4 listopada 2015 r. – Bukareszt, Rumunia; 8 czerwca 2018 r. – Warszawa, Polska; 28 lutego 2019 r. – Koszyce, Słowacja; 10 maja2021 r. – Bukareszt, Rumunia.

Pierwsze ze spotkań – spotkanie założycielskie w 2015 r. – nazwane zostało miniszczytem NATO. Omawiano na nim kwestie bezpieczeństwa tzw. wschodniej flanki NATO i uzgadniano wspólne stanowisko wobec niechętnym zmianom „starych" państw Sojuszu Północnoatlantyckiegow Europie. Szczyt wypracował wspólną deklarację pod nazwą „Solidarność Sojusznicza i Wspólna Odpowiedzialność" (ang. *Allied Solidarity and Shared Responsibility*). Obejmowała ona kilka zasadniczych kwestii:

- kolejny szczyt B9, który odbędzie się w Warszawie, będzie miałcharakter decyzyjny, a nie refleksyjny;
- jego celem stanie się podjęcie konkretnych decyzji w zakresie rozbudowy infrastruktury bezpieczeństwa i zwiększenia obecności wojsk NATO na terenie całego Sojuszu, co oznacza dozbrojenie jego flanki wschodniej;
  - NATO ma być sojuszem obronnym stojącym po stronie prawa, co wyznacza wstępne warunki dialogu z Rosją,
  - urealnienie możliwości wejścia w struktury Sojuszu państw,które spełniają warunki akcesji (np. Czarnogóra),
  - wszystkie państwa B9 zadeklarują przeznaczenie minimum2% PKB na obronność.

Ta deklaracja została przyjęta przez stronę polską jako przekraczająca wcześniejsze oczekiwania, a uzyskana jednomyślność przyczyniła się do powstania łańcucha bezpieczeństwa od Morza Czarnego do Morza Bałtyckiego.

Kolejne spotkanie państw B9 odbyło się w Warszawie 8 czerwca 2018 r. i stanowiło ono zdecydowany i jednomyślny głos wschodniej flanki NATO. Prezydenci państw B9 oraz przewodniczący Izby Deputowanych Republiki Czeskiej przyjęli wspólną deklarację państw Bukaresztańskiej Dziewiątki na szczyt NATO w Brukseli. Deklaracja zawierała wspólną wizję przyszłości Sojuszu oraz wspólną koncepcję kierunku, jaki powinien objąć szczyt w Brukseli, i dalszej adaptacji NATO do nowych wyzwań i zagrożeń. Państwa Dziewiątki zgodnie oceniły też niebezpieczeństwa, w których znajduje się flanka wschodnia. Podkreślono wówczas, że wobec wszelkich zagrożeń wynikających z agresywnej polityki Rosji konieczne stają się odstraszanie i obrona oraz zwiększanie gotowości Sojuszu do takich działań. Podkreślano ponadto znaczenie wzmożonej obecności wojskowej Stanów Zjednoczonych i Kanady w Europie. W ramach gotowości obronnej akcentowano szczególnie konieczność zaangażowania militarnego we wszystkich obszarach – na lądzie, na morzu, w powietrzu i w →cyberprzestrzeni [t. 1]. Przywódcy podkreślili również, że zwiększenie gotowości i zdolności sił NATO do odpowiedzi, a także – mobilności wojskowej na terytorium sojuszu, ma zasadnicze znaczenie w kontekście

odstraszania i obrony wschodniej flanki NATO. Podczas spotkania sformułowano następujące wnioski i zalecenia:

- pozycjonowanie szczytu NATO w 2018 r. jako wzmacniającego jedność sojuszu oraz dążącego do utrzymania perspektywy sojuszników w duchu zasady 360 stopni, a więc do wypracowania odpowiednich narzędzi wobec współczesnych → z a g r o ż e ń b e z p i e c z e ń s t w a [t. 4], w tym – → za g r o ż e ń h y b r y d o w y c h [t. 4];
- utrzymanie działań w ramach wysuniętej obecności NATO na wschodniej flance, jak również dalsze przeznaczanie odpowiednich środków w celu umocnienia sojuszniczych zdolności do odstraszania i zbiorowej obrony wszystkich członków NATO zarówno na lądzie, w powietrzu, na morzu, jak i w cyberprzestrzeni;
- odwoływanie się do kluczowych decyzji podjętych w Walii i w Warszawie;
- zapewnienie spójnego i zintegrowanego podejścia do obrony wschodniej flanki, opartego na efektywnej strukturze dowodzenia NATO, skupionej na regionie;
- wzmocnienie sił morskich, silnej obrony powietrznej oraz realistycznej → s t r a t e g i i [t. 4] wsparcia;
- zwiększenie gotowości i zdolności do odpowiedzi, a także mobilności wojskowej na terytorium sojuszu (utrzymanie wydatków na obronność na poziomie 2% PKB lub odpowiednie zbliżanie się do tego poziomu ma na celu inwestowanie w nowoczesne zdolnościi udział w operacjach i misjach NATO;
- umacnianie stabilności również poza terytorium Sojuszu w celu przeciwdziałania złożonym zagrożeniom i wyzwaniom: od → w o j n y [t. 4] konwencjonalnej i → w o j n y h y b r y d o w e j [t. 4] aż po terroryzm, masową migrację i rozprzestrzenianie broni masowego rażenia;
- wspieranie rozwoju zdolności obronnych państw oraz ich odporności na istniejące zagrożenia i wyzwania;
- utrzymanie podejścia NATO do Rosji opartego na wzmocnionej postawie odstraszania i obrony przy jednoczesnym otwarciu na dialog polityczny;
- odwoływanie się do tzw. polityki otwartych drzwi, przyczyniającej się do umacniania pokoju, dobrych rządów, bezpieczeństwa i stabilności w Europie i na świecie;
- zaangażowanie się w dalsze wdrażanie wszystkich uzgodnionych obszarów współpracy NATO-UE, zgodnie z tzw. wspólną deklaracją warszawską, przy czym priorytetowe obszary tej współpracy obejmują m.in.: mobilność wojskową, poprawę infrastruktury, zwalczanie zagrożeń hybrydowych, zwiększanie odporności na zagrożenia krajów partnerskich z Bałkanów Zachodnich i wschodniego sąsiedztwa, bezpieczeństwo w cyberprzestrzeni i komunikację strategiczną.

Kolejne spotkanie państw B9 zorganizowano 28 lutego 2019 r. w Koszycach, z udziałem głów państw Dziewiątki oraz sekretarza generalnego NATO Jensa Stoltenberga. Stanowiło ono swoistą demonstrację jedności, współpracy oraz solidarności. Wysunięto wtedy następujące tezy:

- Rozwój sytuacji w Ukrainie budzi uzasadnione obawy m.in. państw regionu Morza Bałtyckiego dotyczące własnego bezpieczeństwa, a państwa flanki wschodniej są zjednoczone i zdolne pomagać sobie nawzajem.
- Istnieje uzasadniona potrzeba większej obecności wojsk sojuszuw tej części Europy. Struktury dowodzenia NATO powinny przesuwać się coraz bardziej w kierunku tego regionu, Sojusz powinien być też obecny na Morzu Czarnym.
- Należy utrzymać politykę otwartych drzwi i wsparcie dla partnerów sojuszu – Gruzji, Ukrainy, Mołdawii i krajów BałkanówZachodnich – a także wzmocnić i zacieśnić współpracę między NATO a UE.

Szczyt B9 w Bukareszcie w maju 2021 r. przyniósł kolejną deklarację jedności i współpracy w zakresie bezpieczeństwa, a także potwierdzenie, że Pakt Północnoatlantycki pozostaje podstawą stabilności i bezpieczeństwa w regionie euroatlantyckim, a najważniejszym gwarantem pokoju są Stany Zjednoczone. Podkreślono jednocześnie, że budując swoje zdolności odstraszania i obrony, państwa członkowskie NATO pozostają otwarte na dialog z Rosją.

Obok ewidentnych zalet i korzyści współpracy w ramach B9 uwagę zwracają liczne wyzwania i ograniczenia tego formatu, m.in.:

- luźna, niezinstytucjonalizowana i konferencyjna forma współpracy;
- różna determinacja poszczególnych państw do podejmowania działań zwiększających potencjał militarny wschodniej flanki –wśród członków B9 znajdują się państwa różniące się pod względem tempa wzrostu wydatków wojskowych i udziału budżetu obronnego w PKB: w jednych tempo wzrostu wydatków na obronność sytuuje je w czołówce, inne są daleko w tyle;
- w praktyce nieco zróżnicowany stosunek do polityki Rosji w regionie Europy Środkowej i Wschodniej – generalnie państwa B9są zgodne w ocenie najważniejszych wyzwań dla bezpieczeństwa europejskiego, jednak część z nich nie graniczy z Rosją i często ma zbieżne interesy ekonomiczne oraz energetyczne, a przy tym nie upatruje bezpośredniego → z a g r o ż e n i a m i l i t a r n e g o [t. 4] w jej polityce, ale raczej postrzega Rosję jako źródło zagrożeń pozamilitarnych, np. w cyberprzestrzeni;
- postrzeganie regionalnej inicjatywy B9 jako próbę „rozbijania”NATO;
- podatność na zmiany polityczne w poszczególnych państwach członkowskich (np. zmiany ekip rządzących), co w perspektywie może osłabić współpracę w ramach B9;
- ograniczona rozpoznawalność inicjatywy B9;
- postrzeganie – przez część zachodnioeuropejskich członków NATO – Bukareszteńskiej Dziewiątki oraz (bliskiej jej) Inicjatywy Trójmorza jako inicjatyw z założenia proamerykańskich, wzmacniających polityczną i militarną obecność Stanów Zjednoczonych w Europie Środkowej i Wschodniej, rozbijających jedność państw UE;

- nieobecność w strukturach B9 innych państw Europy Środkowej i Południowej, będących członkami NATO – Słowenii, Chorwacji,Albanii i Macedonii Północnej – których uczestnictwo zwiększałoby spójność regionalną sojuszu w odpowiedzi na współczesne wyzwania i zagrożenia bezpieczeństwa międzynarodowego.

Pomimo wyzwań i potencjalnych ograniczeń format bukaresztańskistał się symbolem jedności i współpracy oraz adaptacji Sojuszu Północnoatlantyckiego do wyzwań i zagrożeń w subregionie Europy Środkowej i Wschodniej. Działania NATO w tym formacie są dowodem na niepodzielność bezpieczeństwa swoich członków oraz na solidarność członków tego paktu, także w zakresie bezpieczeństwa regionalnego. Dialog i współpraca w ramach B9 prowadzą do wzmocnienia pozycji międzynarodowej i siły głosu państw sojuszniczych w debacie na temat bezpieczeństwa regionalnego i europejskiego oraz kierunków rozwoju współpracy w dziedzinie obronności, prowadzonej na forum NATO. W dalszej perspektywie sukces kooperacji państw Europy Środkowej i Wschodniej w formule B9 może wpłynąć na wzrost poczucia bezpieczeństwa oraz przyciągnąć do współpracy państwa sąsiedzkie: Mołdawię, Gruzję czy Ukrainę.

Sabina Olszyk

J. Bondalski, *Format bukaresztański jako strategiczny wymiar współpracy państw wschodniej flanki NATO*, [w:] *Bezpieczeństwo północno-wschodniej flanki NAT*O, M. Żyła, P. Krzykowski, J. Grabowski (red.), Akademia Sztuki Wojennej, Warszawa 2020; A.M. Kamińska, M. Svarovsky, *Rosja ma na oku wrażliwe miejsce Sojuszu, musimy je wzmacniać*, https://www.polskieradio24.pl/5/1223/ Artykul/2428529,Ekspert-Martin-Svarovsky-Rosja-ma-na-oku-wrazliwe-miejsce-Sojuszu-musimy-je-wzmacniac (dostęp 1.08.2021); K. Pawłowski, *Bukaresztańska Dziewiątka: współpraca państw wschodniej flanki NAT*O, Instytut Europy Środkowej i Institute of Central Europe, Lublin 2020, https://ies.lublin.pl/wp-content/ uploads/2020/11/ies-policy-papers-pl-2020-004.pdf (dostęp 1.08.2021); *Wspólna deklaracja głów państw Bukaresztańskiej Dziewiątki*, https://www.prezydent.pl/ aktualnosci/wydarzenia/art,1031,wspolna-deklaracja-glow-panstw-bukaresztan-skiej-dziewiatki.html (dostęp 1.08.2021).

BUNDESWEHRA – siły zbrojne Republiki Federalnej Niemiec (RFN) utworzone 5 maja 1955 r. na terenie Niemiec Zachodnich. Budowę nowej armii w latach 50. XX w. oparto na 3 głównych zasadach: Bundeswehra miała być armią o charakterze obronnym, funkcjonującą w ramach → NAT O [t. 3] i opartą na powszechnym obowiązku służby wojskowej. Nowe siły zbrojne RFN powstały jako całkowite zaprzeczenie wcześniejszych sił zbrojnych z okresu Republiki Weimarskiej (Reichswehra) oraz Trzeciej Rzeszy (Wehrmacht). Miały być one zintegrowane ze społeczeństwem, poddane kontroli parlamentu i rządu, działające jedynie w obronie terytorium Niemiec Zachodnich i niezdolne do prowadzenia szeroko zakrojonych operacji zaczepnych.

Funkcjonowanie Bundeswehry od momentu jej powstania aż po czasy współczesne bazuje na koncepcji wewnętrznego dowodzenia (niem. *Innere Führung*). Jest ona określana jako nowa filozofia dowodzenia i kierowania niemieckimi siłami zbrojnymi.

Najważniejszym założeniem wszelkich prac w dziedzinie *Innere Führung* stało się stworzenie i stałe doskonalenie nowoczesnego żołnierza, który jest równocześnie:

- wolnym człowiekiem, tzn. takim, który odczuwa poszanowanie swojej godności i nie posiada ograniczonych indywidualnych swobód i praw,
- świadomym swojej roli obywatelem, tzn. takim, który kieruje się rozsądkiem i poczuciem odpowiedzialności za sprawy swojego kraju i społeczeństwa,
- pełnowartościowym żołnierzem, tzn. żołnierzem gotowym do działania, który służbę wojskową pojmuje jako wkład w pomyślny rozwój państwa niemieckiego oraz jego demokratycznego ustroju i który gotów jest wystąpić w obronie tych wartości nawet z narażeniem własnego życia.

Tak ukształtowanego żołnierza określono mianem „obywatela w mundurze" (niem. *Staatsbürger in Uniform*). Oznaczało to, że wszyscy żołnierze Bundeswehry włączeni są w polityczne, społeczne i publiczne życie Niemiec, a także utrzymują ścisłe, służbowe bądź osobiste, kontakty z organami administracji i gospodarki wszelkich szczebli oraz z organizacjami i zrzeszeniami, które są świadectwem integracji armii ze społeczeństwem. Idea *Innere Führung* miała spełniać 4 zasadnicze cele:

- legitymizować służbę wojskową – żołnierz powinien być świadomy celu i sensu pobytu w armii,
- motywować żołnierzy do sumiennego wykonywania swoich obowiązków, przy jednoczesnym umacnianiu dyscypliny i zwartości wojska,
- kształtować wewnętrzny tok służby w taki sposób, aby zachować subordynację i posłuszeństwo oraz rygor wojskowy, a zarazem chronić prywatność i osobowość jednostki,
- integrować armię z państwem i społeczeństwem.

W koncepcji tej podkreślano jednak nie tylko szczególną rolę każdego żołnierza wchodzącego w skład Bundeswehry, ale przede wszystkim – przełożonych, którzy mieli stanowić przykład właściwej postawy, wykonywania obowiązków oraz zgodnego z poszanowaniem praw i wolności kierowania swoim zespołem.

Szczegółowe koncepcje użycia Bundeswehry, jak również jej strukturę określono w dokumentach strategicznych RFN – tzw. Białych Księgach Bundeswehry (niem. *Weißbücher der Bundeswehr*). Do momentu zjednoczenia Niemiec w 1990 r. wydano 8 Białych Ksiąg (1969, 1970, 1971/1972, 1973/1974, 1975/1976, 1979, 1983 i 1985 r.). Po 1990 r. wydano 3 dokumenty strategiczne, w 1994, 2006 oraz 2016 r.

Zjednoczenie Niemiec 3 października 1990 r. oznaczało inkorporację wschodnioniemieckiej Nationale Volksarmee (Narodowej Armii Ludowej) do zachodnioniemieckiej Bundeswehry. Po 1990 r. zmianie uległy rola i zadania tej armii. Zgodnie z Białą Księgą z 1994 r. należały do nich: ochrona Niemiec i ich obywateli przed szantażem politycznym i → z a g r o ż e n i e m [t. 4] zewnętrznym, wspieranie dążeń do wojskowej stabilizacji i integracji Europy, obrona Niemiec i ich sojuszników, służba dla pokoju i →b e z p i e c z e ń s t w a m i ę d z y n a r o d o w e g o – zgodnie z Kartą

Narodów Zjednoczonych, pomoc w przypadku katastrof, pełnienie funkcji ratowniczych w stanach wyższej konieczności oraz wspieranie akcji humanitarnych.

Bundeswehra pozostała armią sojuszniczą, wnoszącą istotny wkład w główne siły obronne oraz siły reagowania NATO. Jej zadaniem było wsparcie dialogu wojskowo-politycznego, uczestnictwo we wspólnych ćwiczeniach w ramach NATO i Unii Zachodnioeuropejskiej (UZE) oraz wysyłanie obserwatorów na misje ONZ i KBWE/OBWE. Siły zbrojne RFN spełniały 2 ważne funkcje: po pierwsze musiały być w stanie wraz ze swoimi sprzymierzeńcami i partnerami wnieść odpowiedni wkład w szybkie i skuteczne przezwyciężanie międzynarodowych konfliktów i → k r y z y s ó w [t. 2], po drugie – w razie konieczności obrony terytorium Niemiec i Sojuszu (który to przypadek jest mało prawdopodobny) musiały dysponować wystarczającymi siłami obronnymi.

W latach 90. Bundeswehra pozostała armią opartą na powszechnym obowiązku służby wojskowej. Tworzyły ją 3 rodzaje sił zbrojnych: siły lądowe (Heer), siły powietrzne (Luftwaffe) oraz siły morskie (Marine). Do 1994 r. miała być zredukowana do 370 tys. żołnierzy. Nowy model Bundeswehry obejmował 3 kategorie sił zbrojnych:

- siły reagowania kryzysowego (Krisenreaktionskräfte, KRK), pozostające w gotowości operacyjnej; były przeznaczone do zapobiegania powstawaniu → s y t u a c j i k r y z y s o w y c h [t. 4], do ich przezwyciężania oraz do rozwiązywania konfliktów, jak również do uczestnictwa w międzynarodowych operacjach pokojowych; mogły być ponadto wykorzystane do obrony terytorium Niemiec i zabezpieczenia → m o b i l i z a c j i [t. 3];
- główne siły obronne (Hauptverteidigungskräfte, HVK), przeznaczone do obrony terytorium Niemiec i Sojuszu, w których skład wchodziły wszystkie siły pozostające w dyspozycji w czasie pokoju oraz siły rozwijane w trakcie mobilizacji;
- podstawową organizację wojskową sił zbrojnych (Militärische Grundorganisation, MGO), której zadaniem było dowodzenie, zapewnianie wsparcia logistycznego, koordynacja współpracy cywilno-wojskowej oraz wsparcie sojuszników stacjonujących na terytorium Niemiec.

W Białej Księdze z 2006 r. podkreślono, że misją Bundeswehry będącej instrumentem polityki bezpieczeństwa i obrony jest zabezpieczanie skuteczności działania polityki zagranicznej Niemiec, przyczynianie się do stabilności europejskiej oraz globalnej, gwarantowanie narodowego → b e z p i e c z e ń s t w a i obrony, wnoszenie wkładu w obronę sojuszników oraz wspieranie wielonarodowej współpracy i integracji.

Podstawą działania Bundeswehry pozostała obrona Niemiec przed zagrożeniami z zewnątrz, ochrona terytorium oraz obywateli i infrastruktury państwa. Do jej zadań należały: przezwyciężanie międzynarodowych konfliktów i zapobieganie kryzysom, w tym zwalczanie międzynarodowego → t e r r o r y z m u [t. 4] (udział w operacjach sojuszniczych musi być rozpatrywany pod kątem interesów niemieckich), wspieranie partnerów Sojuszu oraz ochrony Republiki Federalnej i jej obywateli, uczestnictwo

w akcjach ratowniczych i ewakuacyjnych, partnerstwo i kooperacja wewnątrz sił zbrojnych oraz subsydiarne działania niesienia pomocy (m.in. podczas → k a t a s t r o f n a t u r a l n y c h [t. 2] czy odbudowy porządku lub infrastruktury na terenach objętych katastrofą).

Bundeswehra oparta była na powszechnym obowiązku służby wojskowej. Do 2010 r. miała być zredukowana do 327,5 tys. żołnierzy. Dzieliła się na 5 rodzajów sił zbrojnych: siły lądowe, powietrzne i morskie, bazę sił zbrojnych oraz centralną służbę medyczną.

Jej charakter odzwierciedlało określenie *Armee im Einsatz* – oznacza ono nowoczesne, zmotywowane oraz zdolne do działania siły zbrojne RFN, szkolone i przeznaczone głównie do udziału w misjach poza granicami kraju. Podkreślano, że działając w wielonarodowych ramach, Bundeswehra przyczynia się do wzmacniania międzynarodowych organizacji bezpieczeństwa, globalnej równowagi oraz odbudowy stosunków opartych na partnerstwie i zaufaniu. Wskazano ponadto podstawowe obszary umiejętności, do których należą: zdolność dowodzenia i kierowania, → w y w i a d [t. 4] i rozpoznanie, mobilność, skuteczność działania na misjach / w operacjach, wsparcie i zdolność przetrwania, ochrona.

W celu określenia udziału Bundeswehry w operacjach wielonarodowych wymieniono następujące zobowiązania międzynarodowe, które należy uwzględnić jako najważniejsze przesłanki operacyjne:

- udział w siłach reagowania NATO wymagający stałego utrzymywania w gotowości kontyngentu ogólnowojskowego, jego przygotowania i utrzymania w gotowości (ok. 15 tys. żołnierzy);
- w ramach European Headline Goal RFN zobowiązała się, stosownie do sytuacji, do utworzenia kontyngentu liczącego do 18 tys. żołnierzy. W tym zawiera się niemiecki wkład w ramach → g r u p b o j o w y c h U E [t. 2] w celu polepszenia zdolności reagowania;
- w ramach United Nations Standby Arrangements System Niemcy gwarantują utrzymanie w gotowości pododdziałów transportowych, medycznych, żandarmerii, saperów, pododdziałów dalekiego rozpoznania morskiego i przeciwminowych – w sumie ok. 1 tys. żołnierzy nowocześnie uzbrojonych i wyposażonych;
- dodatkowo utrzymanie ok. 1 tys. żołnierzy do prowadzenia operacji ratowniczych i ewakuacyjnych.

Nowa reorganizacja Bundeswehry przewidziała 3 kategorie sił zbrojnych:

- siły uderzeniowe/reagowania (*Eingreifkräfte*), przewidziane przede wszystkim do udziału w wielonarodowych, połączonych operacjach o dużej intensywności, prowadzonych we wszystkich wymiarach (operacje lądowe, powietrzne, morskie, kosmiczne). Mogą one realizować przedsięwzięcia wymuszające pokój nawet przeciwko zbrojnie zorganizowanemu przeciwnikowi, przy możliwie niskich stratach własnych; mają być formowane z najlepiej uzbrojonych i zdolnych do szybkiego reagowania sił lądowych, powietrznych i morskich, którym zapewnia się

odpowiednie wsparcie. Ten kontyngent będzie generował niemiecki udział w Siłach Odpowiedzi NATO oraz w siłach NATO i UE uczestniczących w operacjach o najwyższej intensywności, a także w akcjach ratowniczych i ewakuacyjnych. Siły te mają liczyć ok. 35 tys. żołnierzy;

- siły stabilizacyjne (*Stabilisierungskräfte*), przewidziane do prowadzenia wojskowych operacji o małej i średniej intensywności oraz wydłużonym czasie, o szerokim spektrum przedsięwzięć związanych z utrzymaniem pokoju. Między siłami uderzeniowymi a stabilizacyjnymi może dojść do operacyjnej wymiany zadań; powinny one być zdolne do skutecznego rozstrzygania konfliktu, gdy przeciwnik jest częściowo zorganizowany pod względem militarnym, oraz do walki z asymetrycznymi siłami przy możliwie minimalnych stratach własnych. Ich trzonem powinny być siły ciężkie. Umiejętności tych sił to: rozdzielenie stron konfliktu, nadzorowanie warunków zawieszenia broni, eliminowanie sił naruszających pokój, realizacja zadań wynikających z nałożonego embarga, odpieranie lokalnie ograniczonych ataków sił przeciwko siłom stabilizacyjnym, środkom, obiektom i ludności powierzonej ich opiece oraz ochrona autorytetu państwa i publicznej infrastruktury, stworzenie warunków odbudowy struktur państwowych i społecznych w ścisłym współdziałaniu z organizacjami rządowymi i pozarządowymi, a także nadzorowanie panowania nad obszarami, urządzeniami i łącznością na lądzie, w powietrzu i na morzu. Siły te mają liczyć 70 tys. żołnierzy; przewiduje się, że czasowo będą one w stanie wydzielić po 14 tys. osób na 5 równocześnie prowadzonych operacji stabilizacyjnych;
- siły wsparcia (*Unterstützungskräfte*), których główne zadanie obejmuje przeprowadzenie rozległego, ogólnowojskowego wsparcia dla sił operacyjnych oraz stabilizacyjnych (przygotowanie do operacji oraz jej prowadzenie), jak również prowadzenie wsparcia na terenach operacji oraz w samych Niemczech. W ich skład wchodzą struktury dowodzenia i szkoleniowe sił zbrojnych. Siły te miały obejmować ok. 147,5 tys. żołnierzy.

Reforma z 2011 r. ustanowiła poziom liczebności Bundeswehry na 185 tys. żołnierzy i 40 tys. rezerwistów. Wówczas zrezygnowano również z powszechnego obowiązku służby wojskowej, wprowadzono zaś służbę ochotniczą. W Białej Księdze z 2016 r. w dużej mierze powtórzono zadania Bundeswehry zapisane w dokumencie z 2006 r.

Agnieszka Polończyk

BMVg, *Weißbuch 1994. Weißbuch zur Sicherheit der Bundesrepublik Deutschland und zur Lage und Zukunft der Bundeswehr*, Bonn 1994; BMVg, *Weißbuch zur Sicherheitspolitik Deutschlands und zur Zukunft der Bundeswehr*, Berlin 2006; T. Cymek, *Reforma Bundeswehry 2000–2001. Kontynuacja zaangażowania Niemiec w międzynarodowe struktury wojskowe*, Wydawnictwo Adam Marszałek, Toruń 2003; Die Bundesregierung, *Weißbuch 2016 zur Sicherheitspolitik und zur Zukunft der Bundeswehr*, Berlin 2016; H.-A. Jacobsen, L. Souchon, *W służbie pokoju. Bundeswehra 1955–1993*, Bellona, Warszawa 1993; P. Pietrzak, *Bundeswehra w operacjach międzynarodowych. Podstawy prawne, stan obecny, perspektywy*, Wydawnictwo MON, Warszawa

2004; A. Polończyk, *Bundeswehra 1955–2030. Kulturowe i strategiczne uwarunkowania użycia sił zbrojnych RFN*, Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2019; taż, *Bundeswehra – w poszukiwaniu swojej tożsamości*, „Zeszyty Naukowe Wyższej Szkoły Oficerskiej Wojsk Lądowych im. gen. T. Kościuszki" 2012, nr 3 (165); taż, *Strategiczne uwarunkowania użycia sił zbrojnych RFN w latach 1955–1989*, „Politeja" 2017, nr 49.

BURIEWIESTNIK 9M730 – → p o c i s k m a n e w r u j ą c y [t. 5] o napędzie atomowym wystrzeliwany z lądu, mogący przenosić ładunki nuklearne. Buriewiestnik w 2022 r. był wciąż w trakcie przygotowania. Dzięki wyposażeniu w napęd atomowy ma być bronią o nieograniczonym zasięgu. Informacje na ten temat zostały przedstawione przez Władimira Putina w przemówieniu, które wygłosił 1 marca 2018 r. do członków Zgromadzenia Federalnego, rządu, Sądu Najwyższego i Sądu Konstytucyjnego Federacji Rosyjskiej, gubernatorów oraz przedstawicieli najważniejszych mediów. Prezydent Rosji wymienił wówczas 6 rosyjskich systemów uzbrojenia, które miały być odpowiedzią na naruszenie równowagi strategicznej przez Stany Zjednoczone przez rozbudowę obrony przeciwrakietowej. Na „wielką szóstkę" składają się:

- kompleks rakietowy z ciężkim pociskiem międzykontynentalnym Sarmat;
- naziemna międzykontynentalna rakieta hipersoniczna RS-26Awangard;
- kompleks hiperdźwiękowy pocisków rakietowych → K i n d ż a ł;
- laserowe systemy uzbrojenia dużej mocy;
- bezzałogowe, autonomiczne pojazdy podwodne z napędem atomowym i głowicą nuklearną (Posejdon);
- rakiety manewrujące z napędem atomowym (Buriewiestnik).

Szczególną uwagę prezydent poświęcił Buriewiestnikowi oraz torpedzie Posejdon. Zdaniem Putina nisko lecący pocisk wyposażony w głowicę nuklearną przez zmienianie trajektorii lotu powinien skutecznie omijać systemy obrony przeciwnika, by dotrzeć do celu. Pocisk będzie mógł z dowolnego miejsca Rosji osiągać cele w Stanach Zjednoczonych. Dodatkowo przez pewien czas od wystrzelenia będzie mógł się przemieszczać w powietrzu – aż do momentu otrzymania współrzędnych ataku.

Obok odstraszania broń ta miała również odgrywać istotną rolę polityczną w ramach negocjacji Rosji ze Stanami Zjednoczonymi nad przedłużeniem Traktatu o redukcji zbrojeń strategicznych (→ N o w y S T A R T ; New START Treaty, NST). Ponieważ nowy pocisk nie podlega precyzyjnym definicjom i limitom NST, Rosja chciała go wykorzystać jako argument do utrzymania zapisów traktatowych z 2010 r. Gdyby jednak USA wypowiedziały układ, Rosja zamierzała w dalszym ciągu pracować nad pociskiem Buriewiestnik – do czasu, aż stanie się on kategorią uzbrojenia, którą powinno objąć zupełnie nowe porozumienie.

Od momentu przedstawienia pierwszych oficjalnych zdjęć i wizualizacji broni na konferencji w marcu 2018 r. pojawiło się na ten temat wiele artykułów zarówno w prasie amerykańskiej, jak i rosyjskiej. Zdaniem autorów długość pocisku wynosi 12 m w czasie startu oraz 9 m w czasie lotu. Jego nos ma kształt elipsy o wymiarach 1 m

na 1,5 m. Wysokość, na jakiej może się przemieszczać, szacowana jest na 50–100 m. Jest on dwa razy większy niż strategiczny pocisk manewrujący powietrze–ziemia z głowicą konwencjonalną Kh-101. Prawdopodobnie waży również kilka razy więcej niż Kh-101, tym samym wyklucza to samoloty Tu-160 i Tu-95MS jako platformy przenoszenia. Nośnikami Buriewiestnika mogą być jednak pojazdy naziemne typu TEL (Transporter Erector Launcher).

Wywiad amerykański po raz pierwszy miał zlokalizować 9M730 2 lata przed oficjalną prezentacją w 2016 r. na poligonie Kapustin Jar. Pocisk oznaczono jako KY-30. Po kolejnych przeprowadzonych testach otrzymał kod NATO SSC-X-9 Skyfall. Do stycznia 2019 r. przeprowadzonych zostało co najmniej 13 prób, spośród których 11 zakończyło się rozbiciem w trakcie startu. W 2 próbach pocisk wystartował, jednak po kilku minutach lotu na niskich dystansach maszyna przestała działać. Najtragiczniejsza próba została przeprowadzona w sierpniu 2019 r. na poligonie Nienoksa (45. Centralny Poligon Doświadczalny Marynarki Wojennej Federacji Rosyjskiej) w obwodzie archangielskim na północy Rosji. Podczas próby odzyskania silnika eksplozja zabiła 5 rosyjskich naukowców nuklearnych oraz doprowadziła do skażenia promieniotwórczego na Morzu Białym, gdzie poziom promieniowania wzrósł od 4 do 16 razy powyżej normy. Wydarzenie to było szeroko komentowane przez media na całym świecie, ponieważ na poligonie tym nie prowadzono do tej pory prób z bronią jądrową, a jedynie z jej nośnikami. Ostatnie próby rakiet z głowicami jądrowymi podjęto w Związku Radzieckim w 1962 r. Nie kontynuowano ich ze względu na świadomość możliwych awarii w momencie startu, czego konsekwencją byłoby trudne do opanowania skażenie terenu oraz zamknięcie poligonu. Zaskoczenie było większe, gdy przekazano → i n f o r m a c j e [t. 2], że ofiarami byli pracownicy firmy Rosatom, która oficjalnie zajmuje się cywilnym zastosowaniem energii jądrowej, a nieoficjalnie pracą nad technologiami wojskowymi wykorzystującymi materiały rozszczepialne. Rosyjskie ministerstwo obrony narodowej przyznało także, że wypadeknastąpił podczas prac nad pociskiem z izotopowym źródłem energii na platformie morskiej i miał charakter niejądrowy. Wnioski wyciągnięte z tych komunikatów przez zachodnich ekspertów były jednoznaczne –w sierpniu 2019 r. testowano broń nie z głowicą jądrową, ale z napędem jądrowym – pocisk Buriewiestnik.

Widmo katastrofy ekologiczne w samej Rosji nie jest jedynym → r y z y k i e m związanym z użyciem 9M730, nazywanym również „latającym Czarnobylem". Zagrożenie stanowi również możliwość wycieku promieniowania w trakcie poruszania się pocisku w powietrzu z dużą prędkością. Reaktor jądrowy byłby wówczas wystawiony na działanie wysokiego ciśnienia i wysokiej temperatury, co skutkowałoby wzrostem jego temperatury do ekstremalnych wielkości. Narażone na opad radioaktywny byłyby samoloty cywilne lecące wzdłuż toru lotu pocisku. Można zatem wyobrazić sobie sytuację, w której dochodzi do proliferacji tego rodzaju technologii i wiele innych państw podejmuje próby jej zbudowania, stwarzając tym samym poważne zagrożenia ekologiczne dla środowiska naturalnego i człowieka.

Jak podkreślił litewski analityk Lukas Trakimavičius, Buriewiestnik przypomina amerykański pocisk z okresu → z i m n e j w o j n y [t. 4] Supersonic Low Altitude Missile (SLAM), opracowywany w ramach projektu Pluto w Siłach Powietrznych USA. SLAM zaprojektowany był tak, aby zrzucać 16 bomb wodorowych w czasie lotu, a po wyczerpaniu zapasów uderzyć w kolejny cel własną głowicą termojądrową. Ponadto jego „zabójcze" zdolności wynikały nie tylko z ładunku, jaki przenosił, ale także ze sposobu poruszania się. Rektor pokładowy miał wytwarzać 500 MW mocy i pracować w temperaturze 2,5 tys. stopni Celsjusza. Przewidywano, że nisko lecący SLAM nad miastami Związku Radzieckiego powodowałby zniszczenia budynków, wybijanie szyb, ogłuszanie przechodniów, lecz również pozostawiałby po sobie skarżenie promieniotwórcze. Oznaczało to, że nie mógł się poruszać w przestrzeni powietrznej sojuszników USA oraz mógł być wystrzelony wyłącznie w pobliżu granicy z ZSRR. 14 maja 1961 r. inżynierowie pracujący nad projektem Pluto uruchomili na kilka sekund system napędowy SLAM mieszczący się w wagonie, a następnie na 5 minut. Silnik wytworzył wówczas 513 MW mocy, co odpowiadało 35 tys. buntów. Było to o 6 tys. więcej niż w wypadku silnika Pratt & Whitney F100-PW-229 włączonego dopalaczem, wykorzystywanego w F-16. Biorąc pod uwagę skalę zniszczenia, jaką powodował pocisk w czasie lotu, oraz wizję możliwej odpowiedzi ze strony Związku Radzieckiego w postaci budowy własnej wersji SLAM, Stany Zjednoczone anulowały projekt Pluto 1 lipca 1964 r.

Od momentu pojawienia się informacji na temat Buriewiestnika zachodni eksperci podawali w wątpliwość powodzenie tego projektu. Opinie te potwierdziły wszystkie prowadzone do 2019 r. nieudane próby. Głównymi zaletami rakiety miały być: nieograniczony zasięg; tor lotu pozwalający na omijanie systemów obrony przeciwlotniczej i przeciwrakietowej; czas startu umożliwiający wystrzelenie Buriewiestnika „wcześniej" niż innych tego rodzaju pocisków, co umożliwiało oczekiwanie na wskazanie celu w powietrzu. Tymczasem opublikowane filmy wskazują, że czas lotu rakiety był nie dłuższy niż 2 min, a zasięg nie większy niż 36 km. Mogłoby to oznaczać, że konstruktorom nie udało się uruchomić reaktora i pocisk przemieszcza się tylko na taką odległość, na jaką pozwala standardowe paliwo. Ponadto aby osiągnąć prędkość zbliżoną do prędkości hipersonicznej (4 Ma), Buriewiestnik musiałby być wyposażony w silnik strumieniowy, który wciągałby chłodne powietrze, rozszerzał je pod wpływem ciepła reaktora, a następnie wykorzystywał rozprężone powietrzne do napędzania pocisku. Tego rodzaju silnik nigdy nie był jednak montowany na pociskach manewrujących.

Jak podkreślił Leah Walker z Michigan State University, pocisk taki jak Buriewiestnik należy traktować jako kolejną rosyjską próbę redukcji luki technologicznej dzielącej Rosję od Stanów Zjednoczonych. Systemy tego rodzaju są często oparte na starych rozwiązaniach z czasów sowieckich i choć w teorii wydają się imponujące, w praktyce okazują się kosztowne i bardzo trudne do zastosowania.

Mimo porażek Rosja nie zaprzestała jednak prac nad pociskiem.W 2020 r. telewizja CNN poinformowała, że w stacji badawczej Pankowo na Nowej Ziemi planowane

jest wznowienie prób Buriewiestnika. Potwierdzili to również badacze z Middlebury Institute of International Studies w Monterey, Jeffrey Lewis i Michael Duitsman. Analizując zdjęcia satelitarne udostępnione przez Planet Labs, wskazali, że na stacji badawczej pojawiła się nowa → i n f r a s t r u k t u r a w o j s k o w a [t. 2], na którą składały się platformy startowe służące do wstrzeliwania pocisków, lądowisko dla helikopterów, droga dojazdowa, budynek mogący pełnić funkcję montażowni oraz liczne kontenery transportowe. Prace miały być prowadzone w bardzo szybkim tempie między 18 a 20 września 2020 r., co podkreśla priorytetowe znaczenie Buriewiestnika dla Sił Zbrojnych Federacji Rosyjskiej. W styczniu 2021 r. opublikowany został z kolei raport Defense Intelligence Ballistic Missile Analysis Committee *Ballistic and Cruise Missile Threat*. Poświęcono go broni balistycznej rozwijanej przez 4 państwa: Chiny, Rosję, Koreę Północną oraz Iran. Autorzy scharakteryzowali Buriewestnika jako „rozwojową" broń strategiczną, dzięki której Rosja może osiągać cele o zasięgu międzykontynentalnym.

Tomasz Wójtowicz

Congressional Research Service, *Russia's Nuclear Weapons: Doctrine, Forces, and Modernization*, R45861, 21.04.2022, https://sgp.fas.org/crs/nuke/R45861.pdf (dostęp 8.03.2022); Defense Intelligence Ballistic Missile Analysis Committee, *Ballistic and Cruise Missile Threat*, 2020, https://media.defense.gov/2021/ Jan/11/2002563190/-1/-1/1/2020%20BALLISTIC%20AND%20CRUISE%20MISSILE%20THREAT_FINAL_2OCT_REDUCEDFILE.PDF (dostęp 12.04.2023); M. Dura, *„Buriewiestnik" pierwszym niewypałem putinowskiego superuzbrojenia*, 15.09.2019, https://defence24.pl/buriewiestnik-pierwszym-niewypalem-putinowskiego-superuzbrojenia-opinia (dostęp: 12.04.2023); A. Hollings, *Project Pluto: The Most Insane Missile America Ever Built*, 27.10.2021, https://www.sandboxx.us/blog/ project-pluto-the-craziest-nuclear-weapon-in-history/ (dostęp 9.03.2022); T. Kadam, *Russia's 'Nuclear-Powered' Cruise Missile Dubbled 'Flying Chernobyl' Could Be Ready For Deployment By 2025 – Reports*, 16.08.2022, https://eurasiantimes.com/ russias-nuclear-powered-burevestnik-cruise-missile-flying-chernobyl/ (dostęp 12.04.2023); J. Lewis, *Burevestnik Testing to Resume. Russia Preparing to Resume Nuclear-Powered Cruise Missile Tests*, 20.10.2020, https://www.armscontrolwonk. com/archive/1210186/burevestnik-testing-to-resume/ (dostęp 12.04.2023); R. Muczyński, *Rosja wznawia próby nuklearnego Buriewiestnika*, 22.10.2020, https:// milmag.pl/rosja-wznawia-proby-nuklearnego-buriewiestnika/ (dostęp 12.04.2023); M.A. Piotrowski, *Wojskowe zastosowanie napędu nuklearnego: rosyjski projekt pocisku 9M730 Buriewiestnik*, „PISM" 2019, nr 84 (1832), https://pism.pl/publikacje/ Wojskowe_zastosowanie_napedu_nuklearnego_rosyjski_projekt_pocisku_ 9M730_Buriewiestnik (dostęp 8.03.2022); T. Szulc, *Rosyjska rakieta Buriewiestnikz napędem atomowym*, https://www.magnum-x.pl/artykul/rosyjska-rakieta-buriewiestnik-z-napedem-atomowym (dostęp 12.04.2023); L. Trakimavičius, *The Future Role of Nuclear Propulsion in the Military*, „Energy Highlights" 2022, no. 17, https://enseccoe.org/data/public/uploads/2021/10/d1_the-future-role-of-nuclear-propulsion-in-the-military.pdf (dostęp 8.03.2022); L. Walker, *Nuclear-Powered Cruise Missiles: Burevestnik and its Implications*, „Journal of Science Policy & Governance" 2020, vol. 16, no. 1, https://www.sciencepolicyjournal.org/uploads/5/4/3/4/5434385/ walker_jspg_v16.pdf (dostęp 12.04.2023); *Wybuch na poligonie w obwodzie archangielskim – nieudany test „Buriewiestnika"?*, 12.08.2019, https://defence24.pl/ sily-zbrojne/wybuch-na-poligonie-w-obwodzie-archangielskim-nieudany-testburiewiestnika (dostęp 9.03.2022).

BUSINESS PROCESS MANAGEMENT **(BPM)** – zarządzanie procesowe, zarządzanie procesami, podejście procesowe – model zarządzania wykorzystywany m.in. w organizacjach systemu → b e z p i e c z e ń s t w a n a r o d o we g o.

Głównym założeniem podejścia procesowego jest dostosowanie procesów do celów biznesowych, poszukiwanie sposobów ich ulepszania i ustalenia mierników realizacji tych procesów, co ma prowadzić do ciągłego monitorowania i ich optymalizacji.

Podejście procesowe ma silne podstawy zaczerpnięte z teorii psychologii społecznej, odwołującej się do teorii X i teorii Y D. McGregora, analizującej postawy, zachowania i potrzeby współczesnego pokolenia. Podejście procesowe idzie dalej, uwzględniając zbiór założeń nazwanych przez A. Maslowa teorią Z, która uznaje wspólne podejmowanie decyzji, wzajemne zaufanie, bliskość, opiekę i współpracę za niezbędne do rozwoju organizacji. Zakłada złożone i zmienne relacje między ludźmi na wszystkich szczeblach organizacyjnych. Potrzeby osobistego wzrastania i szacunku są równie ważne jak → b e z p i e c z e ń s t w o f i n a n s o w e. Teoria Z przyczynia się do nowego spojrzenia na zarządzanie organizacją i daje początek innowacjom, np. takim jak udział pracowników w podejmowaniu decyzji czy zarządzanie przez cele, co przyczynia się do udoskonalenia miejsca pracy.

W celu wyjaśnienia pojęcia procesu odwołano się do pojęcia działania, które jest kluczowym elementem procesu. G. Hostelet definiuje działanie w następujący sposób:

> działać – a przynajmniej działać z namysłem – to tyle, co zmieniać rzeczywistość w sposób mniej lub bardziej świadomy; to zmierzać do określonego celu w danych warunkach przy pomocy właściwych środków po to, by dojść od warunków istniejących do warunków odpowiadających przyjętemu celowi.

Według T. Kotarbińskiego wszelka działalność składa się z czynów prostych, czyli jednoimpulsowych i jednopodmiotowych. Czyn wielopodmiotowy i złożony to współdziałanie. 2 podmioty współdziałają, jeżeli przynajmniej jeden z nich drugiemu pomaga (współdziałanie dodatnie) lub przeszkadza (współdziałanie ujemne). Współdziałanie właściwe zachodzi wtedy, gdy istnieje wspólny cel. W działaniu zbiorowym wyróżnia się czynności składowe i podmioty działające. Podział czynności polega na tym, że różni uczestnicy wykonują odmienne czynności, funkcje. Jeśli dany podmiot pełni określoną funkcję przez wykonywanie stale określonej czynności wymagającej odrębnego wdrożenia, jest to specjalizacja.

M. Weber definiuje działanie jako ludzkie zachowanie, jeśli i o ile działający wiąże z nim subiektywny sens. Wyróżnia 3 typy działań:

- działania racjonalne ze względu na cel – działający kieruje się racjonalnością instrumentalną: ze zbioru wartości podmiot wybiera cele i przy uwzględnieniu alternatywnych kosztów i korzyści dobiera odpowiednie środki;
- działania racjonalne ze względu na wartości – działający podmiot nie uwzględnia następstw działania; to działania afektywne, odpowiadające aktualnym stanom emocjonalnym;

- działania tradycjonalne – opierające się na nawyku.

Jak uważa Weber, najistotniejsze dla rozwoju gospodarczego są działania racjonalne ze względu na cel.

M. Porter określa proces jako łańcuch wartości, w którym poprzez realizację poszczególnych działań zwiększa się wartość zaangażowana w tworzenie lub dostarczanie produktu czy też usługi. Każde kolejne działanie wykonywane w procesie powinno dodawać nową wartość do efektu wcześniejszej czynności. M. Hammer i J. Champy definiują proces jako „sekwencję czynności realizowanych wewnątrz przedsiębiorstwa, a wykonywanych w celu dostarczenia klientowi konkretnej usługi lub produktu". R. Kaplan i D. Norton uważają, że procesy zachodzące w organizacji mają umożliwić „kreowanie wartości, która przyciągnie i zatrzyma klientów docelowego segmentu rynku oraz zapewni spełnienie oczekiwań akcjonariuszy odnośnie do wyników finansowych organizacji".

W normie ISO 9000:2000 proces określony jest jako zbiór działań wzajemnie powiązanych lub wzajemnie oddziałujących, które przekształcają wejścia w wyjścia. Wyjścia jednego procesu są wejściami innych procesów, a procesy powinny być uporządkowane i realizowane tak, aby przyczyniać się do wzrostu wartości organizacji.

Proces jest definiowany również jako przebieg następujących po sobie działań, mających początek i koniec oraz jasno zdefiniowany wkład i rezultat. Proces można określić jako serię operacji lub przebieg działań, podejmowanych w określony sposób i prowadzących do osiągnięcia pewnego rezultatu. Procesy te to ciągi działań ukierunkowane na klienta, których celem jest zadowolenie. Procesem nazywamy zbiór czynności, które przetwarzają produkty o podobnym charakterze i odwołują się do wspólnego obszaru wiedzy.

Proces biznesowy służy osiągnięciu celów, jakie ma zrealizować organizacja, instytucja czy przedsiębiorstwo, obejmuje powiązania występujące u klientów, dostawców i innych podmiotów, partnerów biznesowych itp. Pojedyncza przemiana występująca w procesie biznesowym (gospodarczym) to funkcja. Dekompozycja funkcji powoduje przekształcenie jej w podproces.

R. Boulton i B. Libert twierdzą, że procesy to faktyczne funkcjonowanie organizacji; są one „szeregiem operacji, metod, zadań i funkcji prowadzących do wytworzenia produktów i usług". A. Badiru i B. Ayeni przedstawiają hierarchię elementów procesu, wyróżniając: czynności, działania, proces, system. Za P. Grajewskim można wyodrębnić cechy typowe dla procesu:

- proces jest zestawem działań – złożony jest z określonej sekwencji czynności składających się na konkretne działania, które wchodzą w skład procesu;
- proces to działanie uporządkowane – działania w ramach danego procesu muszą być wykonywane w odpowiedniej kolejności, działania zbędne powinny być eliminowane, gwarantuje to powtarzalny przebieg procesu;

- działania w procesie muszą zmierzać do realizacji wspólnego celu – cele poszczególnych jednostek organizacyjnych podporządkowane są celowi nadrzędnemu, czyli np. zrealizowaniu zamówienia.

Niektórzy autorzy zwracają uwagę na różnice między pojęciami procesu i procesu biznesowego: pojęcie procesu nic nie mówi o ograniczeniach, rozpiętości, zawartości, strukturze i odbiorcach procesu. Na proces biznesowy składają się komponenty takie jak:

- wymagania klienta i oczekiwania klienta;
- wkład (ang. *input*);
- świadczenie mające wartość dla klienta;
- rezultat (ang. *output*);
- osoba odpowiedzialna za realizację procesu (właściciel, menedżer procesu);
- cel procesu;
- mierniki sterujące procesem.

Proces biznesowy rozpoczyna się i kończy u klienta. Procesy można dzielić wg różnych kryteriów. Ze względu na rangę zadań (funkcji) wykonywanych w organizacji wyróżnia się procesy:

- podstawowe – związane z obsługą klienta zewnętrznego/studenta, a więc kreujące wartość dodaną;
- pomocnicze – zbiory uporządkowanych działań wspierających procesy podstawowe;
- zarządzania – mające strategiczny wpływ na generowanie wartości, odgrywające rolę regulacyjną w stosunku do procesów podstawowych i pomocniczych.

Ze względu na miejsce w łańcuchu wartości wyróżnia się:

- procesy innowacyjne – badanie potrzeb klienta i projektowanie produktu lub usługi, np. nowych kursów;
- procesy operacyjne – wytwarzanie produktu i dostarczanie go klientowi, procesy dydaktyczne, procesy administracyjne;
- procesy obsługi posprzedażnej – obsługa klienta po dostarczeniu mu produktu lub usługi, w organizacji edukacyjnej będą to produkty dodatkowe i marka.

Ze względu na ich podległość można dzielić procesy na megaprocesy, procesy główne i podrzędne (subprocesy).

Megaproces to łańcuch czynności prowadzących do wytworzenia produktu lub wykonania usługi odpowiadającej wymaganiom klienta. Można zatem mówić o hierarchii procesów, w której megaprocesy mają charakter nadrzędny wobec procesów głównych i podrzędnych. Megaproces obejmuje wszystkie obszary organizacji. Szacuje się, że w przedsiębiorstwie występuje 4–6 megaprocesów, natomiast procesów głównych – kilkanaście do kilkudziesięciu, w zależności od wielkości i specyfiki organizacji.

Standardowa Klasyfikacja Procesów opracowana przez American Productivity and Quality Center (APQC) wyodrębnia 12 podstawowych kategorii procesów, które

dotyczą wszystkich typów przedsiębiorstw. Pierwsze 5 kategorii to procesy główne (operacyjne), charakteryzujące działalność podmiotu. Decydują one o zakresie funkcjonowania przedsiębiorstwa. Są to:

- rozwój wizji i → s t r a t e g i i [t. 4];
- projektowanie i rozwój produktów i usług;
- sprzedaż produktów i usług;
- dostarczanie produktów i usług;
- zarządzanie obsługą klienta.

Natomiast kolejne 7 kategorii wchodzi w skład procesów wspomagających, które przenikają wszystkie procesy podstawowe:

- rozwój i zarządzanie kapitałem ludzkim;
- zarządzanie technologią informacyjną i wiedzą;
- zarządzanie zasobami finansowymi;
- przejmowanie, konstruowanie i zarządzanie majątkiem;
- zarządzanie środowiskiem zdrowia i → b e z p i e c z e ń s t w a;
- zarządzanie relacjami zewnętrznymi;
- zarządzanie doskonaleniem i zmianami.

W ramach procesu wyróżnić można podprocesy; te z kolei można podzielić na operacje składające się z: zabiegów, czynności i ruchów roboczych.

Bez względu na powyższy podział można wyróżnić następujące cechy wszystkich procesów w organizacji:

- procesy są celowe – w toku realizacji procesu ważny jest dla organizacji wynik;
- procesy cechuje orientacja na klienta – myślenie w kategoriach potrzeb i oczekiwań klienta;
- procesy są holistyczne – wykonywanie procesów wymaga współpracy, aby cały proces przebiegał bez zakłóceń, mimo że jego fragmenty (czynności, działania) wykonywane są przez jednostki w innych pionach funkcjonalnych;
- procesy są metodami wykonywania pracy – organizacja stara się uzyskać wysoką powtarzalność kolejnych sekwencji działań i całego procesu, który generuje określone efekty. Efekty te rozpatrywane są z punktu widzenia terminowości, efektywności ekonomicznej i jakości; procesy muszą być wykonywane przez świadomych pracowników – reorientacja sposobu myślenia i postrzegania działalności wiąże się z przeprowadzaniem szkoleń.

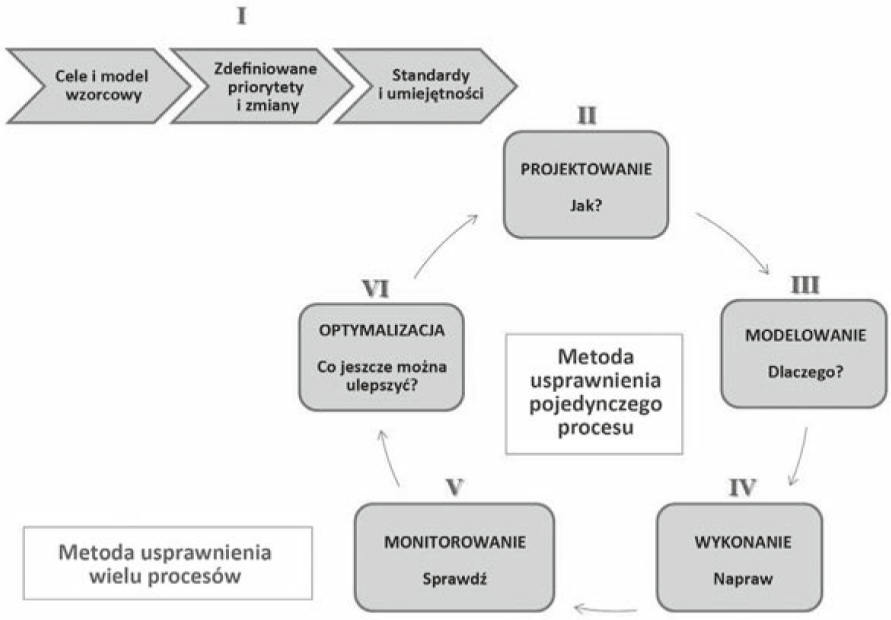
System procesów przedsiębiorstwa to współpracujące ze sobą procesy. Zależności między nimi opisane są poprzez relacje zachodzące na wejściach i wyjściach poszczególnych procesów. Nieciągłości i zaburzenia na styku procesów powodują, że cały system staje się mniej wydajny. Cały system można scharakteryzować następująco:

- system procesów jest systemem sztucznym – jest powoływany jako podsystem organizacji w celu zapewnienia realizacji założeń strategii przełożonych na cele

procesów i stanowisk; w systemie procesów działa wiele podsystemów, które tworzą swój własny system procesów;
- system procesów jest systemem koherentnym – zmiana jednego elementu może pociągnąć zmiany w innych elementach systemu, np. oczekiwania klientów, zmiany wprowadzane przez właściciela procesu lub osoby realizujące proces;
- system procesów jest systemem otwartym – wpływa na niego otoczenie zewnętrzne i wewnętrzne;
- system procesów jest systemem złożonym – ma rozbudowaną strukturę, na którą składają się: podsystem celów, podsystem pomiaru wyników procesów, podsystem uprawnień właściciela procesu. Podsystemy te współpracują ze sobą.

Metodologia wdrożenia podejścia procesowego opiera się na 5-etapowym cyklu zarządzania procesami DMEMO. Każdy z etapów odgrywa istotną rolę w procesie usprawniania i wdrażania zmian, a także zawiera istotne wskazówki dla wykonawców:
- DEFINE (projektowanie) – zdefiniuj procesy takie, jakie są i jakie być powinny. Jak wykonujemy zadania dzisiaj? Jakie są etapy realizacji zamówienia, usługi?
- MODEL (modelowanie) – modeluj procesy, opracuj warianty danego procesu, przeprowadź symulacje, by określić optymalne usprawnienie. Dlaczego robimy to w ten sposób? Czy można zrobić to lepiej? Czy można wyeliminować dany etap?
- EXECUTE (wykonanie) – wprowadź zmiany w procesie. Naprawianie błędów – nawet małe ulepszenie jest ważne.
- MONITOR (monitorowanie) – kontroluj i dokonaj pomiaru rezultatów procesu. Sprawdź efekt zmiany.
- OPTIMIZE (optymalizacja) – dbaj o ciągłe doskonalenie procesów. Co jeszcze można ulepszyć w procesie?

Metoda DMEMO jest właściwa, aby usprawnić pojedynczy proces. Usprawnienie głównych procesów w całej organizacji wymaga dodatkowo określenia celów strategicznych, priorytetów i standardów, co zobrazowano na rysunku 1.



Rys. 1. Metoda usprawnienia wielu procesów
Źródło: *BPM Methodology Practical Guidance*, Resepkuini.com (dostęp 20.08.2015).

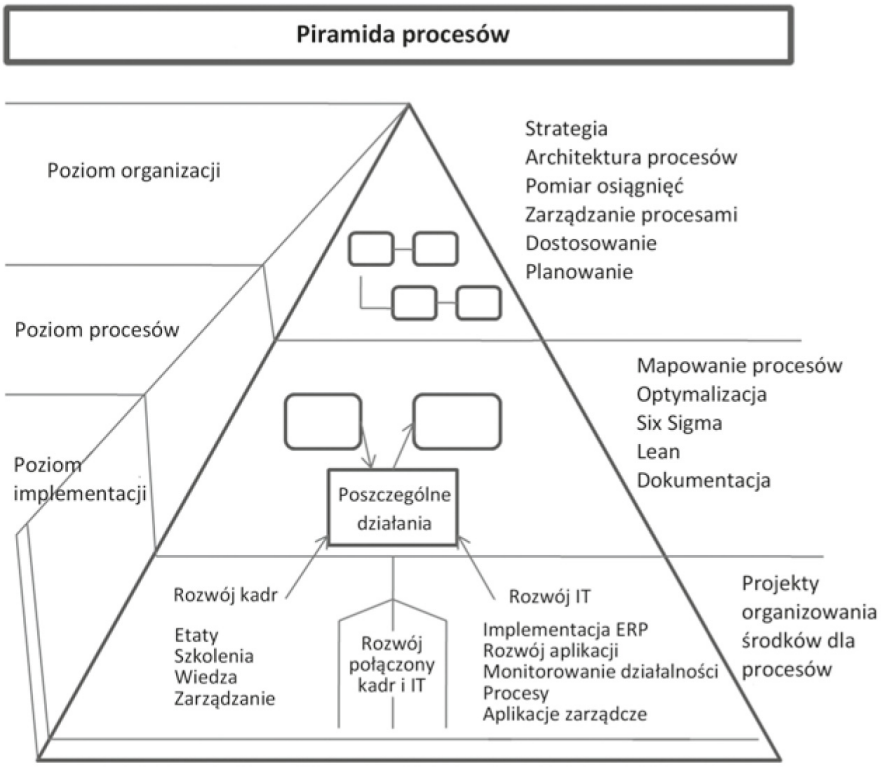
I. Wyznaczanie celów

Pierwszym elementem jest obszar związany z wyznaczaniem celów procesów. Identyfikacja celów dokonywana jest na drodze analizy celów strategicznych odpowiednio do poziomu celów procesów.

Na najwyższym, strategicznym poziomie identyfikowane są cele strategiczne, które najwyższe kierownictwo zamierza osiągnąć w perspektywie od 3 do 5 lat. Są formułowane na podstawie → i n f o r m a c j i [t. 2] zawartych w wizji, misji i strategii organizacji.

II. Projektowanie. identyfikacja procesów

Kolejnym elementem modelowego rozwiązania jest projektowanie, identyfikacja procesów.



Rys. 2. Piramida *BPTrends* i poziomy procesów w organizacji
Źródło: P. Harmon, C. Wolf, *The State of Business Process Management*, BPTrends.com, 2014 (dostęp 11.09.2014).

Najwyższy poziom działalności organizacji jest niezależny od procesów szczegółowych – codziennej działalności organizacji. Na tym poziomie działania skupiają się na dostosowaniu procesów i strategii, określaniu architektury procesów, mierników, systemu zarządzania procesami, analizy potrzeb procesów, ustaleniu priorytetów i planów ich reorganizacji. Poziom procesów opisuje logikę działania organizacji ujętą w formie projektów tworzenia, przemodelowania lub usprawniania istniejących procesów; to analiza, projektowanie i modelowanie działań, które pojawiają się na tym poziomie.

Poziom wdrożenia dostarcza zasobów potrzebnych do wdrożenia zmian w istniejących procesach. To warstwa realizacji, udokumentowana w każdej niemalże organizacji jako zakresy obowiązków, procedury i zarządzenia. Na tym poziomie inicjowane są projekty wdrażania i zastosowania rozwiązań informatycznych, oprogramowań do szkolenia pracowników, wsparcia procesów. Narzędzia wykorzystywane w tym obszarze to np. *Business Process Model and Notation.*

Poziomy te oznaczają stopień uszczegółowienia opisu (modelu) procesu, ale nie hierarchie procesów. W miarę poruszania się w górę model staje się coraz bardziej abstrakcyjny, a idąc w dół – zawiera coraz więcej szczegółów.

Liczba poziomów modelowania zależy od skali działania firmy. Istnieją zawsze 3 kluczowe poziomy, w ramach każdego z nich można wydzielić ich szczegółowe warstwy (z możliwością dodawania kolejnych szczegółów 5+).

Poziom procesów (środkowy) pozwala zrozumieć wewnętrzne zależności, których może być dużo i mogą być złożone (zawiłe); to, ile „poziomów" powstanie w warstwie środkowej, zależy wyłącznie od stopnia złożoności danej organizacji i zawsze jest to indywidualna jej cecha, tylko w części zależna od wielkości organizacji.

Na tym etapie należy również opisać stan obecny (ang. *as is*) procesów i stan docelowy (ang. *to be*), tzw. mapy procesów.

Pytania, na które należy odpowiedzieć, analizując stan obecny procesów i tworząc stan docelowy, oczekiwany po wdrożeniu usprawnień procesów zgodnie ze strategią, to: co organizacja robi na rynku? jak to robimy? jak teraz pracujemy, żeby to robić?

Zidentyfikowane poprawnie procesy wraz z informacją o relacji pomiędzy elementami pozwolą stworzyć modele.

III. Modelowanie

Modelowanie jest często utożsamiane z mapowaniem procesów. Pojęcia te nie są tożsame. Mapa nie opisuje, jak potrzeba jest przekształcana w jej zaspokojenie, nie nadaje się do badania sprawności. Mapa pokazuje jedynie relacje pomiędzy procesami/obiektami w procesie, podczas gdy modelowanie pokazuje przebieg, funkcjonowanie procesu, pozwala ustalić powiązania, interakcje z innymi procesami i systemami.

Zidentyfikowane stan obecny i stan docelowy procesów stanowią podstawę do pracy nad usprawnieniami procesów. Prace te polegają na opracowaniu różnych wariantów realizacji danego procesu, przewidywaniu ewentualnych barier, luk. Można zasymulować zaprojektowany proces i przetestować jego działanie. Przetestowane procesy można uruchamiać w środowisku testowym, sprawdzić ich wydajność za pomocą odpowiednich narzędzi, np. *Business Activity Monitoring* (BAM), poprawić (jeżeli to niezbędne). Dzięki temu można wyeliminować mankamenty takie jak marnotrawstwo czasu i zasobów, wykonywanie niepotrzebnych działań i brak komunikacji między pracownikami.

Proces, czyli szereg operacji, metod, zadań i funkcji lub ciąg działań prowadzą do wytworzenia określonych produktów czy usług; jakość tych produktów i usług, a w konsekwencji efektywność całej organizacji, zależy od organizacji tego szeregu lub ciągu działań. Organizacja jest na tyle efektywna i skuteczna, na ile efektywny i skuteczny jest jej system procesów.

Notacja wykorzystana w niniejszej pracy do modelowania procesów to Notacja BPMN (*Business Process Model and Notation*), która została stworzona specjalnie do opisywania procesów biznesowych i obecnie stanowi podstawowy sposób ich zapisu. Proces, jak wskazuje M. Piotrowski, opisują następujące składowe:

- nazwa procesu;
- dane wejściowe;
- dane wyjściowe;
- operacje – czynności, jakie muszą zostać wykonane w celu skompletowania procesu;
- trajektoria – opis sposobu, kolejności i warunków następowania po sobie operacji;
- wykonawcy (aktorzy) – kto wykonuje poszczególne operacje;
- zdarzenia wpływające na proces: inicjujące, wstrzymujące i uwalniające wykonywanie niektórych operacji, wyjątki (wywołujące procedury obsługi błędów), synchronizujące proces z innymi procesami, wynikowe (generowane w wyniku działania procesu);
- elementy kontrolne – balans obciążenia, statystyki, miary jakości. Notacja BPMN umożliwia modelowanie procesów biznesowych z wykorzystaniem szerokiej palety elementów. Elementarz BPMN podzielono na 4 podstawowe kategorie:
- elementy przepływu (ang. *flow objects*);
- połączenia (ang. *connecting objects*);
- miejsca realizacji (ang. *swimlanes*);
- artefakty (ang. *artifacts*) – elementy graficzne niebędące elementami przepływu. Służą do umieszczania informacji uzupełniających. 3 artefakty są zdefiniowane w BPMN: dane, adnotacje i grupy. Można dodawać własne artefakty.

Metodyka BPMN zakłada operowanie trzema podstawowymi typami obiektów aktywnych (przepływu), są to:

- zdarzenie (ang. *event*) – symbolizowane przez prostokąt z zaokrąglonymi rogami. Zdarzenia mogą być początkowe (pojedyncza cienka linia ciągła), pośrednie (podwójna cienka linia ciągła) i końcowe (pojedyncza gruba linia ciągła). Wyróżniamy następujące typy zdarzeń: nieokreślone, wysłanie/odebranie wiadomości, zasada, czas, anulowanie, zerwanie, wyjątek/usterka, kompensacja;
- zadanie (ang. *task*) – symbolizowane przez prostokąt z zaokrąglonymi rogami z ciemniejszym polem. Zadanie to „praca" wykonywana w procesie;
- bramka logiczna (ang. *gateway*) – symbolizowana przez romb.
  Bramki mogą rozdzielać lub łączyć przepływy.
  Dodatkowo, jak wskazuje Piotrowski, mogą występować:
- połączenia:
  - linia ciągła – przebieg procesu (ang. *sequence flow*);
  - linia przerywana – przebieg wiadomości (komunikatów) (ang. *message flow*);
  - linia kropkowana – powiązanie – asocjacja (ang. *association*);
- miejsca realizacji procesu:
  - „pasy pływackie";
  - uczestnicy (ang. *pools*), reprezentujący uczestników procesu (np. firmy/systemy informatyczne) i opisujący zwykle sytuacje B2B;

– tory (ang. *lanes*), będące elementami struktury organizacyjnej, na jakie w razie potrzeby dzielimy uczestników (najczęściej role biznesowe występujące u danego uczestnika).

Narzędziem informatycznym wykorzystanym do opracowania przykładowego modelu procesów jest ARIS ToolSet, stosowany np. w resorcie → o b r o n y n a r o d o w e j [t. 3].

W koncepcji zarządzania procesami zakłada się interakcje pomiędzy obszarami formułowania celów, identyfikowania i wizualizowania procesów, a także odpowiedzialności i uprawnień osób zarządzających procesem. Właściciel procesu może partycypować w działaniach w każdym z wymienionych obszarów.

IV. Wykonanie/wdrożenie

Ten etap wymaga stworzenia odpowiednich warunków, aby wdrożyć modelowane procesy, wiąże się z przygotowaniem kadry, odpowiednim oprogramowaniem i technologią. Raz wdrożony i ustalony model procesów będzie funkcjonował i rozwijał się niezależnie.

V. Monitorowanie / kontrola procesów

A) wyniki procesów

W *Traktacie o dobrej robocie* Kotarbiński wskazuje, że wszelkie działania należy oceniać z punktu widzenia sprawności. Sprawność działania obejmuje skuteczność, ekonomiczność, jak również wydajność pracy żywej, dokładność, udatność, czystość, prostotę, pewność, racjonalność, energiczność, solidność oraz twórczość. Organizacja to czynność organizowania bądź osiągnięty na skutek takiej czynności ustrój przedmiotu złożonego, układ jego wewnętrznych zależności bądź wreszcie sam obiekt tak zorganizowany.

R.W. Griffin podaje następującą definicję: „organizacja to grupa ludzi, którzy współpracują ze sobą w sposób uporządkowany i skoordynowany, aby osiągnąć pewien zestaw celów".

J.A.F. Stoner, R.E. Freeman i D.R. Gilbert podają, że: „organizacja to dwie lub więcej osób współpracujących w ramach określonej struktury stosunków, aby osiągnąć określony cel lub zbiór celów".

Również P. Drucker twierdzi, że aby firma miała osiągnięcia, musi zadbać o to, by każda praca była ukierunkowana na cele przedsiębiorstwa jako całości.

Cel jest tym, co organizacja stara się osiągnąć; organizacje często mają więcej niż jeden cel; cele są podstawowymi elementami organizacji. J. Zieleniewski definiuje cel jako:

> działanie dotyczące przyszłości, przewidywany stan jakichś rzeczy, który pod pewnymi względami jest dla podmiotu działającego pod jakimś względem cenny, pożądany oraz wyznacza kierunek i strukturę jego działania, zmierzającego do spowodowania lub utrzymania tego stanu rzeczy.

Słownik współczesnego języka polskiego definiuje cel jako „planowany wynik każdego racjonalnego działania; to, do czego się dąży, o co się zabiega". Stopień osiągnięcia celów może być mierzony efektywnością. Efektywność organizacji to miara sprawności i skuteczności organizacji, miara tego, w jakim stopniu osiąga ona odpowiednie cele. Sprawność to „robienie rzeczy we właściwy sposób", minimalizowanie zużycia zasobów przy osiąganiu celów organizacji. Skuteczność to „robienie właściwych rzeczy", umiejętność wyznaczania odpowiednich celów, jest kluczem do powodzenia organizacji. Skuteczność jest więc miarą osiągnięcia określonych, wcześniej uzgodnionych i przyjętych przez organizację celów.

Każdy proces w organizacji poprzez realizowanie sekwencyjnych działań przekształca nakłady obecne na wejściu w efekty, które są widoczne na wyjściu procesu. Proces biznesowy (gospodarczy) to łańcuch przemian wymagający na wejściu wkładu i dający na wyjściu określony rezultat, efekt założonego celu. Przemianom tym podlegają zasoby stanowiące elementy materialne lub niematerialne organizacji, instytucji, przedsiębiorstwa czy jednostki. Każdy proces można więc rozpatrywać pod względem efektywności. Nakłady to różnego rodzaju zasoby: rzeczowe (np. urządzenia, infrastruktura), ludzkie (wiedza pracowników), niematerialne (dane wykorzystywane do realizacji procesów), finansowe (środki pieniężne). Wynikiem przekształcania nakładów mogą być efekty materialne (np. dokumentacja produktu, sylabusy, produkty gotowe: kursy, szkolenia) i efekty niematerialne (np. nowe informacje powstające podczas realizacji procesu, wyższe kwalifikacje personelu).

Pomiar poszczególnych procesów daje informację o stanie całej organizacji. Efektywne procesy są stabilnym i pewnym źródłem wartości dodanej, to znaczy choćby w organizacji pracowali najbardziej utalentowani i zmotywowani pracownicy, to mogą wpływać na poprawę efektywności tylko w takim stopniu, w jakim pozwalają na to procesy.

B) Pomiar efektywności działania organizacji edukacyjnej. wybór narzędzia pomiarowego

Do całościowego pomiaru efektywności organizacji edukacyjnej proponowanym narzędziem jest *Strategiczna Karta Wyników*, narzędzie pomiarowe opracowane przez R.S. Kaplana i D.P. Nortona. Przekłada ono strategię na cele i mierniki pogrupowane ze względu na 4 różne perspektywy: finansową, klienta, procesów i rozwoju. Autorzy zakładają, że organizacja, przygotowując strategię (plan działania), ukierunkowuje ją na realizacje określonych celów. Formułując cele, powinna wiedzieć też, jak zmierzyć poziom ich realizacji. Sukces organizacji w osiągnięciu określonych celów spójnych ze strategią należy ocenić z kilku perspektyw. Jak twierdzą sami twórcy *Strategicznej Karty Wyników*, perspektywy przez nich zasugerowane należy traktować jako wzorzec, a nie sztywne ramy. Przyjęte perspektywy i mierniki powinny odzwierciedlać te czynniki, które prowadzą do uzyskania przewagi konkurencyjnej i sukcesu danej organizacji. Karta powinna być dostosowana do potrzeb i uwarunkowań organizacji.

W celu oceny efektywności procesu należy zdefiniować pewne kluczowe dla danego procesu miary, które pozwolą obiektywnie mierzyć wyniki procesów.

Działania zmierzające do opracowania zestawu mierników powinny uwzględnić elementy takie jak

- cel procesu – jest uszczegółowieniem celów strategicznych;
- miernik procesu – pozwala określić stopień realizacji celu procesu, a więc skuteczność i efektywność procesu, np. indeks satysfakcji klienta, czas trwania projektowania kursu e-learningowego;
- jednostki miar – określają jednostki, w jakich wyrażone będą wartości mierników, np. pozycja uczelni w rankingach, ocena PKA, liczba braków;
- wartości docelowe miernika – określają liczbowo planowane wyniki, jakie powinien osiągnąć proces;
- częstotliwość pomiaru – określa przedział czasowy dokonania pomiaru, np. raz na pół roku;
- struktura algebraiczna – opisuje w matematyczny sposób konstrukcję miernika, np. stopień wykorzystania potencjału intelektualnego kadry: rzeczywisty potencjał/teoretyczny potencjał × 100%;
- źródło danych – określenie informacji, z których korzysta się przy obliczaniu wartości;
- osoba odpowiedzialna – pracownik odpowiedzialny za wyniki procesu, właściciel procesu.

VI. Optymalizacja

Optymalizacja procesu to łączna zmiana istniejącego procesu w zakresie wybranych parametrów (kosztów, czasu, jakości), która daje (podnosi) satysfakcję klientowi procesu i jednocześnie przynosi korzyści organizacji.

Optymalizacja wymaga udziału pracowników, ich wiedzy o realnych warunkach i możliwościach, wiąże konieczną wiedzę o procesach z kreatywnością nowych rozwiązań.

Optymalizacja najczęściej realizowana jest w zespołach pracowników z różnych wydziałów, którzy opracowują w ramach wielu spotkań najpierw stan docelowy dla usprawnianego procesu, opierając się na analizie stanu obecnego. Zidentyfikowane słabe strony procesu są podstawą do ustalania działań usprawniających.

Procesy można systematycznie, ciągle usprawniać (tym się zajmuje zarządzanie procesami) i to wg wielu ekspertów jest lepsze podejście.

Systematyczne usprawnianie procesów sprawi, że organizacja będzie osiągać kolejne poziomy doskonałości procesowej (od poziomu 1 w górę), zapisane w tzw. modelu dojrzałości. Poziom dojrzałości procesowej w organizacji, czyli stan organizacji i jej procesów, może zostać oceniony następująco wg skali modelu CMMI:

- Początkowy – na tym etapie przedsiębiorstwo nie ma świadomości odbywających się procesów.
- Powtarzalny – organizacja ma świadomość tego, że procesy się powtarzają, ale nie są w żaden sposób opisane.

- Zdefiniowany – organizacja jest zorientowana procesowo, a procesy mają swoje definicje.
- Zarządzany – to etap, na którym procesy są kontrolowane i mierzone.
- Optymalizowany – celem wszystkich prac jest doskonalenie procesów.
- Organizacja traktująca priorytetowo procesy nie musi jednorazowo wprowadzać wszystkich elementów szeroko rozumianego zarządzania procesami. Zalecane jest podzielenie na etapy i rozszerzanie prac: od jednorazowych projektów usprawnień wybranych (kluczowych) procesów do stałego ich doskonalenia (zarządzania procesami).

Wdrażanie zarządzania procesami można rozpocząć od stworzenia kilku projektów usprawniania procesów. Jeśli doświadczenia zdobyte w trakcie realizacji tych projektów są pozytywne, to należy rozważyć sformalizowane zarządzanie procesami, przynajmniej dla kluczowych procesów.

Danuta Kaźmierczak

BPM Methodology Practical Guidance, Resepkuini.com (dostęp 20.08.2015); P. Grajewski, *Procesowe zarządzanie organizacją*, PWE, Warszawa 2012; R.W. Griffin, *Podstawy zarządzania organizacjami*, tłum. A. Jankowiak, Wydawnictwo Naukowe PWN, Warszawa 2013; P. Harmon, C. Wolf, *The State of Business Process Management*, BPTrends.com, 2014 (dostęp 11.09.2014); R.S. Kaplan, D.P. Norton, *Strategiczna karta wyników*, Wydawnictwo Naukowe PWN, Warszawa 2011; D. Kaźmierczak, *Edukacja w zakresie bezpieczeństwa i obronności w ujęciu procesowym*, Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2018; *Kierowanie*, J.A.F. Stoner, R.E. Freeman, D.R. Gilbert (red.), tłum. A. Ehrlich, PWE, Warszawa 2011; M. Piotrowski, *Procesy biznesowe w praktyce*, Helion, Gliwice 2014; B. Skrzypek, M. Hofman, *Zarządzanie procesami w przedsiębiorstwie*, Wolters Kluwer Polska, Warszawa 2010.

C

C4ISR – (ang. *Command, Control, Communication, Computers, Intelligence, Surveillance, Reconnaissance*), termin używany w amerykańskiej nomenklaturze wojskowej oznaczający „dowodzenie, kontrolę, komunikację, komputery, → w y w i a d [t. 4], nadzór i rozpoznanie". Geneza C4ISR sięga lat 70. XX w., kiedy innowacje wojskowe będące skutkiem rewolucji informacyjnej oraz zmiany mentalne w Siłach Zbrojnych Stanów Zjednoczonych umożliwiły budowę systemów pozwalających usprawnić dowodzenie, wymianę → i n f o r m a c j i [t. 2] oraz zbieranie danych wywiadowczych.

Jedną z zasadniczych przyczyn przystąpienia do prac nad C4SIR były wydarzenia z 8 czerwca 1967 r. Wówczas podczas trzeciej → w o j n y [t. 4] arabsko-izraelskiej (nazywanej wojną sześciodniową) doszło do omyłkowego zaatakowania amerykańskiego okrętu wojskowego USS „Liberty" przez izraelski myśliwiec. W rezultacie

zginęło 34 członków załogi, a 171 zostało rannych. Przyczyny omyłkowego zaatakowania to – z jednej strony – błędna ocena sytuacji przez siły obrony Izraela, które amerykański okręt poruszający się niedaleko półwyspu Synaj uznało za jednostkę wroga, a z drugiej strony – brak systemów komunikacji umożliwiających szybką wymianę informacji między dowództwem Marynarki Wojennej USA a jej poszczególnymi okrętami. Rozkaz przesłany drogą radiową, nakazujący oddalenie się USS „Liberty" od wybrzeży w związku z rozpoczętą wojną, dotarł do okrętu dopiero 3 godziny po izraelskim ataku rakietowym. Tyle że tragiczne wydarzenia z 8 czerwca 1967 r. nie stały się jednak przyczyną powstania systemów typu C4ISR. Ich pojawienie wiąże się również z działalnością wysokich rangą wojskowych i urzędników rozumiejących konieczność jakościowej zmiany w obszarze dowodzenia i kontroli, takich jak: Robert Hermann – dyrektor Narodowego Biura Rozpoznania, Harry L. Van Trees – specjalista w obszarze radarów, sonarów i komunikacji, zarazem asystent Sekretarza Obrony USA, czy generał major Jasper A. Welch Jr. – zastępca szefa sztabu ds. badań i rozwoju w kwaterze głównej Sił Powietrznych USA. W wyniku starań tych osób Kongres USA, początkowo sceptyczny, zgodził się przyznać dodatkowe środki na badania nad C4ISR, którym równolegle towarzyszyły zmiany instytucjonalne. W Pentagonie powołano do życia biuro asystenta Sekretarza Obrony C3I, łączące zespoły zajmujące się do tej pory dowodzeniem i kontrolą, systemami łączności, wywiadem oraz wsparciem obronnym (wojna elektroniczna i nawigacja). Szkoła Podyplomowa Marynarki Wojennej USA (Naval Postgraduate School) uruchomiła program nauczania C3, którego celem było wykształcenie specjalistów potrzebnych do oceny i obsługi nowych systemów komunikacyjnych. Wreszcie – Biuro Badań Marynarki Wojennej (Office of Naval Research) utworzyło we współpracy z Massachusetts Institute of Technology wieloletni program badawczy wspierający wysiłki zmierzające do budowy C4ISR. Efektem wszystkich powyższych zabiegów było powstanie C2 (ang. *Command & Control*), następnie – jego ewolucja do C3 (ang. *Command, Control & Communication*), C4 (ang. *Command, Control, Communication & Computers*), C4ISR (ang. *Command, Control, Communication, Computers, Intelligence, Surveillance, Reconnaissance*), a obecnie także C5ISR (ang. *Command, Control, Communication, Computers, Cyber-Defense, Intelligence, Surveillance, Reconnaissance*) oraz C6ISR (ang. *Command, Control, Communication, Computers, Cyber-Defense, Combat-Systems, Intelligence, Surveillance, Reconnaissance*). Departament Obrony USA definiuje dowodzenie i kontrolę (C2) jako „sprawowanie dowodzenia i kontroli przez właściwego dowódcę nad przydzielonymi mu siłami w celu wykonania misji". *Dowodzenie* oznacza władzę nabytą, którą oficer albo podoficer sprawuje zgodnie z obowiązującymi przepisami nad podwładnymi. *Kontrola* natomiast odnosi się do sposobu przydzielania zadań, do wyznaczania celów oraz do kierowania niezbędnego do realizacji misji. Zatem C2 opisuje sposób, w jaki sposób wojskowi dowodzą siłami zbrojnymi, aby uzyskać sukces w wyniku

planowania i wykonywania działań związanych z konkretną misją. To pojęcie, podobnie jak późniejsze, ma również 2 znaczenia: zależnie od tego, czy postrzegane jest jako proces, czy – jako system. W rozumieniu procesu C2 to „podejmowanie, rozpowszechnianie i wdrażanie świadomych decyzji w celu uzyskania skuteczności działania sił zbrojnych w czasie pokoju, → k r y z y s u [t. 2] i wojny". Obejmuje ono 3 główne obszary:

- zarządzanie informacją (zbieranie aktualnych i dokładnych informacji, a następnie przekazywanie ich dowódcy i wykorzystanie w procesie podejmowania decyzji);
- zarządzanie decyzjami (podejmowanie decyzji przez oficera lub podoficera dowodzącego misją);
- zarządzanie wykonaniem (działania podejmowane przez oddziały i pododdziały na podstawie wydanych decyzji).
- Z koeli C2 rozumiane jako system jest połączeniem technologii i praktyk, wspierających procesy realizowane przez żołnierzy,a opisywanych za pomocą 6 cech. Są nimi:
- niezawodność (system powinien wykonywać określone funkcje w różnych warunkach i czasie);
- przeżywalność (system powinien być solidny i móc wytrzymać ataki wroga w szerokim spektrum konfliktów);
- elastyczność (system powinien szybko dostosowywać się do zmieniającego się środowiska i postępu technologicznego);
- zdolność do odpowiedzi (system powinien szybko i precyzyjnie reagować);
- interoperacyjność (systemy w poszczególnych rodzajach sił zbrojnych powinny harmonijnie współdziałać, aby umożliwić prowadzenie operacji połączonych);
- orientacja na użytkownika (informacje przekazywane za pomocą C2 powinny być czytelne i jednoznaczne).

Generalna zasada funkcjonowania systemu C2 koncentruje się więc na zaspokojeniu potrzeb dowódcy dzięki dostarczeniu mu skutecznych narzędzi dowodzenia. Kiedy procesy i systemy działają efektywnie, tworzą one pełny system C2, definiowany jako „wynik netto udanej interakcji złożonej architektury składającej się z ludzi, procedur i technologii". Pierwsza fala rozwoju C2 nastąpiła w latach 70. XX w. Druga – na początku lat 90. XX w., pod wpływem przebiegu pierwszej wojny w Zatoce Perskiej, będącej poligonem doświadczalnym dla technologii opracowanych wcześniej. Nad Irakiem pojawiła się wówczas najnowocześniejsza amerykańska broń informacyjna w postaci systemu AWACS (ang. *Airborne Warning nad Control System* – system wczesnego ostrzegania i kierowania obroną przeciwlotniczą) oraz jego odpowiednika wykrywającego obiekty naziemne – systemu J-STAR (ang. *Joint Surveillance and Target Attack RadarSystem* – połączony radarowy system rozpoznania i ataku). Jak podkreślił Alvin Toffler, tej wojnie towarzyszyła największa → m o b i l i z a c j a [t. 3] środków łączności w historii wojskowości.

Z uwagi na ograniczone możliwości przesyłania informacji w regionie Bliskiego Wschodu i wśród państw – sojuszników wybudowano skomplikowany zestaw połączonych sieci. Opierały się one na 118 ruchomych naziemnych stacjach łączności satelitarnej, wspomaganych przez 12 komercyjnych terminali łączności satelitarnej, dysponujących 81 zwrotnicami, które z kolei umożliwiały utworzenie 329 kanałów fonicznych i 30 kanałów do przekazu danych. Te połączenia obsługiwały do 700 tys. rozmów telefonicznych oraz pozwalały na nadanie 152 tys. komunikatów dziennie, z wykorzystaniem 30 tys. częstotliwości radiowych. Sukces wojsk amerykańskich w 1991 r. został przypisany m.in. dominacji informacyjnej i technologicznej, jaką uzyskały one nad armią iracką. Stało się to impulsem do prowadzenia kolejnych badań i prac nad C2.

W 1993 r. ukazały się 2 istotne publikacje: *Memorandum of Policy No 30*, opublikowane przez biuro Komitetu Szefów Sztabów Sił Zbrojnych USA, oraz raport RAND pt. *Cyberwar is coming* autorstwa Johna Arquilla i Davida Ronfeldta. W obu systemy C2 opisano jako kluczowy i niezbędny element budowania przewagi nad przeciwnikiem, konieczny do prowadzenia → c y b e r w o j n y [t. 1]. W kolejnych latach postępująca rewolucja w sprawach wojskowych oraz pojawienie się nowych technologii w obszarze rozpoznania umożliwiły rozbudowanie struktury C2. Obok „dowodzenia i kontroli" pojawiły się „komputery i komunikacja", uwzględniające nowe obiekty, sprzęt, personel i procedury (C4). Następnie C4 rozbudowano do C4ISR, oznaczającego wywiad, nadzór i rozpoznanie (ang. *intelligence, surveillance, reconnaissance*). Wywiad jest tu rozumiany jako ciągłe gromadzenie, przetwarzanie i analiza informacji dotyczących innych państw, ze szczególnym uwzględnieniem ich sił zbrojnych oraz miejsc, w których mogą być prowadzone przyszłe operacje wojskowe. Nadzór należy rozumieć jako systematyczną obserwację przestrzeni powietrznej, → c y b e r p r z e s t r z e n i [t. 1], powierzchni Ziemi, powierzchni oraz głębin mórz i oceanów, jak również osób, miejsc lub obiektów, za pomocą środków wizualnych, dźwiękowych, fotograficznych, elektronicznych lub innych.

Z kolei rozpoznanie jest działaniem polegającym na obserwacji wizualnej przeciwnika, na ustaleniu jego lokalizacji oraz na zebraniu informacji na temat właściwości meteorologicznych, hydrograficznych i geograficznych. Obecnie do struktury C4ISR dodawane są kolejne dwa „C" – powstały C5ISR oraz C6ISR. C5ISR oznacza „dowodzenie, kontrolę, komputery, komunikację, cyberobronę, wywiad, nadzór i rozpoznanie. W C6ISR znalazł się natomiast element podkreślający wykorzystanie systemów walki (ang. *combat systems*). Przykładem systemu C4ISR może być stanowisko dowodzenia i kontroli podłączone z internetem, z serwerami i stacjami roboczymi, komunikujące się z pobliskimi pojazdami naziemnymi, samolotami i żołnierzami piechoty zbierającymi informacje o środowisku, w którym prowadzona jest misja. Do systemu C5ISR zalicza się stanowisko dowodzenia i kontroli połączone z internetem, z serwerami i stacjami roboczymi oraz z zabezpieczeniami w zakresie

→ c y b e r b e z p i e c z e ń s t w a [t. 1], takimi jak oprogramowanie zabezpieczające system Linux lub samoszyfrujące dyski wspierające działania wywiadowcze, nadzoru i rozpoznania prowadzone przez pobliskie pojazdy naziemne, samoloty i → ż o ł n i e r z y [t. 4]. Przykładem systemu C6ISR może być natomiast centrum obserwacyjno-bojowe znajdujące się na pokładzie okrętu marynarki wojennej: połączone z internetem, z serwerami, ze stacjami roboczymi i z systemami obrony cyberprzestrzeni, wspieranymi przez inne systemy, takie jak Aegic Combat System.

Tomasz Wójtowicz

D. Brett, *C2 vs. C4ISR vs. C5ISR vs. C6ISR: What's the Difference?*, https://www.trentonsystems.com/blog/c2-c4isr-c5isr-c6isr-differences (dostęp 15.11.2021); *C4ISR: The Military's Nervous System*, https://www.defenseone.com/insights/cards/c4isr-military-nervous-system/?oref=d1-cards-prev-nav (dostęp 15.11.2021); W. Perry, D. Signori, J. Boon, *Exploring Information Superiority a Methodology for Measuring the Quality of Information and Its Impact on Shared Awareness, RAND 2004,* https://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR1467. pdf (dostęp 15.11.2021); P.K. Sowell, *The C4ISR Architecture Framework: History, Status, and Plans for Evolution*, https://www.mitre.org/publications/technical-papers/the-c4isr-architecture-framework-history-status-and-plans-for-evolution (dostęp 15.11.2021).

CAMBRIDGE ANALYTICA (CA) – zarejestrowana w Wielkiej Brytanii firma analityczna wyspecjalizowana w prowadzeniu działań z zakresu marketingu politycznego, podejrzewana o używanie narzędzi ułatwiających manipulowanie preferencjami wyborczymi. CA została założona w styczniu 2015 r. z siedzibą w Westferry Circus w Londynie. Jej dyrektorem generalnym został A.J.A. Nix. Był on również dyrektorem 9 podobnych spółek mających siedziby pod tym samym adresem w Londynie, w tym: Firecrest, Emerdata i 6 spółek SCL Group, również SCL Elections Ltd. N. Oakes założył SCL Group, która jest spółką macierzystą CA. Na oficjalnej stronie CA określono jej działalność jako połączenie analiz predykcyjnych, nauk behawioralnych i technologii reklamowych opartych na zbieraniu danych. Celem tej kombinacji było stworzenie grupy docelowej i wykorzystanie danych do przekonania i motywacji wyborców.

O CA → o p i n i a p u b l i c z n a [t. 3] po raz pierwszy dowiedziała się w 2015 r. Usługi firmy zostały wykorzystane podczas kampanii T. Cruza (ubiegał się o nominację Partii Republikańskiej w wyborach prezydenckich w USA). W grudniu 2015 r. pojawiły się pierwsze → i n f o r m a c j e [t. 2] o wykorzystaniu danych osobowych użytkowników Facebooka przez CA. Według różnych źródeł Strategic Communications Laboratories (SCL Group) współpracowała z Global Science Research (GSR).

Wspólnie firmy zaprojektowały sposób zdobywania danych użytkowników Facebooka. Głównym pomysłodawcą był założyciel GSR A. Kogan *vel* Dr Spectre. Używał on Amazon Mechanical Turk zwanego też MTurk. Jest to usługa oferowana za pomocą platformy Amazon, polegająca na odpłatnym wykonywaniu pewnych prostych zadań przez użytkowników (Human Intelligence Task). Na ogół są to bardzo małe kwoty za wypełnienie ankiety, w tym przypadku wiązało się to z udzieleniem dostępu do kont

Facebooka. Dzięki MTurk jeden użytkownik udostępniał średnio ok. 340 kontaktów wraz z informacjami o lokalizacji i zainteresowaniach, stanie cywilnym, sympatiach politycznych oraz innych danych udostępnianych przez użytkowników. Te dane zebrano i przeanalizowano za pomocą 5-czynnikowego modelu, tzw. dyspozycyjnego modelu osobowości (Positive Psychology Program). Analiza umożliwiła poznanie cech takich jak: ekstrawersja, życzliwość, sumienność, stabilność emocjonalna i otwartość na doświadczenie, a także ich przeciwieństw. Amazon zablokował dostęp GSR do MTurk po licznych skargach. Facebook poinformował, że w 2017 r. GSR otrzymało dane z ok. 30 mln kont użytkowników serwisu.

18 marca 2018 r. „The New York Times" opublikował artykuł, w którym zdemaskowano działania CA. Dochodzenie wykazało, że CA zebrało dane osobowe co najmniej 50 mln użytkowników. Prawdopodobnie może to być największy wyciek danych w historii Facebooka, chociaż zasadność używania terminu wycieku danych jest w tym kontekście dyskusyjna. Postawa władz Facebooka może budzić spore wątpliwości. Facebook uznał, że nie ma mowy o „naruszeniu danych", ponieważ wszyscy użytkownicy dobrowolnie je przekazali, zatem wszystko odbyło się legalnie.

Istnieją podejrzenia, że CA brało udział w kampanii referendalnej brexitu, a także w → w o j n i e i n f o r m a c y j n e j [t. 4] między Rosją i Ukrainą, działało też w Afryce, Meksyku i Malezji, a w najbliższej przyszłości planowało być aktywne w Brazylii, Chinach i Australii. Według jednego z pracowników CA za pomocą „innego podmiotu" przeprowadzono bardzo pomyślny projekt w jednym z krajów Europy Wschodniej.

„Przeniknęli po cichu, zrobili swoje i wynieśli się po cichu, dostarczając naprawdę świetny materiał". Ta wypowiedź została zauważona w Polsce, pojawiły się opinie, że CA mogło pomagać w kampanii Andrzeja Dudy.

W związku z doniesieniami prasowymi przeprowadzono dochodzenia śledcze, m.in. w USA i Wielkiej Brytanii. Brytyjski urząd ICO (Information Commissioner's Office) nałożył karę na Facebooka w wysokości 500 tys. GBP. Uznano, że Facebook niewłaściwie przetwarzał dane i pozwalał na dostęp do nich bez uzyskania wystarczająco wyraźnej i świadomej zgody użytkowników portalu. W USA stwierdzono, że narzędzia CA były wykorzystywane w kampanii prezydenckiej D. Trumpa.

Skandal CA miał duży wpływ na zmiany w prawie i przyjęcie wielu nowych regulacji. 18 kwietnia 2018 r. Facebook zmienił zasady polityki ochrony danych osobowych. 2 maja 2018 r. SCL Elections Ltd i spółka córka CA złożyły wniosek o wszczęcie postępowania upadłościowego. Oficjalną przyczyną była „nagonka prasowa", która zdaniem wymienionych opierała się na bezpodstawnych oskarżeniach o stosowanie nielegalnych metod, tymczasem firma używała legalnych i powszechnie akceptowalnych narzędzi. W związku z tym CA uznało, że nie ma dalszej możliwości działania.

Afera CA zapewne stała się też impulsem do zmiany prawa w UE. 25 maja 2018 r. przyjęto tzw. RODO, przepisy regulujące zasady przechowywania informacji

personalnych i obrotu nimi przez firmy internetowe. W dniu 15 czerwca 2018 r. byli pracownicy CA otworzyli nową firmę doradczą pod nazwą Data Propria. Według Associated Press przedsiębiorstwo planuje wziąć aktywny udział w kampanii prezydenckiej Trumpa w 2020 r. Data Propria oferuje praktycznie tę samą usługę polegającą na projektowaniu profilu psychologicznego elektoratu na podstawie danych z sieci społecznościowych.

Przemysław Mazur

E.L. Boldyreva, N.Y. Grishina, Y. Duisembina, *Cambridge Analytica: Ethics and Online Manipulation with Decision-making Process*, „The European Proceedings of Social & Behavioural Sciences" 2018; D. Ćwiklak, *Facebook okazał się wyborczą bronią masowego rażenia*, Newsweek.pl, 21.03.2018 (dostęp 15.04.2019); H. Davies, *Ted Cruz Using Firm that Harvested Data on Millions of Unwitting Facebook Users*, TheGuardian.com, 11.12.2015 (dostęp 15.04.2019); European Data Protection Supervisor, *Opinion 3/2018: EDPS Opinion on Online Manipulation and Personal Data*, 19.03.2018; J. Horwiz, *Trump 2020 Working with Ex-Cambridge Analytica Staffers*, APNews.com, 15.06.2018 (dostęp 15.04.2019); P. Mazur, *Cambridge Analytica*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; M. Rosenberg, S. Frenkel, *Facebook's Role in Data Misuse Sets Off Storms on Two Continents*, NYTimes.com, 18.03.2018 (dostęp 15.04.2019).

CASUS BELLI – w dosłownym tłumaczeniu z łaciny powód, pretekst do wypowiedzenia → w o j n y [t. 4] lub podjęcia działań zbrojnych.

Koncepcja → w o j n y s p r a w i e d l i w e j [t. 4], rozwijana od starożytności, znajdująca ideologiczne oparcie w poglądach św. Augustyna i św. Tomasza z Akwinu, zakładała, że podstawą prowadzonych działań wojennych ma być *iusta causa*, czyli „słuszna przyczyna" rozumiana jako podjęcie działań zbrojnych w obronie dobra lub w celu przeszkodzeniu złu. Z czasem zaczęto rezygnować z wymogu właściwego uzasadnienia wojny i przywiązywać większą wagę do formalnych przesłanek związanych z rozpoczęciem konfliktu zbrojnego. W XVII w. H. Grocjusz postulował ograniczenie odniesień do prawa boskiego w koncepcji wojny sprawiedliwej. Przyjmuje się, że począwszy od czasu pokoju westfalskiego z 1648 r. idea wojny sprawiedliwej została stopniowo zarzucona, ale okoliczności i sposób wypowiedzenia wojny nie utraciły na znaczeniu z perspektywy prawa międzynarodowego. Przez długi czas koncepcja wojny sprawiedliwej nie była przedmiotem zainteresowania teoretyków prawa. Ponieważ zawierano coraz więcej umów międzynarodowych, częściej wybierano podejście pragmatyczne, przedkładając uregulowania konwencyjne nad tworzenie uniwersalnej teorii. Do koncepcji wojny sprawiedliwej w nowej wersji, pozbawionej odniesień do filozofii chrześcijańskiej, powrócono dopiero w 2. poł. XX w. Zgodnie ze współczesną interpretacją koncepcji wojny sprawiedliwej wojna może być moralnie akceptowalną metodą rozstrzygania sporów, gdy jest prowadzona w celu przywrócenia sprawiedliwości, wolności i → p r a w c z ł o w i e k a [t. 3]. Założenie, że można wskazać jedną ze stron sporu jako sprawiedliwą, towarzyszy omawianej koncepcji od jej zarania, stanowiąc jednocześnie jej mankament.

Zgodnie z koncepcją wojny sprawiedliwej *casus belli* powinien odpowiadać sprawiedliwej przyczynie (*iusta causa*). Lista przyczyn, które mogą zostać uznane za sprawiedliwe, ulega stałemu poszerzeniu, co było widoczne zwłaszcza w XX w. w związku z występowaniem nowych typów konfliktów i zmianami w stosunkach międzynarodowych. Pierwotnie jako *iusta causa* wskazywano samoobronę oraz pomoc sojusznikowi w toczeniu wojny obronnej. Teoretycy, dążąc do aktualizacji listy, są skłonni uznawać za sprawiedliwe wojnę z → t e r r o r y z m e m [t. 4], interwencję w → w o j n i e d o m o w e j [t. 4], atak uprzedzający (antycypacyjny), → i n t e r w e n c j ę h u m a n i t a r n ą [t. 2]. Wspólnym mianownikiem wszystkich wymienionych przyczyn jest pośrednie odwołanie do praw człowieka jako zbioru wartości uniwersalnych, które muszą być chronione zawsze i w każdych okolicznościach. Z tej perspektywy terroryzm jest niedopuszczalny jako wymierzony w dobra bezbronnych i przypadkowych cywilów, ingerencja w wojnie domowej to wsparcie słabszej strony dążącej do obalenia tyrana naruszającego prawa człowieka, atak uprzedzający stanowi *ultima ratio* dla obrony obywateli przed naruszeniem ich praw, interwencja humanitarna opiera się na założeniu, że łamanie praw człowieka nie może pozostać bez odpowiedzi – powinno zostać zatrzymane i ukarane. Można prognozować, że wyodrębnienie innych, nowych przykładów akceptowanych *casus belli* opierać się będzie w przyszłości także na odniesieniach do praw człowieka. Trzecia konwencja haska z 1907 r. zabrania rozpoczynania działań wojennych bez uprzedniego i niedwuznacznego zawiadomienia, które będzie mieć formę bądź umotywowanego wypowiedzenia wojny, bądź ultimatum z warunkowym wypowiedzeniem wojny. Zaznaczyć należy jednak, że nie istnieją → s a n k c j e [t. 4] względem państw nieprzestrzegających tej zasady. W przypadku każdej wojny – zarówno rozpoczętej w ten sposób, jak i z naruszeniem wskazanych zasad – obowiązuje prawo wojenne.

Casus belli ma często znaczenie propagandowe (zob. → p r o p a g a n d a [t. 3]) i kierowane jest do własnych obywateli celem uzyskania poparcia, do społeczności międzynarodowej w tym samym celu lub do drugiej strony konfliktu. Krytycy amerykańskiej → i n w a z j i [t. 2] na Irak w 2003 r. wskazują, że administracja prezydenta G.W. Busha manipulowała → i n f o r m a c j a m i [t. 2] mającymi pochodzić z raportów wywiadowczych w celu wywołania wrażenia, że → r e ż i m [t. 3] Saddama Husajna jest większym → z a g r o ż e n i e m [t. 4], niż był w rzeczywistości. Trzeba więc oddzielać *casus belli* wskazywane w czasie rzeczywistego prowadzenia działań zbrojnych od przyczyn konfliktu ustalanych później przez historyków, często opierających się na informacjach źródłowych, niedostępnych dla → o p i n i i p u b l i c z n e j [t. 3] w czasie wojny. Na podkreślenie zasługuje przy tym istotna relacja współczesnej roli mediów i *casus belli*. Media nie tylko informują o *casus belli*, ale też pośrednio biorą udział w jego kształtowaniu, mają więc niezaprzeczalny wpływ na kształt publicznego dyskursu.

Anna Pacholska, Jakub Idzik

R. Bierzanek, J. Symonides, *Prawo międzynarodowe publiczne*, Wydawnictwo LexisNexis, Warszawa 2004; A. Calabrese, *Casus Belli: U.S. Media and the Justification of the Iraq War*, „Television & New Media", vol. 6, iss. 2; B.A. Garner, *A Dictionary of Modern Legal Usage*, Oxford University Press, Oxford 1995; A. Kleczkowska, *Użycie siły zbrojnej między państwami w świetle międzynarodowego prawa zwyczajowego*, Wydawnictwo Naukowe Scholar, Warszawa 2018; A. Kumankov, *Humanism as Casus Belli: Carl Schmitt's Critique of Just War Theory*, „Russian Sociological Review" 2015, vol. 14, no. 4; T. Lensford, *Casus belli*, [w:] *The Encyclopedia of Political Science*, G.T. Kurian (ed.), CQ Press, Washington 2011; J.S. Nye jr, *Konflikty międzynarodowe. Wprowadzenie do teorii i historii*, tłum. M. Madej, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2009.

CENTO (CENTRAL TREATY ORGANIZATION) – było jedną z wielu organizacji i sojuszy polityczno-wojskowych powstałych w latach 50. i 60. XX w., zwykle tworzonych w celu wzmocnienia wpływu jednego z 2 supermocarstw w niektórych regionach uznanych za mające strategiczne znaczenie dla ich interesów. Powstawanie tego rodzaju organizacji było stałym elementem → z i m n e j w o j n y [t. 4], czyli militarnej, politycznej i ideologicznej bezpośredniej lub pośredniej konfrontacji 2 supermocarstw – USA i ZSRR – w latach 1945–1991.

Założona dokładnie 10 lat po zakończeniu II wojny światowej organizacja odegrała szczególną rolę w wysiłkach podejmowanych przez USA i Wielką Brytanię w celu zablokowania sowieckich inicjatyw na Bliskim Wschodzie. Pomysł utworzenia CENTO, początkowo znanej jako Pakt Bagdadzki lub METO (Organizacja Traktatu Bliskiego Wschodu), pojawił się w latach 1950–1953, kiedy USA, Wielka Brytania i Francja zamierzały wciągnąć państwa arabskie i Izrael do systemu antyradzieckiego. Początek lat 50. był naznaczony rosnącymi napięciami na Bliskim Wschodzie na tle konfliktu między państwami arabskimi a nowo utworzonym państwem izraelskim. 25 maja 1952 r. USA, Wielka Brytania i Francja, obawiając się sowieckiej próby narzucenia swoich wpływów na tym obszarze, wydały Deklarację Trójstronną. Zgodnie z tym dokumentem zarówno państwa arabskie, jak i Izrael miały otrzymać pomoc wojskową i broń do samoobrony. 31 października wraz z Turcją zaproponowały zorganizowanie Dowództwa Obrony Bliskiego Wschodu w tym samym celu, tj. skutecznego blokowania wpływów radzieckich. Wysiłki były kontynuowane w 1953 r. przez administrację Eisenhowera, szczególnie ukierunkowane na Egipt i Izrael. Egipt odmówił zaangażowania się w 1951 r. z uwagi na to, że przywódcy Egiptu przygotowywali początek negocjacji z Wielką Brytanią w celu przejęcia Kanału Sueskiego.

Zachodnie starania ostatecznie zostały uwieńczone sukcesem w 1955 r. W lutym 1954 r. Turcja podpisała pakt o wzajemnej współpracy z Pakistanem. Rok później, 24 lutego 1955 r. w Bagdadzie podpisano umowę wojskową między Królestwem Iraku a Republiką Turcji i zaczęto używać terminu Pakt Bagdadzki. Następnie Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej, Dominium Pakistanu i Królestwo Iranu przystąpiły do paktu o wzajemnej współpracy, zobowiązując się do współpracy, a także ochrony i poszanowania zasady nieingerencji w sprawach wewnętrznych.

Należy podkreślić ważny wkład USA w zawarcie paktu, chociaż wielu zachodnich analityków uważa go za jeden z mniej udanych sojuszy amerykańskich w okresie → z i m n e j w o j n y [t. 4]. Mając na uwadze istotę globalnej polityki promowanej przez Biały Dom w latach 50. i 60., pojawienie się CENTO należy traktować jako jedną z wielu amerykańskich inicjatyw dążących do stworzenia systemu polityczno-wojskowego w celu zneutralizowania działań i rosnących wpływów ZSRR. System obejmował sojusze takie jak → NAT O [t. 3], ANZUS (Pakt Bezpieczeństwa Pacyfiku, sygnowały go Australia, Nowa Zelandia i USA) czy SEATO (Organizacja Paktu Azji Południowo-Wschodniej).

Chociaż zawarcie paktu wydawało się nie napotykać żadnych przeszkód, brytyjskie zaangażowanie zaniepokoiło państwa w regionie. Oczekiwania rządu w Londynie, że Syria i Jordania również dołączą do Paktu Bagdadzkiego, okazały się nierealne. Popularna arabska opozycja znalazła wpływowego zwolennika w osobie nowego prezydenta Egiptu G.A. Nasera, który ujawnił brytyjskie ambicje przywrócenia dominacji kolonialnej.

Ponadto Naser miał inny powód do niezadowolenia – w 1954 r. USA udzieliły Irakowi pomocy wojskowej i gospodarczej, podczas gdy prezydent Egiptu (ówczesny premier) chciał zostać przywódcą świata arabskiego. Jednocześnie miały miejsce gwałtowne demonstracje uliczne w Jordanii, w co niewątpliwie zaangażowany był Pakt Bagdadzki i Wielka Brytania. Na arenie międzynarodowej napięcia powstałe po podpisaniu traktatu doprowadziły do opracowania kilku raportów i analiz od samego początku podkreślających kruchość strukturalną CENTO. Bardziej niż wymowny w tym aspekcie był tajny telegram, który kanadyjski sekretarz stanu ds. zewnętrznych wysłał do stałego przedstawiciela Kanady przy Radzie Północnoatlantyckiej. Telegram z dnia 17 marca 1955 r. wskazywał na fakt, że uznanie zawarcia paktu za sukces nie jest niczym innym jak wielkim błędem, a dopóki CENTO nie uzyska właściwego kształtu dzięki uznaniu przez inne państwa regionu i zawarciu konkretnych umów wojskowych, trudno uwierzyć, że pakt może zapewnić wymaganą stabilność na Bliskim i Dalekim Wschodzie.

Spokój ZSRR zarówno po zawarciu Paktu Bagdadzkiego, jak i późniejszym utworzeniu CENTO nie trwał długo. Radzieccy przywódcy rozumieli, że dzięki powstaniu serii sojuszy polityczno-wojskowych, które pojawiły się przy wsparciu anglo-amerykańskim, możliwości manewrowe ZSRR w różnych regionach świata, takich jak Azja Południowo-Wschodnia oraz Bliski i Daleki Wschód, pozostają ograniczone. W ten sposób można wyjaśnić silną i daleko idącą reakcję polityczno-dyplomatyczną rządu w Moskwie, a także wrogie nastawienie do członków CENTO na początku lat 60. XX w. 16 kwietnia 1955 r. Minister spraw zagranicznych ZSRR wydał publiczne oświadczenie, w którym jednoznacznie skrytykował założenie CENTO, a zaangażowanie USA i Wielkiej Brytanii na Bliskim i Dalekim Wschodzie uznał za wyraźny dowód agresywnych planów dominacji 2 mocarstw zachodnich. Oświadczenie wskazywało

m.in. na fakt, że tworząc bloki wojskowe, brytyjskie koła polityczne starały się utrzymać i przywrócić swoją pozycję siły ze szkodą dla żywotnych interesów narodów na Bliskim i Dalekim Wschodzie, które wybrały drogę niezależnego rozwoju. Argumentowano, że aby ukryć te plany, amerykańskie i brytyjskie koła imperialistyczne powoływały się na absurdalne → z a g r o ż e n i e [t. 4] sowieckie przeciwko krajom w regionie.

Oświadczenie radzieckiego ministra spraw zagranicznych podkreślało, że polityka zagraniczna rządów radzieckich dążyła do zapewnienia pokoju między narodami opartego na przestrzeganiu zasad równości, nieinterwencji w wewnętrzne sprawy i → s u w e r e n n o ś c i p a ń s t w a [t. 4]. Dokument przypominał, że ZSRR był pierwszym krajem, który uznał niepodległość Afganistanu, naprawił błędy popełnione przez były system carski wobec Iranu, udzielił znacznego wsparcia Turcji, Arabii Saudyjskiej, Jemenowi, Syrii, Libanowi i Egiptowi w ramach ich walk o realizację → i n t e r e s ó w n a r o d o w y c h [t. 2]. Tak więc w dokumencie wspomniano, że jeśli kontynuowane będą zachodnie groźby i polityka nacisków wobec państw Bliskiego i Dalekiego Wschodu, kwestia zostanie skierowana do rozpatrzenia przez ONZ, a ZSRR wykazuje całkowity brak zgody w sprawie anglo-amerykańskich inicjatyw w tym obszarze.

Niemniej najważniejsza reakcja ZSRR na te przedsięwzięcia, próbująca ograniczyć możliwości działań Zachodu, miała miejsce 14 maja 1955 r., kiedy powołano do istnienia Układ Warszawski. Ustanawiając tę strukturę, ZSRR próbował m.in. zrównoważyć działalność NATO.

W art. 6 paktu z Bagdadu wspomniano o utworzeniu Stałej Rady na szczeblu ministerialnym, która miała ustanowić własne zasady i procedury. Taki sposób organizacji dowodził, że według swoich inicjatorów CENTO miało odgrywać aktywną rolę w regionie nie tylko z politycznego i dyplomatycznego punktu widzenia, ale także, w razie potrzeby, wojskowego. Stała Rada na szczeblu ministerialnym miała siedzibę w Ankarze, w geograficznym położeniu raczej niecentralnym w stosunku do rzeczywistości, na którą organizacja miała wpływać w terenie. Decyzja była motywowana obawami Brytyjczyków, że ZSRR mógł zdobyć polityczną przewagę nad Turcją. CENTO istniało do 1979 r., ale już w latach 60. XX w. pojawiły się liczne przeciwności. Przede wszystkim od samego początku konflikt arabsko-izraelski uczynił bezużytecznymi starania o pozyskanie nowych członków na Bliskim i Dalekim Wschodzie. Niepowodzenia w negocjacjach z Syrią i Jordanią były niekorzystne dla brytyjskiej polityki w regionie. W 1956 r. wybuchła tzw. wojna synajska. Wszystkie kraje regionu musiały określić swoją pozycję na tle napiętych stosunków między ZSRR, USA i Wielką Brytanią, a ZSRR zagroził bezpośrednią interwencją zbrojną przeciwko Brytyjczykom, Francuzom i Izraelczykom.

W 1958 r. na tle rosnącej sowieckiej i egipskiej potęgi wojskowej w regionie Egipt i Syria zgrupowały się i utworzyły Zjednoczoną Republikę Arabską (ZRA) pod

przewodnictwem Nasera. Na początku lat 60., w kontekście wzrostu wpływów Izraela i z uwagi na bezpośrednią pomoc udzieloną państwu żydowskiemu przez USA, organizacja ta straciła na znaczeniu. Ponadto w 1961 r. Syria wycofała się ze ZRA. W 1959 r., po rewolucji w Iraku, wprowadzono → r e ż i m [t. 3] polityczny sprzyjający ZSRR, a Irak nie był już częścią CENTO. Kolejny trudny moment pojawił się w 1965 r., kiedy Pakistan próbował uzyskać wsparcie przeciwko Indiom w toczącym się między tymi państwami konflikcie. W czasie wojny siedmiodniowej (5–11 czerwca 1967 r.) państwa arabskie ponownie oskarżyły o wsparcie polityczne i dyplomatyczne udzielone Izraelowi przez USA. CENTO powoli traciło rację bytu.

Jeden z ostatnich momentów, w którym CENTO zwróciło uwagę międzynarodowej dyplomacji, był 1971 r., kiedy Pakistan po raz drugi i ostatni próbował uzyskać poparcie przeciwko Indiom. Ponownie spotkał się z odmową Wielkiej Brytanii, Turcji i Iranu. Rok 1979 przyniósł rozwiązanie organizacji przez wycofanie się z niej Iranu i Pakistanu.

Jakub Idzik, Rafał Klepka

M.J. Cohen, *Strategy and Politics in the Middle East 1954–1960. Defending the Northern Tier*, Frank Cass, London–New York 2005; M.-C. Ghenghea, *The Central Treaty Organization – Element of the Western Anti-Soviet System*, „Buletinul Universităţii Petrol – Gaze din Ploieşti" 2010, vol. LXII, no. 1; G. Hadley, *CENTO: The Forgotten Alliance: A Study of the Central Treaty Organisation*, Institute for the Study of International Organisation, Brighton 1971; Pact of Mutual Cooperation Between the Kingdom of Iraq, the Republic of Turkey, the United Kingdom, the Dominion of Pakistan, and the Kingdom of Iran (Baghdad Pact), February 24, 1955; B.K. Yeşilbursa, *The Baghdad Pact. Anglo-American Defence Policies in the Middle East, 1950–1959*, Taylor & Francis, London–New York 2005.

CENTRALNE BIURO ANTYKORUPCYJNE (CBA) – wyspecjalizowana służba systemu → b e z p i e c z e ń s t w a Rzeczypospolitej Polskiej, właściwa w sprawach zwalczania → k o r u p c j i [t. 2] w życiu publicznym i gospodarczym oraz działalności godzącej w ekonomiczne interesy państwa. Przez ustawodawcę została określona jako → s ł u ż b a s p e c j a l n a [t. 4] i z punktu widzenia rzeczywistości prawnej oraz funkcjonowania w ramach współczesnego systemu bezpieczeństwa państwa powinna być tak postrzegana, obok służb kontrwywiadowczych (→ A g e n c j i B e z p i e c z e ń s t w a W e w n ę t r z n e g o i → S ł u ż b y K o n t r w y w i a d u W o j s k o w e g o [t. 4]) oraz służb wywiadowczych (→ A g e n c j i W y w i a d u i → S ł u ż b y W y w i a d u W o j s k o w e g o [t. 4]).

Jest jedną z nielicznych polskich służb tego typu, która była tworzona od podstaw w okresie transformacji systemowej i nie miała wcześniej swojego odpowiednika. Powołanie CBA w 2006 r. stanowiło wyraz konieczności wzmocnienia systemu bezpieczeństwa państwa w przedmiocie przeciwdziałania jednemu z najpoważniejszych → z a g r o ż e ń [t. 4] i zarazem patologii życia publicznego okresu transformacji systemowej, tj. korupcji. Podstawą prawną jego działania jest Ustawa z dnia 9 czerwca

2006 r. o Centralnym Biurze Antykorupcyjnym, która w art. 2 stawia przed nim następujące zadania do realizacji:

- rozpoznawanie i wykrywanie wskazanych przestępstw, zapobieganie im oraz ściganie ich sprawców: przeciwko działalności instytucji państwowych oraz samorządu terytorialnego, określonych odpowiednimi przepisami kk oraz ustawy o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne (dotyczy to głównie przestępstw o charakterze korupcyjnym lub związanych z przekroczeniem uprawnień przez → f u n k c j o n a r i u s z y p u b l i c z n y c h [t. 2] oraz nieprawidłowości w oświadczeniach majątkowych); przeciwko wymiarowi sprawiedliwości, wyborom i referendom, porządkowi publicznemu, wiarygodności dokumentów, mieniu, obrotowi gospodarczemu, obrotowi pieniędzmi i papierami wartościowymi, jeżeli pozostają w związku z korupcją lub działalnością godzącą w interesy ekonomiczne państwa; przeciwko finansowaniu partii politycznych, jeżeli pozostają w związku z korupcją; przeciwko obowiązkom podatkowym i rozliczeniom z tytułu dotacji i subwencji, jeżeli pozostają w związku z korupcją lub działalnością godzącą w interesy ekonomiczne państwa; przeciwko zasadom rywalizacji sportowej; przeciwko obrotowi lekami, środkami spożywczymi specjalnego przeznaczenia żywieniowego i wyrobami medycznymi;
- ujawnianie mienia zagrożonego przepadkiem w związku z przestępstwami, o których mowa powyżej;
- ujawnianie i przeciwdziałanie przypadkom nieprzestrzegania przepisów o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne;
- dokumentowanie podstaw i inicjowanie realizacji przepisów dotyczących zwrotu korzyści uzyskanych niesłusznie kosztem Skarbu Państwa lub innych państwowych osób prawnych;
- ujawnianie przypadków nieprzestrzegania określonych przepisami prawa procedur podejmowania i realizacji decyzji w przedmiocie: prywatyzacji i komercjalizacji, wsparcia finansowego, udzielania zamówień publicznych, rozporządzania mieniem jednostek lub przedsiębiorców oraz przyznawania koncesji, zezwoleń, zwolnień podmiotowych i przedmiotowych, ulg, preferencji, kontyngentów, plafonów, poręczeń i gwarancji kredytowych;
- kontrola prawidłowości i prawdziwości oświadczeń majątkowych lub oświadczeń o prowadzeniu działalności gospodarczej osób pełniących funkcje publiczne;
- prowadzenie działalności analitycznej dotyczącej zjawisk występujących w obszarze właściwości CBA oraz przedstawianie w tym zakresie → i n f o r m a c j i [t. 2] Prezesowi Rady Ministrów, Prezydentowi RP, Sejmowi oraz Senatowi;
- podejmowanie innych działań określonych w odrębnych ustawach i umowach międzynarodowych.

CBA pełni przede wszystkim funkcję policyjną, w ramach której podejmuje → czynności operacyjno-rozpoznawcze (w celu rozpoznawania i wykrywania przestępstw oraz zapobiegania im), a także dochodzeniowo-śledcze, ukierunkowane na wynik procesowy (w celu ścigania sprawców przestępstw). Funkcja kontrolna CBA przejawia się w wykonywaniu czynności kontrolnych mających na celu ujawnianie przypadków korupcji w instytucjach państwowych i samorządzie terytorialnym oraz nadużyć osób, które pełnią funkcje publiczne, jak również w odniesieniu do działalności na szkodę ekonomicznych interesów państwa. Funkcja informacyjna tej instytucji sprowadza się z kolei do wykonywania czynności operacyjno-rozpoznawczych i analityczno-informacyjnych, ukierunkowanych na pozyskiwanie oraz przetwarzanie (gromadzenie, analizę, opracowywanie) informacji istotnych z punktu widzenia prowadzonej działalności w przedmiocie zwalczania korupcji oraz działalności godzącej w interesy ekonomiczne państwa.

CBA jest urzędem administracji rządowej obsługującym jej szefa, który stoi na czele Biura i nim kieruje. Szef CBA jest centralnym organem administracji rządowej i podlega nadzorowi ze strony Prezesa Rady Ministrów oraz kontroli sejmowej. Działalność CBA jest finansowana z budżetu państwa, natomiast w stosunku do działań niejawnych prowadzonych przez CBA nie mają zastosowania przepisy o finansach publicznych, rachunkowości i zamówieniach publicznych. Działalność w tym zakresie finansowana jest ze specjalnie utworzonego w tym celu funduszu operacyjnego.

Struktura organizacyjna CBA określana jest w jego statucie wprowadzanym w drodze zarządzeń Prezesa Rady Ministrów. Po ostatnich zmianach w tym zakresie z 2019 r. CBA ma następujące jednostki organizacyjne:

- Departament Operacyjno-Śledczy;
- Departament Ochrony;
- Departament Postępowań Kontrolnych;
- Departament Analiz;
- Biuro Techniki Operacyjnej;
- Biuro Prawne;
- Biuro Finansów;
- Biuro Kadr i Szkolenia;
- Biuro Logistyki;
- Biuro Teleinformatyki;
- Biuro Kontroli i Spraw Wewnętrznych;
- Gabinet Szefa;
- Zespół Audytu Wewnętrznego.

CBA ma ponadto 12 delegatur (w Białymstoku, Bydgoszczy, Gdańsku, Katowicach, Krakowie, Lublinie, Łodzi, Poznaniu, Rzeszowie, Szczecinie, Warszawie i Wrocławiu).

Piotr Swoboda

P. Swoboda, *Służby specjalne w Polsce po 1989 roku – problemy definicyjne*, [w:] *Niepodległa Polska. Bezpieczeństwo i polityka w latach 1918–2018*, P. Łubiński (red.), Katolicki Uniwersytet Lubelski Jana Pawła II w Lublinie, Stalowa Wola 2018; Ustawa z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne, Dz. U. 1997, nr 106, poz. 679; Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, Dz. U. 1997, nr 88, poz. 553; Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym, Dz. U. 2006, nr 104, poz. 708; Zarządzenie nr 72 Prezesa Rady Ministrów w sprawie nadania statutu Centralnemu Biuru Antykorupcyjnemu z dnia 6 października 2010 r., M.P. 2010, nr 76, poz. 953.

CENTRALNE BIURO ŚLEDCZE POLICJI (CBŚP) – jest jednostką specjalistyczną powołaną w celu zwalczania → p r z e s t ę p c z o ś c i z o r g a n i z o w a n e j [t. 3]. → P r z e s t ę p c z o ś ć [t. 3] zorganizowana funkcjonuje w różnych sektorach życia społecznego i manifestuje się w różnorodnych formach działania. Do najbardziej niebezpiecznych możemy zaliczyć: przemyt narkotyków, handel ludźmi, bronią, materiałami radioaktywnymi, działania korupcyjne wobec aparatu władzy oraz pranie brudnych pieniędzy. Na forum międzynarodowym od kilkudziesięciu już lat trwa ożywiona dyskusja na temat przestępczości zorganizowanej – jej struktury, dynamiki oraz rodzajów działań kryminalnych, które możemy do niej zaliczyć. Podstawowym problemem jest definicyjne ujęcie fenomenu przestępczości zorganizowanej. O tym, że problem ten nie jest łatwy do rozstrzygnięcia, świadczy stosowanie w zachodniej literaturze naukowej kilkunastu różnych terminów na jej określenie. Fakt, że eksperci nie byli zgodni co do wypracowania jednolitej definicji przestępczości zorganizowanej, wynika z tego, że dostosowuje ona swoje różnorodne działania kryminalne do szybko zmieniających się struktur społecznych i gospodarczych państwa i równie szybko odpowiada na przedsięwzięcia kontrolne i represyjne ze strony państwa.

Przestępczość zorganizowana została scharakteryzowana przez A. Politiego, który wskazał 4 wspólne dla niej elementy. Są to: zorganizowana i stabilna hierarchia w ramach struktur przestępczych, generowanie przez nie zysków z działalności kryminalnej, używanie siły i zastraszania oraz stosowanie metod korupcyjnych w celu uniknięcia odpowiedzialności karnej. Konwencja Narodów Zjednoczonych przeciwko międzynarodowej przestępczości zorganizowanej, przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 15 listopada 2000 r., definiuje zorganizowaną grupę przestępczą jako:

> posiadającą strukturę grupę składającą się z trzech lub więcej osób istniejącą przez pewien czas oraz działającą w porozumieniu w celu popełniania jednego lub więcej poważnych przestępstw określonych na podstawie tej Konwencji, dla uzyskania w sposób bezpośredni lub pośredni korzyści finansowej lub innej korzyści materialnej.

Przestępczość zorganizowana pojawiła się w Polsce na początku lat 90. XX w., jako negatywne zjawisko towarzyszące transformacji ekonomiczno-ustrojowej RP. Wtedy powstały pierwsze duże zorganizowane grupy przestępcze, spośród których najbardziej znane to te działające głównie na terenie Warszawy: grupa pruszkowska, wołomińska, mokotowska, żyrardowska. Na Śląsku działała grupa Krakowiaka, a na Pomorzu N. Skotarczaka. Wykorzystywały one istniejące luki w prawie, niewydolność aparatu ścigania, swobodniejszy ruch graniczny i wzrastający popyt na towary (zwłaszcza akcyzowe) do rozwoju działalności przestępczej, także tej o charakterze transgranicznym i międzynarodowym. Gromadziły pokaźne zyski, przeznaczane je nie tylko konsumpcję, ale także na rozwój i dynamizowanie dalszej działalności przestępczej. Wykształciły swoisty kodeks przestępczych zachowań, ukierunkowany na zapewnienie hermetyczności grupy i jej wewnętrznej solidarności. Swoje działania koncentrowały na maksymalizacji zysków i poszerzaniu wpływów.

Polska → Po l i c j a [t. 3] nie była przygotowana na taką sytuację, co skutkowało gwałtownym wzrostem przestępczości, brutalizacją przestępców i wojną gangów, w której często ginęły także przypadkowe ofiary. Aby skutecznie zwalczać to nowe zjawisko generujące → z a g r o ż e n i a [t. 4] nie tylko obywateli, ale także instytucji państwowych, Policja musiała szybko stworzyć nową koncepcję i → s t r a t e g i ę [t. 4] działania. Ważnym jej elementem było powołanie wyspecjalizowanej służby zajmującej się zwalczaniem przestępczości zorganizowanej. W 1994 r. w Komendzie Głównej Policji (KGP) utworzono Biuro do Walki z Przestępczością Zorganizowaną. Było to ogniwo elitarne, ale ograniczone kadrowo. Miało wprawdzie swoje oddziały w największych aglomeracjach w Polsce, ale wraz z centralą w Warszawie liczyło zaledwie 250 funkcjonariuszy. Nowa koncepcja działania tej służby zakładała nowatorskie rozwiązania, takie jak:

- zasada podmiotowego prowadzenia działań wobec grup przestępczych i ich liderów, niezależnie od formy popełnianych przestępstw;
- rezygnacja z ukierunkowania policjantów na określony obszar czynności operacyjnych i śledczych na rzecz uniwersalności działania – ten sam policjant prowadzi sprawę od początku do końca, zarówno w sferze czynności operacyjnych, jak i procesowych;
- charakter scentralizowany służby, który nadano jej poprzez podporządkowanie wszystkich policjantów dyrektorowi Biura, co pozwoliło w razie potrzeby na szybką koncentrację sił i środków w określonym czasie i miejscu; każdy policjant mógł podejmować działania w dowolnym miejscu w kraju;
- bezpośrednie podleganie komendantowi głównemu Policji i działanie w strukturze KGP, co dawało jej możliwości łatwiejszego pozyskania i stosowania wysokiej klasy środków technicznych oraz bardziej efektywnego motywowania policjantów.

Analiza rozwoju przestępczości zorganizowanej wykazała, że służba odpowiedzialna za jej zwalczanie powinna zostać rozbudowana kadrowo, a dodatkowo oprzeć się na bieżącej, międzynarodowej wymianie → i n f o r m a c j i [t. 2] i współpracy z policjami innych państw. Aby ten zamysł zrealizować, w lutym 2000 r. na wniosek komendanta głównego Policji ówczesny minister spraw wewnętrznych M. Biernacki wyraził zgodę na powołanie spełniającej wskazane wymogi nowej służby. 15 kwietnia 2000 r. powstało Centralne Biuro Śledcze KGP, które utworzono z połączenia Biura do Walki z Przestępczością Zorganizowaną i Biura do Walki z Przestępczością Narkotykową KGP. W toku prowadzonych działań okazało się, że prawne relacje pomiędzy dyrektorem CBŚ a komendantem KGP nie gwarantują oczekiwanej wysokiej skuteczności w zwalczaniu przestępczości zorganizowanej. Należało odejść od dotychczasowego pełnego uzależnienia dyrektora CBŚ od komendanta głównego i delegować szereg uprawnień powołanemu komendantowi nowej służby, która po uzyskaniu autonomii przyjęła nazwę Centralnego Biura Śledczego Policji. 9 października 2014 r. jednostka ta formalnie rozpoczęła działalność. Jej organizację oraz przedmiot działania definiuje Zarządzenie nr 54 Komendanta Głównego Policji w sprawie organizacji, rzeczowego i miejscowego zakresu działania oraz zasad współdziałania Centralnego Biura Śledczego Policji z innymi jednostkami organizacyjnymi Policji. Dokument ten wyznacza również rzeczowy zakres działania CBŚP, który obejmuje w szczególności:

- planowanie, koordynowanie i podejmowanie działań ukierunkowanych na rozpoznawanie i zwalczanie przestępczości zorganizowanej krajowej i międzynarodowej, w szczególności o charakterze kryminalnym, narkotykowym i ekonomicznym oraz jej zapobieganie;
- prowadzenie postępowań przygotowawczych w sprawach dotyczących zorganizowanych grup przestępczych;
- organizowanie i podejmowanie → c z y n n o ś c i o p e r a c y j n o r o z p o z n a w c z y c h we współpracy z jednostkami organizacyjnymi Policji;
- ochronę świadków koronnych i osób dla nich najbliższych oraz osób zagrożonych;
- wykonywanie zadań związanych z wydawaniem dokumentów:
  - uniemożliwiających ustalenie danych identyfikujących policjantów lub osoby udzielające pomocy Policji oraz środków, którymi posługują się przy wykonywaniu zadań służbowych,
  - umożliwiających używanie innych niż własne danych osobowych świadkom koronnym lub osobom im najbliższym;
- prowadzenie operacji specjalnych;
- prowadzenie przedsięwzięć werbunkowych zapewniających wsparcie w zakresie rozpoznawania i zwalczania zagrożeń;
- koordynowanie działań w zakresie rozpoznawania operacyjnego zagrożeń terrorystycznych i ekstremistycznych oraz współdziałanie z jednostkami organizacyjnymi Policji i podmiotami pozapolicyjnymi;

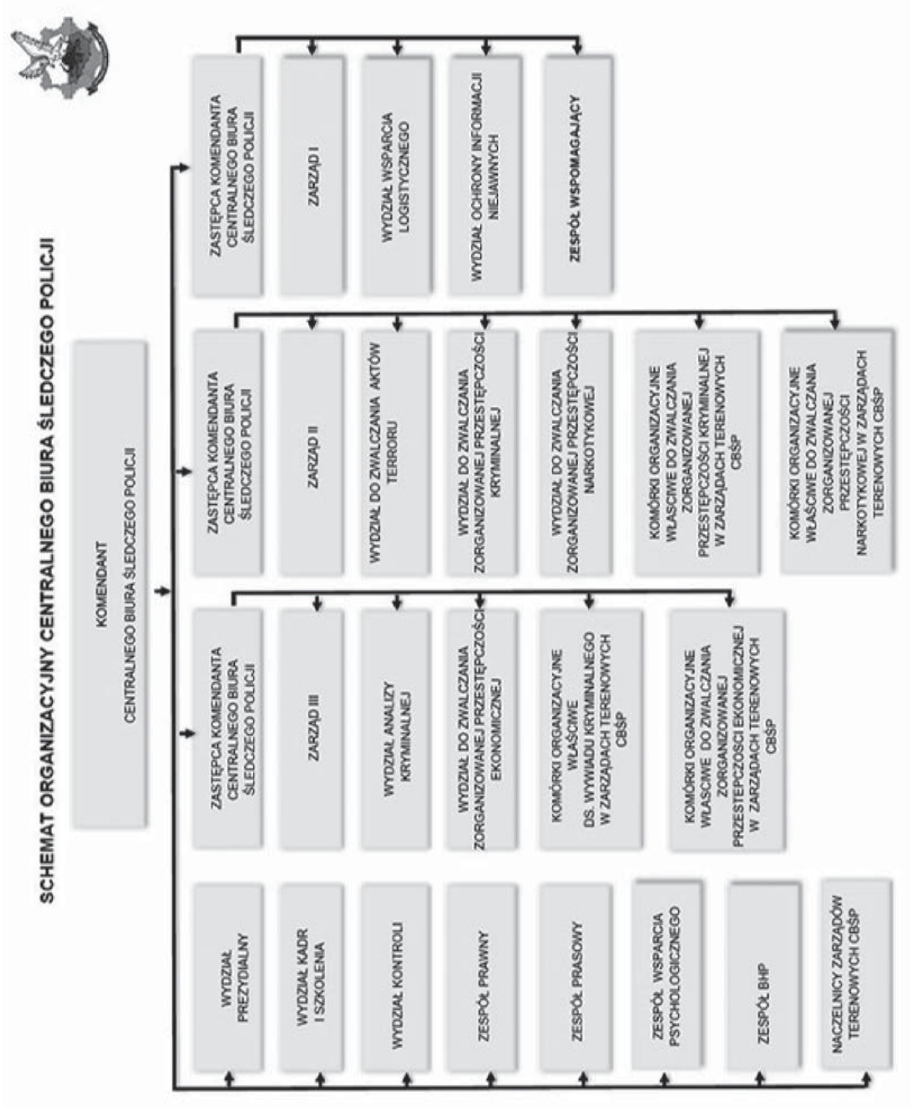
- prowadzenie czynności wykrywczych w sprawach przestępstw uprowadzeń osób dla okupu w kraju i poza jego granicami oraz nadzorowanie, koordynowanie i wspieranie tych czynności prowadzonych przez jednostki organizacyjne Policji, w tym wykonywanie zadań krajowego Centrum ds. Uprowadzeń, o którym mowa w rozdziale IV Podręcznika dotyczącego zwalczania porwań i uprowadzeń, przyjętego w dniu 26 kwietnia 2006 r. przez Biuro Narodów Zjednoczonych ds. Narkotyków Środków Odurzających i Przestępczości;
- prowadzenie działań mających na celu rozpoznawanie i zwalczanie przestępczości zorganizowanej w → c y b e r p r z e s t r z e n i;
- wykonywanie analiz kryminalnych i prowadzenie zbiorów danych, wykorzystywanych przy realizacji zadań w zakresie rozpoznawania i zwalczania przestępczości zorganizowanej oraz zagrożeń terrorystycznych i ekstremistycznych;
- prowadzenie operacji pościgowych w stosunku do członków zorganizowanych grup przestępczych;
- współpracę z policjami innych państw, a także z krajowymi i międzynarodowymi służbami i urzędami administracji publicznej w zakresie niezbędnym do skutecznego zwalczania przestępczości zorganizowanej i zapobiegania jej;
- wykonywanie zadań punktów kontaktowych i informacyjnych na podstawie odrębnych przepisów;
- prowadzenie Międzynarodowego Centrum Szkoleniowego do Zwalczania Nielegalnych Laboratoriów Narkotykowych;
- współpracę z jednostkami naukowymi i instytutami badawczymi w zakresie prowadzenia badań i opracowywania rozwiązań dotyczących przeciwdziałania i zwalczania zagrożeń pozostających w zainteresowaniu CBŚP.

CBŚP stanowi specjalistyczne narzędzie zapobiegania i zwalczania rozwijającej się dynamicznie przestępczości zorganizowanej. Grupy przestępcze swoją działalnością obejmują różnego rodzaju przestępstwa – od zwykłych kradzieży poprzez pobicia, zastraszanie, wymuszanie haraczy, uprowadzanie osób dla okupu czy też handel ludźmi. Nie bez znaczenia jest także rosnący terytorialny zasięg działalności tych grup – od ogólnopolskiego aż po działalność międzynarodową. Przestępczość zorganizowana przejawia się głównie w 3 aspektach: kryminalnym, narkotykowym i ekonomicznym (podatkowym). Zorganizowana przestępczość o charakterze kryminalnym obejmuje głównie napady rabunkowe, kradzieże pojazdów, napady na kierowców tirów zarówno w kraju, jak i za granicą. Grupy przestępcze stosują również uprowadzenia dla okupu czy wymuszenia haraczy od osób prowadzących działalność gospodarczą.

Inną grupą przestępstw kryminalnych o charakterze zorganizowanym jest też proceder przemytu migrantów o nieuregulowanym statusie prawnym i powiązane z nim zmuszanie do niewolniczej pracy czy też czerpanie korzyści z uprawiania prostytucji. W sferze przestępczości narkotykowej grupy przestępcze zajmują się:

produkcją narkotyków syntetycznych w tworzonych przez siebie profesjonalnych laboratoriach, wytwarzaniem środków odurzających, głównie marihuany i haszyszu, poprzez prowadzenie zewnętrznych upraw konopi i plantacji ukrytych w różnego rodzaju budynkach mieszkalnych i przemysłowych, przemytem na hurtową skalę różnego rodzaju narkotyków z krajów dzisiejszej UE oraz z krajów Ameryki Południowej. Jednym z głównych trendów obserwowanych w przestępczości ekonomicznej jest działanie grup polegające na przemycie towarów akcyzowych takich jak papierosy, alkohol i paliwa. Wielkie zyski generowane są ze względu na duże różnice cenowe tych wyrobów w krajach byłego bloku wschodniego w stosunku do naszego kraju. Podobne różnice w tym zakresie występują także między cenami tych towarów w Polsce i krajach zachodniej Europy. W ten sposób grupy zorganizowane uszczuplają wpływy do budżetu państwa poprzez nieuiszczanie należności z tytułu podatków akcyzowych.

Szczególnie groźna w obszarze przestępczości ekonomicznej jest także tzw. przestępczość vatowska. Początkowo ograniczała się ona do fikcyjnego obrotu towarami, głównie paliwem i stalą. Wystawiano pomiędzy nieistniejącymi firmami (tzw. słupami) fikcyjne faktury, bez faktycznego obrotu towarem. Obecnie grupy przestępcze fizycznie mają określoną ilość towaru, jednak faktury na ten towar są powielane, co skutkuje wyłudzeniem podatku VAT. Straty ponoszone z tego tytułu przez skarb państwa są ogromne. Zorganizowane grupy przejawiają także aktywność wobec instytucji finansowych. W zakresie wyłudzania kredytów początkowo mechanizm polegał na fałszowaniu dokumentacji związanej z posiadaniem wymaganej zdolności kredytowej. Obecnie mechanizm ten wykorzystuje fałszowanie opinii stwierdzających wartość nieruchomości wskazywanych pod zastaw zaciąganych kredytów bankowych. Zupełnie nowym trendem w przestępczości ekonomicznej jest mechanizm wyłudzania funduszy unijnych. Podstawione firmy starają się o pozyskanie projektów unijnych. Ważnym przedmiotem rozpoznania operacyjnego są zagrożenia terrorystyczne, czym również zajmuje się CBŚP. Zadania w tym obszarze zostały zdefiniowane w Zarządzeniu Komendanta Głównego Policji nr pf-845 z dnia 29 lipca 2004 r., a uszczegółowione w regulaminie CBŚP. W strukturze CBŚP utworzono Wydział do Zwalczania Aktów Terroru. Ogniwo to na bieżąco koordynuje pracę Zespołów Przeciwdziałania Aktom Terroru działających we wszystkich komendach wojewódzkich Policji. Współpracuje także z Centrum Antyterrorystycznym → Agencji Bezpieczeństwa Wewnętrznego. W tym zakresie na bieżąco zespoły prowadzą rozpoznanie operacyjne grup, organizacji, związków lub stowarzyszeń, co do których istnieje podejrzenie o działalność terrorystyczną i ekstremistyczną oraz o finansowanie takiej działalności w Rzeczypospolitej Polskiej lub innym państwie.



Andrzej Czop

J. Badziak, *Przestępstwo z art. 258 Kodeksu Karnego. Studium prawnodogmatyczne*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2014; A. Czop, P. Czop, *Analiza porównawcza przestępczości zorganizowanej i międzynarodowego terroryzmu*, „Kultura Bezpieczeństwa. Nauka – Praktyka – Refleksje" 2016, nr 24; ciż, *Konieczność kompleksowych i interdyscyplinarnych działań na rzecz współczesnego bezpieczeństwa w kontekście sektorowości zagrożeń*, „Kultura Bezpieczeństwa. Nauka – Praktyka – Refleksje" 2016, nr 22; M. Kędzierski, W. Mądrzejowski, *Centralne Biuro Śledcze KGP i Centralne Biuro Śledcze Policji we wspomnieniach twórców i pracowników*, Wydawnictwo Wyższej Szkoły Policji w Szczytnie, Szczytno 2015; W. Mądrzejowski, *Przestępczość zorganizowana. System zwalczania*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2015; J. Stelmach, *Działania antyterrorystyczne w kontekście identyfikacji*

znamion przestępstwa o charakterze terrorystycznym, [w:] *Polska Ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, W. Zubrzycki, K. Jałoszyński, A. Babiński (red.),Wydawnictwo Wyższej Szkoły Policji w Szczytnie, Szczytno 2016.

CENTRUM ANALIZ PROPAGANDY I DEZINFORMACJI (CAPD) – pierwsza polska organizacja pozarządowa, w której centrum zainteresowania znalazły się → w o j n a i n f o r m a c y j n a [t. 4] i → w o j n a p s y c h o l o g i c z n a [t. 4]. Centrum działające od kwietnia 2017 r. jest organizacją niezależną i apolityczną, a zatem wolną od jakichkolwiek nacisków i wpływów władzy, chociaż zapewnia, że jest otwarta na współpracę ze strukturami rządowymi i pozarządowymi zarówno z Polski, jak i z zagranicy. Fundacja została założona przez M. Kowalską oraz A. Lelonka. Głównym obszarem działalności fundacji jest Polska, realizując jednak działalność statutową, może ona powoływać swoje oddziały lub wewnętrzne jednostki oraz podejmować aktywność na obszarze innych państw, co wpisuje się w misję CAPD – współpracę z różnymi zagranicznymi podmiotami w obszarze zagadnień → d e z i n f o r m a c j i [t. 2], → p r o p a g a n d y [t. 3] i → w o j n y h y b r y d o w e j [t. 4].

Rolą fundacji jest wzmacnianie struktur społeczeństwa obywatelskiego nie tylko w Polsce, ale również w państwach sojuszniczych obszaru transatlantyckiego. Ponadto CAPD dąży do podniesienia poziomu świadomości społeczeństw w zakresie → z a g r o ż e ń [t. 4] wywołanych działaniami propagandowymi i dezinformacyjnymi, charakterystycznymi dla → w o j n y [t. 4] hybrydowej, psychologicznej czy też informacyjnej. Aktywność fundacji dotyczy także prac nad polskim systemem odpowiedzi rozproszonej na ewentualne wrogie formy działania w → p r z e s t r z e n i i n f o r m a c y j n e j [t. 3]. CAPD, współpracując ze środowiskiem naukowym, eksperckim oraz dziennikarskim, prowadzi również działalność badawczo-analityczną, której owocem są liczne analizy, komentarze, raporty, rekomendacje oraz prognozy z zakresu zagadnień propagandy i dezinformacji. W ofercie CAPD znajduje się także działalność edukacyjna, skierowana głównie do środowiska dziennikarskiego, podkreślająca konieczność rzetelnej weryfikacji → i n f o r m a c j i [t. 2]. Odzwierciedleniem prężnego rozwoju fundacji jest jej aktywność wydawnicza, szkoleniowa oraz konferencyjna. CAPD organizuje również sympozja, debaty, warsztaty, a także kursy – koncentrują się one na zagadnieniach manipulacji, dezinformacji, propagandy, przeciwdziałania oddziaływaniom informacyjnym, rosyjskiej przestrzeni informacyjnej i jej wpływie na państwa Europy Środkowo-Wschodniej.

Fundacja podejmuje próby integracji działań i inicjowania współpracy krajowych i zagranicznych ośrodków naukowych, środowisk eksperckich i dziennikarskich, sektora biznesowego i elit politycznych, a także instytucji rządowych i pozarządowych w obszarze szeroko rozumianych zagrożeń przestrzeni informacyjnej. W planach CAPD jest również opracowanie szczegółowej i profesjonalnej oferty adresowanej zarówno do przedstawicieli sektora publicznego, jak i prywatnego. Propozycje

mają dotyczyć szkoleń, konsultingu oraz opracowywania materiałów analitycznych. Eksperci CAPD są nie tylko organizatorami szkoleń, ale również sami uczestniczą w różnych kursach i warsztatach (np. GLOBSEC w Bratysławie), które umożliwiają wymianę doświadczeń, pomysłów i dobrych praktyk z przedstawicielami organizacji pozarządowych z regionu transatlantyckiego.

CAPD zainicjowało w lutym 2019 r. ogólnopolski projekt „Zwiększanie zdolności polskiego społeczeństwa w zakresie przeciwdziałania dezinformacji", który uzyskał wsparcie amerykańskiej fundacji National Endowment for Democracy. Pierwszy etap projektu polegał na analizie codziennych wyzwań w zakresie → b e z p i e c z e ń s t w a i n f o r m a c y j n e g o mieszkańców 16 polskich miast wojewódzkich. Badanie opierało się na serii wywiadów środowiskowych z lokalnymi przedstawicielami → s p o ł e c z e ń s t w a o b y w a t e l s k i e g o [t. 4], a ich celem było zdobycie wiedzy na temat charakterystyki problemów społeczności lokalnych. W badaniu podkreślono istotność procesu integracji regionalnych podmiotów działających na rzecz przeciwdziałania zewnętrznym zagrożeniom informacyjnym. Badanie dostarczyło informacji na temat pojmowania przez społeczeństwo dezinformacji i metod radzenia sobie z tym problemem, pozwoliło na identyfikację możliwości polskiego środowiska zajmującego się monitorowaniem i analizowaniem zagrożeń informacyjnych oraz umożliwiło poznanie specyfiki lokalnych problemów i zidentyfikowanie grup podatnych na wpływ kampanii (dez)informacyjnych w danym regionie.

Kolejnym równie ciekawym pomysłem CAPD okazał się projekt „Analiza i przeciwdziałanie negatywnym i fałszywym narracjom na temat Polski i Polaków w rosyjskiej przestrzeni informacyjnej". Zadanie publiczne było współfinansowane przez Ministerstwo Spraw Zagranicznych RP w ramach konkursu „Dyplomacja publiczna 2019". W przedsięwzięciu wzięli udział eksperci i przedstawiciele mediów m.in. z Estonii, Białorusi i Ukrainy.

Julia Anna Gawęcka

CAPD.pl (dostęp 2.04.2019); *O dezinformacji na marginesie Warsaw Security Forum*, Pulaski.pl (dostęp 2.04.2019); *Raport: Jak budować odporność społeczną w przestrzeni informacyjnej i cyberprzestrzeni: przeciwdziałanie propagandzie i dezinformacji*, 10.10.2017, CAPD.pl (dostęp 2.04.2019).

CENTRUM BEZPIECZEŃSTWA NOWEJ AMERYKI – (ang. The Center for a New American Security, CNAS) pozarządowa organizacja non-profit z siedzibą w Waszyngtonie, która dzięki zaangażowaniu decydentów, ekspertów oraz → o p i n i i p u b l i c z n e j [t. 3] podejmuje działania mające na celu podniesienie poziomu → b e z p i e c z e ń s t w a n a r o d o w e g o [t. 1]. CNAS za sprawą prowadzonych badań, publikacji analiz oraz inicjacji dyskusji i debat tworzy dynamiczny program badawczy, który poprzez informowanie przedstawicieli

świata polityki i sektora prywatnego ma za zadanie zapewniać wsparcie dla interesów oraz → s t r a t e g i i → b e z p i e c z e ń s t w a [t. 1] USA. Organizację założyli w 2007 r. Kurt M. Campbell oraz Michèle A. Flournoy. Obecnie personel CNAS liczy 40–45 osób pracujących w pełnym wymiarze godzin. Oprócz nich są tam stażyści oraz pracownicy pomocniczy, realizujący określone badania i analizy na wskazany temat, właściwy specjalizacji. Gdy organizacja zleca opracowanie analiz w danej dyscyplinie, dokłada starań, aby osoba za to odpowiedzialna miała odpowiednie doświadczenie i wiedzę. Dlatego do CNAS należy wielu autorów, którzy zajmowali lub nadal zajmują ważne stanowiska w rządzie USA, w Departamencie Obrony, w Białym Domu, w Centralnej Agencji Wywiadowczej, w Kongresie, w Departamencie Stanu i w sektorze prywatnym. Te osoby, mające bogate doświadczenie zawodowe oraz szeroką wiedzę związaną z kwestiami bezpieczeństwa narodowego i obronności, wchodzą w skład Rady Dyrektorów CNAS, którą nadzorują przewodnicząca Michèle A. Flournoy oraz wiceprzewodniczy James Murdoch. Najważniejsze zadania zarządu to nadzór nad realizowanymi projektami i nad stanem finansowym CNAS oraz weryfikacja zgodności prowadzonych działań z obowiązującymi przepisami prawnymi oraz nadzór nad poszanowaniem praw własności intelektualnej. Innym ważnym organem jest Rada Doradcza, także składająca się z wybitnych przedstawicieli środowiska akademickiego, wojskowego oraz sektora prywatnego i rządowego, którzy aktywnie przyczyniają się do rozwoju badań prowadzonych przez CNAS oraz do realizacji nowych zadań. Członkowie Rady Doradczej, w przeciwieństwie do zasiadających w Radzie Dyrektorów, nie mają kompetencji umożliwiających zarządzanie organizacją lub nadzór nad nią. Zespół Wykonawczy CNAS tworzą Richard Fontaine (dyrektor generalny), Anna Saito Carson (wiceprezes ds. rozwoju) oraz Paul Scharre (wiceprezes i dyrektor ds. badań). Organizacja nadzoruje łącznie 7 programów badawczych podzielonych na 2 kategorie:

1. Główne programy badawcze CNAS

- **Program Obronny** obejmuje tematykę kluczowych wyzwań dla rywalizacji militarnej między Stanami Zjednoczonymi, Chinami a Rosją. Efektem analiz oraz debat stały się zalecenia CNAS w kwestiach obronnych i politycznych, dotyczące możliwych skutków rywalizacji wielkich → m o c a r s t w dla strategii obronnej, budżetu oraz reform instytucjonalnych USA.
- **Energia, Ekonomia i Bezpieczeństwo** – dzięki badaniom poruszającym specyfikę zmieniającego się globalnego rynku finansowego i handlowego zespół tego programu przygotowuje opracowania, które w zamyśle autorów umożliwią politycznym liderom jeszcze efektywniejsze wykorzystanie aktywów gospodarczych w celu obrony i promowania interesów narodowych USA.
- **Program Wojskowość, Weterani i Bezpieczeństwo** obejmuje badania mające na celu ustalenie właściwej koncepcji związanej z przyszłością, jaka czeka członków amerykańskiej służby, weteranów oraz ich rodziny. Szczególnie

ważnym elementem programu są rozważania ws. ponownego wdrożenia *All-Volunteer Force*, a także analiza trendów ujawniających się wśród społeczności weteranów oraz stosunków cywilno-wojskowych. Z myślą o bieżącej i dającej się przewidzieć problematyce wojskowej organizacja publikowała w ostatnich latach raporty i komentarze zawierające kompleksowe spojrzenie na przyszłość sił ochotniczych, analizę skłonności młodzieży z rodzin wojskowych do służby czy ocenę samobójstw wojskowych. Wprowadzono również rozwiązania umożliwiające poprawę rekrutacji do służby oraz dotyczące późniejszego utrzymania i wsparcia oferowanego przez wojsko członkom służby i ich rodzinom. Podobne badania dotyczą weteranów – CNAS stara się ocenić, jakie potrzeby mają weterani w skali lokalnej, stanowej i regionalnej. Ponadto zespół MVS wchodzący w skład CNAS stale monitoruje skalę zatrudnienia oraz przedsiębiorczości weteranów, a także wydaje zalecenia umożliwiające poprawę ich ogólnych wyników ekonomicznych.

- **Technologia i bezpieczeństwo narodowe** – tempo rozwoju sztucznej inteligencji, automatyzacji, systemów bezzałogowych, infrastruktury cyfrowej, sieci i mediów społecznościowych oraz technik → d e z i n f o r m a c j i [t. 1] wpływa na postrzeganie bezpieczeństwa narodowego. Kluczowym celem tego programu stało się zbliżenie środowisk technologicznych i politycznych – aby obie strony lepiej mogły zrozumieć wyzwania i wspólnie wypracować odpowiednie rozwiązania. Szczególnie istotne w tym zakresie okazują się – z jednej strony – wątek posiadania nowych narzędzi, z wykorzystaniem których państwa autorytarne mogę stosować ucisk czy wywierać polityczne wpływy, a z drugiej – kwestia roli człowieka w konfliktach i → w o j n a c h [t. 4] w obliczu postępującej automatyzacji i rozwoju sztucznej inteligencji.

2. Regionalne programy badawcze CNAS

- Program Bezpieczeństwo Indo-Pacyfiku określa szanse i wyzwania, przed jakimi stoją organy USA w rejonie Indo-Pacyfiku, a także analizuje trendy, w wyniku czego tworzy praktyczne oraz kreatywne rozwiązania polityczne wokół 4 głównych priorytetów badawczych:
  - Zespół *China Challenge* stara się ocenić, w jaki sposób USA mogą wzmocnić swoją strategiczną przewagę w rywalizacji z Chinami. Obszary badawcze zespołu w 2021 r. obejmują także osłabienie cyfrowej ekspansji Chin oraz analizę politycznych i wojskowych zachowań chińskich władz w następstwie → p a n d e m i i C O V I D - 1 9 .
  - Zespół *Regionalne Sojusze i Partnerstwa* to cykl analiz badających sposób, w jaki USA mogą wzmocnić relacje z tamtejszymi sojusznikami i partnerami, czyli z Japonią, Koreą Południową,Australią, Tajwanem oraz Indiami. Zgodnie z założeniami na 2021 r., USA będą dążyć do wzmocnienia współpracy między partnerami z regionu Indo-Pacyfiku z myślą o sprostaniu wyzwaniom gospodarczym po pandemii COVID-19.

  - Zespół *India Opportunity* poszukuje możliwości partnerstwa strategicznego USA – Indie przy szczególnym uwzględnieniu powiązań w zakresie obronności i bezpieczeństwa, a także współpracy technologicznej, bezpieczeństwa zdrowotnego oraz zmian klimatycznych. Relacje między Stanami Zjednoczonymi a Indiami nabrały znaczenia w następstwie COVID-19 i indyjsko-chińskiego → k r y z y s u [t. 2] granicznego w 2020 r.
  - Zespół *The North Korea Threat* bada innowacyjne rozwiązania i tworzy strategie, które z wykorzystaniem polityki zagranicznej USA mogłyby ograniczyć ekspansję północnokoreańskiego arsenału jądrowego lub przyczynić się do rozpoczęcia procesu denuklearyzacji Koreańskiej Republiki Ludowo-Demokratycznej.
- **Program Bezpieczeństwa Bliskiego Wschodu** podejmuje się prowadzenia innowacyjnych badań dotyczących kluczowych problemów na Bliskim Wschodzie. Koncentruje się na przyczynach braku stabilności w regionie oraz na sposobach ich rozwiązywania. Co więcej, analitycy starają się wyciągać wnioski dotyczące utrzymania kluczowych partnerstw strategicznych USA na Bliskim Wschodzie, a także prognozować zmieniające się → z a g r o ż e n i a [t. 4]. Zespół tworzą osoby z doświadczeniem rządowym i pozarządowym w badaniach regionalnych, w polityce zagranicznej USA i w → b e z p i e c z e ń s t w i e m i ę d z y n a r o d o w y m [t. 1]. Szczególne znaczenie miały raporty dotyczące ISIS – w 2016 r. powołano grupę badawczą CNAS ISIS, która opracowała raporty strategiczne odnoszące się do kluczowych czynników umożliwiających znaczne ograniczenie niebezpieczeństwa w regionie. Dotyczyły one m.in. budowy regionalnych zbrojnych grup opozycyjnych, zwiększenia bezpośredniego wsparcia wojskowego USA dla grup opozycyjnych oraz amerykańskich działań skierowanych przeciwko ISIS, wykorzystania zwiększonych inwestycji amerykańskich w terenie do wywierania wpływu dyplomatycznego z kluczowymi podmiotami zewnętrznymi, a także przywrócenia legalnych i akceptowalnych rządów. Dzięki podobnym analizom i zaleceniom powstaje pewna alternatywna koncepcja, którą polityczni decydenci mogą rozważyć. Jej wprowadzenie może się bezpośrednio przełożyć na ochronę i wsparcie interesów USA.
- **Program Bezpieczeństwa Transatlantyckiego** to wielopłaszczyznowe analizy oraz opracowania rekomendacji, które mogą przyczynić się do poprawy relacji, zacieśniania współpracy oraz do osiągania założonych celów strategicznych między amerykańskimi a europejskimi decydentami politycznymi. Skład zespołu badawczego, obok amerykańskich ekspertów, uzupełniają przedstawiciele europejskich uczelni, urzędów państwowych oraz sektora prywatnego. Wsparcie dialogu amerykańsko-europejskiego na wysokim szczeblu odbywa się m.in. poprzez organizację publicznych forów, seminariów i stałą współpracę z mediami.

Zgodnie z jedną ze swoich głównych misji, CNAS sponsoruje również kilka programów kształcących kolejne pokolenie ekspertów ds. bezpieczeństwa narodowego.

Każdego roku wybiera grupę 20–25 liderów bezpieczeństwa narodowego w wieku od 27 do 35 lat, którzy następnie biorą udział w programie *Shawn Brimley Next Generation National Security Leaders Program.* Kolejna nagroda to *The Bacevich Award*, którą CNAS przyznaje corocznie wschodzącym liderom, którzy swoją działalnością dają przykład odwagi, uczciwości i zaangażowania w służbę publiczną. Osoby wysoko wykwalifikowane, wykazujące się potencjałem, uczciwością oraz zaangażowaniem w służbę, otrzymują stypendium Roberta M. Gatesa. Oprócz wspomnianych nagród i stypendiów, organizacja przyznaje nagrodę *Writers in Residence*, umożliwiającą dziennikarzom zajmującym się tematyką bezpieczeństwa narodowego i obronnością realizację pobytu badawczego, umożliwiającego przygotowanie monografii z wykorzystaniem zasobów naukowych CNAS. Kolejny program – *Senior Military Fellows* – umożliwia przedstawicielom Sił Powietrznych, Korpusu Piechoty Morskiej i Marynarki Wojennej USA roczny pobyt w CNAS w celu przygotowania publikacji naukowej poruszającej wybrane zagadnienia z zakresu bezpieczeństwa. Od 2019 r. CNAS prowadzi badania dotyczące roli i służby kobiet w sektorze bezpieczeństwa narodowego USA – szczegółowo opisywane są doświadczenia kobiet służących w amerykańskim wojsku. Program *Women in National Security* to zbiór podcastów prezentujących historie, lekcje i porady pracy kobiet od najniższego do najwyższego szczebla w sektorach zatrudnienia obejmujących bezpieczeństwo narodowe. Flagowym wydarzeniem CNAS jest coroczna Konferencja Bezpieczeństwa Narodowego, która odbywa się w czerwcu w Waszyngtonie i gromadzi ok. 800 interesariuszy zajmujących się bezpieczeństwem narodowym. Budżet operacyjny CNAS w roku obrotowym 2020 wyniósł 11 mln dolarów.

Artur Jach-Chrząszcz

S. Bryant, B. Swaney, *Deconstructing the "Warrior Caste". The Beliefs and Backgrounds of Senior Military Elites*, https://inss.ndu.edu/Media/News/Article/1428887/deconstructing-the-warrior-caste-the-beliefs-and-backgrounds-of-senior-military/ (dostęp 28.10.2021); *Center for a New American Security*, https:// www.cnas.org (dostęp 28.10.2021); H. Forrest, *New Cybersecurity Primer by theCenter for a New American Security*, https://www.justsecurity.org/13276/cybersecurity-primer-center-american-security/ (dostęp 28.10.2021); M. Harrell, N. Berglass, *Employing America's Veterans Perspectives from Businesses*, https://heavy.com/ wp-content/uploads/2013/03/cnas_employingamericasveterans_harrellberglass. pdf (dostęp 28.10.2021); B. Heinz, E. Jung, *The Military-Industrial-Think Tank Complex: Conflicts of Interest at the Center for a New American Security*, https:// therevolvingdoorproject.org/wp-content/uploads/2021/02/2021-02-CNAS-Heinz-and-Jung.pdf (dostęp 28.10.2021); F.G. Hoffman, *U.S. Defense Policy and Strategy*, https://ndupress.ndu.edu/Portals/68/Documents/Books/charting-a-course/ Ch3_US-Defense-Policy-and-Strategy.pdf?ver=2016-12-12-140243-260 (dostęp 28.10.2021); K. Kidder, A. Schafer, P. Carter, A. Swick*, From College to Cabinet*, https://www.jstor.org/stable/resrep06313?seq=1#metadata_info_tab_contents (dostęp 28.10.2021); P. Scharre, *Autonomous Weapons and Operational Risk*, https:// www.files.ethz.ch/isn/196288/CNAS_Autonomous-weapons-operational-risk.pdf (dostęp 28.10.2021); United States Institute of Peace, *The U.S. 'Cannot Avoid orIgnore' the War in Syria*, https://www.usip.org/publications/2019/10/us-cannot-avoid-or-ignore-war-syria (dostęp 28.10.2021).

CENTRUM DOSKONALENIA OBRONY PRZED CYBERATAKAMI (Cooperative Cyber Defense Centre of Excellence, CCD CoE) – międzynarodowa organizacja wojskowa z siedzibą w Tallinie (Estonia), której misją jest zwiększenie zdolności, współpracy i wymiany → i n f o r m a c j i [t. 2] między → N A T O [t. 3], jego państwami członkowskimi i partnerami w zakresie cyberobrony na podstawie prowadzenia interdyscyplinarnych badań nad → c y b e r b e z p i e c z e ń s t w e m, przeprowadzanie ćwiczeń oraz szkoleń edukacyjnych i doskonalących w tym obszarze. Zostało założone 14 maja 2008 r., uzyskało pełną akredytację NATO i status międzynarodowej organizacji wojskowej 28 października 2008 r. Ma na celu prowadzenie badań i szkoleń w zakresie obrony w → c y b e r p r z e s t r z e n i. Centrum zostało powołane podczas szczytu w Rydze w 2006 r. z inicjatywy Estonii, która jest bardzo silnie dotknięta działaniami w cyberprzestrzeni. Dość powiedzieć, że w 2007 r. Estonia stała się celem jednego z najbardziej zaawansowanych ataków bądź serii ataków przeprowadzonych w cyberprzestrzeni. Do dziś nie można z całkowitą pewnością określić, czy działania te były zorganizowane przez inne państwo, tj. Federację Rosyjską, czy też przez niezależnie działające osoby zamieszkujące FR lub będące Rosjanami mieszkającymi w innych miejscach.

Funkcja NATO w obszarze cyberobrony ma charakter dychotomiczny. Priorytetem jest zabezpieczenie własnych sieci, zgodnie z założeniami przyjętymi przez sojusz na zakończenie obrad szczytu, który odbył się w Walii w 2014 r. Sojusz musi sprawić, by systemy teleinformatyczne, z których korzysta podczas realizowanych operacji, były skutecznie chronione przed → z a g r o ż e n i a m i [t. 4] pochodzącymi z cyberprzestrzeni. Drugim z celów NATO w obszarze cyberbezpieczeństwa jest wspomaganie swoich członków w rozbudowie ich własnych zdolności i potencjału. Służy temu 2-letni proces ustalania celów zbiorowej cyberobrony, które muszą zaakceptować wszyscy członkowie NATO, co w konsekwencji pozwala na tworzenie wspólnej → s t r a t e g i i [t. 4] w zakresie cyberobrony. Efekty w realizacji tak ustalanych celów są w sposób ciągły audytowane. Procesom tym towarzyszy szeroka oferta w zakresie edukacji i praktycznych ćwiczeń, prowadzonych przez akredytowane przez NATO CCD CoE. Przyjęło ono założenie, że każda sieć jest tak silna, jak jej najsłabsze ogniwo. Stąd → b e z p i e c z e ń s t w o sojuszu oraz jego zdolność do bieżącego wykonywania uzgodnionych celów w zakresie obrony zbiorowej, → z a r z ą d z a n i a k r y z y s o w e g o [t. 4] oraz bezpieczeństwa bazującego na wzajemnej współpracy w znacznej mierze uzależnione są od potencjału cyberobrony oraz od zdolności poszczególnych państw członkowskich. Ćwiczeniem i kontrolowaniem tych zdolności zajmuje się CCD CoE.

CCD CoE w Tallinie jest jednym z 21 akredytowanych centrów doskonałości (Centre of Excellence, CoE) do szkolenia w zakresie zaawansowanych technicznie aspektów operacji NATO. Jest finansowane na poziomie krajowym i międzynarodowym – CoE są ściśle powiązane z transformacją dowodzenia alianckiego i promują cele transformacji zatwierdzone przez sojusz. Głównymi celami CCD CoE są:

- poprawienie interoperacyjności cyberobrony w środowisku NATO;
- opracowanie doktryny i koncepcji oraz ich walidacja;
- zwiększenie bezpieczeństwa informacji i edukacji, świadomości i szkoleń w zakresie cyberobrony;
- zapewnienie wsparcia cyberobrony w eksperymentach;
- analizowanie prawnych aspektów cyberobrony. CCD CoE ma również inne obowiązki, które obejmują:
- wkład w rozwój praktyk i standardów Centrum z udziałem NATO, kandydatów do NATO i państw nienależących do NATO;
- wkład w rozwój polityki bezpieczeństwa NATO związanej z cyberobroną, określenie jej zakresu i odpowiedzialności wojska w cyberobronie;
- przeprowadzanie szkoleń z zakresu cyberobrony, kampanii uświadamiających, warsztatów i kursów;
- opracowywanie i przeprowadzanie ćwiczeń z zakresu cyberobrony i zdolność do zapewniania wsparcia dla ćwiczeń;
- regularne konferencje międzynarodowe CyCon (Cyber Conference).

To, że tak ważne ogniwo NATO zostało usytuowane w stolicy Estonii, nie powinno dziwić, gdyż właśnie ten kraj wiosną 2007 r. stał się ofiarą zmasowanych, kilkunastodniowych cyberzamachów. Gdy estoński rząd podjął decyzję o przeniesieniu pomnika upamiętniającego → ż o ł n i e r z y [t. 4] radzieckich poległych w walkach o Tallin, serwis rządowy został zaatakowany za pomocą ataku typu DoS (ang. *denial of service*). Wkrótce ataki te objęły całą infrastrukturę informatyczną, paraliżując strony internetowe parlamentu, ministerstw obrony i sprawiedliwości, partii politycznych, → p o l i c j i [t. 3] oraz szkół publicznych. Apogeum → k r y z y s u [t. 2] miało miejsce 9 maja, w dniu kiedy Rosjanie świętują zwycięstwo nad → f a s z y z m e m [t. 2]. Wtedy zaatakowane zostały również 2 największe banki, Hansapank i SEB Ühispank, które zostały zmuszone do przerwania prowadzenia usług online i wstrzymania transakcji zagranicznych. Unieruchomiona została także strona największego estońskiego dziennika „Postimees". Przebywający wówczas w Estonii G. Evron, izraelski ekspert ds. bezpieczeństwa, skomentował sytuację słowami: „Za pomocą cyberbomby Estonia została niemal zepchnięta do epoki kamiennej". Rosyjscy → h a k e r z y [t. 2] uzyskali ważny efekt psychologiczny – wywołali u przeciętnych obywateli zaniepokojenie, strach i obawy, którym na skutek zablokowania stron rządowych towarzyszyły utrudnienia w informowaniu społeczeństwa o rozwoju sytuacji. Rząd Estonii uważał, że w tej sytuacji winien zostać zastosowany art. 5 traktatu NATO, zgodnie z którym: „Strony zgadzają się, że zbrojna napaść na jedną lub więcej z nich w Europie lub Ameryce Północnej będzie uznana za napaść przeciwko nim wszystkim". Wobec braku odpowiednich procedur i międzynarodowych uregulowań, a także przy sprzeciwie niektórych państw członkowskich przyjęcie takiej kwalifikacji było jednak niemożliwe. Członkowie Sojuszu udzielili Estonii wsparcia technicznego, użyczyli jej swoich

serwerów, wysłali do niej własne zespoły CERT oraz ekspertów w dziedzinie cyberbezpieczeństwa. Efektem estońskich doświadczeń był szczyt w Budapeszcie w 2008 r., na którym wprowadzono szereg istotnych zmian w polityce NATO dotyczącej cyberprzestrzeni. Deklaracja końcowa wyeksponowała konieczność ochrony kluczowych systemów informacyjnych, upowszechniania dobrych praktyk oraz udzielania przez sygnatariuszy wzajemnej pomocy w przypadku cyberzamachów.

W 2015 r. CCD CoE opublikowało opracowanie dotyczące użytkowania urządzeń mobilnych przez wysokich urzędników państwowych, którzy gromadzą w nich szereg informacji poufnych i wrażliwych. Urządzenia te mogą być bowiem łatwym celem, nawet bez wiedzy ich użytkowników. W konsekwencji może to skutkować ujawnieniem → i n f o r m a c j i n i e j a w n y c h [t. 2], co grozi poważnymi implikacjami politycznymi, nawet o zasięgu międzynarodowym. Opublikowane przez CCD CoE opracowanie zdefiniowało zagrożenia oraz ryzyka wynikające ze stosowania urządzeń mobilnych, a także zarekomendowało mechanizmy zaradcze. Eksperci CCD CoE wypracowali także stanowisko głoszące, że wszystkie państwa muszą ustalić wspólne normy, prawa i definicje dotyczące cyberprzestrzeni. Zalecili oddzielenie czerwoną linią tego, co jest akceptowalne w sieci, od aktów → a g r e s j i, które nie mogą być tolerowane. To oni wspierają powstanie cyfrowej konwencji genewskiej, postulują prace nad międzynarodowymi uregulowaniami mogącymi ograniczyć wrogą aktywność w cyberprzestrzeni.

Swoje propozycje rozwiązań zaprezentowali w monografii *International Cyber Norms: Legal, Policy & Industry Perspectives* (*Międzynarodowe cybernormy – perspektywy prawne, polityczne i przemysłowe*), w której zwrócili uwagę, że pod pojęciem cyberobrony kryje się także zdolność ofensywna dająca możliwość przeprowadzenia ataku. Zdiagnozowali, że w sieci nie obowiązuje żaden tzw. *framework* oznaczający wspólne regulacje i ramy działania określające granice, których musieliby przestrzegać wszyscy cybergracze. Ich naruszenie w obszarze wirtualnym powinno skutkować alienacją i ostracyzmem, a także surowymi sankcjami – podobnymi do tych, jakie stosuje się w przypadku zbrojnej interwencji w świecie realnym. Zdaniem ekspertów cyberprzestrzeń nie może być nieuregulowanym obszarem bezprawia, a tworzenie międzynarodowych norm dla tej sfery musi być procesem ewolucyjnym. Za cel tego procesu uznali, by przy użyciu istniejących zasad prawa międzynarodowego oraz narzędzi politycznych wynegocjować konsensus – regulacje, których przyjęcie byłoby możliwe przez wszystkich. Zauważyli, że dotychczasowy brak konstruktywnego dyskursu uniemożliwia osiąganie ekonomicznych i społecznych zysków z cyberprzestrzeni. Jest też istotną barierą rozwoju bezpieczeństwa informacji i technologii komunikacyjnych. W trakcie jednej z debat minister spraw zagranicznych Estonii M. Kaljurand, będąca współautorką omawianej monografii, szukała odpowiedzi na pytanie, w jaki sposób prawo międzynarodowe może przeciwdziałać ofensywnej aktywności niektórych państw w cyberprzestrzeni. Zachęcała też do poszukiwań politycznych porozumień

niezbędnych do zapewnienia międzynarodowej stabilizacji w sieci. Dostrzegła, że istotną rolę odgrywa w tych kwestiach przemysł zajmujący się opracowywaniem i wytwarzaniem nowoczesnych technologii informatycznych.

Każdego roku CCD CoE organizuje Locked Shields, które są największymi i najbardziej zaawansowanymi ćwiczeniami z zakresu cyberobrony, przeprowadzanymi w czasie rzeczywistym. Ich głównym celem jest zdobywanie praktycznego doświadczenia przez sojuszników poprzez działanie w międzynarodowym środowisku, wypracowywanie zasad współpracy w ramach własnego zespołu oraz możliwość przetestowania umiejętności i zdolności reagowania pod silną presją czasu, wynikającą z konieczności obrony przed wzmożonymi atakami cybernetycznymi. Zespoły poza wykazaniem się sprawnością techniczną rozwiązują również zadania z obszaru informatyki śledczej oraz zagadnień politycznych, prawnych i medialnych, które w sposób nierozerwalny towarzyszą kwestiom związanym z cyberbezpieczeństwem. Te praktyczne ćwiczenia, z symulacją opartą na realnych → c y b e r z a g r o ż e n i a c h , służą stałemu kontrolowaniu i podnoszeniu poziomu zdolności obronnych NATO w cyberprzestrzeni.

Przejawem praktycznych rozwiązań proponowanych członkom przez CCD CoE jest opracowanie dotyczące korzystania z urządzeń mobilnych przez urzędników wysokiego szczebla. Wykorzystanie tych narzędzi jest współcześnie nieuniknione, a urzędnicy używają urządzeń mobilnych do gromadzenia, przetwarzania i przechowywania poufnych informacji, które powinny być chronione w sposób szczególny. W publikacji wskazano, że zasadniczo nie są one zabezpieczone, gdyż nie ma absolutnie bezpiecznego systemu. Opisano złe praktyki, takie jak instalacja darmowych gier czy innych aplikacji wykorzystujących złośliwe reklamy lub niewłaściwe ustawienia sieciowe usług społecznych.

Aktywnym członkiem CCD CoE jest także Polska. W ramach tej organizacji 28 marca 2019 r. odbyło się w Tallinie spotkanie T. Zdzikota, wiceministra MON, z sekretarzem stanu w ministerstwie obrony Estonii E. Kodarem. Tematem rozmów było rozszerzenie wojskowej kooperacji przy realizacji projektów w zakresie cyberbezpieczeństwa, m.in. Cyber.mil.pl, oraz wymiana wypracowanych dobrych praktyk. Politycy zajęli się również kwestiami związanymi z zapewnianiem bezpieczeństwa wschodniej flanki NATO w aspekcie cyberobrony. Za istotną sprawę uznano, by w celu przeciwdziałania zagrożeniom cybernetycznym stworzyć długoterminową strategię → o d s t r a s z a n i a [t. 3], która objęłaby nie tylko Polskę czy Estonię, lecz wszystkie państwa regionu i całe NATO. Wskazano, że tylko wspólnie wypracowane i zaakceptowane rozwiązania zdiagnozowanych problemów oraz pełne wykorzystywanie ofensywnego potencjału do obrony kolektywnej mogą wzmocnić efektywność dotychczasowej cyberobrony. Spotkanie było też okazją do omówienia kolejnej edycji ćwiczeń Locked Shields, których założeniem było utrzymanie bezpieczeństwa sieci oraz wykreowanie skutecznych rozwiązań przeciwdziałających wykrytym incydentom.

W trakcie wizyty w Tallinie wiceszef MON wziął także udział w seminarium zorganizowanym przez CCD CoE. Zasadniczym tematem było tworzenie bezpiecznej cyberprzestrzeni, proporcjonalne reagowanie na dynamicznie zmieniające się zagrożenia oraz aktualizacja strategii bezpieczeństwa cybernetycznego państw NATO. W trakcie seminarium poruszono również kwestię prawnych aspektów regulujących funkcjonowanie w cyberprzestrzeni. Przedmiotem debaty były też akty normatywne, dokumenty i wytyczne prawa międzynarodowego odnoszące się do prowadzenia militarnych operacji cybernetycznych.

Andrzej Czop

A. Czop, *Centrum Doskonalenia Obrony Przed Cyberatakami*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; *International Cyber Norms: Legal, Policy & Industry Perspectives*, A.M. Osula, H. Rõigas (eds.), CCD CoE, Tallinn 2016; J. Jalonen, *Dni, które wstrząsnęły Estonią*, tłum. P. Bukalska, Eesti.pl (dostęp 17.10.2019); B. Józefiak, *Centrum Doskonalenia NATO w Tallinie: niezbędne międzynarodowe prawo cyberprzestrzeni*, 30.03.2016, CyberDefence24.pl (dostęp 17.10.2019); P.M.A. Linebarger, *Wojna psychologiczna*, tłum. E. Niemirska, Wydawnictwo MON, Warszawa 1959; J. Olędzka, *Rosyjski haktywizm. Specyfika zjawiska*, [w:] *Haktywizm (cyberterroryzm, haking, protest obywatelski, cyberaktywizm, e-mobilizacja*), M. Marczewska-Rytko (red.), Wydawnictwo UMCS, Lublin 2014; Traktat Północnoatlantycki sporządzony w Waszyngtonie dnia 4 kwietnia 1949 r., Dz. U. 2000, nr 87, poz. 970.

CENTRUM EKSPERCKIE NATO DS. KOMUNIKACJI STRATEGICZNEJ (Strategic Communications Centre of Excellence, StratCom CoE) – akredytowana przez → NAT O [t. 3] międzynarodowa organizacja wojskowa, która nie stanowi części struktury dowodzenia NATO ani nie jest podporządkowana żadnej innej jednostce NATO. Centrum to nie jest więc oficjalnym przedstawicielem Paktu Północnoatnaltyckiego. Swym działaniem ma przyczyniać się do poprawy strategicznych zdolności komunikacyjnych w ramach sojuszu i państw członkowskich. → K o m u n i k a c j a s t r a t e g i c z n a [t. 2] stanowi integralną część wysiłków służących osiąganiu celów politycznych i wojskowych, dlatego coraz istotniejsze jest, by NATO na temat swoich zmieniających się ról, celów i misji komunikowało się w aktualny, dokładny, szybki i adekwatny do sytuacji sposób. Misją StratCom CoE jest konkretny wkład w strategiczne zdolności komunikacyjne NATO, poszczególnych sojuszników i partnerów NATO. Jego potencjał tworzą międzynarodowi i międzysektorowi uczestnicy reprezentujący sektory: cywilny, wojskowy, prywatny i akademicki, którzy wykorzystują nowoczesne technologie, wirtualne narzędzia analityczne oraz badania naukowe. Siłę NATO StratCom CoE stanowi grupa międzynarodowych ekspertów ze środowisk wojskowych, rządowych i akademickich będących trenerami, nauczycielami, analitykami i badaczami. Centrum jest obsadzone kadrowo i finansowane przez państwa sponsorujące i uczestników wnoszących określony wkład.

Centrum zostało powołane do życia w styczniu 2014 r. 1 lipca tego samego roku w Norfolk w USA odbyła się ceremonia podpisania protokołu ustaleń ws. ustanowienia

i funkcjonowania NATO Strategic Communications Centre of Excellence w stolicy Łotwy – Rydze. W imieniu ministra obrony narodowej RP porozumienie podpisał płk R. Romanowski, narodowy przedstawiciel łącznikowy przy Sojuszniczym Dowództwie ds. Transformacji NATO (Allied Command Transformation, ACT). Łotwę, będącą państwem ramowym, reprezentowali: ambasador Łotwy w USA

A. Razans, minister obrony Łotwy R. Vejonis oraz dyrektor nowo utworzonego Centrum J. Karklins. Porozumienie podpisali także przedstawiciele pozostałych państw przystępujących do StratCom CoE – Estonii, Niemiec, Litwy, Włoch, Wielkiej Brytanii – a także dowódca ACT gen. J.-P. Paloméros. W uroczystości uczestniczyli ponadto doradca polityczny dowódcy ACT, ambasador K. Stewart, oraz zastępca dowódcy ACT gen. M. Zuliani. Centrum otrzymało akredytację NATO 1 września 2014 r., a w deklaracji ze szczytu w Walii sojusznicy z zadowoleniem przyjęli ustanowienie StratCom CoE, uznając jego znaczący wkład w wysiłki NATO podejmowane w obszarze komunikacji strategicznej. W 2016 r. do organizacji dołączyły Holandia i Finlandia, w 2017 r. Szwecja, w 2018 r. Kanada, a na początku 2019 r. Słowacja.

Mottem organizacji stał się fragment preambuły konstytucji → U N E S C O [t. 4] uchwalonej w 1946 r., który brzmi: „Ponieważ wojny zaczynają się w umysłach ludzi, w umysłach ludzi należy budować obronę pokoju". W epoce społeczeństwa informatycznego trudno sobie wyobrazić realizację jakiejkolwiek operacji bez zapewnienia jasno określonej i sprawnej komunikacji strategicznej. Do głównych zadań organizacji należy dbanie o dobry wizerunek NATO. Gros pracy organizacji skupia się na portalach społecznościowych, takich jak Facebook czy Twitter, które wykorzystywane są do rozpowszechniania i promowania wiedzy na temat działań podejmowanych przez organizację. Ponadto zajmuje się ona operacjami psychologicznymi – używa wielu środków komunikacji nakierowanych na poszczególnych widzów, tak aby wpłynąć na ich postawy oraz zachowania.

StratCom CoE jest również cennym źródłem → i n f o r m a c j i [t. 2] na tematy geopolityczne. Przygotowuje wartościowe, merytoryczne analizy dotyczące różnych aspektów polityki światowej. Opublikowało m.in. raport poświęcony działaniom komunikacyjnym podejmowanym przez Rosję. Ten obszerny materiał zawiera gruntowną analizę „informacyjnej geopolityki" Rosji (termin autorstwa prof. N. Malikevičiusa, politologa z Instytutu Stosunków Międzynarodowych i Nauk Politycznych na Uniwersytecie Wileńskim), która ma na celu lansowanie sprzyjających Kremlowi interpretacji działań politycznych. Ta i inne analizy centrum są cennym źródłem wiedzy o obecnej sytuacji politycznej, których w dobie szumu informacyjnego nie można przecenić.

StratCom CoE powołano do życia w 2014 r. jako ośrodek badawczy typu think tank, którego celem jest badanie międzynarodowej przestrzeni komunikacyjnej i tworzenie rekomendacji dla państw Sojuszu w zakresie komunikacji strategicznej, czyli komunikacji zorientowanej na osiąganie określonych celów. W rozumieniu przyjętym

w NATO w jej zakres wchodzi zarówno dyplomacja publiczna, jak i współpraca z mediami. Deklaracja szczytu w Strasburgu i Kehl stanowi, że:

> coraz ważniejsze jest, aby Sojusz komunikował się w odpowiedni, terminowy, dokładny i elastyczny sposób o swoich zmieniających się rolach, celach i misjach. Komunikacja strategiczna stanowi integralną część naszych wysiłków na rzecz osiągnięcia politycznego sojuszu i celów wojskowych.

Obecne → ś r o d o w i s k o i n f o r m a c y j n e [t. 4] – charakteryzujące się cyklem informacyjnym 24/7, wzrostem liczby portali społecznościowych i wzajemnym powiązaniem odbiorców z obszaru państw NATO – w istotny sposób wpływa na postrzeganie działań sojuszu przez kluczowych odbiorców. Ta percepcja może determinować powodzenie poszczególnych operacji i globalnej polityki NATO. Stąd Pakt Północnoatlantycki winien korzystać z różnych kanałów obejmujących zarówno → m e d i a t r a d y c y j n e [t. 3], jak i internet, aby budować świadomość, zrozumienie i wsparcie dla podejmowanych decyzji i prowadzonych operacji. W tym celu konieczne jest spójne podejście instytucjonalne, koordynujące wysiłki wszystkich członków tak, aby były one zgodne z politykami, procedurami i zasadami przyjętymi w NATO. Komunikacja strategiczna musi więc polegać na skoordynowanym i właściwym wykorzystaniu działań i zdolności komunikacyjnych NATO, aby przyspieszyć realizację założonych celów.

Do działań tych można zaliczyć:

- dyplomację publiczną – komunikację NATO w celu budowania świadomości, zrozumienia oraz poparcia polityki i działań Sojuszu, będącą ważnym uzupełnieniem wysiłków podejmowanych przez poszczególne państwa członkowskie;
- cywilne sprawy publiczne – obejmujące cywilne zaangażowanie NATO, przy wykorzystaniu mediów, ukierunkowane na informowanie → o p i n i i p u b l i c z n e j [t. 3] o polityce, operacjach i działaniach Sojuszu – ważne jest tu zachowanie zasad takich jak terminowość, dokładność, elastyczność i proaktywność;
- wojskowe sprawy publiczne wiążące się z promowaniem wojskowych celów i zadań NATO, aby zwiększyć świadomość i zrozumienie militarnych problemów sojuszu;
- operacje informacyjne – doradztwo wojskowe NATO i koordynacja wojskowych działań informacyjnych w celu uzyskania pożądanego wpływu na świadomość przeciwników, aby zapewnić skuteczność operacji, misji i celów realizowanych przez Sojusz;
- → o p e r a c j e p s y c h o l o g i c z n e [t. 3] – zaplanowane działania psychologiczne z wykorzystaniem metod komunikacji i innych środków skierowanych do określonych adresatów w celu wpłynięcia na ich postawy i zachowania, wspierające osiągnięcie celów politycznych i wojskowych.

Strategiczne cele komunikacji NATO uwzględniające okoliczności i teatry prowadzonych działań to:

- bezpośrednie wspieranie pomyślnego osiągnięcia celów prowadzonych operacji, misji i działań sojuszu poprzez włączenie planowania komunikacji strategicznej do wszystkich planów operacyjnych i politycznych;

- budowanie w ścisłej koordynacji ze wszystkimi członkami sojuszu świadomości społecznej, zrozumienia i wsparcia dla konkretnych polityk, operacji i innych działań NATO we wszystkich docelowych grupach odbiorców.

Najważniejsze przedsięwzięcia zrealizowane przez StratCom CoE w 2019 r. to:

- ciągły rozwój doktryny i polityki StratCom CoE;
- Eksperyment w zakresie Międzynarodowych Operacji Informacyjnych (Multinational Information Operations Experiment, MNIOE);
- Międzynarodowa Kampania na rzecz Rozwoju Zdolności (Multinational Capability Development Campaign, MCDC);
- badania: „Sieci robotyczne w mediach społecznościowych", „Pojawiające się problemy w mediach społecznościowych", „Przeciwdziałanie kampanii informacyjnej Rosji w krajach nordyckich i bałtyckich", „StratCom w walce z terroryzmem – aktualne działania informacyjne grup terrorystycznych z Bliskiego Wschodu", „Strategiczna komunikacja z Arktyką";
- ilościowe badania kampanii w mediach społecznościowych w kontekście Dalekiego Wschodu;
- prace nad ulepszeniem terminologii StratCom;
- kurs „Komunikacja strategiczna dla wyższych urzędników"; kursy i seminaria w mediach społecznościowych;
- wsparcie edukacyjne i szkoleniowe ACT.

Na 2020 r. StratCom CoE zaplanowało następujące działania:

- ciągły rozwój doktryny i polityki NATO StratCom;
- Eksperyment w zakresie Międzynarodowych Operacji Informacyjnych (Multinational Information Operations Experiment, MNIOE);
- Międzynarodowa Kampania na rzecz Rozwoju Zdolności (Multinational Capability Development Campaign, MCDC);
- badania: „Sieci robotyczne w mediach społecznościowych";
- seminarium „Komunikacja strategiczna dla wyższych urzędników";
- doroczna konferencja „Dialog Riga StratCom";
- wydanie kolejnego numeru rocznika „Defense Strategic Communications";
- seminarium i kursy w mediach społecznościowych;
- wsparcie edukacyjne i szkoleniowe ACT;
- wspieranie ćwiczeń NATO.

Andrzej Czop, Marek Pietrzyk

M. Chyliński, *Kompetencje informacyjne i kompetencje medialne wobec procesów zarządzania uwagą masowej publiczności*, „Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie" 2017, z. 106; A. Czop, M. Pietrzyk, *Centrum Eksperckie NATO ds. Komunikacji Strategicznej*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; P.M.A. Linebarger, *Wojna psychologiczna*, Wydawnictwo MON, Warszawa 1959; N. Maliukevičius, *The Roots of Putin's Media Offensive in the Baltic States: Learning*

Lessons in Counterstrategies, [w:] *Baltic Visions European Cooperation Regional Stability*, K. Redłowska (ed.), http:// geopolitika.lt/files/baltic-visions.pdf (dostęp 12.01.2020); W. Schwartau, *Information Warfare, Chaos on the Electronic Superhighway*, Thunder's Mouth Press, New York 1995; Strasbourg / Kehl Summit Declaration, issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Strasbourg / Kehl, 4.04.2009.

CENTRUM KOMUNIKACJI STRATEGICZNEJ I BEZPIECZEŃSTWA INFORMACJI (ukr. *Центр стратегічних комунікацій та інформаційної безпеки*) – organizacja rządowa powołana w ramach Ministerstwa Kultury i Polityki Informacyjnej Ukrainy w marcu 2021 r. jako jeden z mechanizmów budowy odporności narodowej, zwalczania zagrożeń informacyjnych i → d e z i n f o r m a c j i [t. 2], wraz z odpowiednimi instytucjami publicznymi, organizacjami społeczeństwa obywatelskiego i partnerami międzynarodowymi. Zespół redakcyjny Centrum jest jednostką strukturalną Ukraińskiej Narodowej Agencji Informacyjnej Ukrinform. Po rozpoczęciu pełnej → i n w a z j i [t. 2] Rosji na Ukrainę ośrodek stał się jednym z czołowych kanałów rządowej komunikacji o → w o j n i e [t. 4] w Ukrainie.

Centrum zostało powołane 31 marca 2021 r., a jego pierwszym przewodniczącym została Lubow Cybulska. Od 6 września 2021 r. na czele ośrodka stoi Ihor Sołowiej. Zastępcą przewodniczącego jest Mykoła Bałaban. W grudniu 2021 r. Centrum zorganizowało pierwsze w Ukrainie forum → k o m u n i k a c j i s t r a t e g i c z n e j [t. 2] Kyiv Stratcom Forum. Zgromadziło ono 32 ukraińskich i międzynarodowych ekspertów, którzy uczestniczyli w dyskusjach panelowych i rozmawiali o współpracy między rządem a → s p o ł e c z e ń s t w e m o b y w a t e l s k i m [t. 4] w celu kształtowania narodowej odporności na zagrożenia informacyjne i dezinformację.

„Teraz mamy państwowy mechanizm do walki z dezinformacją, który pozwoli nam chronić przestrzeń informacyjną przed zniekształceniami i manipulacjami. Centrum ma na celu jednoczenie wysiłków organizacji publicznych i władz w walce z dezinformacją, szybkie reagowanie na fałszerstwa, a także upowszechnianie ukraińskich narracji" – podkreślił minister kultury i polityki informacyjnej Ołeksandr Tkaczenko podczas otwarcia Centrum. „Zwalczanie dezinformacji, zwłaszcza wrogiej dezinformacji, celowego rozpowszechniania fałszywych informacji, jest priorytetem dla rządu i resortu" – powiedział wiceminister Taras Szewczenko. Kierownik Centrum, Cybulska, przedstawiła cele i zadania oraz oczekiwane rezultaty pracy. „Chcemy stworzyć potężny ośrodek z wiedzą ekspercką. Ostatnie siedem lat zmagań z Rosją potwierdziło, że dysponujemy tą wiedzą, a także licznymi inicjatywami na poziomie zarówno państwa, jak i społeczeństwa obywatelskiego. Wzywam nas wszystkich do zjednoczenia się, ponieważ mamy ten sam cel i razem walczymy z agresorem" – podkreśliła. Misją Centrum jest zapewnienie integralności → ś r o d o w i s k a i n f o r m a c y j n e g o [t. 4], podnoszenie świadomości Ukraińców na temat zagrożeń informacyjnych, wzmacnianie potencjału społeczeństwa obywatelskiego i odporności ludzi.

Celem jest zbudowanie trwałej komunikacji rządowej w celu przeciwdziałania dezinformacji i kształtowania odporności na nią ukraińskiego społeczeństwa. Kluczowe zadania Centrum to:

- analiza środowiska informacyjnego, monitorowanie narracji dezinformacyjnych, a także badanie wrażliwych odbiorców;
- podnoszenie świadomości społeczeństwa na temat zagrożeń informacyjnych przez tworzenie objaśnień, organizowanie konferencji prasowych oraz angażowanie mediów i partnerów do wspólnej pracy;
- wspieranie rządowej komunikacji publicznej przez rozwijanie umiejętności komunikacyjnych urzędników służby cywilnej orazdoskonalenie systemu łączności szybkiego reagowania;
- zwiększenie odporności urzędników służby cywilnej na dezinformację i → a t a k i i n f o r m a c y j n e [t. 1];
- udział w opracowaniu systemu komunikacji strategicznej, organizacja i koordynacja działań na rzecz jej rozwoju;
- wzmacnianie odporności wrażliwych odbiorców w Ukrainie na dezinformację przez ukierunkowane kampanie uświadamiającei działania edukacyjne;
- nawiązywanie współpracy między państwem a instytucjami społeczeństwa obywatelskiego w celu budowania odporności na dezinformację i → z a g r o ż e n i a h y b r y d o w e [t. 4];
- organizacja wydarzeń informacyjno-edukacyjnych, aby zwiększać umiejętności korzystania z mediów przez Ukraińców.

Główne kierunki pracy Centrum:

- rozwój komunikacji strategicznej, w tym opracowywanie kontrnarracji wobec Federacji Rosyjskiej, prowadzenie kampanii informacyjnych, włączanie narracji ukraińskiej do codziennych komunikatów rządu;
- współpraca ze społeczeństwem obywatelskim i wzmacnianie jego głosu;
- szybka komunikacja i informowanie o najważniejszych wydarzeniach w internecie i na platformach społecznościowych, takich jak: Facebook, Telegram, Instagram, X (dawniej Twitter), Viber, YouTube;
- wspólne opracowywanie z instytucjami państwowymi i ekspertami algorytmów działania w warunkach wojny oraz ich dystrybucjaw postaci przystępnych materiałów źródłowych;
- regularne informowanie o rosyjskiej agresji hybrydowej na poziomie międzynarodowym, wspólne wypracowanie mechanizmów komunikacji strategicznej i przeciwdziałania dezinformacji wrazz międzynarodowymi partnerami.

23 czerwca 2021 r. Ukrinform zaprezentował broszurę zatytułowaną *Na wypadek zagrożenia lub wojny*. Dokument został opracowany przez Centrum we współpracy z Państwową Służbą Ratunkową Ukrainy, Ministerstwem Obrony Ukrainy, Urzędem Naczelnego Dowódcy Sił Zbrojnych Ukrainy oraz organizacjami społeczeństwa obywatelskiego.

Broszura została wydana w formacie PDF (28 stron) w 3 językach: ukraińskim, angielskim i rosyjskim. Zawierała praktyczne porady, które uwzględniają doświadczenia ukraińskie i zagraniczne oraz zalecenia dotyczące → b e z p i e c z e ń s t w a i n f o r m a c y j n e g o [t. 1]. Początek wojny wraz z eskalacją sytuacji na granicach Ukrainy ujawnił ogromne zapotrzebowanie na praktyczne → i n f o r m a c j e [t. 2] na temat tego, jak mają postępować cywile. Pierwszy nakład broszury wyniósł 100 tys. egzemplarzy i był rozpowszechniany na terenach frontowych oraz w południowych i wschodnich regionach kraju przy wsparciu Sił Zbrojnych Ukrainy.

23 lutego 2022 r. Centrum udostępniło zaktualizowaną internetową wersję broszury (36 stron). Przez cały czas jest ona uzupełniana odpowiednimi informacjami. Wraz z katalogiem powstała również strona dovidka.info. W skład projektu wchodzą także 2 chatboty bezpieczeństwa w komunikatorach Telegram oraz Viber. W ciągu pierwszych 2 miesięcy ich istnienia do chatbotów zapisało się ponad 160 tys. użytkowników. Projekt stale się rozwija, by sprostać wyzwaniom, przed którymi stoi społeczeństwo ukraińskie. Głównym zadaniem portalu dovidka.info jest szybkie dostarczanie sprawdzonych i wysokiej jakości informacji, które mogą uratować życie i pomóc wyjść z trudnej sytuacji.

„Wojna hybrydowa w XXI w." to nie tylko ostrzał artyleryjski czy z broni strzeleckiej. Wróg przeprowadza ataki w przestrzeni informacyjnej, próbując osłabić naszą zdolność do stawiania oporu. Dlatego każdy z nas powinien znać proste zasady: jakim informacjom ufać, jakich źródeł słuchać, jak odróżnić fałsz od prawdy i jak nie dać się nabrać na dezinformację. Wszyscy ponosimy zbiorową odpowiedzialność za bezpieczeństwo naszego kraju. A kiedy armia robi wszystko, co możliwe i niemożliwe na froncie, my – na tyłach – musimy zrobić wszystko, by zachować jasność umysłu, a w razie niebezpieczeństwa każdy z nas ma jasny algorytm postępowania, aby skuteczniej radzić sobie z kryzysem i minimalizować jego negatywne konsekwencje – podkreślił Tkaczenko.

Centrum Komunikacji Strategicznej i Bezpieczeństwa Informacji wspólnie z Instytutem Informacji Masowej wiosną 2023 r. przygotowało zalecenia i ostrzeżenia dotyczące stosowania terminologii w odniesieniu do wydarzeń i zjawisk wojny rosyjsko-ukraińskiej. Nie mogąc wygrać na polu → b i t w y [t. 1], Rosja nie ustaje w próbach narzucenia światu własnej interpretacji tego, co dzieje się w Ukrainie i z Ukrainą. Niestety, echa rosyjskiej → p r o p a g a n d y [t. 3] w postaci zaangażowanego słownictwa wojennego wciąż można znaleźć nawet na łamach szanowanych zachodnich publikacji. Szczególnie niepoprawne jest sformułowanie „kryzys ukraiński". Prawidłowe wyrażenia to: „rosyjska inwazja na Ukrainę", „wojna rosyjsko-ukraińska". Sformułowania typu „wojna ukraińska" maskują rolę agresora i przerzucają odpowiedzialność za problem na Ukrainę. Również niewłaściwe jest określenie dotyczące „terytoriów spornych", chodzi o „terytoria czasowo okupowane", „terytoria nielegalnie zaanektowane". Tereny Ukrainy zajęte i kontrolowane przez Rosję nigdy nie były przedmiotem

międzynarodowego sporu. Bezwzględna większość państw uznaje integralność terytorialną Ukrainy.

Olga Wasiuta

Є. Брайлян, *Як стратегічні комунікації допомагають Україні налагодити міжнародну співпрацю з протидії ворожій дезінформації*, 9.12.2021, https://armyinform.com.ua/2021/12/09/yak-strategichni-komunikacziyi-dopomagayut-ukrayini-nalagodyty-mizhnarodnu-spivpraczyu-z-protydiyi-vorozhij-dezinformacziyi/ (dostęp 15.04.2023); *Презентовано Центр стратегічних комунікацій та інформаційної безпеки Міністерство культури та інформаційної політики України*, 1.04.2021, https://www.kmu.gov.ua/news/prezentovano-centr-strategichnihkomunikacij-ta-informacijnoyi-bezpeki (dostęp 15.04.2023); *Ткаченко окреслив повноваження Центру стратегічних комунікацій та інформбезпеки*, 23.03.2021, https://detector.media/infospace/article/186232/2021-03-23-tkachenko-okreslyvpovnovazhennya-tsentru-strategichnykh-komunikatsiy-ta-informbezpeky/ (dostęp 18.04.2023); *Центр стратегічних комунікацій*, https://spravdi.gov.ua/pro-nas/ (dostęp 15.04.2023); *Центр стратегічних комунікацій та інформаційної безпеки презентував брошуру «У разі надзвичайної ситуації або війни»*, 23.06.2021, https://mkip.gov.ua/news/5641.html (dostęp 18.04.2023); *Центр стратегічних комунікацій та ІМІ розробили словник термінології щодо подій в Україні*, 14.04.2023, https://www.ukrinform.ua/rubric-society/3696026-centr-strategicnihkomunikacij-ta-imi-rozrobili-slovnik-terminologii-sodo-podij-v-ukraini.html (dostęp 25.04.2023); *Центр Стратегічних комунікацій та інформаційної безпеки при Міністерстві культури та інформаційної політики*, 6.01.2022, https://mkip.gov.ua/content/centr-strategichnih-komunikaciy-ta-informaciynoi-bezpeki-pri-ministerstvi-kulturi-ta-informaciynoi-politiki.html (dostęp 18.04.2023); *Центр стратегічних комунікацій та інформаційної безпеки при МКІП інформує!*,2 26.05.2022, https://smu.dsp.gov.ua/news/tsentr-stratehichnykhkomunikatsii-ta-informatsiinoi-bezpeky-pry-mkip-informuie/ (dostęp 25.04.2023).

CENTRUM KOSMICZNE NATO – w grudniu 2019 r. na szczycie w Londynie → N A T O [t. 3] zadeklarowało, że przestrzeń kosmiczna jest „piątą domeną" operacji Sojuszu, obok lądu, morza, powietrza i → c y b e r p r z e s t r z e n i [t. 1]. Wcześniej, w czerwcu 2019 r., podczas posiedzenia Rady Ministerialnej NATO w Brukseli przyjęto zapisy polityki kosmicznej NATO (dokument jest niejawny). Następstwem tych zmian w postrzeganiu przestrzeni kosmicznej była decyzja ministrów obrony państw NATO o utworzeniu Centrum Kosmicznego w kwaterze głównej Sojuszniczego Dowództwa Sił Powietrznych (NATO Allied Air Command) w Ramstein w Niemczech. Decyzja zapadła podczas spotkania w październiku 2020 r. W towarzyszącym temu wydarzeniu komunikatowi sekretarza generalnego NATO Jensa Stoltenberga przypomniano o roli systemów satelitarnych w podtrzymaniu funkcjonowania naszego świata w wielu różnych aspektach, szczególnie gospodarczych i społecznych. Wspomniano również, że przestrzeń kosmiczna jest niezbędna dla NATO, ponieważ umożliwia nawigację, gwarantuje łączność, pozwala na gromadzenie danych wywiadowczych oraz wczesne wykrywanie i śledzenie toru lotu pocisków rakietowych. Stąd też niezbędne jest, by Sojusz utrzymał odpowiedni poziom świadomości sytuacyjnej w kosmosie, zapewnił w każdych warunkach niezawodny dostęp do usług kosmicznych, a także zachował przewagę techniczną w tej dziedzinie.

Z punktu widzenia ogromnego znaczenia kosmosu dla NATO nowego wymiaru nabierają zmiany w przestrzeni pozaziemskiej, jakie nastąpiły w ostatniej dekadzie. Szczególnie niepokojące dla NATO są wysiłki niektórych państw, głównie Chin i Rosji, zmierzające do stworzenia możliwości wrogiego oddziaływania na infrastrukturę satelitarną. Opracowywane i rozwijane przez te kraje systemy przeciwsatelitarne mogą zniszczyć, dezaktywować lub zakłócić funkcjonowanie satelitów należących do innych państw. Część z tych systemów, działająca na zasadzie fizycznej → d e s t r u k c j i [t. 5] satelitów – mowa tu szczególnie o systemach działających na bazie pocisków rakietowych bezpośredniego wznoszenia, niszczących cele orbitalne za pomocą głowicy kinetycznej – niesie za sobą również niebezpieczeństwo zanieczyszczenia środowiska kosmicznego przez chmury kosmicznego gruzu powstające w wyniku zderzenia pocisku z satelitą. Te niepokojące tendencje są wzmacniane przez przekształcenia środowiska kosmicznego, które – choć mogą mieć korzystne następstwa, jak w wypadku procesu komercjalizacji działalności kosmicznej – stwarzają wyzwania związane chociażby z postępującym zatłoczeniem kosmosu i wpływem tego czynnika na bieżące operacje kosmiczne.

Powstanie Centrum Kosmicznego NATO wynika z konstatacji, że przestrzeń kosmiczna jest niezbędna do odstraszania wrogów i obrony Sojuszu. Zadania wielonarodowego zespołu obsługującego ośrodek to: pomoc w koordynowaniu działań Sojuszu w kosmosie, w ochronie systemów kosmicznych Sojuszu przez wymianę → i n f o r m a c j i [t. 2] o potencjalnych → z a g r o ż e n i a c h [t. 4] oraz wspieranie działań i operacji NATO. Realizacja tych zadań polega przede wszystkim na monitorowaniu sytuacji kosmicznej w celu zbierania informacji o potencjalnych zagrożeniach. Zakłada się, że Centrum będzie miało potencjał do przekształcenia się w przyszłości w pełnoprawne centrum dowodzenia siłami obronnymi w przestrzeni kosmicznej, czyli jego zadaniem byłaby obrona sojuszniczych aktywów kosmicznych.

Centrum ściśle współpracuje z narodowymi agencjami i organizacjami kosmicznymi Sojuszu oraz strukturą dowodzenia NATO w celu wymiany danych, produktów i usług dostarczanych przez państwa, takich jak obrazowanie, nawigacja i wczesne ostrzeganie. Prośby o wsparcie w przestrzeni kosmicznej nie ograniczają się do sojuszników dysponujących możliwościami w przestrzeni kosmicznej. Wszystkie państwa mogą przekazywać dane, produkty i usługi, które można połączyć w jeden „produkt". Ten wspólny obraz domeny kosmicznej może być następnie udostępniany na potrzeby całego Sojuszu. Wsparcie udzielane przez Centrum Kosmiczne NATO ma być użyteczne nie tylko na poziomie dowództw operacyjnych, lecz również na poziomie taktycznym.

Początkowo do realizacji zadań w Centrum przydzieleni zostali eksperci ze Stanów Zjednoczonych, z Wielkiej Brytanii, Hiszpanii, Holandii i Niemiec. Zakładano jednak, że ośrodek będzie zasilany dodatkowym personelem pochodzącym z kolejnych państw NATO. Pod koniec 2022 r. w prace Centrum zaangażowany był personel z 12 państw.

Dyrektorem jednostki jest ppłk John Patrick z → Sił Kosmicznych Stanów Zjednoczonych.

Działalność Centrum Kosmicznego NATO jest wspomagana przez Centrum Doskonałości NATO ds. Kosmosu (NATO Space Center of Excellence).

Decyzję o jego lokalizacji we francuskim mieście Tuluza podjęto 28 stycznia 2021 r. Konkurencyjną propozycją było niemieckie miasto Kalkar. Czynnikiem decydującym o wyborze Tuluzy był fakt, że Centrum Kompetencyjne zostało umieszczone razem z francuskim wojskowym Dowództwem Kosmicznym (Commandement de l'Espace) na terenie Centrum Badań Kosmicznych(Centre National d'Études Spatiales, CNES).

Centrum Kompetencyjne rozpoczęło działalność latem 2021 r., zakłada się, że pełny skład 42 ekspertów (w tym 25 Francuzów) osiągnie do 2025 r. Jego zadaniem jest zapewnianie fachowej wiedzy i doświadczenia w określonej dziedzinie z korzyścią dla NATO, przy jednoczesnym unikaniu dublowania zasobów i zdolności już dostępnych w ramach Sojuszu. Polegać ma ono szczególnie na szkoleniu specjalistów w zakresie operacji kosmicznych z państw członkowskich NATO i krajów partnerskich, wypracowaniu doktryn, testowaniu i zatwierdzaniu koncepcji oraz poprawianiu interoperacyjności Sojuszu w przestrzeni kosmicznej. Razem z centrum ds. kompetencji kosmicznych w ramach NATO funkcjonuje 27 centrów kompetencyjnych.

Rafał Kopeć

K.-H. Brunner, *Space and Security – NATO's Role*, NATO Parliamentary Assembly, Brussels 2021; I. de la Cuetara, J. Schlosberg, T. Brooksbank, *Inside NATO's Space Centre, Where Allied Forces Keep a Close Eye on Russian, Chinese Satellite Threats*, 15.11.2022, https://abcnews.go.com/International/inside-natos-secretivespace-commands-critical-mission/story?id=93332144 (dostęp 11.03.2023); V. Machi, *NATO's Forthcoming Space Center for Excellence Hits Key Milestone*, 25.01.2023, https://www.defensenews.com/global/europe/2023/01/25/natos-forthcomingspace-center-for-excellence-hits-key-milestone/ (dostęp 15.04.2023).

CENTRUM POWIADAMIANIA RATUNKOWEGO (CPR) – ośrodek obsługi (odbioru, weryfikacji, przetwarzania, przekazywania) zgłoszeń alarmowych, najczęściej telefonicznych, wykonywanych pod numery alarmowe. Tego typu centra funkcjonują na całym świecie i mogą pracować w 3 podstawowych modelach:

- operatorskim,
- operatorsko-dyspozytorskim,
- dyspozytorskim.

W Polsce CPR tworzą system powiadamiania ratunkowego, tj. jednolity system do obsługi zgłoszeń alarmowych, kierowanych do numerów alarmowych 112, 997, 998 i 999, umożliwiający przekazanie zgłoszenia alarmowego w celu zaangażowania właściwych zasobów ratowniczych. CPR funkcjonują więc w modelu operatorskim, co oznacza, że zatrudnieni w CPR operatorzy numerów alarmowych obsługują wpływające zgłoszenia, a następnie przesyłają (drogą elektroniczną) wszystkie zebrane → informacje [t. 2] do dyżurnych/dyspozytorów podmiotów ratowniczych.

→ P o l i c j a [t. 3], → P a ń s t w o w a S t r a ż Po ż a r n a [t. 3], dysponenci zespołów ratownictwa medycznego dysponują do przekazanych zdarzeń własne zasoby ratownicze.

Formalnie po raz pierwszy nazwa CPR pojawiła się w grudniu 1999 r. w nowelizacji rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie szczegółowej organizacji krajowego systemu ratowniczo-gaśniczego (KSRG). Za podstawowy element systemu przyjmującego informacje o zdarzeniach alarmowych uznano wówczas stanowiska kierowania w komendach Państwowej Straży Pożarnej. W kolejnych latach tworzono centra powiadamiania ratunkowego i wojewódzkie centra powiadamiania ratunkowego zgodnie z ideą „CPR w każdym powiecie". Taka koncepcja okazała się jednak niezwykle kosztowna i mało wydolna. Zgodnie z przyjętymi rozwiązaniami systemowymi już od dekady CPR tworzone są przez wojewodów i powinny przyjmować zgłoszenia pod numery alarmowe 112, 997, 998 i 999, choć do 2020 r. udało się „przejąć" do CPR, prócz numeru 112, jedynie jeden numer branżowy, tj. 997.

Głównym zadaniem CPR jest obsługa zgłoszeń alarmowych i przekazanie ich w celu zaangażowania właściwych służb ratowniczych. Poza tym aktualne przepisy nakładają na CPR jeszcze szereg innych obowiązków:

- ewidencjonowanie i przechowywanie w systemie teleinformatycznym danych dotyczących treści zgłoszeń alarmowych, w tym nagrań rozmów telefonicznych, danych osób zgłaszających i osób wskazanych w trakcie przyjmowania zgłoszenia, informacji o miejscu zdarzenia, jego rodzaju oraz skróconego opisu zdarzenia;
- wykonywanie analiz związanych z funkcjonowaniem systemu oraz tworzenie statystyk w zakresie liczby, rodzaju i czasów realizacji zgłoszeń;
- współpracę oraz wymianę informacji z centrami → z a r z ą d z a n i a k r y z y s o w e g o [t. 4];
- wymianę informacji i danych, z wyłączeniem danych osobowych, na potrzeby analiz z Policją, Państwową Strażą Pożarną, dysponentami zespołów ratownictwa medycznego oraz podmiotami, których numery telefoniczne są obsługiwane w ramach systemu;
- zapewnienie w CPR całodobowej realizacji zadań wykonywanych przez lekarza koordynatora ratownictwa medycznego;
- sporządzanie co najmniej raz w roku wraz z Komendą Wojewódzką Policji, Komendą Wojewódzką Państwowej Straży Pożarnej oraz dysponentami zespołów ratownictwa medycznego mających w swojej strukturze stanowiska dyspozytorów medycznych oceny współpracy z systemem powiadamiania ratunkowego na obszarze danego województwa;
- sporządzenie wykazu podmiotów ratowniczych współpracujących z jednostkami systemu powiadamiania ratunkowego.

We wszystkich CPR funkcjonuje sfera kierownicza, administracyjna, techniczna, merytoryczna oraz zatrudniony jest psycholog. Podstawowa dokumentacja, na bazie której funkcjonuje CPR, jest zunifikowana i obejmuje:

- regulamin organizacyjny CPR,
- plan postępowania na wypadek wystąpienia sytuacji awaryjnej,
- plan zwiększania obsad osobowych w sytuacjach nadzwyczajnych,
- plan obsługi numeru 112,
- zasady organizacji pracy operatorów numerów alarmowych,
- procedury obsługi zgłoszeń alarmowych.

Na terenie kraju funkcjonuje 17 CPR zatrudniających łącznie ok. 1350 operatorów numerów alarmowych. Przynajmniej jedno takie centrum znajduje się w każdym województwie (wyjątek stanowi województwo mazowieckie, gdzie CPR funkcjonuje w Warszawie i Radomiu).

Operatorem numerów alarmowych może być osoba, która ma co najmniej średnie wykształcenie, posługuje się co najmniej jednym językiem obcym, ukończyła szkolenie i zdała odpowiedni egzamin oraz ma wydany na 3 lata certyfikat operatora numerów alarmowych. Przed upływem okresu ważności certyfikatu operator jest zobowiązany odbyć szkolenie realizowane w ramach doskonalenia zawodowego oraz zdać egzamin sprawdzający.

CPR znajdują się w strukturze urzędów wojewódzkich, chyba że wojewoda, w drodze porozumienia, powierzy jego organizowanie i prowadzenie staroście lub prezydentowi miasta na prawach powiatu, służbie, inspekcji lub straży wchodzącej w skład zespolonej administracji wojewódzkiej. W CPR praca wykonywana jest w systemie zmianowym, w którym zmiana trwa 12 h, a więc pokrywa się to z organizacją systemu pracy w stanowiskach kierowania Policji i zintegrowanych dyspozytorniach ratownictwa medycznego (w stanowiskach kierowania Państwowej Straży Pożarnej służba pełniona jest najczęściej 24 h).

Wykonywanie zadań CPR wspomaga system teleinformatyczny, którego administratorem jest minister właściwy ds. administracji publicznej. System teleinformatyczny łączy się i wymienia dane z systemami teleinformatycznymi Policji, Państwowej Straży Pożarnej oraz dysponentów zespołów ratownictwa medycznego. Funkcjonalność systemu informatycznego pozwala również na wzajemne zastępowanie się CPR. Jeżeli z jakichś przyczyn (natłok zgłoszeń alarmowych po przejściu huraganu, wypadek masowy, awaria techniczna) operatorzy numerów alarmowych z CPR w jednym województwie nie są wstanie odebrać zgłoszeń alarmowych w ciągu 30 s, zgłoszenie takie trafia do wolnego operatora w innym województwie.

Według raportów ministra właściwego ds. administracji w latach 2014–2019 liczba wywołań alarmowych kierowanych do CPR oscylowała w granicy 20 mln każdego roku, z czego tylko ok. 20% kończyło się przekazaniem zgłoszenia do jednej z 3 podstawowych służb lub podmiotów wspomagających, tj. pogotowie gazowe,

energetyczne, straże miejskie, gminne (zob. → S t r a ż M i e j s k a / Gm i n n a [t. 4]) itp. Zdecydowana większość zgłoszeń alarmowych kierowana jest do CPR w tradycyjny sposób, tj. poprzez połączenie telefoniczne, niemniej przyjmowane są również zgłoszenia SMS-owe (od osób głuchoniemych) czy też z systemu e-Call.

Łukasz Szewczyk

Dyrektywa 2002/22/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników (dyrektywa o usłudze powszechnej); Dyrektywa Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r. zmieniająca dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów; B. Kogut, *Współczesność oraz perspektywy KRSG*, SA PSP w Krakowie, Kraków 2015; Raporty MSWiA z funkcjonowania systemu powiadamiania ratunkowego w Polsce w latach 2014, 2015, 2016, 2017, 2018; Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 28 kwietnia 2014 r. w sprawie organizacji i funkcjonowania centrów powiadamiania ratunkowego, Dz. U. 2014, poz. 574; Rozporządzenie Ministra Spraw Wewnętrznych i Administracji w z dnia 17 września 2007 r. w sprawie szczegółowej organizacji centrów powiadamiania ratunkowego, Dz. U. 2007, nr 178, poz 1263; Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 31 lipca 2009 r. w sprawie organizacji i funkcjonowania Centrów Powiadamiania Ratunkowego i Wojewódzkich Centrów Powiadamiania Ratunkowego, Dz. U. 2009, nr 130, poz. 1073; Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 grudnia 1999 r. w sprawie szczegółowych zasad organizacji krajowego systemu ratowniczo-gaśniczego, Dz. U. 1999, nr 111, poz. 1311; Ustawa z dnia 22 listopada 2013 r. o systemie powiadamiania ratunkowego, Dz. U. 2013, poz. 1635.

CENTRUM PRZYSZŁOŚCI WOJNY – (ang. Center on the Future of War) struktura działająca na Uniwersytecie Stanowym Arizony **(**aSU, ang. *Arizona State University*) i badająca społeczne, polityczne, gospodarcze i kulturowe konsekwencje zmieniające charakter → w o j e n [t. 4] i konfliktów.

Centrum ma na celu opisanie przyszłości działań wojennych w miarę ich ewolucji w ciągu najbliższych lat, przewidzenie ich prawdopodobnego wpływu na państwa i na inne formy organizacji społecznych oraz opracowanie nowych paradygmatów zrozumienia i rozwiązywanie konfliktów.

Centrum, stworzone w roku akademickim 2014/2015, łączy w zasadzie wszystkie wydziały ASU, kilkadziesiąt ośrodków i programów uniwersyteckich z ponad 30 stowarzyszonych ekspertów z „Nowej Ameryki" (New America) – niezależnej organizacji badawczej, ośrodkiem analitycznym, pionierem nowego rodzaju think and action tank: platformy obywatelskiej, która łączy instytut badawczy, laboratorium technologiczne, sieć rozwiązań, centrum mediów i forum publiczne. Dana organizacja prowadzi różnorodne badania, przygotowuje ekspertyzy, wydaje publikacje, zajmuje się tematyką szeroko rozumianego → b e z p i e c z e ń s t w a [t. 1]. Centrum ma siedzibę w Waszyngtonie w Szkole Polityki i Studiów Globalnych i łączy ASU

z decydentami i mediami krajowymi, organizuje wspólne projekty badawcze, tworzy raporty i publikacje oraz projektuje i wdraża innowacyjne programy edukacyjne.

W centrum zaprojektowano wspólny program bezpieczeństwa międzynarodowego „Inicjatywa przyszłości wojny proxy", badający rolę → w o j n y z a s t ę p c z e j [t. 4] w dzisiejszych konfliktach, a także sposoby, w jakie przeobrażają się → g l o b a l i z a c j a , postęp technologiczny, proliferacja → b r o n i m a s o w e g o r a ż e n i a [t. 1] i rozwój transnarodowych ruchów niepaństwowych. Wymaga to aktualizacji metod badawczych oraz samego rozumienia – przez decydentów i naukowców – charakteru wojny zastępczej i jej obecnych przejawów m.in. w Syrii, Libii, Jemenie, Iraku, Afganistanie i Ukrainie.

Ponadto przez centrum jest co roku organizowane Forum Bezpieczeństwa Przyszłości. Ostatnie odbyło się w dniach 13–14 września 2021 r. pt. „Redefinicja bezpieczeństwa narodowego w 2040 r." Uwagę skupiono tam na zagadnieniach ubiegłych 2 dekad amerykańskiej polityki bezpieczeństwa oraz nakreślono krajowe i międzynarodowe trendy w zakresie bezpieczeństwa na kolejnych 20 lat.

Forum jest najważniejszym dorocznym wydarzeniem projektu Future Security New America oraz Arizona State University – partnerstwa badawczego, edukacyjnego i politycznego, które opracowuje nowe paradygmaty zrozumienia i rozwiązywania globalnych wyzwań. Forum gromadzi przedstawicieli środowisk akademickich, rządu, wojska i mediów, aby omówić → b e z p i e c z e ń s t w o m i ę d z y n a r o d o w e [t. 1] oraz przedstawić trendy → b e z p i e c z e ń s t w a n a r o d o w e g o [t. 1] i międzynarodowego. Powstające technologie zmieniają charakter działań wojennych. Szybkie postępy w systemach bezzałogowych, robotyce, przetwarzaniu danych i innych technologiach wspomagających mają potencjał, aby pobudzić zupełnie nowy → r e ż i m [t. 3] wojenny. Zarówno podmioty państwowe, jak i niepaństwowe będą dążyć do wykorzystania tych i innych nowych technologii, z których wiele jest napędzanych przez innowacje sektora komercyjnego w zakresie technologii informatycznych.

Olga Wasiuta

Center on the Future of War, https://military.asu.edu/center-future-war (dostęp10.10.2021); *Center on the Future of War. Explores the Changing Nature of War and Conflict,* https://futureofwar.asu.edu/ (dostęp 10.10.2021); *Future of Proxy Warfare,* https://futureofwar.asu.edu/future-proxy-warfare (dostęp 10.10.2021); *Future of Warfare,* https://www.cnas.org/research/technology-and-national-security/defense-technology/future-of-warfare-1 (dostęp 10.10.2021); *Future Security Forum 2021,* https://futureofwar.asu.edu/conference/future-security-forum-2021 (dostęp 10.10.2021); *Future Security Forum 2021: Day One. 20x20: Redefining National Security for 2040,* https://www.newamerica.org/international-security/events/ future-security-forum-2021-day-1/ (dostęp 10.10.2021).

CENZURA – polega na ograniczaniu obiegu → i n f o r m a c j i [t. 2], idei i obrazów lub opinii politycznych, kulturowych, religijnych i artystycznych; występuje głównie wtedy, gdy rządzący uważają, że mogą one osłabić ich autorytet. Charakterystyczna

dla niedemokratycznych systemów politycznych, a także obecna w niektórych demokracjach, cenzura jest zazwyczaj stosowana przez organ odpowiedzialny za monitorowanie rozpowszechniania idei, w tym wypowiadanych przez ośrodki rządowe, ale przede wszystkim przez osoby prywatne i organizacje krytyczne wobec rządu. Termin „cenzura" ma swój początek w starożytnym republikańskim Rzymie, gdzie „cenzorem" była osoba, która kontrolowała rozpowszechnianie idei politycznych. Słowo „cenzura" wywodzi się z łacińskiego źródłosłowu *censeo* oznaczającego 'oszacować, ocenić, osądzić'. Cenzor był tytułem nadawanym 2 sędziom w starożytnym Rzymie, którzy byli odpowiedzialni za administrowanie spisem i nadzorowanie moralności publicznej. W okresie Świętego Cesarstwa Rzymskiego Kościół przejął główną odpowiedzialność za cenzurę. Obecnie istnienie internetu i wielu źródeł informacji utrudnia działanie cenzury, jednak coraz większą rolę odgrywa autocenzura, jednostki żyją także w → b a ń k a c h i n f o r m a c y j n y c h i ulegają efektowi komory pogłosowej (ang. *echo chamber*), w których docierają do nich wiadomości zgodne z ich poglądami i odczuciami.

Od czasów przednowoczesnych cenzura istniała w różnych → r e ż i m a c h [t. 3] politycznych. Zaczęła być kwestionowana w XVII w., kiedy krytycy absolutystycznych państw tego okresu zaczęli domagać się ograniczenia władzy państwowej i dyskrecji oraz instytucjonalizacji praw obywatelskich i politycznych, a zwłaszcza wolności słowa. Cenzura istniała również w instytucjach społecznych, takich jak Kościół katolicki, a także w innych religiach, takich jak islam. W tym przypadku wyższe szczeble hierarchii religijnej cenzurują, aby upewnić się, że treść pism księży i biskupów jest zgodna z głównymi zasadami religii.

Wczesny Kościół użył swego autorytetu do ustanowienia zasad wiary i tępienia herezji. Pismo Święte skodyfikowało zasady wiary chrześcijańskiej i zabezpieczyło ziemski autorytet Kościoła, ale duchowieństwo miało monopol na interpretację świętego tekstu. Nauczanie świeckich było prawie wyłącznie ustne. Z nielicznymi wyjątkami tylko osoby przystępujące do kapłaństwa miały zaawansowany poziom wykształcenia i dostęp do materiałów do czytania, które były przechowywane w klasztorach, zajmujących się zresztą rękopiśmiennym powielaniem ksiąg. Kościół zaczął katalogować zakazane teksty już w II w. Rozwój prasy Gutenberga w XV w. stanowił poważne wyzwanie dla władzy kościelnej. Druk ułatwił rozpowszechnianie heterodoksyjnych pomysłów, zwłaszcza reform protestanckich. Kościół odpowiedział poprzez stworzenie rozbudowanego systemu administracyjnego cenzury prewencyjnej, wymagano licencji na publikację (imprimatur, dosł. z łac. 'niech będzie odbite') i poświadczenia, że książka została zbadana przez miejscowego ordynariusza, zwykle biskupa. Kościół opublikował swój pierwszy indeks ksiąg zakazanych, znany jako *Indeks paulinów*, w 1559 r. *Indeks librorum prohibitorum* miał 42 edycje, zanim zaprzestano jego publikacji w 1966 r. Indeks stanowił najbardziej wszechstronny zapis cenzury, jaki kiedykolwiek powstał. Biurokracja cenzury państwowej dostosowała model administracyjny

wprowadzony przez Kościół, z jego władzą centralną i lokalnym egzekwowaniem. Tam, gdzie Kościół publicznie potępiał budzące sprzeciw pomysły, cenzura państwowa rutynowo działała potajemnie i otwarcie. → B e z p i e c z e ń s t w o n a r o d o w e , często kontrowersyjny konstrukt z ekspansywnymi granicami, stanowiło nierzadko uzasadnienie dla tajnej cenzury państwowej, zwłaszcza w czasie → w o j ny [t. 4], kiedy wszystkie państwa narodowe stosują zwykle cenzurę. Cenzura jest na ogół sprzeczna z demokracją, która charakteryzuje się instytucjonalizacją praw obywatelskich i politycznych, wolności obywatelskich oraz istnieniem opozycji. Chociaż wolność wypowiedzi jest centralną wartością demokratyczną, niektórzy przeciwnicy cenzury uznają wyjątki. Jednym z najczęściej proponowanych wyjątków jest pornografia dziecięca ze względu na jej związek z osobami lub organizacjami, które popełniają przestępstwa takie jak pedofilia. Zwolennicy cenzury w takich przypadkach twierdzą, że prawo do swobodnej wypowiedzi jest mniej ważne od potrzeby zapobiegania niezwykle szkodliwemu wpływowi na dzieci spowodowanemu tworzeniem i rozpowszechnianiem pornografii dziecięcej. Przeciwnie, krytycy cenzury w odniesieniu do pornografii dziecięcej twierdzą, że związek między pornografią a rzeczywistą krzywdą dzieci nie został ustalony. Chociaż niektórzy zwolennicy wolności słowa uważają, że ma ona pierwszeństwo przed obroną interesów dzieci, większość zachodnich demokracji zakazuje posiadania, produkcji i dystrybucji pornografii dziecięcej.

Mowa nienawiści jest kolejnym typem wypowiedzi, który prowokuje do dyskusji na temat cenzury. Także w tym przypadku zwolennicy twierdzą, że mowa pełna nienawiści zachęca do rzeczywistej → p r z e m o c y [t. 3] i że ta potencjalna szkoda przewyższa wartość wolności wypowiedzi. Na przykład takie argumenty uzasadniają cenzurę → p r o p a g a n d y [t. 3] neonazistowskiej (zob. → n e o n a z i z m [t. 3]) zarówno w USA, jak i w Europie.

Wykorzystanie cenzury może być postrzegane nie tylko w sposób formalny – to znaczy przez urzędników uprawnionych do kontrolowania informacji politycznych przy użyciu znanych środków politycznych – ale także poprzez mechanizmy nieformalne, takie jak grożenie niezależnym dziennikarzom, karanie prasy krytycznej poprzez odmowę zapłaty za reklamy czy groźbę redukcji popytu na nie. Owe nieformalne mechanizmy cenzury można znaleźć w młodych demokracjach ustanowionych po reżimach wojskowych lub autorytarnych, w których istnieją polityczne ograniczenia odziedziczone po uprzednim porządku politycznym ograniczającym instytucjonalizację praw politycznych lub spowodowanych brakiem demokratycznych przekonań wśród elity rządzącej. W demokracjach takich niekiedy elity nie uchylają ograniczeń poprzedniego reżimu dotyczących wolności prasy lub uznają, że cenzura jest w niektórych przypadkach konieczna ze względu na → b e z p i e c z e ń s t w o narodowe. W tym drugim przypadku jest to argument wykorzystywany do ograniczenia publikowania informacji o kwestiach uważanych za bardzo wrażliwe dla sił zbrojnych oraz do unikania ewentualnych napięć i zapewnienia konsolidacji demokracji. W nieskonsolidowanych

demokracjach lub reżimach hybrydowych cenzura urzędników zatrudnionych przez rządzących jest sprawowana za pomocą formalnych i nieformalnych mechanizmów, w tym grożenia dziennikarzom. Eliminacja cenzury jest jednym z priorytetowych wymogów związanych z procesem konsolidacji demokracji. W nieskonsolidowanych demokracjach, takich jak Wenezuela za czasów prezydentury H. Cháveza (u władzy od 1999 do 2013 r.), urzędnicy publiczni stosowali różne metody ograniczania wolności prasy, nie stosowali tylko do cenzury, lecz także podejmowali działania takie jak anulowanie licencji telewizyjnych i radiowych. Chociaż cenzura jest formalnie odrzucana w demokracjach, wolność słowa może być ograniczona nie jako decyzja rządzących, ale jako konsekwencja struktury własnościowej mediów, gdy ludzie biznesu starają się wpływać na → o p i n i ę p u b l i c z n ą [t. 3] swoimi przekonaniami lub poglądami politycznymi, odrzucając rozpowszechnianie przeciwnych stanowisk. W takich sytuacjach redaktorzy mogą stosować rozległą autocenzurę, aby zablokować rozpowszechnianie wiadomości i pomysłów, które mogą zaszkodzić rządowi.

Cenzura może być narzucona zapobiegawczo – poprzez określenie warunków rozpowszechniania i obiegu idei przez dowolny kanał – lub *ex post facto*, z organem sankcjonującym tych, którzy naruszają normy ustanawiające ograniczenia wolności słowa.

Chociaż cenzura jest niezgodna z demokracją, nie oznacza to, że urzędnikom publicznym brakuje środków, aby próbować przekonać media do blokowania wiadomości i informacji potencjalnie szkodliwych dla władzy lub faworyzowania treści o negatywnym wydźwięku dla opozycji. Jednym z tych kluczowych narzędzi jest umieszczanie opłacanych przez rząd lub spółki skarbu państwa reklam, które mogą być ważnym źródłem przychodów dla mediów, lub rezygnacja z tego.

Wraz z rozwojem nowoczesnej technologii, w szczególności internetu, narzucanie cenzury jest trudniejsze niż wcześniej dla urzędników publicznych, którzy chcą ograniczyć rozpowszechnianie informacji i wiadomości krytycznych dla rządu. Internet otworzył nowy kanał komunikacji dla dysydentów w niedemokratycznych reżimach (np. na Kubie i w Chinach), którzy za pośrednictwem sieci starają się potępiać nadużycia i ujawniać światu żądania pluralizmu i wolności. Działania te z kolei wywołują wsparcie ze strony organizacji pozarządowych i partii politycznych oraz rządów w krajach demokratycznych, co pomaga chronić autorów przed represjami. Duże międzynarodowe korporacje – zwłaszcza Google – pojawiły się również jako nowi gracze na rzecz większego pluralizmu w niedemokratycznych reżimach lub nieskonsolidowanych demokracjach.

Cenzura odgrywa bardzo ważną rolę w reżimach autorytarnych. Służy jako narzędzie zapewniające, że ograniczony pluralizm – centralny element ich tożsamości – pozostaje w granicach ustalonych przez władze. Reżimy te pozwalają niektórym sektorom na elitarny dostęp, a nawet kontrolę nad mediami i wydawnictwami, poprzez które dążą do zdobycia władzy politycznej lub wpływów, a jednocześnie ograniczają

dostęp tym częściom elity, które cieszyły się specjalnymi względami wcześniej. Autocenzura jest powszechnie stosowana w tych reżimach przez redaktorów prywatnych firm medialnych, którzy wspierają reżim, są zainteresowani jego ciągłością i zwracają szczególną uwagę na zapobieganie publikowaniu negatywnych wiadomości, zwłaszcza dotyczących działań opozycyjnych lub konfliktów i podziałów w ramach elit rządzących.

Władza F. Franco w Hiszpanii (1939–1975) stanowi przykład ewolucji cenzury, która nie była stosowana jednolicie podczas jego reżimu, ale uległa wielu zmianom w wyniku konfliktów między frakcjami elity rządzącej, które miały większy wpływ, gdy reżim został skonsolidowany. Wraz z konsolidacją władzy politycznej oraz w kontekście rozwoju gospodarczego i postępu społecznego pojawiła się tendencja do rozluźniania cenzury, aby umożliwić prasie odgrywanie roli w kontrolowaniu ekscesów, nadużyć władzy, a zwłaszcza → k o r u p c j i [t. 2] wśród najwyższych urzędników. Zmiany wprowadziła także ustawa prasowa z 1966 r., która rozpoczęła pewną liberalizację oficjalnej prasy i przyniosła większą przejrzystość decyzji władz. Jednak informacje dotyczące nadużywania władzy, zwłaszcza o charakterze gospodarczym, były wykorzystywane przez sektory elity rządzącej do osłabienia pozycji władzy innych frakcji, prowokując skandal, który doprowadził do zmian w gabinecie i zwolnienia ministrów zaangażowanych w ten konflikt. Pozwoliło to jednak na pojawienie się publikacji opozycyjnych, a nawet czasopism (np. „Cuadernos para el Diálogo"), które osłabiły reżim i przyniosły znaczny wzrost liczby negatywnych informacji politycznych, np. przez publikację informacji o przypadkach korupcji i konfliktów w ramach rządu i elity władzy. W wyniku tych bezpośrednich i pośrednich skutków liberalizacji prasy cenzura została w praktyce przywrócona.

Liberalizacja reżimów autorytarnych zawsze oznaczała rozluźnienie cenzury i autocenzury, jak w reżimie Pinocheta w Chile (1973–1990) w okresie niestabilności politycznej spowodowanej → k r y z y s e m [t. 2] gospodarczym w latach 1983–1984. Niezależne radiostacje i czasopisma mogły w szerszy sposób informować o kilku ocenionych wcześniej politycznych faktach, w tym represjach wobec organizacji opozycyjnych. Jednak rząd nadal groził dziennikarzom i karał ich poprzez formalne i nieformalne mechanizmy oraz stosował cenzurę w określonych przypadkach. Przestrzeń polityczna otwarta przez osłabienie cenzury była szeroko wykorzystywana przez dziennikarzy i media, co prowadziło do znacznego wzrostu informacji politycznych, w tym informacji negatywnych, i sprzyjała rozwojowi opozycji, a w rezultacie osłabieniu politycznych podstaw autorytarnego rządu.

Cenzura może przynosić także szerokie konsekwencje dla tych, którzy się jej przeciwstawiają, zwłaszcza w islamie. W fundamentalistycznych teokracjach (→ f u n d a m e n t a l i z m r e l i g i j n y [t. 2]) władza jest absolutna, a jej zakres może wykraczać poza zwykłą ekskomunikę. Tak było, gdy ajatollah Chomeini z Iranu wydał fatwę skazującą na śmierć urodzonego w Indiach autora S. Rushdiego, który nie

jest praktykującym muzułmaninem, za krytyczną i bluźnierczą w stosunku do islamu książkę z 1988 r. *Szatańskie wersety*. Fatwa zobowiązywała wszystkich wiernych muzułmanów do wykonania wyroku, zmuszając Rushdiego do wieloletniego ukrywania się. Japoński tłumacz książki H. Igarashi został zamordowany, a włoski tłumacz autora i jego norweski wydawca doznali poważnych obrażeń, gdy zostali pchnięci nożem przez napastników wykonujących rozkazy fatwy. Inni, w tym urodzony w Egipcie autor nagrodzony Nagrodą Nobla w dziedzinie literatury N. Mahfuz, również otrzymali groźby śmierci za obronę prawa Rushdiego do wolności wypowiedzi. Odrodzeniu i upolitycznieniu fundamentalistycznych form islamu po rewolucji irańskiej w 1979 r. towarzyszyło ściślejsze egzekwowanie kodeksów moralnych i przywracanie lub wzmacnianie cenzury. W Iranie cenzura zaostrzyła się dramatycznie od 2005 r., gdy obowiązywać zaczęły nowe ograniczenia wobec wydawnictw książkowych, filmów i przedstawień teatralnych oraz niektórych gazet. Prześladowaniami zostali dotknięci nawet posiadacze anten satelitarnych na dachach. Ministerstwo, które od wielu lat blokowało dostęp do wielu internetowych serwisów informacyjnych, w 2006 r. wprowadziło nowe środki mające na celu kontrolowanie blogerów. Rząd postawił również zarzuty dziennikarzom za zamieszczanie postów na stronach internetowych.

Ponieważ telewizja satelitarna i internet sprawiły, że coraz częściej można obejść cenzury krajowe, reakcje międzynarodowe stały się coraz bardziej powszechne. Represje obraźliwych form wyrazu przybrały także nowe, pozaprawne formy poprzez międzynarodowe protesty, w tym gwałtowne, jak np. gdy duńska gazeta „Jyllands-Posten" opublikowała serię satyrycznych rysunków wyśmiewających proroka Mahometa pod koniec 2005 r., a niektóre z nich zostały przedrukowane i potępione jako rasistowskie w egipskiej gazecie „Al Fagr". W ciągu następnych kilku miesięcy wywołało to światowe protesty i kontrprotesty, w tym gwałtowne konflikty w Libii, Pakistanie, Afganistanie, Nigerii i Somalii, w których zginęło co najmniej 139 osób, a ranne zostały 823. Redaktor duńskiej gazety przeprosił za opublikowanie rysunków.

Podczas gdy w zachodnich państwach demokratycznych nadal trwają debaty o zniesieniu wszelkich form cenzury, koncentrujące się na tym, w jakim stopniu dopuszczalne są ograniczenia dotyczące zniesławienia, prywatności i poufnych informacji, reżimy autorytarne w Chinach i Arabii Saudyjskiej stosują jedne z najbardziej rygorystycznych form administracyjnej cenzury. W ciągu ostatnich lat oba państwa rozszerzyły stosowanie ograniczeń wstępnych na jedną z najbardziej aktualnych metod publicznego rozpowszechniania informacji, czyli internet. W grudniu 2000 r. chiński rząd przyjął szereg rozwiązań detalicznie wyliczających, dlaczego i jak cenzurowany będzie internet. Stworzono ogólnokrajową zaporę, która blokuje tysiące stron internetowych, uznanych przez rząd za nieodpowiednie. Używając krajowego oprogramowania, Chiny filtrują nie tylko materiały erotyczne, ale także strony internetowe, które uważają za wrażliwe politycznie, takie jak strony zagranicznych organizacji → p r a w c z ł o w i e k a [t. 3], niektóre organizacje informacyjne i strony związane

z Tajwanem, Tybetem, ruchem Falun Gong oraz dysydentami i ruchami prodemokratycznymi.

Podobnie rząd saudyjski ustanowił najszerszy i najbardziej zaawansowany technologicznie system filtrowania na świecie, aby blokować cały materiał online, o którym rodzina rządząca twierdzi, że jest sprzeczny z obyczajami i wartościami muzułmańskich Arabów. Organ rządowy wykorzystuje wyspecjalizowany sprzęt proxy, który przetwarza wszystkie żądania stron internetowych z kraju i porównuje je z czarną listą zabronionych witryn. Jeśli żądana witryna znajduje się na czarnej liście, dostęp do niej jest blokowany. Czarne listy są nabywane od firm komercyjnych i odnawiane w sposób ciągły. Oprócz komercyjnych czarnych list saudyjscy cenzorzy wskazują także inne strony internetowe, które uznają za nieodpowiednie. Internet, który w państwach zachodnich stanowi autonomiczne źródło informacji i cyrkulacji opinii, będące antytezą cenzury, w państwach rządzonych autorytarnie podlega najdalej idącym działaniom cenzorskim.

Jakub Idzik, Rafał Klepka

S. Ahmed, *Censorship*, [w:] *The International Encyclopedia of Communication*, W. Donsbach (ed.), Blackwell Publishing, Malden–Oxford–Carlton 2015; J. Green, N.J. Karolides, *Encyclopedia of Censorship*, Facts on File, New York 2005; C. Huneeus, *Censorship*, [w:] *International Encyclopedia of Political Science*, B. Badie, D. Berg-Schlosser, L. Morlino (eds.), Sage, Los Angeles 2011; J. Idzik, R. Klepka, *Cenzura*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; S.C. Jansen, *Censorship, History of*, [w:] *The International Encyclopedia of Communication*, W. Donsbach (ed.), Blackwell Publishing, Malden–Oxford–Carlton 2015; D. Jones, *Editor's note*, [w:] *Censorship: A World Encyclopedia*, D. Jones (ed.), Taylor & Francis Group, London–New York 2001; R. Klepka, *Medialna stronniczość polityczna jako nowa forma cenzury: przypadek Wiadomości TVP*, [w:] *Cenzuro wróć? Mechanizmy ograniczania wolności słowa w Polsce po 1990 roku*, Z. Romek, K. Kamińska-Chełminiak (red.), ASPRA-JR, Pułtusk–Warszawa 2018; D. Robertson, *The Routledge Dictionary of Politics*, Routledge, London–New York 2003; D. Welch, *Censorship*, [w:] *Propaganda and Mass Persuasion. Historical Encyclopedia 1500 to the Present*, N. Cull, D. Culbert, D. Welch (eds.), ABC-CLIO, Santa Barbara–Denver–Oxford 2003.

CHIŃSKI WIELKI PODWODNY MUR (Underwater Great Wall, UGW) – projekt realizowany przez przedsiębiorstwo China State Shipbuilding Corporation (CSSC) od 2015 r. W jego ramach powstaje system obserwacyjny na Morzu Południowochińskim, umożliwiający lokalizowanie i śledzenie w czasie rzeczywistym celów nawodnych i podwodnych. System ma składać się z: okrętów nawodnych i podwodnych, bezzałogowych statków podwodnych, sieci sonarów, urządzeń służących do poszukiwania ropy i gazu oraz różnego rodzaju sensorów. Jest on określany także jako zaawansowana wersja amerykańskiego Sound Surveillance System, który używany był przez → Marynarkę Wojenną Stanów Zjednoczonych w czasie → zimnej wojny [t. 4] do wykrywania okrętów podwodnych Związku Radzieckiego. W wypadku Chin UGW będzie pełnić następujące funkcje:

- obserwacja oceanów – monitorowanie ruchu okrętów podwodnych i nawodnych na obszarze Morza Południowochińskiego;
- monitorowanie stanu środowiska naturalnego – obserwacja i analiza stanu zanieczyszczenia wody, w tym skażenia chemicznego, biologicznego i jądrowego. Sieć czujników ma umożliwiać także określenie kierunków prądów oceanicznych, wiatrów, dokładniejsze przewidywania pogody oraz zmian klimatycznych;
- reagowanie na → k l ę s k i ż y w i o ł o w e [t. 5] – informowanie → l u d n o ś c i c y w i l n e j [t. 3] zamieszkującej wschodnie wybrzeże Chin o zbliżających się niebezpieczeństwach, takich jak: tajfuny, trzęsienia ziemi i tsunami;
- nadzór taktyczny – rozpoznanie, wykrywanie, namierzanie i klasyfikacja celów o niskiej sygnaturze, które weszły w obszar chińskich wód terytorialnych;

Chiński Wielki Podwodny Mur jest zatem projektem wielowymiarowym, który ma na celu ochronę państwa przed → z a g r o ż e n i a m i [t. 4] od strony morza, o charakterze zarówno militarnym, jak i niemilitarnym. Nie jest on pierwszym systemem monitorowania Morza Południowochińskiego. Pierwszy system rozpoznania optycznego uruchomiony został w 2010 r. w pobliżu miasta Qingdao, gdzie znajduje się dowództwo Floty Północnej. Drugi został zbudowany w pobliżu wyspy Hajnan w 2011 r. Systemy te składały się ze stacji brzegowej, kabli optycznych, stacji przyłączeniowej i rozdzielni, zestawów sensorów obserwacyjnych oraz węzłów obserwacyjnych. Obecnie rozwijany UGW ma podobną strukturę. Tworzy go kilka komponentów: naziemny w postaci stacji brzegowych, umieszczone ok. 2 tys. m pod wodą stacje badawcze, sensory (bezzałogowe statki podwodne) oraz czujniki monitorujące ruchy sejsmiczne Ziemi.

Nie wiadomo, w którym dokładnie miejscu Morza Południowochińskiego powstaną elementy systemu. Zdaniem części obserwatorów projekt dzięki swoim zasięgom będzie zdecydowanie wykraczał poza wody znajdujące się pod jurysdykcją Chin i obejmie obszary ważne z punktu widzenia interesu tego państwa. Mowa tutaj o Oceanie Indyjskim i zachodnim Pacyfiku. Z punktu widzenia Waszyngtonu oraz sojuszników amerykańskich w Azji Południowo-Wschodniej najistotniejszą kwestią jest militarne wykorzystanie systemu. Wojskowi obu stron zdają sobie sprawę z faktu, że kluczową rolę w → k o n f l i k c i e z b r o j n y m [t. 5] na zachodnim Pacyfiku odegrają okręty podwodne. Okręty nawodne oraz lotniska narażone będą na zniszczenie przez → p o c i s k i b a l i s t y c z n e [t. 5] i → p o c i s k i m a n e w r u j ą c e [t. 5]. W związku z powyższym kluczowe z punktu widzenia Pekinu wydaje się rozwijanie floty okrętów podwodnych oraz systemu monitorującego Morze Południowochińskie i zachodni Pacyfik.

Według dostępnych danych z marca 2023 r. mimo dynamicznego rozwoju chińskiej → m a r y n a r k i w o j e n n e j [t. 3] Stany Zjednoczone wciąż mają znaczną przewagę. Potencjał amerykańskich okrętów podwodnych składa się z 4 klas operacyjnych: Ohio, Los Angeles, Seawolf i Virginia. Wszystkie napędzane są energią

jądrową. Okręty typu Ohio są jednym z elementów triady nuklearnej, przenoszą pociski balistyczne z głowicami atomowymi. Trzy pozostałe klasy mają za zadanie atakować i niszczyć wrogie statki, wspierać operacje → w o j s k l ą d o w y c h [t. 4] oraz prowadzić obserwacje. Łącznie USA mają 64 okręty podwodne.

Trzonem chińskiej floty okrętów podwodnych są wciąż jednostki z silnikiem Diesla. Szacuje się, że jest ich 44. Ponadto jest to 6 okrętów wyposażonych w pociski balistyczne (SSBN) oraz 6 okrętów o napędzie atomowym. Łącznie ChRL ma 56 okrętów podwodnych. Przewagę amerykańską Chińczycy zamierzają neutralizować m.in. za pomocą bezzałogowych statków podwodnych (zdalnie sterowanych i autonomicznych) – integralną część budowanego systemu. Początki rozwoju podwodnych dronów (UUV) sięgają w Chinach lat 80. XX w. W 1986 r. ówczesny premier Zhao Ziyang zainicjował przyjęcie Krajowego Planu Rozwoju Zaawansowanych Technologii, określanego również jako plan 863. W 1996 r. dokument rozszerzono, dodając do niego technologie morskie, w tym pojazdy podwodne. Od tej pory prace nad rozwojem UUV koncentrują się w Chinach wokół 3 ośrodków badawczych: Instytutu Automatyki Shenyang, China Shipbuilding Industry Corporation oraz Politechniki w Harbinie.

Szacuje się, że w 2019 r. na 40 uczelniach realizowanych było 159 projektów badawczych dotyczących rozwoju bezzałogowych pojazdów podwodnych. Mimo że większość z nich znajduje się na wczesnym etapie opracowań naukowych, wszystko wskazuje na to, że → M a r y n a r k a W o j e n n a C h i ń s k i e j A r m i i L u d o w o - W y z w o l e ń c z e j [t. 5] zainteresowana jest wykorzystaniem UUV w obszarze:

- obserwacji oceanów i taktycznego nadzoru;
- walki minowej;
- nadzoru kabli morskich;
- walki z okrętami podwodnymi.

W zakresie monitorowania oceanów oraz nadzoru taktycznego wykorzystywane są → d r o n y [t. 2]: Sea Wing (Skrzydło Morskie), Sea Swallow (Jaskółka Morska) oraz Sea Flyer (Lotnik Morski). Sea Wing opracowany został przez Instytut Oceanologii Chińskiej Akademii Nauk. Oficjalnie służył do badań oceanograficznych dzięki czujnikom pomiaru temperatury wody morskiej, zasolenia, zawartości tlenu czy zdolności do analizy zmian prądów morskich. W 2014 r. przeszedł 30-dniowy test na Morzu Południowochińskim, w czasie którego przepłynął dystans 1022,5 km. → I n f o r m a c j e [t. 2] dotyczące pozostałych dwóch maszyn są szczątkowe.

Kolejną możliwością wykorzystania UUV jest minowanie i przeciwdziałanie minom morskim. Chińska marynarka wykorzystuje w tym obszarze m.in. HSU-001, Qianlong 1, 2 i 3 czy maszyny z serii Haishen. HSU-001 zaprezentowany został w 2019 r. na paradzie wojskowej z okazji 70. rocznicy powstania państwa. Biorąc pod uwagę jego duży rozmiar, należy przypuszczać, że poza minowaniem będzie wykorzystywany do prowadzenia patroli morskich na dalekich dystansach. W kadłubie maszyny

znajdują się silniki odrzutowe pozwalające jej unosić się pionowo, jak również na boki. Duży sonar z kolei ma umożliwiać wykrywanie celów podwodnych. Najnowsza maszyna serii Qianlong wyglądem przypomina rybę. Oficjalnie wykorzystywana jest do badania dna morskiego, jego zasobów naturalnych i energetycznych. Pod wodą może przebywać wiele dni, operując na głębokości 4,5 tys. m (ok. 14,8 tys. stóp). Bezzałogowy statek podwodny Haishen, określany także jako Poseidon 6000, ma 7,6 m długości, 3 t wyporności oraz może zanurzyć się na głębokość 6 tys. m. Rozwija prędkość do 4 węzłów, a liczne czujniki na pokładzie pozwalająmu na wykrywanie min i torped.

Jeśli chodzi o nadzór nad kablami morskimi z użyciem UUV, to polega on z jednej strony na ich naprawie, z drugiej – na ich niszczeniu. Do niedawna Pacyfik pod względem ilości kabli morskich przypominał „strefę tranzytową", w której największe gospodarki zlokalizowane na obrzeżach Oceanu Spokojnego budowały system kabli punkt-punkt, aby zapewnić wzajemne połączenia międzysieciowe. Główne węzły kablowe znajdowały się na zachodnim wybrzeżu Stanów Zjednoczonych, w Japonii, Hongkongu oraz w Singapurze. Był to zatem obszar 2 prędkości, w którym duże gospodarki były połączone za pomocą → p o d m o r s k i e j k a b l o w e j i n f r a s t r u k t u r y i n t e r n e t o w e j o dużej przepustowości i niskim opóźnieniu, a wszystkie pozostałe musiały korzystać z satelitów geostacjonarnych. W ostatnich latach doszło jednak do „wypełniania" luki i montażu kabli, które połączyły mniej zamożne państwa. Obecnie największymi węzłami łączności kablowej są Hongkong, Singapur i Japonia. Ponadto wiele kabli znajduje się na dnie Morza Południowochińskiego i w cieśninie Luzon. Szczególnie narażone na ataki ze strony chińskich podwodnych dronów są kable znajdujące się na północ od Tajwanu. Mają one kluczowe znaczenie w ramach bieżącej wymiany danych oraz dostępu do internetu.

Przykładem UUV, który w przyszłości może pojawić się w Chinach, jest opracowany przez firmę Kawasaki SPICE (Subsea Precise Inspector with Close Eyes) – autonomiczny dron poruszający się na głębokości 3 tys. metrów. W przeciwieństwie do wyprodukowanych wcześniej zdalnie sterowanych pojazdów typu ROV nie musi być połączony kablem ze statkiem macierzystym. Dzięki temu może poruszać się na znacznie większym obszarze. W przedniej części maszyny znajduje się jego ramię, za którego pomocą może sprawdzać podmorskie kable i rurociągi, by wykryć na nich uszkodzenia. Porusza się ze średnią prędkością 2 węzłów na godzinę, a jego praca może być wykonywana przez nieprzerwanie długi czas ze względu na możliwość ładowania na morzu. Kiedy pojawia się taka potrzeba, SPICE powraca do stacji dokującej i po naładowaniu może kontynuować działanie.

Wykorzystanie UUV do walki z okrętami podwodnymi znajduje się obecnie w fazie koncepcyjnej. Wszystko wskazuje jednak na to, że w przyszłości podwodne statki bezzałogowe zostaną uzbrojone i zmodernizowane do wersji umożliwiających zatapianie okrętów podwodnych przeciwnika. Wśród możliwych maszyn, które staną się uzbrojoną wersją UUV, wymienia się HSU-001, Haishen 6000, czy Sea Whale 2000

(Wieloryb). Jak zauważył Ryan Fedasiuk w opracowaniu dla Center for International Maritime Security, chińskie przedsiębiorstwa i ośrodki badawcze zajmujące się produkcją bezzałogowych pojazdów podwodnych napotykają znaczne bariery, co opóźnia budowę okrętów i tym samym powstanie wielkiego podwodnego muru. Do najważniejszych przeszkód zaliczył żywotność baterii umożliwiających wykonywanie zadań – poniżej 24 h, → s z t u c z n ą i n t e l i g e n c j ę [t. 4] – będącą wciąż technologią „wschodzącą", systemy rozpoznawania celów pod wodą – wciąż niewystarczająco dokładne, oraz biurokratyczny bezwład będący konsekwencją kultury centralnego planowania.

Tomasz Wójtowicz

China Submarine Capabilities, 6.03.2023, https://www.nti.org/analysis/articles/ china-submarine-capabilities/ (dostęp 6.04.2023); R. Fedasiuk, *How China isMilitarizing Autonomous Underwater Vehicle Technology*, 22.08.2021, https://www. jura.lt/en/internet-publications/11146-how-china-is-militarizing-autonomous-underwater-vehicle-technology (dostęp 9.04.2023); tenże, *Leviathan Wakes: China's Growing Fleet of Autonomous Undersea Vehicles*, 17.08.2021, https://cimsec.org/ leviathan-wakes-chinas-growing-fleet-of-autonomous-undersea-vehicles/ (dostęp 10.04.2023); G. Huston, *The Politics of Submarine Cable in the Pacific*, 5.06.2022, https://circleid.com/posts/20220605-the-politics-of-submarine-cable-in-the-pacific (dostęp 4.04.2023); P.C. Katoch, *New Chinese Drones – Formidable Challenge*,4.07.2018, https://www.sps-aviation.com/experts-speak/?id=310&h=New-Chinesedrones-formidable-challenge (dostęp 12.04.2023); D. Tsering, *China's 'Undersea Great Wall' Project: Implications*, National Maritime Foundation, 9.12.2026, https://www.maritimeindia.org/View%20Profile/636168593758883600.pdf (dostęp 4.04.2023); *Underwater Robots for Inspection of Pipelines*, November 2021, https://www.gov-online.go.jp/eng/publicity/book/hlj/html/202111/202111_10_en.html (dostęp 2.04.2023); *United States Submarine Capabilities*, 6.03.2023, https://www. nti.org/analysis/articles/united-states-submarine-capabilities/ (dostęp 5.04.2023); J.R. Wilson, *Unmanned Submarines Seen as Key to Dominating the World's Oceans*,15.10.2019, https://www.militaryaerospace.com/unmanned/article/14068665/ unmanned-underwater-vehicles-uuv-artificial-intelligence (dostęp 11.04.2023).

CHMURA OBLICZENIOWA – dostarczanie usług polegające na zdalnym udostępnieniu mocy obliczeniowej urządzeń (w tym – serwerów), baz danych, sieci, oprogramowania, za pośrednictwem internetu, w celu zaoferowania szybszych innowacji, elastycznych zasobów i ekonomii skali. Jest to pula współdzielonych, dostępnych „na żądanie" przez sieci teleinformatyczne, konfigurowalnych zasobów obliczeniowych (np. sieci, serwerów, pamięci masowych, aplikacji, usług), które mogą być dynamicznie dostarczane lub zwalniane przy minimalnych nakładach pracy zarządczej i przy minimalnym udziale ich dostawcy.

Dane są zarządzane na zdalnych serwerach obsługiwanych przez zewnętrznych dostawców. Idea *cloud* zakłada przechowywanie danych,plików oraz aplikacji na serwerach rozmieszczonych po całym świecie, poza lokalną siecią. Za utrzymanie infrastruktury jest odpowiedzialny administrator. Definicja chmury obliczeniowej wciąż ewoluuje.

Skąd wzięła się metafora „chmury"? Zamiast próbować uchwycić i nazwać wszystkie elementy, które tworzą sieć, podjęto starania w kierunku stworzenia symbolu obrazującego zbiór urządzeń. Dodatkowo, chmura była stosunkowo łatwa do ręcznego naszkicowania, przez co szybko można było zilustrować elementy połączone z siecią.

U progu XXI w. chmura obliczeniowa wyłoniła się jako interesującanowa technologia, której rozwojem i potencjałem zaczęli interesować się badacze i specjaliści IT z całego świata. Pierwsza wzmianka o chmurze pojawiła się w latach 90. XX w., ale już wcześniej inżynierowie używali chmury do oznaczenia sieci. Jak wskazuje Anders Lisdorf, pierwszy raz termin *chmura* pojawił się publicznie w 1994 r. w magazynie „Wired". Artykuł dotyczył firmy o nazwie General Magic, a jego autorem był Steven Levy, amerykański dziennikarz. Słowo *chmura* nie zostało od razu przyjęte przez → o p i n i ę p u b l i c z n ą [t. 3]. Dopiero w 1996 r. Compaq, amerykańskie przedsiębiorstwo komputerowe, umieściło je w swoim wewnętrznym regulaminie i zbudowało strategię dla swojej firmy, opartą na założeniu, że w niedalekiej przyszłości oprogramowania biznesowe i przechowywanie plików zostaną przeniesione do internetu. W 1997 r. określenia *chmura* użył Ramnath K. Chellappa w artykule pt. *Intermediaries on Cloud Computing*.

W 2006 r., kiedy Eric Schmidt, ówczesny dyrektor generalny Google, przedstawił ten termin na konferencji poświęconej strategiom wyszukiwarek, „chmura" osiągnęła najwyższy poziom zainteresowania w historii. Rok później, artykuł pt. *IBM to Push 'Cloud Computing' using Data from Afar* w „The New York Times" ugruntował termin w opinii publicznej. Od tego czasu użycie metafory chmury, podobnie jak sama branża, nabrało tempa. Pierwsze tego typu rozwiązania pozwalały firmom korzystać z oprogramowania, które nie było zainstalowane na ich serwerach. Obecnie „usługi chmurowe" są powszechnie dostępne także dla użytkowników indywidualnych.

Wyróżnia się:

1) **chmury publiczne** – oferujące swoje usługi pełnej gamie klientów. Publiczny charakter funkcjonowania tego modelu jest podobny do działania internetu – dlatego że użytkownicy i usługi mogą znajdować się w dowolnym miejscu w sieci WWW. Środowisko komputerowe jest udostępniane wielu najemcom w modelu darmowym lub płatnym, ale w wysokości zależnej od zużycia. Chmura znajduje się w posiadaniu dostawcy usług chmury obliczeniowej lub jest przez niego bezpośrednio zarządzana. Korzystanie z chmury o charakterze publicznym rodzi → z a g r o ż e n i a [t. 4] związane z → b e z p i e c z e ń s t w e m [t. 1] danych gromadzonych przez instytucje publiczne, często przechowywanych na serwerach poza granicami państwa. Jak wskazują Katarzyna Śledziewska i Renata Włoch: „państwa zaczynają myśleć o nowym wymiarze suwerenności – suwerenności danych, opartej na założeniu, że → i n f o r m a c j e [t. 2] powinny być przetwarzane i przechowywane w tym samym kraju, w którym zostały wytworzone".

2) **chmury prywatne** – ograniczają swoich użytkowników do wybranego podzbioru, zwykle do konkretnej organizacji, w ramach danej firmy. Chmura prywatna działa na podobnej zasadzie co intranet: usługi są świadczone wewnętrznie za pośrednictwem wewnętrznej organizacji sieci;
3) **chmury hybrydowe** – oferują swoje usługi wąskiej grupie prywatnych użytkowników, którą w razie potrzeby można rozszerzyć. Składają się z połączenia 2 lub więcej osobnych chmur obliczeniowych (publicznej, prywatnej, społecznościowej), a poprzez standaryzację użycia lub odpowiednią technologię możliwe jest przenoszenie czynności przetwarzania informacji między chmurami obliczeniowymi, które ją tworzą.

Tabela 1. Podstawowe rodzaje usług chmurowych

Rodzaj usługi	Dostęp do:
Infrastruktura traktowana jako usługa (ang. *Infrastructure as a Service*, IaaS)	przestrzeni dyskowej i mocy obliczeniowej; zapewnienie bezpośredniego dostępu do zwirtualizowanego lub skonteneryzowanego sprzętu. Przykłady dostawców: AWS EC2 (Elastic Compute Cloud), OpenStack, Eucalyptus, CloudFiles Rackspace.
Platforma jako usługa (ang. *Platform asa Service*, PaaS)	wachlarza aplikacji i oprogramowania. Przykłady dostawców: AppEngine firmy Google, Microsoft Azure.
Software jako usługa (ang. *Software asa Service*, SaaS)	konkretnego oprogramowania; skoncentrowany na użytkownikach końcowych Przykłady dostawców: Google.com, Gmail.
Komunikacja jako usługa (ang. *Communications as a Service*, CaaS),	rozwiązań komunikacyjnych.
Platforma integracyjna jako usługa (ang. *Integration Platform as a Service*, IPaaS).	infrastruktury integrującej programy i aplikacje działające w różnych środowiskach operacyjnych.

Źródło: K. Śledziewska, R. Włoch, *Gospodarka cyfrowa. Jak nowe technologie zmieniają rząd*, s. 39, https://www.delab.uw.edu.pl/wp-content/uploads/2020/04/Katarzyna-%C5%9Aledziewska-Renata-W%C5%82och-Gospodarka-cyfrowa.pdf (dostęp 16.10.2021); N.K. Sehgal, P. Chandra, P. Bhatt, *Cloud Computing: Concepts and Practices*, Springer, Cham 2018.

Do zalet korzystania z chmury obliczeniowej można zaliczyć: skalowalność, pełną dostępność, ograniczenie kosztów, wysoki poziom bezpieczeństwa, wydajność, szybkość, produktywność i niezawodność.

Ryzyko korzystania z chmury obliczeniowej przekłada się m.in. na utratę bezpośredniej wiedzy i kontroli nad podstawowym sprzętem, na trudności w zdiagnozowaniu problemów z wydajnością ze względu na ograniczoną widoczność i wirtualizację, jak również na potencjalne zagrożenia bezpieczeństwa związane z umieszczaniem wrażliwych danych na zdalnych serwerach.

Przykłady usług w chmurze, które mogą być obecnie oferowane przez dostawców, to: przesyłanie strumieniowe audio i wideo, dostarczanie oprogramowania na żądanie, analiza danych, przechowywanie danych i odzyskiwanie kopii zapasowych.

W ostatnim czasie powstało wiele regulacji dotyczących przetwarzania w chmurze, mających na celu głównie ujednolicenie standardów oraz zminimalizowanie zagrożeń. Przykładowo: 19 lutego 2020 r. Komisja Europejska opublikowała **Europejską strategię danych** (ang. *European Data Strategy*), w której znalazły się zapisy dotyczące chmury obliczeniowej. W dokumencie czytamy, że Unia Europejska jest w dużym stopniu zależna od dostawców zewnętrznych, podatna na zewnętrzne zagrożenia danych i narażona na utratę potencjału inwestycyjnego dla europejskiego przemysłu cyfrowego na rynku przetwarzania danych. Autorzy → s t r a t e g i i [t. 4] wskazują, że cyfrowa transformacja gospodarki UE jest uzależniona od dostępności bezpiecznych, energetycznie efektywnych (np. przejście wyłącznie na „zielone" źródła energii), jakościowo najlepszych metod przetwarzania danych, w tym – poprzez chmurę obliczeniową.

Unia Europejska chce uniezależnić się od zewnętrznych dostawców. Dla KE bezpieczeństwo danych to lokalizacja w UE, a zależność od zewnętrznych dostawców jest zagrożeniem. Celem jest połączenie potencjału w europejskiej chmurze obliczeniowej. Inne unijne inicjatywy związane z chmurą obliczeniową dotyczą m.in. swobodnego przepływu danych oraz ich przenoszenia i ochrony, certyfikacji dostawców usług chmurowych oraz ustandaryzowanych umów o poziomie usług w chmurze (SLA).

W maju 2021 r. 27 firm technologicznych przedstawiło Komisji Europejskiej tzw. mapę drogową, czyli plan działań zawierający priorytety inwestycyjne, które wzmocnią pozycję Europy w *cloud* oraz w *edge computingu*. Budżet na realizację planu oszacowano na 19 mld euro. Plan złożony w Komisji Europejskiej określa 3 priorytetowe obszary, wymagające wspólnych działań i strategicznych inwestycji:

1) przywództwo europejskie i rozwój kompetencji w obszarach znacząco wpływających na globalny rynek usług chmury obliczeniowej i obliczeń brzegowych;
2) stworzenie nowoczesnej europejskiej infrastruktury chmurowej i obliczeń brzegowych;
3) stworzenie warunków do realizowania specyficznych usług branżowych, aby lokalne firmy mogły konkurować na globalnym rynku pod względem usług, standardów, bezpieczeństwa oraz ceny.

Firmy, które współpracowały w opracowaniu planu działań europejskiego rozwoju nowej generacji usług chmurowych, to: 3DS Outscale, Airbus, Amadeus, Aruba, Atos, Capgemini, CloudFerro, DE-CIX, Deutsche Telecom, Ericsson, German Edge Cloud, GIGAS, Indra, IONOS, IRIDEOS, Leaseweb Global, Magic Cloud, Nabiax, Nokia, Orange, OVHcloud, Retelit, SAP, Schneider Electric, Siemens, Telefonica, Telecom Italia.

W Polsce również są tworzone standardy dotyczące chmury obliczeniowej. Wśród rozwiązań branżowych można wymienić – przykładowo – *Komunikat dotyczący*

przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej, opublikowany 23 stycznia 2020 r. przez Urząd Komisji Nadzoru Finansowego, a także standard chmury obliczeniowej dla branży ubezpieczeniowej, ogłoszony w czerwcu 2021 r. przez Polską Izbę Ubezpieczeń, we współpracy z Polską Izbą Informatyki i Telekomunikacji.

W 2020 r. w Polsce z płatnych usług chmury obliczeniowej korzystało 24,4% przedsiębiorstw. Największą popularność zyskały one wśród firm zatrudniających co najmniej 250 osób (59,5%), a ze względu na rodzaj prowadzonej działalności – w podmiotach z sekcji „informacja i komunikacja" (63,5%). Najmniejsze zainteresowanie tego rodzaju technologiami odnotowano w firmach małych (20,6%) oraz w sekcji „zakwaterowaniei gastronomia" (15,2%). W 2019 r. odsetek przedsiębiorstw w Polsce kupujących usługi w chmurze obliczeniowej był niższy o 13 punktów procentowych niż w średnio w Unii Europejskiej (24%). Najwyższy odsetek wystąpił w Finlandii (65%), a najniższy – w Bułgarii (8%). Wielka Brytania już w 2013 r. przyjęła zasadę „Chmura na pierwszym miejscu" (*Cloud First*), nakładającą na instytucje publiczne obowiązek sięgania po rozwiązaniachmurowe w procesie rozwijania usług publicznych.

Zatem przetwarzanie w chmurze to nowy model obliczeniowy i biznesowy, w którym użytkownicy mogą uzyskać dostęp do swoich aplikacji, bez względu na lokalizację. Chmura obliczeniowa jest w dużej mierze napędzana przez coraz trudniejszą do zarządzania złożoność IT. Sam rozwój chmury jako usługi stanowi kluczowy czynnik przyśpieszający transformację cyfrową firm, gdyż pozwala na wykorzystanie potencjału nowych technologii bez konieczności ponoszenia kosztów inwestycji w sprzęt i w infrastrukturę. Trend w kierunku *Cloud Computing* trwa ze względu na uzyskane korzyści finansowe zarówno użytkowników, jak i dostawców. Anders Lisdorf wymienia tzw. wielką piątkę dostawców usług w chmurze: Amazon Web Services, Google Cloud Platform, IBM Cloud, Microsoft Azure i Oracle.

Agnieszka Warchoł

Co to jest chmura obliczeniowa?, https://www.chmuramicrosoft.pl/co-to-jest-chmura-obliczeniowa/ (dostęp 13.10.2021); *Czym jest chmura obliczeniowa?*, https://azure. microsoft.com/pl-pl/overview/what-is-cloud-computing/ (dostęp 14.10.2021); *European Industrial Technology Roadmap for the Next Generation Cloud-edge Offering*, https://ec.europa.eu/newsroom/repository/document/2021-18/European_CloudEdge_Technology_Investment_Roadmap_for_publication_pMdz85DSw6nqPppq8hE9S9RbB8_76223.pdf (dostęp 14.10.2021); *Europejska strategia w zakresie danych*, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_pl (dostęp 18.10.2021); *Europejski plan na chmurę i obliczenia brzegowe,* https://www.cloudforum.pl/2021/05/28/europejski-plan-na-chmure-i-obliczenia-brzegowe/ (dostęp 14.10.2021); *Government Cloud First Policy*, https://www.gov.uk/guidance/government-cloud-first-policy (dostęp 14.10.2021); Komunikat Urzędu Komisji Nadzoru Finansowego dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej, 2020, https://www.knf.gov.pl/knf/pl/komponenty/ img/Komunikat_UKNF_Chmura_Obliczeniowa_68669.pdf (dostęp 14.10.2021); A. Lisdorf, *Cloud Computing Basics. A Non-technical Introduction*, Apress, New York 2021; M. Nowakowski, *Będziemy mieć unijną*

chmurę obliczeniową? Strategia KE ws. danych osobowych, https://alebank.pl/bedziemy-miec-unijna-chmure-obliczeniowa-strategia-ke-ws-danych-osobowych/?id=314752&catid=625&cat2id=361 (dostęp 17.10.2021); *Pakt na rzecz europejskiej chmury obliczeniowej*, https://przemyslprzyszlosci.gov.pl/pakt-na-rzecz-europejskiej-chmury-obliczeniowej/ (dostęp 14.10.2021); *Secure Data Outsourcing. A Brief Overview*, [w:] *Encyclopedia of Cryptography and Security*, https://link.springer.com/ referenceworkentry/10.1007%2F978-1-4419-5906-5_675 (dostęp 14.10.2021); N.K. Sehgal, P. Chandra, P. Bhatt, *Cloud Computing: Concepts and Practices*, Springer, Cham 2018; *Społeczeństwo informacyjne w Polsce w 2020 r*., https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2020-roku,1,14.html (dostęp 14.10.2021); *Standard chmury obliczeniowej dla branży*, https://piu.org.pl/ standard-chmury-obliczeniowej-dla-branzy/ (dostęp 18.10.2021); K. Śledziewska, R. Włoch, *Gospodarka cyfrowa. Jak nowe technologie zmieniają rząd*, https://delab. uw.edu.pl/wp-content/uploads/2020/04/Katarzyna-%C5%9Aledziewska-Renata-W%C5%82och-Gospodarka-cyfrowa.pdf (dostęp 16.10.2021); G. Wang, *Cloud Computing*, [w:] *Web Information Systems Engineering – WISE 2009*, G. Vossen, D.D.E. Long, J. Xu Yu (eds.), Springer, Berlin 2009.

CHOROBY INFORMACYJNE – rodzaj niedomagań człowieka zidentyfikowanych na Zachodzie na początku lat 80. XX w. (ang. *diseases of information*). Należą do specyficznych chorób cywilizacji informacyjno-medialnej, atakujących nie tylko pojedyncze osoby, ale i całe społeczności, głównie w krajach wysoko rozwiniętych, mogą przeradzać się w epidemie informacyjne. Przyczyną większości tych chorób jest stres informacyjny powstały w wyniku nieradzenia sobie z nadmiarem informacji w obszarze zarządzania przepływem → i n f o r m a c j i [t. 2] oraz → p r z e c i ą ż e n i e i n f o r m a c y j n e [t. 3] zmuszające do powierzchowności i skrótowości w myśleniu oraz uniemożliwiające głębszą refleksję. Funkcjonując w permanentnym chaosie i szumie informacyjnym, jednostka jest atakowana przez zniekształconą informację, a tzw. infotoksyny (→ i n f o t o k s y k a c j a [t. 2]), infowirusy powodują u niej infoparaliż, zmęczenie informacyjne, którego konsekwencją może być depresja informacyjna prowadząca do niesprawności i niezdolności do pracy w → ś r o d o w i s k u i n f o r m a c y j n y m [t. 4], a w konsekwencji do całkowitego braku odporności na → z a g r o ż e n i a [t. 4] występujące w → i n f o s f e r z e [t. 2] (tzw. informacyjny AIDS).

Choroby te bywają niejednoznaczne i niezrozumiałe, nikt nimi nie zarządza i dlatego wg W. Babika są tak niebezpieczne. Wyszczególnia on wśród nich grupy chorób, na które zapadają nadawcy i odbiorcy informacji. Nadawców dotyka najczęściej:

- niefrasobliwość informacyjna – brak poczucia odpowiedzialności za komunikat i troski o jego prawdziwość,
- zakłamanie informacyjne – celowe zniekształcanie treści komunikatu,
- urojenia informacyjne – generowanie informacji opartych na własnych domysłach niepopartych faktami,
- obłuda informacyjna – infekowanie informacji w celu manipulowania zachowaniami odbiorców.

Natomiast choroby, na które zapadają najczęściej odbiorcy informacji, to:

- bulimia i anoreksja informacyjna – potrzeba pozyskiwania informacji w nadmiarze lub całkowity brak zapotrzebowania na nią,
- paraliż informacyjny,
- infoholizm,
- stres informacyjny,
- informacyjna samotność, frustracja, głupota – bezkrytyczny odbiór informacji,
- ignorancja informacyjna,
- alergia informacyjna,
- nerwica informacyjna,
- stwardnienie informacyjne,
- demencja informacyjna.

Długotrwałe i masowe zachowania informacyjne noszące znamiona patologii przeradzają się w epidemie informacyjne charakterystyczne dla cywilizacji cyfrowej. Zaliczyć do nich można:

- konsumpcjonizm informacyjny – zastępowanie analizy informacji jej konsumpcją, pozyskiwanie informacji nie dla podnoszenia poziomu wiedzy, lecz poczucia przynależności do grupy, nieuzasadniona i nadmierna potrzeba posiadania informacji,
- fetyszyzację informacji – przypisywanie informacji zbyt dużej roli w stosunku do jej rzeczywistej wartości, tworzenie mitu o potędze informacji, przeświadczenie, że im więcej informacji się zgromadzi, tym jest się mądrzejszym,
- stres informacyjny – niemożność podjęcia właściwej decyzji,
- głód inwigilacji – zabieganie o upublicznienie własnego życia w celu zyskania aprobaty cyfrowej publiczności, traktowanie inwigilacji jako antidotum na wykluczenie,
- cyfrową demencję – spadek zdolności przetwarzania informacji i jej rozumienia wśród osób nadmiernie korzystających z cyfrowych mediów, przejawiający się powierzchowną wiedzą, zubożeniem struktur informacyjnych, ignorowaniem informacji nieistotnych, wielozadaniowością umysłu prowadzącą do powierzchowności i mniej efektywnego przetwarzania danych, zanikiem umiejętności dostrzegania problemu w ujęciu całościowym i w interdyscyplinarnej refleksji.

Przejawem patologii informacyjnej jest również zakłamanie (tendencyjność w odbiorze komunikatów), intencjonalność (niewłaściwe rozumienie komunikatów), fanatyzm (wyolbrzymianie znaczenia informacji). Wszystkie te „schorzenia" powodują trudności w prawidłowym odbiorze komunikatów i obiektywnym odzwierciedleniu rzeczywistości.

Łatwość publikowania różnych informacji w sieci przyczynia się w dużym stopniu do obniżenia ich parametrów jakościowych. Każdy może wprowadzić w obieg informacje zarówno w celu tworzenia wspólnej wiedzy i dzielenia się doświadczeniem, jak też manipulowania innymi osobami, wywierania wpływu na ich postawy,

wprowadzania chaosu w wymiarze jednostkowym, lokalnym, narodowym, a nawet globalnym. Zjawisko nadmiarowości informacji, przeciążenia informacyjnego, nadprodukcji danych czy zalewu komunikatów wywołuje choroby informacyjne, które można podzielić na 4 kategorie wynikające z obszaru ich oddziaływania na człowieka. Są to choroby stanowiące zagrożenie dla bezpieczeństwa personalnego, bezpieczeństwa organizacji, bezpieczeństwa państwa i bezpieczeństwa globalnego.

Zagrożenia dla bezpieczeństwa personalnego wynikające z przyspieszenia technologicznego i nadmiarowości informacji Babik podzielił na zagrożenia o charakterze: psychologicznym, technicznym, medycznym, prawnym, społecznym. Do zagrożeń psychologicznych należy wewnętrzny przymus bycia w sieci (internetoholizm) i zagubienie się w nadmiarze niezweryfikowanych, często szkodliwych i destrukcyjnych informacji, których nie sposób odróżnić od prawdziwych i wartościowych. Spośród zagrożeń o charakterze technicznym niebezpieczny jest niekontrolowany dostęp osób nieuprawnionych do danych osobowych, a spośród zagrożeń o charakterze medycznym niebezpieczne są konsekwencje stresu informacyjnego i braku higieny informacyjnej. Zagrożenia o charakterze prawnym nawiązują do przestępstw przeciwko prawu autorskiemu i wykorzystywaniu cudzej własności intelektualnej, uznaniu zasobów internetu jako wspólnej własności ludzkości, który można dowolnie poddawać technice remiksu, kolażu, miksowania w celu tworzenia „nowych" wytworów. Zagrożenia o charakterze społecznym łączą się z napływem informacji niezamawianej, nieprawdziwej, niekompletnej, z nierównomiernym dostępem do informacji (wykluczeniem cyfrowym, informacyjnym, technologicznym jednostek, grup).

Zagrożenia dla bezpieczeństwa organizacji wynikające z nadmiarowości informacji lub zjawiska szumu informacyjnego związane są głównie z walką konkurencyjną, w której wykorzystuje się informacje, z denuncjacją konkurenta handlowego, z inwigilacją konsumencką, → m a n i p u l a c j ą i n f o r m a c j ą [t. 3], infekowaniem systemu komunikacyjnego w firmie, z niewystarczającymi kompetencjami informacyjnymi pracowników firmy oraz jej klientów, z upadkiem kultury komunikacyjnej i → k u l t u r y i n f o r m a c y j n e j [t. 2], brakiem kultury uczenia się i kultury → b e z p i e c z e ń s t w a i n f o r m a c y j n e g o w organizacji. Organizacje – zabiegając o kreowanie korzystnego dla siebie wizerunku i wyeliminowanie konkurencji z rynku – niejednokrotnie wykorzystują do tego celu zjawisko przeciążenia informacyjnego, zasypując klientów odpowiednio spreparowanymi informacjami.

Zagrożenia dla bezpieczeństwa państwa mają swoje podłoże np. w źle uprawianej → p o l i t y c e i n f o r m a c y j n e j [t. 3], w zakłócaniu społecznego ładu informacyjnego, w złej polityce bezpieczeństwa informacyjnego, w bagatelizowaniu potrzeby kształtowania → k u l t u r y b e z p i e c z e ń s t w a i n f o r m a c y j n e g o [t. 2] narodu, w uwikłaniu go w → w a l k ę i n f o r m a c y j n ą [t. 4], w paraliżu systemów informacyjno-decyzyjnych, w tolerowaniu, a nawet kultywowaniu → p o s t p r a w d y [t. 3], w eliminowaniu społeczeństw niedoinformowanych

i nienadążających za rozwojem technologiczno-komunikacyjnym ze światowych rynków opartych na wiedzy.

Zagrożenia dla bezpieczeństwa globalnego mają bezpośredni związek np. z globalną → w o j n ą i n f o r m a c y j n ą [t. 4], z → o p e r a c j a m i p s y c h o l o g i c z n y m i [t. 3] w walce informacyjnej prowadzącymi do globalnego chaosu, z katastrofami technologicznymi wynikającymi z niewiedzy o skutkach ubocznych rozwoju nauki, ze światowym terroryzmem medialnym (zob. → t e r r o r y z m a m e d i a [t. 4]), → c y b e r t e r r o r y z m e m itp.

Współcześnie człowiek narażony na zbyt dużą ilość bodźców informacyjnych oraz negatywne skutki rozpowszechniania fałszywych, fragmentarycznych, sprzecznych ze sobą lub zniekształconych informacji ulega zmęczeniu informacją, które utrudnia funkcjonowanie w życiu codziennym i wykonywanie obowiązków. Jest ono symptomem chorób fizycznych i psychicznych charakteryzujących się podwyższonym ciśnieniem krwi, osłabieniem widzenia, niestrawnością, stresem, frustracją, problemami z koncentracją, wyższym poziomem → a g r e s j i itp.

Niemożność percepcji docierających do człowieka różnymi kanałami informacji (ich analizy, syntezy, uogólnienia) połączona z uzależnieniem od dopływu tych informacji powoduje powstawanie licznych patologii informacyjnych. Niedostrzeganym przez młodzież skutkiem ubocznym przeciążenia informacją staje się wewnętrzny przymus całodobowego monitorowania aktywności sieci, ucieczka od świata realnego do wirtualnego prowadząca do alienacji. Konsekwencją uzależnienia od sieci są zaburzenia infoholiczne, do których M. Jędrzejko zalicza: kompulsywne używanie internetu, nałóg komputerowy, zaburzenia korzystania z informacji, cyberuzależnienie telewizyjne, zaburzenia nałogowego grania, korzystania z telefonu komórkowego, cyberyzaburzenia od gier i innych urządzeń technologii informacyjno-komunikacyjnych. Są to patologie, uzależnienia i choroby ściśle związane ze światem wirtualnym. Do tej grupy można zaliczyć także cyberuzależnienia od Facebooka i smartfona, a także cyberstres oraz cyberlęk, np. FOMO (ang. *fear of missing out*) czy nomofobię oraz cyberchondrię.

Najbardziej dotkliwą chorobą jest uzależnienie od internetu wywołujące niemożność kontroli wykorzystania tego medium, co powoduje zaburzenia w prawidłowym funkcjonowaniu w życiu codziennym. Znany w psychologii termin zespołu uzależnienia od internetu, definiowany jako zespół zależności polegający na wielogodzinnym korzystaniu z internetu, co jest dla pacjenta źródłem stresu oraz negatywnie wpływa na jego funkcjonowanie w sferze fizycznej, psychicznej, interpersonalnej, społecznej, rodzinnej i ekonomicznej. Uzależnienie od internetu stanowi problem ogólnoświatowy, a jego konsekwencją jest pojawienie się zachowań nałogowych oraz zagrożeń wynikających z wpływu niewłaściwych wzorców generujących niewłaściwe postawy, zachowania, działania. Z kolei cyberlęk jest chorobą wynikającą z popadania jednostki w stan FOMO i nomofobii. Terminy te oznaczają lęki społeczne i alienację oraz wykluczenie

społeczne powodowane przez wirtualizację kontaktów interpersonalnych i ograniczanie się do aktywności tylko na portalach społecznościowych. FOMO charakteryzuje się lękiem, że coś nas ominie, że zostaniemy pominięci w wirtualnej społeczności, że zostanie się przez nią wykluczonym. Jest to choroba cywilizacyjna współczesności, która czerpie swoje toksyny z obawy, że bez naszej wiedzy dzieje się coś naprawdę ciekawego i satysfakcjonującego, w czym uczestniczą inne osoby, a nie my. FOMO objawia się nerwowym zerkaniem na smartfona, poczuciem dyskomfortu i strachu, kiedy nie jesteśmy „na bieżąco". Innym rodzajem cyberlęku jest nomofobia rozumiana jako lęk przed brakiem dostępu do telefonu komórkowego, przed odcięciem od dopływu informacji i możliwości wchodzenia w interakcje z nadawcami wiadomości otrzymywanych za pośrednictwem tego urządzenia, zarówno od osób znajomych, jak i anonimowych z sieci. Jeszcze inną odmianą choroby wynikającej ze zbyt dużej ilości danych atakujących zmysły człowieka jest cyberchondria, rozumiana jako wzmożone martwienie się normalnymi, często nieuzasadnionymi objawami medycznymi, szukaniem informacji o symptomach i schorzeniach na różnych portalach internetowych, w różnych publikacjach zamieszczanych w sieci, konsultowanie się z innymi internautami mającymi podobne doświadczenia, sprawdzanie wpisów na forach itp. Wszystkie wyszczególnione powyżej choroby i lęki są wynikiem przekroczenia tzw. *attention crush*, czyli granicy, za którą człowiek z powodu swojej konstrukcji biologicznej nie jest w stanie przyswoić więcej informacji.

Hanna Batorowska, Katarzyna Batorowska

T.R. Aleksandrowicz, K. Liedel, *Społeczeństwo informacyjne – sieć – cyberprzestrzeń. Nowe zagrożenia*, [w:] *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*, K. Liedel, P. Piasecka, T.R. Aleksandrowicz (red.), Difin, Warszawa 2014; W. Babik, *Ekologia informacji*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2014; tenże, *O natłoku informacji i związanym z nim przeciążeniu informacyjnym*, [w:] *Człowiek – Media – Edukacja*, J. Morbitzer (red.), Kraków 2010; tenże, *O niektórych chorobach powodowanych przez informację*, [w:] *Komputer w edukacji*, J. Morbitzer (red.), Uniwersytet Pedagogiczny im. KEN w Krakowie, Kraków 2006; H. Batorowska, *Information literacy powinnością w społeczeństwie informacyjnym*, „Bibliotheca Nostra" 2012, nr 2 (28); taż, *Zanik umiejętności dostrzegania problemu w ujęciu całościowym i w interdyscyplinarnej refleksji*, [w:] *Kultura informacyjna w ujęciu interdyscyplinarnym*, t. 1, H. Batorowska (red.), Uniwersytet Pedagogiczny im. KEN w Krakowie, Kraków 2015; K. Batorowska, *Bezpieczeństwo w czasach nadprodukcji informacji*, [w:] *Bezpieczeństwo informacyjne i medialne w czasach nadprodukcji informacji*, H. Batorowska, P. Motylińska (red.), Wydawnictwo SBP, Warszawa 2020; H. Batorowska, R. Klepka, O. Wasiuta, *Media jako instrument wpływu informacyjnego i manipulacji społeczeństwem*, Wydawnictwo Libron, Kraków 2019; Z. Bauman, D. Lyon, *Płynna inwigilacja. Rozmowy*, Wydawnictwo Literackie, Kraków 2013; N. Carr, *Płytki umysł. Jak internet wpływa na nasz mózg*, tłum. K. Rojek, Helion, Gliwice 2013; *Człowiek wobec uzależnień. Wybrane problemy*, M. Jędrzejko, M. Netczuk-Gwoździewicz (red.), ASPRA-JR, Warszawa 2013; M. Jędrzejko, *Młodzież w zaburzonym świecie*, WSB, Dąbrowa Górnicza 2013; M. Jędrzejko, D. Morańska, *Cyfrowi tubylcy. Socjopedagogiczne aspekty nowych technologii cyfrowych*, ASPRA-JR, Dąbrowa Górnicza–Warszawa 2013; M. Ledzińska, *Znaczenie wybiórczości umysłu w dobie informacyjnego zalewu*, [w:] *Komputer w edukacji*, J. Morbitzer (red.), Wydawnictwo Naukowe AP,

Kraków 2004; A. Ogonowska, *Uzależnienia medialne, czyli o patologicznym wykorzystaniu mediów*, Wydawnictwo Edukacyjne, Kraków 2014; M. Spitzer, *Cyberchoroby. Jak cyfrowe życie rujnuje nasze zdrowie*, tłum. M. Guzowska, Dobra Literatura, Słupsk 2016; tenże, *Cyfrowa demencja. W jaki sposób pozbawiamy rozumu siebie i swoje dzieci*, tłum. A. Lipiński, Dobra Literatura, Słupsk 2013; S. Wojciechowska-Filipek, Z. Ciekanowski, *Bezpieczeństwo funkcjonowania w cyberprzestrzeni: jednostki – organizacji – państwa*, CeDeWu, Warszawa 2019.

CICHOCIEMNI – → ż o ł n i e r z e [t. 4] Polskich Sił Zbrojnych (PSZ) szkoleni od 1940 r. na terenie Wielkiej Brytanii oraz od końca 1943 r. na terenie Włoch, przerzucani drogą lotniczą do okupowanej Polski do służby w szeregach Związku Walki Zbrojnej / Armii Krajowej (ZWZ/AK) w okresie II wojny światowej.

Cichociemni wywodzili się z różnych formacji PSZ na Zachodzie. Po decyzji przejścia do pracy konspiracyjnej w okupowanej Polsce i odbyciu specjalnego przeszkolenia otrzymywali indywidualne przydziały do ZWZ/AK. Nie stanowili oni jednej zwartej jednostki wojskowej, nie mieli struktury dowódczej klasycznych jednostek wojskowych, barw broni, tradycji, patrona czy sztandaru. Mieli jedynie znak bojowy. Działali w różnych sezonach operacyjnych na całym terenie operacyjnym AK, często wykonywali zadania pojedynczo lub w małych zespołach. Ze względu na nabyte najwyższe kwalifikacje i umiejętności niejednokrotnie po skoku obejmowali kierownicze stanowiska w strukturach Polskiego Państwa Podziemnego (PPP).

Ojcami założycielami grupy cichociemnych stali się dwaj kapitanowie dyplomowani – J. Górski ps. Chomik i M. Kalenkiewicz ps. Kotwicz, przekonani o idei stworzenia łączności lotniczej połączonej z desantowaniem spadochroniarzy w celu wsparcia PPP walczącego z okupantem. Rekrutowanie kandydatów do skoku na teren okupowanej Polski powierzono oficerom z utworzonego 29 czerwca 1940 r. przy Sztabie Naczelnego Wodza Oddziału VI – Samodzielnego Wydziału Krajowego, przemianowanego następnie na Oddział Specjalny. Do jego zadań należało utrzymanie łączności między Naczelnym Wodzem a Komendą Główną ZWZ/AK, wspieranie akcji zamierzonych przez KG ZWZ/AK oraz szkolenie emisariuszy i kurierów politycznych. Oddział Specjalny współpracował z powołanym do życia w lipcu 1940 r. przez premiera W. Churchilla Kierownictwem Operacji Specjalnych (Special Operations Executive, SOE) – organizacją kooperującą z ruchem oporu w całej Europie. Działająca w ramach SOE, utworzona jako pierwsza, polska sekcja cieszyła się autonomią – miała niezależną sieć radiową, własny kod, służbę ekspedycji oraz odbiór zrzutów. SOE udostępniała ponadto Polakom swoje bazy szkoleniowe – ośrodki na terenie całej Wielkiej Brytanii.

Kandydaci na cichociemnych szkoleni byli nieprzerwanie w okresie całej II wojny światowej. Zasadniczo wyodrębnić można 3 grupy skoczków w zależności od powierzanych im zadań:

- skoczkowie do zadań bieżących, specjaliści od → w y w i a d u [t. 4], → d y w e r s j i [t. 2], mikrofotografii, fałszerstwa, łączności, oficerowie sztabowi;

- skoczkowie, którzy mieli odegrać istotną rolę w przygotowaniach do powstania powszechnego oraz w odtwarzaniu Sił Zbrojnych w Kraju: lotnicy, instruktorzy, oficerowie sztabowi, łączności i broni pancernej, dowódcy, a nawet lekarze;
- kurierzy i emisariusze polityczni Ministerstwa Spraw Wewnętrznych do Delegatury Rządu. Część z nich znalazła przydziały w konspiracji wojskowej, AK lub Batalionach Chłopskich.

Werbunek kandydatów oparty był na zaciągu ochotniczym. Początkowo nie prowadzono selekcji, później postanowiono jednak wprowadzić ostre kryteria wymaganych cech moralnych oraz predyspozycji psychicznych i fizycznych. Po tej ocenie chętnych kierowano na szkolenia stanowiące rzeczywistą część selekcji.

Program szkoleniowy podzielony był na 4 grupy kursów: zasadnicze, specjalnościowe, uzupełniające oraz praktyki. Wśród kursów zasadniczych wymienić należy:

- kurs zaprawy dywersyjno-minerskiej, strzeleckiej i fizycznej (Inverlochy Castle k. Fort William, Szkocja, w latach 1942–1944: Garramour k. Arisaig, Invernesshire, Szkocja) – miał na celu selekcję fizyczną kandydatów oraz przygotowanie do dalszego szkolenia dywersyjnego; kładziono tutaj szczególny nacisk na zaprawę fizyczną oraz uczono strzelania z różnych pozycji, terenoznawstwa, walki wręcz, dżiu-dżitsu i posługiwania się prostymi środkami minerskimi;
- kurs badań psychotechnicznych (Guildford, Anglia);
- kurs spadochronowy (Ringway k. Manchesteru, Anglia; Largo House, Upper Largo, Szkocja) – obejmował zaprawę spadochronową i skoki; przygotowanie do skoków odbywało się w brytyjskim ośrodku spadochronowym w Ringway lub w ośrodku treningowym 1. Samodzielnej Brygady Spadochronowej w Largo House, w tzw. Małpim Gaju; celem szkolenia było uelastycznienie sylwetki kandydata oraz nauczenie go odpowiedniej postawy i ułożenia ciała podczas skoku; kandydaci odbywali kilka skoków, także nocą;
- kurs walki konspiracyjnej (Briggens, Anglia; w latach 1942–1944: Audley End, Anglia) – jego celem było nauczenie organizowania i prowadzenia walki małym zespołem dywersyjno-sabotażowym; podczas kursu doskonalono umiejętności minerskie i strzeleckie oraz uczono zasad radiotelegrafii i szyfrów;
- kurs odprawowy (Audley End, Anglia) – jego celem było przekształcenie skoczka w konspiratora; podczas kursu kandydat układał tzw. legendę, dostawał fałszywe dokumenty, kompletował cywilne ubranie; przez cały czas zaznajamiany był z warunkami życia w Polsce, strukturą AK, organizacją niemiecką, metodami terroru stosowanymi przez Gestapo itp., a także ćwiczył zachowanie po skoku; kurs przechodzili wszyscy skoczkowie, którzy mieli odlecieć do kraju – zarówno cichociemni, jak i kurierzy polityczni.

Kandydaci na cichociemnych mieli możliwość brania udziału w licznych kursach specjalnościowych oraz uzupełniających, m.in. w polskim kursie wywiadu, kursie

walk ulicznych, szturmowym, wyrobu materiałów wybuchowych, mikrofotografii, czarnej → p r o p a g a n d y [t. 3] czy zmiany wyglądu fizycznego.

Pod koniec 1943 r. przystąpiono do uruchomienia ośrodka szkoleniowego we Włoszech. Była to Baza Nr 10 „Impudent", zorganizowana pomiędzy Bari a Brindisi. Skoki ćwiczono na lotnisku Campo Cassale w Brindisi.

Po zakwalifikowaniu na skok do Polski skoczkowie składali przysięgę na rotę AK, przybierali pseudonimy oraz wyjeżdżali na stacje wyczekiwania. Na stacji wyczekiwania kontroli poddawano cywilne wyposażenie skoczka, a także zaopatrywano go w ekwipunek bojowy na drogę i skok, na który składały się: kombinezon, spadochron, hełm, bandaże elastyczne, wkładki do obuwia, skórzane rękawice, 2 pistolety oraz amunicja, nóż, łopatka do zakopania spadochronu, kompas, scyzoryk, latarka elektryczna, manierka z alkoholem, pas na pieniądze, porcja żywności, osobista apteczka oraz, na życzenie skoczka, 2 fiolki z trucizną. Tak wyposażony spadochroniarz kierowany był do skoku na teren Polski.

W wyniku rekrutacji spośród grona ochotników na kurs wytypowano 2413 kandydatów. Ekstremalnie trudne, trwające wiele tygodni szkolenie z pozytywnym wynikiem ukończyło pomyślnie 606 skoczków, z których do skoku skierowano 579. Ostatecznie do Polski wyekspediowano drogą powietrzną jedynie 316 cichociemnych, w tym jedną kobietę – E. Zawacką ps. Zo.

Cichociemni zrzucani byli w jasne, księżycowe noce. Skakali z otworu znajdującego w podłodze samolotu na spadochronach typu Irvin QD z wysokości ok. 200 m.

Operacje lotnicze zapoczątkowane zostały w nocy z 15/16 lutego 1941 r. i trwały do 27/28 grudnia 1944 r. Cichociemni skakali w następujących sezonach operacyjnych:

- Okres próbny: 15/16 lutego 1941 r. – 8/9 kwietnia 1942 r.
- „Intonacja": 1/2 września 1942 r. – 2/3 kwietnia 1943 r.
- „Riposta": 9/10 września 1943 r. – 30/31 lipca 1944 r.
- „Odwet" i Powstanie Warszawskie: 1/2 sierpnia 1944 r. – 27/28 grudnia 1944 r.

Zrzuty wykonywano na specjalnie zorganizowane placówki odbiorcze. Za odbiory zrzutów odpowiedzialna była specjalna komórka Oddziału V Komendy Głównej ZWZ/AK, zwana „Syreną". Każdy cichociemny stopniowo wdrażany był do życia w warunkach okupacyjnych, przechodził tzw. aklimatyzację trwającą od 2 do 6 tygodni. Opieką nad skoczkami w okresie aklimatyzacji zajmowały się panie z referatu „Ewa-Pers", tzw. ciotki.

Po skoku oraz czasie aklimatyzacji cichociemni rozpoczynali działalność w szeregach ZWZ/AK. Wyglądała ona następująco:

- dywersja – do zadań przysposobionych do → d y w e r s j i [t. 2] cichociemnych, których kierowano do „Wachlarza", a następnie „Kedywu", należały m.in. niszczące działania na zapleczu, prowadzone z ukrycia w celu osłabienia obronności lub gospodarki okupanta, dezorganizowanie sił przeciwnika, tj. niszczenie linii telefonicznych, wysadzanie szyn, wysadzanie transportów, podpalanie cystern,

ataki na niemieckich urzędników, odbijanie więźniów, prowadzenie akcji odbioru zrzutów itp.;

- wywiad – skoczkowie przeszkoleni w specjalności wywiadowczej pełnili funkcje organizatorów i inspektorów sieci wywiadu; kierowano ich przede wszystkim do Wywiadu Ofensywnego Oddziału II KG AK, na różne stanowiska dowódcze w centrali oraz w terenie;
- zadania legalizacyjne – przystosowani do tych zadań skoczkowie zostali skierowani do Wydziału Techniczno-Legalizacyjnego Oddziału I KG AK o kryptonimach „Park", „Leta", „Izba", gdzie zajmowali się zaopatrywaniem w nielegalne dokumenty wszystkich komórek KG z wyjątkiem Oddziału II;
- prace w Wydziale Lotnictwa KG AK – przydzieleni do tych prac cichociemni rozpoznawali oraz ewidencjonowali wszystkie lotniska oraz lądowiska na terenie kraju; działania te potrzebne były podczas opracowywania planów przygotowywania powstania powszechnego w Polsce, z których ostatecznie zrezygnowano;
- łączność radiowa – przysposobieni do tych działań skoczkowie wnieśli istotny wkład w rozbudowywanie oraz sprawne funkcjonowanie sieci radiowej, głównie jeśli chodzi o łączność zewnętrzną z bazami w Wielkiej Brytanii oraz we Włoszech;
- prace w sztabach konspiracyjnych – przeszkoleni do tych zadań skoczkowie służyli w sztabach Komendy Głównej, przydzielani do obszarów lub okręgów AK; miejsce znaleźli tam również inni specjaliści, tj. pancerniacy, saperzy, lotnicy, a nawet jeden lekarz; cichociemni zatrudniani byli także w inspektoratach rejonowych, obwodach, a nawet rejonach, w zależności od bieżących potrzeb siatki terenowej AK;
- walki w Powstaniu Warszawskim – skoczkowie walczący w Powstaniu znaleźli się na pierwszej linii walk, dowodzili oddziałami, pracowali w sztabach, w sieci łączności radiowej czy przy produkcji środków walki. Po kapitulacji Warszawy część spadochroniarzy AK dostała się do niewoli, inni natomiast dalej pracowali w konspiracji aż do wyzwolenia w styczniu 1945 r.

Z 316 skoczków zginęło 112: 9 podczas lotu lub skoku, 94 w walce lub zostało zamordowanych przez Gestapo (w tym 10 zażyło truciznę po aresztowaniu), na 9 wykonano po → w o j n i e [t. 4] karę śmierci na podstawie wyroków sądów Polski Ludowej w okresie → s t a l i n i z m u [t. 4]. Spośród cichociemnych, którzy brali udział w powstaniu warszawskim, 18 zginęło w walce. Do najbardziej znanych cichociemnych należą: E. Zawacka ps. Zo, S. Bałuk ps. Starba, J. Piwnik ps. Ponury, B. Kontrym ps. Żmudzin, H. Dekutowski ps. Zapora, L. Okulicki ps. Niedźwiadek.

Decyzją nr 119 Ministerstwa Obrony Narodowej z dnia 4 sierpnia 1995 r. dziedzictwo i tradycje Cichociemnych Spadochroniarzy Armii Krajowej przejęła Jednostka Wojskowa GROM, która od tego dnia nosi także ich imię.

Agnieszka Polończyk

Armia Krajowa w dokumentach 1939–1945, t. II: *1941–43*, Studium Polski Podziemnej, Londyn 1973; S. Bałuk, *Commando cichociemni*, Wydawnictwo ASKON, Warszawa 2008;

K. Bieniecki, *Lotnicze wsparcie Armii Krajowej*, Bellona, Warszawa 2005; A. Polończyk, *Cichociemni – dzieje elity polskiej dywersji na kanwie życiorysu Bolesława Polończyka ps. „Kryształ"*, „Bezpieczeństwo. Teoria i Praktyka" 2016, nr 3; taż, *Cichociemni – zarys historii formacji*, [w:] *Wywalcz Polsce wolność lub zgiń. Tobie Ojczyzno!*, A. Tyszkiewicz (red.), Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2017; A. Polończyk, M. Lupa, A. Leśniak, *Analysis of the Polish Home Army Drop Zones During the Second World War Using Geographic Information Systems*, „Geomatics, Landmanagement and Landscape" 2017, no. 3; J. Tucholski, *Cichociemni*, Instytut Wydawniczy PAX, Warszawa 1984; I. Valentine, *Baza 43 Cichociemni*, Wydawnictwo Wołoszański, Warszawa 2005.

CLOUD ACT – (ang. Clarifying Lawful Overseas Use of Data Act) ustawa federalnego prawa amerykańskiego uchwalona w 2018 r., stosowana jako wyjątek od ustawy o przechowywaniu danych (ang. Stored Communications Act, SCA). Celem jej uchwalenia było utworzenie odpowiednich procedur transgranicznych przeznaczonych dla organów ścigania USA i mających uprościć oraz przyśpieszyć procedurę pozyskania dowodów cyfrowych umieszczonych poza terytorium USA (obecnie jest to standard: dzięki rozwiązaniu technologicznemu polegającemu na trzymaniu danych w serwerze lub w kilku połączonych serwerach, co jest potocznie nazywane chmurą – stąd też nawiązanie w nazwie ustawy). Cloud Act ma zastosowanie tylko w przypadku dochodzeń karnych: zmienia jedynie przepisy prawa karnego na podstawie tytułu 18 Kodeksu Stanów Zjednoczonych. Nie zmienia także federalnych zasad postępowania cywilnego, regulowanych przez sądy w sprawach cywilnych. I nie zmienia ustawy o postępowaniu administracyjnym ani żadnej innej ustawy, która upoważnia podmiot rządowy USA do dostępu do dowodów poza postępowaniem karnym.

Ustawa SCA z 1986 r. w zasadzie zakazuje dostawcom usług z siedzibą w USA ujawniania wszelkich przesyłanych danych cyfrowych organom administracji innych państw, także w przypadku ścigania swojego obywatela w ramach śledztwa krajowego – tylko departamenty lub agencje federalne mogą zmusić usługodawcę do ujawnienia danych, przy czym musi zostać wydany przez sędziego Stanów Zjednoczonych nakaz „przeszukania", oparty na podejrzeniu zaistnienia przestępstwa, wskazujący docelowe miejsce, w którym mają się znajdować dowody tego przestępstwa, podlegające udostępnieniu (np. poczta e-mail), oraz zawierający opis dowodów, które mają być udostępnione lub przejęte na potrzeby śledztwa. Ustawa SCA jest ponadto nadrzędna wobec zagranicznych nakazów ujawnienia → i n f o r m a c j i [t. 2]. Dzięki systemowi prawnemu opartemu na ustawie SCA, przy obecnej dynamice → c y b e r p r z e s t ę p c z o ś c i [t. 1], właściwie niemożliwe staje się funkcjonowanie sprawne i skuteczne działanie organów ścigania, czego efektem była sprawa Microsoft Corp vs. United States, 584 US, 138 S. Ct. 1186 (2018), w wyniku której zapadł wyrok o ograniczeniu stosowania SCA danych znajdujących się tylko na terytorium USA (w tej sprawie chodziło o udostępnienie danych z serwerów Microsoftu umieszczonych na serwerach w Irlandii). Ostatecznie w 2018 r., po uchwaleniu Cloud Act oraz i równoczesnym złożeniu przez Departament Sprawiedliwości apelacji do

Sądu Najwyższego, sprawę rozstrzygnięto i umorzono. Od tamtego momentu stosuje się – w drodze wyjątku od SCA – działanie w ramach umowy wykonawczej oraz związanych z nią procedur wynikających z umowy z państwem – stroną Cloud Act. W ten sposób ustawa Cloud skodyfikowała dla SCA pogląd Departamentu Sprawiedliwości na poprzednią, długoletnią doktrynę i praktykę prawa amerykańskiego. Według Departamentu Sprawiedliwości nie rozszerzyło to jurysdykcji prawnej USA.

Warto również wspomnieć, że oprócz ustawy SCA istnieje międzynarodowy system prawny, w ramach którego można uzyskać dowody elektroniczne – tzw. umowa o wzajemnej pomocy prawnej (ang. Mutual Legal Assistance Treaty, MLAT). Jest on nadal wykorzystywany, aczkolwiek uważany za opcję nieskuteczną, ze względu na długi czas rozpatrzenia wniosków w ramach swojej procedury, zwłaszcza w obliczu rosnącej liczby zgłoszeń o udostępnienie danych. W przypadku zawarcia Cloud Act między państwem – stroną a rządem USA te państwa mają osobną drogę administracyjną składania wniosków o udostępnienie informacji bezpośrednio do amerykańskich usługodawców IT. W takiej sytuacji wniosek musi spełniać warunki określone w umowie Cloud Act: we wniosku trzeba zawrzeć cel związany z ściganiem, zapobieganiem, prowadzeniem dochodzeń, wykryciem przestępstwa, w tym także aktów → t e r r o r y z m u [t. 4]. Wniosek powinien również zawierać dane osoby, której dotyczy, w tym – dane osobowe, adres, urządzenia osobiste, konto e-mail lub inne (przy czym ich pozyskanie musi zgodne z prawem krajowym). We wniosku konieczne jest wykazanie uzasadnienia opartego na dowodach, a wszelkie kwestie szczegółowe powinny wynikać z prowadzonego dochodzenia. Wniosek musi także podlegać kontroli odpowiedniego organu sprawiedliwości (sędziego lub innych) i nie może naruszać prawa do wolności słowa. Przy czym uzyskanie konkretnych dowodów elektronicznych, w zależności od ich rodzaju, jest zabezpieczone stosunkowo surowymi wymaganiami proceduralnymi: uzyskanie tzw. podstawowych informacji o abonamencie (ang. *Basic Subscriber Information*, BSI) wymaga wezwania sądowego lub nakazu sądu, przy czym we wskazanych dokumentach musi być wskazany subskrybent lub właściciel konta. Usługodawca ma prawo sprzeciwu – poprzez złożenie wniosku o uchylenie. W konsekwencji wniosek ponownie trafia przed sąd do ponownego rozpatrzenia. Po uzyskaniu od usługodawcy metadanych telekomunikacyjnych i innych danych niezwiązanych z treścią organy → b e z p i e c z e ń s t w a [t. 1] muszą także zdobyć nakaz sądowy oparty na przekonujących dowodach, wskazujących, że dostęp do tych danych okazuje się istotny w dochodzeniu z myślą o uzyskaniu śladów powiązań konkretnego użytkownika, subskrybenta czy właściciela konta z pożądanymi, publikowanymi danymi, treściami itp. W tych okolicznościach dla usługodawcy istnieje taka sama droga składania wniosku o uchylenie. W sytuacji procedury uzyskania dostępu do treści komunikacji wymagane jest także uzyskanie nakazu sądowego opartego na prawdopodobnej przyczynie popełnienia przestępstwa oraz na prawdopodobnej przyczynie tego, że treść będąca przedmiotem wniosku okaże się będzie dowodem przestępstwa. W tym aspekcie

sprawy konieczne staje się także złożenie uzasadnienia w postaci opisu danych dotyczących treści, do których upoważniony będzie organ wnioskujący, przy czym sąd może dodatkowo wymagać zrealizowania operacji w określonych ramach czasu.

Cloud Act składa się z 2 części:

- pierwsza dotyczy zawierania bilateralnych umów wykonawczych między państwami-stronami w ramach tej ustawy, przy czym szerzej precyzuje wszelkie zawarte w niej szczegóły, zwłaszcza dotyczące przepisów USA, kwestii likwidacji obecnych barier prawnych (także w przypadkach pozyskania dowodów w ramach krajowych śledztw), reguluje dostęp zagranicznych organów ścigania do treści komunikacyjnych przechowywanych przez amerykańskich dostawców usług IT;
- druga część przedstawia procedurę dostępu organów ścigania USA do danych, które są na serwerach firm amerykańskich za granicą.

Umowy wykonawcze mogą być zawierane tylko z państwami spełniającymi wysokie wymagania dotyczące praworządności, przestrzegania → p r a w c z ł o w i e k a [t. 3], ochronę prywatności, a ponadto posiadającymi system prawny oraz instytucjonalne siły i środki zapewniające ochronę danych przez organy bezpieczeństwa oraz instytucje sprawujące nadzór nad nimi. Wymagany jest także system autoryzacji dostępu do tych danych, wdrożony na terytorium państw, z którymi zawarto umowę wykonawczą i określono ścieżkę ich ciągłego przetwarzania, zabezpieczania, archiwizowania i usuwania. Państwo-strona umowy wykonawczej musi poddać się także okresowemu przeglądu stosowanych procedur. Przed przystąpieniem do Cloud Act wymagane jest od państwa-strony umowy także unieważnienie aktów prawnych blokujących dostęp służbom USA do treści komunikacyjnych przechowywanych na zagranicznym terytorium. Warto też wspomnieć, że każda umowa wykonawcza jest zawierana odrębnie, co przekłada się na możliwość obustronnego zawężenia zakresu udostępnianych danych. Należy podkreślić, że Stany Zjednoczone muszą mieć osobistą jurysdykcję nad usługodawcą w celu uzyskania dostępu danych będących w jego posiadaniu lub pod jego kontrolą. Konsekwencje prawne wobec podmiotów, które nie przestrzegałyby zapisów z umowy wykonawczej, byłyby wymierzane na podstawie prawa krajowego państwa – strony. Ponadto każda osoba czy podmiot, które zostaną objęte nakazem udostępnienia dowodów, mogą go zakwestionować pod względem niedozwolenia przez prawo, nadmiernej uciążliwości jego wykonania, naruszenia przywilejów prawnych lub dlatego, że stoi w sprzeczności z przepisami prawa w innej jurysdykcji, której podlega. Zgodnie z obowiązującym prawem amerykańskim, procedury dotyczące wniosku organów ścigania USA na podstawie umowy wykonawczej na mocy ustawy Cloud Act byłyby takie same jak w przypadku każdego innego wniosku organów ścigania USA. Warunkiem *sine qua non,* pozostaje wspomniana jurysdykcja amerykańska nad usługodawcą.

Inną kwestią doprecyzowaną w Cloud Act w wyniku nowelizacji po procesie *Microsoft Ireland* jest zagadnienie terytorium, na którym przechowywane są dane – kwestia położenia nie determinuje odmowy do dostępu dla organów prowadzących

dochodzenie: obowiązki prawne dostawcy usług wynikają z zarządzania posiadanymi danymi, bez względu na to na jakim terytorium w chwili złożenia wniosku się znajdują. Obecnie technologicznym standardem jest tzw. zarządzanie brzegowe w zakresie rozwiązań sieciowych, powodujące ciągły proces przenoszenia danych klientów między swoimi centrami danych w różnych krajach. Służby USA mogą nie mieć możliwości dowiedzenia się, gdzie znajdują się poszukiwane dane, a to w zasadzie uniemożliwia uzyskanie do nich dostępu poprzez procedurę MLAT. Ponadto w wielu przypadkach nie ma logicznego ani normatywnego związku między miejscem, w którym znajdują się dane,a jakimkolwiek suwerennym interesem w prowadzonej sprawie.

W zakresie działań operacyjnych zapisy Cloud Act wobec strony amerykańskiej wykluczają stosowanie podsłuchów (prawo USA zabrania wydawania nakazów → p o d s ł u c h u [t. 3] wobec osób znajdujących się poza terytorium kraju), ale zakłada możliwość zapisu w umowie wykonawczej, zezwalające państwu-stronie (czyli innemu niż USA) na podsłuchiwanie usługodawców amerykańskich w określonych okolicznościach i zgodnie z określonymi wymogami: w zakresie czasowym uzgodnionym w ramach dochodzenia, nieprzekraczającym okresu koniecznego do realizacji celów. Do wydania zgody na podsłuch konieczne okazuje się uzasadnienie, że danych informacji nie można uzyskać innymi metodami.

W kontekście prawnym jest to rozwiązanie, które znacznie standaryzuje pod względem globalnym administracyjne procedury, zwłaszcza z uwagi na możliwość zawarcia Cloud Act z Unią Europejską jako całością, zamiast negocjowania odrębnych umów z 27 jej członkami. Pod względem politycznym to także w pewnym sensie narzucenie formy solucji, skrócenie czasu wprowadzenia i zmniejszenie zakresu negocjacji do określonej, klarownie zarysowanej formy systemowej, rozwiązującej wiele problemów organów bezpieczeństwa państw Europy. Argumentem działającym na korzyść takiego rozwiązania jest istniejące podobieństwo do przepisów obowiązujących w UE, gdzie funkcjonuje prawo dające szeroki zakres jurysdykcji prawnej i operacyjnej dotyczącej dowodów elektronicznych, przy czym wniosek UE ma także zastosowanie, jeśli usługodawca oferuje usługi w UE, nawet w przypadku, gdy nie ma tam siedziby ani nie jest reprezentowany w Unii. Istniej także wymóg dla usługodawcy, dotyczący udostępnienia odpowiednich dowodów elektronicznych w odpowiedzi na przymusowy nakaz ujawnienia, bez względu na terytorium ich składowania. Drugim argumentem jest RODO. W kwestii dotyczących przekazywania danych art. 48 RODO stanowi, że „umowa międzynarodowa" może stanowić podstawę prawną do przekazywania danych osobowych poza UE. Przypuszczalnie umowa wykonawcza na mocy ustawy Cloud Act (lub innej umowy między UE a USA) kwalifikowałaby się jako taka umowa międzynarodowa, stanowiąca podstawę prawną dla przeniesień. Ponadto wymagania Cloud Act są zgodne z wymaganiami Kanady, Wielkiej Brytanii, Francji, Belgii, Norwegii, Irlandii, Brazylii, Hiszpanii, Danii, Kolumbii, Portugalii, Australii, Meksyku, Czarnogóry, Peru, Serbii.

Wojciech Cendrowski

S. Bilgic, *Something Old, Something New, and Something Moot. The Privacy Crisis under the CLOUD Act*, „Harvard Journal of Law & Technology" 2018, vol. 32, iss. 1; T. Christakis, F. Terpan, *EU–US Negotiations on Law Enforcement Access to Data. Divergences, Challenges and EU Law Procedures and Options*, „International Data Privacy Law" 2021, vol. 11, iss. 2; J. Hemmings, S. Srinivasan, P. Swire, *Defining the Scope of "Possession, Custody, or Control" for Privacy Issues and the CLOUD Act*, „Journal of National Security Law & Policy" 2020, vol. 10, iss. 3; M. Rojszczak, *CLOUD Act Agreements from an EU Perspective*, „Computer Law & Security Review" 2020, vol. 38; M. Rutherford, *The CLOUD Act. Creating Executive Branch Monopoly over Cross-Border Data Access*, „Berkeley Technology Law Journal" 2019, vol. 34, iss. 4; J. Salehi, *CLOUD Act. From Function to Its Achievements & Defections in Extraterritorial Criminal Investigations in Database of Technology Companies*, „The Judiciary Law Journal" 2020, vol. 84, iss. 111.

COVID-19 (ASPEKT MEDYCZNY) – choroba zakaźna wywołana wirusem SARS-CoV-2, pochodzącym z rodziny koronawirusów (CoV), atakująca w pierwszej kolejności układ oddechowy chorego. Nazwa COVID-19 wywodzi się z angielskich słów: *COronaVIrus* oraz *Disease*. Oznaczają one – odpowiednio – nawiązanie do rodziny koronawirusów oraz chorobę, z kolei liczba wskazuje na rok pojawienia się danego wariantu wirusa, który spowodował wystąpienie choroby.

Pierwsze wzmianki o ludzkich koronawirusach pochodzą z lat 60. XX w., gdy wyodrębniono 2 pierwsze patogeny u ludzi. Wirusy należące do tej rodziny zostały sklasyfikowane do 2 odrębnych podrodzin (*Coronavirinea* oraz *Torovirinea*). Podrodzina *Coronavirinea*, z racji swoich cech genetycznych, jest podzielona na 4 podstawowe rodzaje: alfa-, beta-, gamma-, delta-CoV. Pierwsze 2 rodzaje, najpewniej wywodzące się od koronawirusów zakażających nietoperze, zasadniczo powodują infekcję u ssaków, natomiast gammai deltasą patogenami charakterystycznymi dla ptaków. Spośród całej rodziny koronawirusów kilka przedstawicieli powoduje choroby atakujące ludzki układ oddechowy, objawiające się (najczęściej) lekkim przeziębieniem, jak również (w skrajnych przypadkach) prowadzące do rzadkich i poważnych chorób kończących się zespołem ostrej niewydolności oddechowej, a w konsekwencji – zgonem chorego.

Wirus SARS-CoV-2 nie jest pierwszym drobnoustrojem z rodziny koronawirusów, który został wykryty u ludzi w XXI w. W 2003 r. oraz 2012 r. zidentyfikowano odpowiednio:

– SARS-CoV-1 (inne nazwy: SARS, SARS-CoV – akronim słowa SARS powstał z pierwszych liter angielskiego oznaczenia symptomów wywołanych przez ten wirus, tj. *Severe Acute Respiratory Syndrome*. W tłumaczeniu na język polski oznacza to *ciężki ostry zespół oddechowy*).
– MERS-CoV (*Middle East Respiratory Syndrom w* tłumaczeniu na język polski oznacza: bliskowschodni zespół oddechowy).

Pierwsze zakażenia SARS-COV-1 pojawiły się w listopadzie w 2002 r. w mieście Foshan, w prowincji Guangdong, w Chińskiej Republice Ludowej. Wówczas, podobnie jak w przypadku SARS-CoV-2, do pierwotnego zakażenia wirusem doszło w wyniku

kontaktu człowieka ze zwierzętami na jednym z lokalnych targów. Wirus SARS-CoV-1 w 2003 r. rozprzestrzenił się na inne regiony Chin i kontynentu azjatyckiego oraz na inne państwa na świecie, jednakże skala tego zdarzenia była na tyle niewielka, że nie zakwalifikowano go do zjawiska → p a n d e m i i , a jedynie – jako epidemię występującą ogniskowo.

W przypadku MERS-CoV wzmianki o pierwszych zakażeniach na Półwyspie Arabskim dotyczą 2012 r. Ten wirus został przypadkowo wyizolowany od pacjenta z ostrą niewydolnością układu oddechowego, u którego następnie doszło do niewydolności nerek, a finalnie – do niewydolności wielonarządowej, zakończonej zgonem pacjenta. Analiza prac badawczych prowadzi do wniosku, że odpowiedzialnymi za przenoszenie patogenu koronawirusa MERS na ludzi są wielbłądy jednogarbne (dromadery).

Szacuje się, że śmiertelność w wyniku zakażenia wirusem MERS-CoV wynosi ok. 35%, co czyni go niezwykle groźnym drobnoustrojem z rodziny koronawirusów. Kliniczne przypadki infekcji odnoszą się najczęściej do osób dorosłych, jednakże zakażenia tym wirusem mogą dotyczyć również dzieci. Światowa Organizacja Zdrowia uznała wirus MERS-CoV za patogen mogący być przyczyną kolejnej epidemii. Do 2015 r. ten rodzaj koronawirusa wyizolowano w 21 krajach na całym świecie.

Choroba COVID-19 pojawiła się po raz pierwszy w Chińskiej Republice Ludowej. Epicentrum stanowiła prowincja Hubei. Pierwsze → i n f o r m a c j e [t. 2] o COVID-19 pochodziły z miasta Wuhan w listopadzie 2019 r., według oficjalnych informacji pacjent zero zaraził się wirusem na targu, na którym sprzedawano owoce morza oraz dzikie zwierzęta. Początkowo wirus SARS-CoV-2 został oznaczony jako 2018-nCoV, czyli zupełnie nowy wirus z rodziny koronawirusów. Nieco później dostrzeżono podobieństwo do wirusa z tej samej rodziny – SARS-CoV, z którym świat zetknął się w 2003 r. Rozwój epidemii na przełomie 2019 i 2020 r. okazał się bardzo dynamiczny, głównie za sprawą → g l o b a l i z a c j i.

W krótkim czasie pierwsze ogniska nowej choroby pojawiły się w Azji, w Europie oraz w Ameryce Północnej. Wówczas → Ś w i a t o w a O r g a n i z a c j a Z d r o w i a [t. 4] (WHO), monitorująca rozwój sytuacji epidemiologicznej w każdym rejonie globu, zwracała szczególną uwagę na tempo rozprzestrzeniania się nowych zakażeń. W związku z pogarszającą się sytuacją 11 marca 2020 r. WHO przekształciła epidemię choroby COVID-19 w zjawisko o charakterze pandemicznym.

Zakażenie wirusem SARS-CoV-2 może być niejednoznaczne i przybierać różny przebieg: od całkowicie bezobjawowego bądź skąpoobjawowego, przez pełnoobjawowy, aż po zespół ostrej niewydolności oddechowej lub zespół niewydolności wielonarządowej, najczęściej kończące się zgonem chorego. Początkowo kliniczne objawy choroby COVID-19, (jeśli występowały) pojawiały się po okresie inkubacji ok. 5–6 dnia po kontakcie z patogenem koronawirusa. Charakterystycznymi objawami dla pierwotnego wariantu były:

– gorączka powyżej 38,0°C (w okresie walki z pierwszą i drugą falą pandemii przyjmowano, że umowną granicą była temperatura powyżej 37,5°C);

– suchy kaszel (najczęściej napadowy i uporczywy);
– uczucie duszności, zwykle połączone z odczuwaniem ucisku w klatce piersiowej (objaw często subiektywny, ponieważ z klinicznego doświadczania autorów wiadomo, że zdarzali się pacjenci o prawidłowym nasyceniu krwi tlenem, którzy zgłaszali duszność, oraz pacjenci, którzy nie odczuwali duszności, a gazometria i pomiary nasycenia krwi tlenem sugerowały już stadium niewydolności oddechowej w stopniu średnim lub zaawansowanym);
– utrata węchu i smaku;
– bóle mięśni.

Wraz z mutacją wirusa i tworzeniem się nowych wariantów obraz kliniczny się zmieniał – pojawiały się kolejne często atypowe objawy, m.in.:

• biegunki,
• nudności, wymioty,
• bóle gardła,
• bóle głowy,
• uczucie rozbicia, zmęczenie.

W kontekście samego przebiegu COVID-19 warto zwrócić uwagę na wielokierunkowe działanie patogenu. Objawy i powikłania dotyczą nie tylko układu oddechowego (ostra i przewlekła niewydolność oddechowa, zwłóknienia tkanki płuc), lecz także układu krążenia (zwiększone ryzyko zawału serca, zakrzepicy czy nagłej śmierci sercowej), układu nerwowego (zwiększone ryzyko udaru mózgu, problemy z koncentracją i pamięcią, które nie zawsze ustępują bezpośrednio po przechorowaniu – syndrom tzw. *long covid*), zaburzenia węchu i smaku, problemy z orientacją w czasie i przestrzeni), układu pokarmowego (wymioty, biegunki), układu endokrynnego (zaburzenia metaboliczne, np. wysokie stężenia poziomu glukozy we krwi, pojawiające się w czasie infekcji, ale pozostające już po przechorowaniu i wymagające leczenia w poradni diabetologicznej – zjawisko wyraźnie widoczne u dzieci).

Podstawowym narzędziem służącym do wykrywania zakażenia SARS-CoV-2 jest pobranie wymazu z jamy nosowo-gardłowej, a następnie – analiza materiału za pomocą jednej z dostępnych metod:

• Badanie immunologiczne – test Ag Covid, czyli test antygenowy, wykrywający antygen SARS-CoV-2: wykorzystujący wysoce czułe przeciwciała monoklonalne do wykrywania białka nukleokapsydowego SARS-CoV-2. W ten sposób działają tzw. szybkie testy do skriningowej diagnostyki. Obecnie w ramach systemu opieki zdrowotnej takie szybkie testy wykonywane są na pokładzie ambulansu Zespołu Ratownictwa Medycznego, w Szpitalnych Oddziałach Ratunkowych, w placówkach Podstawowej Opieki Zdrowotnej czy w pracowniach hemodynamiki. Wynik jest otrzymywany w ciągu 15–20 minut. W systemie ochrony zdrowia bardzo często wyniki Ag są weryfikowane testami PCR, charakteryzującymi się wyższą czułością.

- Badanie genetyczne – test RT PCR (łańcuchowa reakcja polimerazy – pozwalająca na powielanie konkretnych odcinków DNA w warunkach laboratoryjnych. Real Time PCR umożliwia jednoczesne namnażanie się DNA oraz monitorowanie ilości produktów powstających podczas kolejnych cykli). Wynik jest możliwy do otrzymania w ciągu 2–4 godzin.
- Badanie serologiczne z krwi – wykrywające przeciwciała w klasie IgA, IgG, IgM lub IgG/IgA, IgG/IgM. Jednak ze względu na okres, jaki musi minąć od kontaktu z wirusem do wytworzenia przeciwciał (wytworzenie przeciwciał IgM – min. 7–10 dni od zakażenia, IgG –później), nie da się za pomocą tego badania ocenić, czy pacjent jest w aktywnej fazie choroby, czy też już ją przeszedł – dlatego wymagane jest potwierdzenie testem RT PCR.

Śmiertelność w przebiegu choroby COVID-19 wynosi ok. 2–3% i najczęściej dotyczy osób w podeszłym wieku, przy czym w zdecydowanej większości są to pacjenci obciążeni wywiadem chorobowym. Jednak z myślą o przebiegu trzeciej i czwartej fali pandemii (wiosna i jesień 2021 r.) trzeba zwrócić uwagę na to, że statystycznie wiek pacjentów w stanie ciężkim, wymagających hospitalizacji, tlenoterapii lub wspomagania oddychania za pomocą respiratora, czy też krążenia pozaustrojowego (ECMO), znacząco się obniżył.

Wirus SARS-CoV-2, podobnie jak inne patogeny, adaptuje się do organizmu ludzkiego i mutuje, w wyniku czego tworzą się nowe warianty.

Jak dotąd wyizolowano kilka podstawowych wariantów o charakterze globalnym. Podstawowe warianty o charakterze pandemicznym to: alfa, beta, gamma, delta (oraz delta plus) i omikron, wykryty 30 listopada 2021 r., bardziej zakaźny, ale mniej zjadliwy. Warianty o charakterze lokalnym to m.in: lambda oraz mu.

Transmisja wirusa SARS-CoV-2 odbywa się najczęściej drogą kropelkową za pomocą wydzielin z dróg oddechowych, np. w momencie kichania (prędkość, z jaką wydostają się w tym momencie drobnoustroje, wynosi ok. 160 km/h), kaszlu, śpiewu czy rozmowy. Jest to tzw. przenoszenie bezpośrednie. Drugą możliwością jest przenoszenie pośrednie, tzw. powietrzne (w badaniach prowadzonych w Hiszpanii i Wielkiej Brytanii przedstawiano możliwość zakażenia się przez przebywanie w pomieszczeniu takim jak toaleta, gabinet, w którym wcześniej przebywała osoba zakażona, a w powietrzu nadal unosiły się patogeny, pomimo że zakażony pacjent opuścił daną strefę wcześniej). W pracach amerykańskich badaczy zwracano także uwagę na przeżywalność wirusa na częściach wspólnych struktur miejskich (klamki, windy, bankomaty, automaty biletowe), co mogłoby także doprowadzić do zakażenia u pacjenta pod warunkiem braku zachowania prawidłowej higieny z jego strony.

Na podstawie opracowań eksperckich oraz przeprowadzonych eksperymentów ustalono, że pierwszym kluczowym elementem przeciwdziałania COVID-19 powinna być profilaktyka. Pierwotnie opierała się ona na 3 fundamentalnych składnikach zasady „DDM", czyli „dystans, dezynfekcja, maseczka". Jest to tzw. profilaktyka nieswoista.

Po wielu miesiącach zmagań udało się pod koniec 2020 r. wprowadzić profilaktykę swoistą, czyli szczepienia, będące jednym z najbardziej skutecznych oręży ochrony przeciwwirusowej. Założeniem powszechnego programu szczepień jest osiągnięcie progu odporności zbiorowej. Dla COVID-19 minimalny próg powinien wynosić ok. 86% przy występowaniu obecnie dominującego wariantu delta oraz delta plus, które – w przeciwieństwie do poprzednich mutacji – są dużo bardziej zaraźliwe, czyli cechują się wyższym wskaźnikiem „R", dotyczącym reprodukcji wirusa (w momencie, gdy wskaźnik „R" wynosi więcej niż 1 i wzrasta, uważa się, że sytuacja epidemiczna jest rozwijająca się, natomiast kiedy wskaźnik „R" jest poniżej 1 i maleje, wtedy pandemia wyhamowuje, czyli mniej osób się zakaża). Powszechny program szczepień w Polsce bazuje na preparatach opartych na technologii mRNA (Pfizer, Moderna) oraz wektorowej (Astra Zeneca, Johnson & Johnson). Te szczepionki cechują się różnym poziomem skuteczności, jednak w badaniach prowadzonych na całym świecie wskazuje się wspólny mianownik, m.in.: w ponad 90% chronią one przed ciężkim przebiegiem COVID-19 oraz redukują ryzyko hospitalizacji i zgonu, znacząco zmniejszają ryzyko zachorowania, jednak – o czym należy pamiętać – nie zapewniają 100% ochrony przed zakażeniem.

Żaneta Zając, Andrzej Ziarko

Coronavirus Disease (COVID-19), World Heatlh Organization, https://www.who. int/emergencies/diseases/novel-coronavirus-2019 (dostęp 19.11.2021); *Koronawirus SARS-CoV-2, przeciwciała IgG ilościowo*, https://sla.pl/koronawirus-sars-cov-2-przeciwciala-igg-ilosciowo/ (dostęp 19.11.2021); *Prevention & Treatment Protocols for COVID-19*, https://covid19criticalcare.com/wp-content/uploads/2020/11/ FLCCC-Alliance-I-MASKplus-Protocol-ENGLISH.pdf (dostęp 19.11.2021); K. Pyrć, *Ludzkie koronawirusy*, „Postępy Nauk Medycznych" 2015, XXVIII (4B); *Real-Time PCR*, http://www.e-biotechnologia.pl/artykuly/real-time-pcr. (dostęp 19.11.2021); *Słowniczek terminów epidemiologicznych*, „Przegląd Epidemiologiczny. Kwartalnik Narodowego Instytutu Zdrowia Publicznego – Państwowego Zakładu Higieny i Polskiego Towarzystwa Epidemiologów i Lekarzy Chorób Zakaźnych", http://www.przeglepidemiol.pzh.gov.pl/slowniczek-terminow-epidemiologicznych (dostęp 19.11.2021); Ł. Szarpak, T. Dzieciątkowski, K.J. Filipiak, *Bezpieczeństwo personelu medycznego w dobie Covid-19 według zasad EBM*, PZWL, Warszawa 2021; D. Vasireddy, R. Vanaparthy, *Review of COVID-19 Variants and COVID-19 Vaccine Efficacy: What the Clinician Should Know?*, „Jorunal Clinical Medical Resarche" 2021, iss. 13(6).

COVID-19 (ASPEKT SPOŁECZNY) – zakaźna choroba dróg oddechowych wywołana przez koronawirus SARS-CoV-2, wcześniej nieznany. → I n f o r m a c j a [t. 2] o wirusie dotarła do → Ś w i a t o w e j O r g a n i z a c j i Z d r o w i a [t. 4] 31 grudnia 2019 r. w postaci doniesień o przypadkach „wirusowego zapalenia płuc" w mieście Wuhan w środkowochińskiej prowincji Hubei. Według źródeł chińskich pierwszy przypadek COVID-19 stwierdzono 17 listopada 2019 r. u 55-letniego mężczyzny. Światowa Organizacja Zdrowia 30 stycznia 2020 r. ogłosiła stan → z a g r o ż e n i a [t. 4] dla zdrowia publicznego, a 11 marca 2021 r. – → p a n d e m i ę. Pierwszy przypadek zakażenia koronawirusem odnotowano w Polsce 4 marca 2020 r.

w szpitalu w Zielonej Górze: u 66-letniego mężczyzny, który przyjechał autokarem z Niemiec.

Jak do tej pory pochodzenie wirusa SARS-CoV-2 pozostaje nieznane. WHO opublikowała 30 marca 2021 r. raport będący wynikiem prac chińskich i międzynarodowych ekspertów, którzy od 14 stycznia do 10 lutego 2021 r. badali w Chinach początki pandemii. Ten raport opisywał 4 scenariusze początku pandemii COVID-19. Jako prawdopodobny lub wielce prawdopodobny scenariusz początku pandemii raport określa przeniesienie pośrednie wirusa z nietoperza na człowieka poprzez inne zwierzę. Za możliwe eksperci uznają bezpośrednie przeniesienie wirusa z nietoperza na człowieka lub przedostanie się go poprzez skażoną żywność. Za najmniej prawdopodobny uznano scenariusz przypadkowego wycieku wirusa w laboratorium. Raport WHO spotkał się z krytyką części środowisk naukowych, a sama organizacja 13 października 2021 r. poinformowała o powołaniu nowego zespołu ekspertów, którzy ponownie majązbadać pochodzenie SARS-CoV-2.

Według danych WHO do 19 listopada 2021 r. na całym świecie potwierdzono ponad 255 mln przypadków zachorowań na COVID-19, a ponad 5,1 mln osób zmarło z powodu COVID-19 i chorób współistniejących z COVID-19. W tym okresie w Polsce zarejestrowano 3,3 mln przypadków, a zmarło 80 399 osób. Najwięcej ofiar śmiertelnych z powodu COVID-19 odnotowano w USA (759 388), Brazylii (611 851), Indiach (465 82), Meksyku (291 573), Federacji Rosyjskiej (261 589), Peru (200 741), Indonezji (143 741), Wielkiej Brytanii (143 559), Włoszech (133 034), Iranie (128 531), Kolumbii (127 912) i Argentynie (116 313).

COVID-19 stwarza największe zagrożenie dla osób starszych i mających choroby współistniejące. Potwierdzają to dane z USA. Do 17 listopada 2021 r. ok. 94% wszystkich śmiertelnych ofiar COVID-19 w USA skończyło 50 lat. Osoby w wieku powyżej 85 lat to niemal 27% wszystkich śmiertelnych ofiar COVID-19 w USA. Osoby w wieku 75–84 lata stanowiły niemal 26% wszystkich zgonów, w wieku 65–74 lata – prawie 23%, a w wieku 50–64 lata – niewiele ponad 18%.

Zgodnie z danymi WHO zakażenia koronawirusem SARS-CoV-2 wśród dzieci stanowią ok. 8,5% wszystkich przypadków. Najmłodsi chorują zatem relatywnie najrzadziej, a także przechodzą zakażenie najłagodniej. Nie jest jednak prawdą, że żadne dziecko (osoba mająca mniej niż 18 lat) nie zmarło na COVID-19. Z danych Amerykańskiej Akademii Pediatrycznej opublikowanych 4 listopada 2021 r. wynika, że w USA w niektórych stanach 0,26% wszystkich zgonów z powodu COVID-19 stanowiły dzieci. W wybranych stanach 0,03% przypadków potwierdzonych zakażeń u dzieci zakończyło się śmiercią.

Choroba najczęściej objawia się gorączką, kaszlem, dusznościami, bólami mięśni, zmęczeniem. Koronawirus SARS-CoV-2 przenosi się między ludźmi przede wszystkim drogą kropelkową. Okres inkubacji SARS-CoV-2 wynosi od 1 do 14 dni, na ogół – 5 dni.

Na pierwszym etapie infekcji wirus zakaża głównie komórki górnych dróg układu oddechowego (w obrębie nosa, gardła i krtani), skąd może rozprzestrzeniać się do dolnych dróg oddechowych i infekować komórki pęcherzyków płucnych. Polscy eksperci z inicjatywy „Nauka przeciw pandemii" przekonują, że „kliniczny przebieg zakażenia wirusem SARS-CoV-2 może być bardzo zróżnicowany, w zależności od cech indywidualnych pacjenta i prawdopodobnie również od dawki wirusa, na którą pacjent został narażony". W przygotowanej przez nich publikacji pt. *Charakterystyka choroby COVID-19, objawy oraz skutki zdrowotne. Rekomendacje i doświadczenia polskich klinicystów* czytamy, że u ok. 20% zakażonych osób przebieg COVID-19 ma charakter bezobjawowy, a u zdecydowanej większości zakażonych infekcja manifestuje się w sposób łagodny, związany głownie z objawami ze strony górnych dróg oddechowych.

„Postać ciężka występuje u ok. 15% zakażonych, stan bardzo ciężki, czyli zagrożenia życia, u ok. 5%. U takich pacjentów obserwuje się zapalenie płuc o ciężkim przebiegu oraz zespół ostrej niewydolności oddechowej. Śmiertelność na podstawie statystyk zakażeń i zgonów wynosi ok. 2%". Z powodu śmiertelności COVID-19, szybkości przenoszenia się wirusa, niewydolności systemów służby zdrowia i braku lekarstwa poszczególne kraje od początku pandemii koronawirusa wprowadzały obostrzenia w funkcjonowaniu obywateli, gospodarki i instytucji publicznych, której główną ideą było zachowanie dystansu społecznego, izolacja zakażonych oraz kwarantanna dla osób podejrzanych o kontakt z osobami zakażonymi. Obostrzenia wprowadzane przez władze krajowe i lokalne, zarówno na szczeblu ogólnokrajowym, jak i na lokalnym, były zazwyczaj warunkowane aktualną sytuacją epidemiczną, stanem opieki zdrowotnej oraz realizowaną polityką rządu.

Wybuchowi pandemii koronawirusa SARS-CoV-2 towarzyszyła infomedia, czyli pandemia informacji. W przestrzeni publicznej, a zwłaszcza w → m e d i a c h s p o ł e c z n o ś c i o w y c h [t. 3], pojawiały się → f a k e n e w s y [t. 2], treści dezinformacyjne, które podważały istnienie choroby COVID-19 i koronawirusa SARS-CoV-2. Te nasiliły się wraz pojawieniem się szczepionek przeciw COVID-19. Jak do tej pory Komisja Europejska zaakceptowała 4 szczepionki na koronawirusa i tym samym dopuściła je do obrotu na terenie Unii Europejskiej: 21 grudnia 2020 r. – szczepionkę Comirnaty (wyprodukowaną przez Pfizer/BioNTech), 6 stycznia 2021 r. – szczepionkę Spikevax (wyprodukowaną przez Moderna Biotech Spain, S.L.), 29 stycznia 2021 r. – szczepionkę Vaxzevria (wyprodukowaną przez AstraZeneca AB) oraz 11 marca 2021 r. – szczepionkę COVID-19 Vaccine Janssen (wyprodukowaną przez Janssen-Cilag International NV). Pierwsze dwie bazują na nowej technologii mRNA, pozostałe to dobrze znane szczepionki wektorowe. W sprawie tych ostatnich głos zabrał Episkopat: stwierdził, że ich przyjmowanie „budzi poważny sprzeciw moralny" ze względu wykorzystanie przy ich produkcji linii komórkowych wytworzonych z abortowanych płodów.

Decyzja Komisji Europejskiej została wydana w trybie warunkowym, co zaniepokoiło część → o p i n i i p u b l i c z n e j [t. 3]. Komisja Europejska tłumaczy, że ze względu na pilną potrzebę związaną z pandemią proces opracowania i zatwierdzenia szczepionek przeciwko COVID-19 był o wiele szybszy niż zwykle. Jednak te szczepionki spełniają wysokie standardy obowiązujące wszystkie inne szczepionki. Zdaniem KE w szybkim opracowaniu szczepionek pomagały ogromne środki zainwestowane w prace. Naukowcom udało się przyśpieszyć niektóre etapy procesu dzięki połączeniu różnych faz badań klinicznych lub prowadzeniu niektórych badań jednocześnie. Europejska Agencja Leków, będąca organem KE, rozpoczęła analizę wyników badań, jeszcze zanim firmy zwróciły się o dopuszczenie szczepionek.

Ze względu na początkowe problemy z dostępnością szczepionek zatwierdzonych przez Komisję Europejską 2 państwa UE (Węgry i Słowacja) zdecydowały się, mimo braku akceptacji przez EMA, na szczepienie swoich obywateli także szczepionką przeciw COVID-19 opracowaną przez Rosjan, nazwaną Sputnik V. Na Słowacji decyzja o zakupie rosyjskiej szczepionki wywołała ogromny → k r y z y s [t. 2] w ramach koalicji rządzącej, zakończony zmianą na stanowisku premiera. Igor Matovič, który zresztą sam zaszczepił się Sputnikiem V, podał się do dymisji, a zastąpił go Eduard Heger.

W ramach projektu KFF COVID-19 Vaccine Monitor badacze postanowili zbadać stosunek Amerykanów do najpopularniejszych fake newsów w sprawie pandemii COVID-19 i szczepionek przeciw koronawirusowi. Ustalono, że 38% Amerykanów jest zdania, że władze zawyżają liczbę zgonów z powodu COVID-19, a kolejnych 22% nie jest pewnych, czy ta informacja jest prawdziwa czy fałszywa. Natomiast 7% Amerykanów uważa, że w szczepionkach zawarto czipy, po których wstrzyknięciu można inwigilować osobę zaszczepioną lub przejąć nad nią kontrolę. Kolejnych 17% dorosłych Amerykanów nie ma co do tego pewności. Niemal co czwarty Amerykanin (21% badanych), obawia się, że szczepionka może zmienić DNA, z czego 8% jest tego pewne. Natomiast 14% ankietowanych uznaje, że to po wstrzyknięciu szczepionki przeciw COVID-19 można zachorować na tę chorobę, a co dziesiąty Amerykanin nie jest pewny, czy można zarazić się koronawirusem poprzez przyjęcie szczepionki.

Polacy także wierzą w fake newsy na temat pandemii COVID-19. Według badania Kantara z lutego 2021 r. aż 25% Polaków uważa, że pandemię wywołały koncerny farmaceutyczne. Z kolei 16% Polaków sądzi, że za pandemią COVID-19 stoi Bill Gates, który wywołał ją w celu depopulacji, 11% uważa, że za koronawirusa odpowiedzialna jest technologia 5G.

Łukasz Grzesiczak

Charakterystyka choroby COVID-19, objawy oraz skutki zdrowotne. Rekomendacje i doświadczenia polskich klinicystów, Nauka przeciw pandemii, Warszawa, 5 maja 2021, https://naukaprzeciwpandemii.pl/app/uploads/2021/05/biala-ksie-ga_charakterystyka-choroby-covid-19_v-1.1._maj-2021.pdf (dostęp 18.11.2021); A. Demczuk, *SARS-CoV-2 i COVID-19. Plotki, dezinformacje i narracje spiskowe w polskim dyskursie publicznym*, Wydawnictwo Uniwersytetu Marii CurieSkłodowskiej, Lublin, 2021; *KFF COVID-19 Vaccine Monitor: Media*

and Misinformation, 8.11.2021, https://www.kff.org/coronavirus-covid-19/poll-finding/ kff-covid-19-vaccine-monitor-media-and-misinformation/ (dostęp 18.11.2021); E. Kubátová, *Matovič jako ‚lobbista' Sputniku v Evropě. Aféra ruské vakcíny na Slovensku nekončí, OĽaNO se propadá*, 14.04.2021, https://www.irozhlas.cz/zpravy-svet/slovensko-matovic-olano-sputnik-rusko-madarsko-krize-ockovanikoronavirus_2104140636_eku (dostęp 18.11.2021); *Number of Coronavirus Disease 2019 (COVID-19) Deaths in the U.S. as of November 17, 2021, by Age,* https://www. statista.com/statistics/1191568/reported-deaths-from-covid-by-age-us/ (dostęp 18.11.2021); *Pierwszy przypadek koronawirusa w Polsce*, https://www.gov.pl/web/ zdrowie/pierwszy-przypadek-koronawirusa-w-polsce (dostęp 18.11.2021); *Public Notice of Proposed New Scientific Advisory Group for the Origins of Novel Pathogens (SAGO) Members*, 13.10.2021, https://www.who.int/news-room/articlesdetail/public-notice-and-comment-on-proposed-new-scientific-advisory-groupfor-the-origins-of-novel-pathogens-(sago)-members (dostęp 18.11.2021); C. Tenn, *WHO Restarts Investigation of COVID-19 Emergence with New Panel*, 28.09.2021*,* https://www.the-scientist.com/news-opinion/who-restarts-investigation-ofcovid-19-emergence-with-new-panel-69244 (dostęp 18.11.2021); *WHO-convened Global Study of Origins of SARS-CoV-2: China Part*, 30.03.2021, https://www. who.int/publications/i/item/who-convened-global-study-of-origins-of-sarscov-2-china-part (dostęp 18.11.2021).

CRIME MAPPING (z ang. mapowanie przestępczości) – technologia tworzenia map → p r z e s t ę p c z o ś c i [t. 3] z wykorzystaniem systemów informacji geograficznej (ang. *geographic information systems*), tj. skomputeryzowanego systemu pozyskiwania, przechowywania, przetwarzania, integrowania, analizowania i udostępniania → i n f o r m a c j i [t. 2] mającej odniesienie przestrzenne do powierzchni Ziemi.

Mapowanie przestępczości jest wykorzystywane przez analityków w organach ścigania do mapowania, wizualizacji i analizy wzorców incydentów przestępczych. Jest to kluczowy element analizy przestępczości i → s t r a t e g i i [t. 4] policyjnej CompStat. Mapowanie przestępczości za pomocą systemów informacji geograficznej pozwala analitykom na identyfikowanie gorących punktów (od ang. *hot spot*) przestępczości wraz z innymi trendami i wzorcami.

Mapowanie danych z raportów organów ścigania może być skutecznym sposobem analizy miejsca przestępstwa. Powstały obraz wizualny można łączyć z innymi danymi geograficznymi (takimi jak lokalizacje szkół, parków i kompleksów przemysłowych) oraz wykorzystywać do analizowania i badania wzorców przestępczości oraz pomocy w udzielaniu odpowiedzi.

Crime mapping służy do wizualizacji, a także analizy oraz interpretacji danych o rozmieszczeniu czynów karalnych. Pozwala m.in. na identyfikację tzw. gorących punktów, tzn. miejsc, w których koncentruje się przestępczość, lub miejsc, w których ludzie narażeni są na wyższe niż przeciętne ryzyko wiktymizacji. *Crime mapping* jest użyteczny przede wszystkim dla → p o l i c j i [t. 3] i innych służb porządkowych, ponieważ pozwala na optymalną dystrybucję sił i środków, przejawiającą się m.in. poprzez kierowanie jednostek w miejsca faktycznie wymagające interwencji. Ponadto dzięki mapowaniu przestępczości możliwe jest poznanie tendencji występowania określonych rodzajów przestępstw na danym obszarze, a także wykonanie profilowania geograficznego pozwalającego na ustalenie, gdzie najczęściej przebywa lub mieszka sprawca danego przestępstwa.

W szczególności w ostatnim dziesięcioleciu odnotowano postępy w zakresie zdolności analitycznych w środowisku wymiaru sprawiedliwości w sprawach karnych, co umożliwia dodanie większej liczby wymiarów geograficznych i społecznych do analiz statystycznych w celu prognozowania, gdzie mogą wystąpić przestępstwa.

Analizując *crime mapping*, J. Hunt, informatyk w Biurze Nauki i Technologii Narodowego Instytutu Sprawiedliwości USA (Office of Research, Evaluation, and Technology, National Institute of Justice, NIJ), podkreśla, że jeszcze w 1829 r. A. Balbi i A.M. Guerry opracowali mapy ukazujące związki między poziomem wykształcenia a → p r z e m o c ą [t. 3] i przestępczością majątkową we Francji i że był to pierwszy przykład mapowania przestępczości. Po tej pracy J. Fletcher w 1849 r. i H. Mayhew w 1861 r. opracowali mapy, które pokazują odpowiednio liczbę uwięzionych mężczyzn i przestępczość w hrabstwach.

Na początku XX w. C. Shaw i H. McKay w USA zmapowali tysiące przypadków przestępczości nieletnich i przeanalizowali związki między przestępczością a różnymi uwarunkowaniami społecznymi.

W 1979 r. H. Goldstein w USA zaproponował podejście policyjne zorientowane na problemy. Podejście to zalecało funkcjonariuszom organów ścigania śledzenie procesu skanowania, analizy, reakcji i oceny (znanego obecnie jako podejście SARA, od ang. *scanning, analysis, response and assessment*) w celu zidentyfikowania, analizy i rozwiązania problemów.

Podstawowe teorie, które pomagają wyjaśnić zachowanie przestrzenne przestępców, obejmują → k r y m i n o l o g i ę [t. 2] środowiskową opracowaną w latach 80. XX w. przez P. i P. Brantinghamów, teorię działałań rutynowych opracowaną przez L. Cohena i M. Felsona, opublikowaną w 1979 r., a także teorię racjonalnego wyboru opracowaną przez R.V. Clarke'a i D. Cornisha, opublikowaną w 1986 r.

Badania nad mapowaniem przestępczości z użyciem technik komputerowych rozpoczęły się w 1986 r., kiedy jedna z agencji rządowych USA – NIJ – sfinansowała projekt w Departamencie Policji w Chicago (Chicago Police Department, CPD), mający na celu przeprowadzenie mapowania przestępczości jako wsparcia działań policji na szczeblu lokalnym. Projekt ten został zrealizowany przez CPD we współpracy z Chicago Alliance for Neighborhood Safety, Uniwersytet Illinois w Chicago i Northwestern University. Sukces tego projektu skłonił NIJ do zainicjowania programu analizy rynku narkotyków w 5 miastach, a techniki opracowane w jego ramach doprowadziły do rozpowszechnienia map przestępczości w USA i innych krajach.

W 1997 r. NIJ założył Crime Mapping Research Center, które sprawdziło departamenty organów ścigania w celu ustalenia, w jaki sposób wykorzystały mapowanie analityczne. Centrum rozpoczęło opracowywanie programów szkoleniowych w celu zwiększenia zdolności departamentów do korzystania z map przestrzennych i zestawów danych. W latach 1997–2014 NIJ finansował rozwój oprogramowania CrimeStat, aby pomóc praktykom i naukowcom w przeprowadzaniu analiz przestrzennych.

Na początku XXI w. NIJ zaczął się rozwijać – od oceny praktyk i strategii policyjnych opartych na lokalizacji do eksploracji technik statystycznych wykorzystywanych do prognozowania i przewidywania przestępczości oraz tego, jak wpływa to na skuteczność i wydajność praktyk policyjnych. W 2008 r. W. Bratton, który był wówczas szefem Departamentu Policji w Los Angeles, rozpoczął współpracę z dyrektorami NIJ i Bureau of Justice Assistance nad nowym podejściem zwanym „zapobiegawczą ochroną". W rezultacie w 2009 r. NIJ sfinansował 7 agencji w celu stworzenia predykcyjnych modeli policyjnych w swoich jurysdykcjach. Od tego czasu *crime mapping* rozwija się prężnie na całym świecie.

W Polsce zainteresowanie mapowaniem przestępczości widoczne jest dopiero od kilku lat, a jednym z wiodących miast prowadzącym analizy w tym obszarze jest Kraków (w ramach programu poprawy → b e z p i e c z e ń s t w a dla miasta Krakowa „Bezpieczny Kraków").

Agnieszka Polończyk

L. Anselin i in., *Spatial Analysis of Crime*, „Measurement and Analysis of Crime and Justice" 2000, vol. 4; S. Chainey, J. Ratcliffe, *GIS and Crime Mapping*, Wiley, New York 2005; T.C. Hart, K. Lersch, *Space, Time and Crime* – 4 Edition, Carolina Academic Press, Carolina 2015; B. Hill, R. Paynich, *Fundamentals of Crime Mapping*, Jones&Barlett Learning, Burlington 2014; J. Hunt, *From Crime Mapping to Crime Forecasting: The Evolution of Place-Based Policing*, „NIJ Journal" 2019, iss. 281; N. Levine, *Crime Mapping and the Crimestat Program*, „Geographical Analysis" 2006, vol. 38; A. Polończyk, A. Leśniak, *A Spatial Analysis of Selected Categories of Offences in Kraków Based on Data from the National Safety Risk Map*, [w:] *Proceedings. 2018 Baltic Geodetic Congress (BGC Geomatics)*, IEEE Computer Society, Los Alamitos–Washington–Tokyo 2018; ciż, *Mapping Public Order Offenses: A Study of the Spatial Distribution of Perceived Risk Intensity in the City of Krakow, Poland*, „Cartography and Geographic Information Science" 2020, vol. 47, no. 2; ciż, *The Impact of Generalised Spatial Data on the Incidence Density of Selected Offences in Kraków*, [w:] *Proceedings. 2018 Baltic Geodetic Congress (BGC Geomatics)*, IEEE Computer Society, Los Alamitos–Washington–Tokyo 2018.

CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN (CPTED) – koncepcja zapobiegania → p r z e s t ę p c z o ś c i [t. 3] przez kształtowanie przestrzeni, której korzenie sięgają lat 60. XX w.

Koncepcja CPTED w swoich głównych założeniach koncentruje się na przestrzeni fizycznej jako istotnym czynniku wpływającym na zachowania przestępcze. Oznacza ona prawidłowe projektowanie środowiska w celu redukcji okazji do popełniania przestępstw, które mogą być integralnie związane z budynkami lub ich otoczeniem. Istotą CPTED stało się uwzględnianie nie tylko fizycznych cech środowiska, ale i czynników socjoekonomicznych, demograficznych oraz angażowanie wspólnot lokalnych. W wyniku popularyzacji tej koncepcji zaczęto zmieniać planowanie urbanistyczne, wdrażać programy rewitalizacyjne oraz stosować najnowsze techniki przyczyniające się do zapobiegania przestępczości.

Bazując na bogatej literaturze przedmiotu (prace E. Wood, J. Jacobs, S. Angela, C.R. Jeffery'ego, O. Newmana, G. Randa, T. Crowe'a i in.), można mówić o CPTED jako o koncepcji:

- koncentrującej się na warunkach, w których powstają przestępstwa, oraz technikach służących ograniczaniu sprzyjających im okoliczności,
- identyfikującej warunki środowiska fizycznego i społecznego, które stwarzają okazje do popełniania przestępstw, oraz zakładającej modyfikację przestrzeni fizycznej w taki sposób, aby przestępstwa nie występowały,
- stanowiącej szczególną formę zarządzania, projektowania oraz manipulowania środowiskiem fizycznym, w którym nieustannie popełniane są przestępstwa,
- będącej praktycznym narzędziem zapobiegania przestępczości opartym na udowodnionym twierdzeniu, że sposób projektowania środowiska może mieć wpływ na przestępczość,
- nawiązującej do odpowiedniego projektowania i efektywnego użytkowania środowiska mogącego redukować zdarzenia przestępcze i lęk przed przestępczością, przyczyniając się do polepszenia jakości życia,
- opartej na zarządzaniu planowaniem przestrzennym, projektem i miejscem w celu zmniejszenia prawdopodobieństwa wystąpienia w tym samym miejscu i czasie elementów składowych przestępstwa.

CPTED można określać również jako zestaw technik i → s t r a t e g i i [t. 4], które powinny być realizowane w odniesieniu do konkretnego terytorium z uwzględnieniem jego specyfiki oraz wyjątkowości społeczności, która je zamieszkuje. Koncepcja ta opiera się na różnych założeniach, spośród których można wskazać te właściwe dla tzw. CPTED pierwszej generacji (obowiązujące do lat 90. XX w.), właściwe dla tzw. CPTED drugiej generacji (powstałe w latach 90. XX w. na fali krytyki dotyczącej stosowania zasad CPTED pierwszej generacji) oraz najnowsze, właściwe dla tzw. CPTED trzeciej generacji.

CPTED pierwszej generacji opiera się na następujących zasadach:

- Naturalna delimitacja terytorialna (ang. *territoriality*) – pojęcie to oznacza zdolność środowiska do tworzenia stref wpływów i w konsekwencji budowania poczucia przynależności do pewnego obszaru, idącego za tym przywiązania do niego oraz chęci jego obrony. Naturalna delimitacja terytorialna wiąże się z jasną i czytelną demarkacją terenu, wyraźnym rozgraniczeniem pomiędzy poszczególnymi rodzajami przestrzeni (publiczną, semipubliczną, semiprywatną, prywatną), jak również z budowaniem w mieszkańcach danego obszaru poczucia przynależności i odpowiedzialności. Założenie to można realizować przez projektowanie przestrzeni sprzyjającej tworzeniu miejsc, które podkreślają lokalną przynależność. Czytelne wyróżnienie poszczególnych typów przestrzeni i jej wyraźne oznaczenie (zarówno poprzez fizyczne, jak i symboliczne bariery) skutkuje tworzeniem „obszarów kontroli", które funkcjonują zgodnie z wewnętrznymi normami i zwyczajowymi sposobami zachowania. Każde obce lub podejrzane zachowanie (np. zachowanie kryminalne) staje się wówczas bardziej widoczne.

- Naturalna obserwacja (ang. *natural surveillance*) – jest to obserwacja dokonywana przez mieszkańców danego obszaru w trakcie wykonywania przez nich codziennych czynności (np. podczas spaceru z psem czy zabawy z dziećmi w piaskownicy). W przeciwieństwie do obserwacji formalnej – przeprowadzanej np. przez patrole policyjne czy firmy wynajęte do ochrony – nie wymaga ona wprowadzenia na teren osiedla obcych osób mogących wywoływać w mieszkańcach wzrost poczucia → z a g r o ż e n i a [t. 4]. Naturalna obserwacja pobudza odpowiedzialność za użytkowany teren oraz wzmacnia poczucie więzi pomiędzy użytkownikami uprawnionymi do korzystania z niego. Jednym ze sposobów zwiększania naturalnej kontroli jest organizowanie miejsc, w których mogą się spotykać ludzie – placów zabaw, boisk, bibliotek itp. Zaleca się również odpowiednie rozmieszczenie oświetlenia i budynków, tak aby użytkownicy terenu mieli większą możliwość zauważenia intruza. Elementem wspierającym wdrażanie tej zasady CPTED jest stosowanie obserwacji technicznej, tj. monitoringu wizyjnego (CCTV).
- Kontrola dostępu (ang. *access control*) – polega na rozgraniczeniu poszczególnych przestrzeni oraz ukształtowaniu terenu tak, by dostęp do stref prywatnych i semiprywatnych był możliwy tylko dla ich użytkowników. Zaleca się w tym względzie wykorzystanie naturalnych środków kontroli dostępu, takich jak odpowiednie usytuowanie budynków, wejść, ścieżek i dróg, terenów zielonych, ogrodzeń itp. Zgodnie z tą zasadą w trosce o codzienne potrzeby mieszkańców należy unikać stosowania zabezpieczeń utrudniających im poruszanie się w przestrzeni osiedla.
- Zarządzanie i konserwacja (ang. *management and maintenance / image and milieu*) – strategia ta opiera się na założeniu, że słaby stan techniczny elementów otoczenia i brak troski o nie sprzyjają pojawianiu się przestępczości na danym obszarze. W związku z tym należy właściwie gospodarować przestrzenią, np. niwelując przejawy wandalizmu, graffiti, rozbite szyby i in., które mogą świadczyć o tym, że dane terytorium nie ma właściciela. Zarządzanie i konserwacja w praktyce oznaczają tworzenie przyjaznego, estetycznego środowiska i jego cykliczne odnawianie (np. odświeżanie elewacji, naprawa uszkodzonych znaków, opróżnianie koszy). Przyczynia się to do tworzenia więzi społecznych i zwiększania poczucia → b e z p i e c z e ń s t w a użytkowników przestrzeni. W konsekwencji stosowania tej zasady zmniejsza się również prawdopodobieństwo popełnienia czynów przestępczych, gdyż z perspektywy sprawcy obszar tak zarządzany staje się nieatrakcyjny.
- Wzmacnianie celu (ang. *target hardening*) – zasada ta polega na wzmacnianiu widocznych systemów bezpieczeństwa w celu odstraszenia potencjalnych przestępców. W praktyce oznacza używanie drzwi antywłamaniowych, odpowiednich zamków, zabezpieczanych okien, alarmów itp. Należy podkreślić, że strategia ta budzi wiele kontrowersji i trwają dyskusje, czy powinna stanowić element CPTED.

- Wsparcie aktywności (ang. *support activities*) – polega na kształtowaniu przestrzeni oraz wykorzystywaniu symboli i znaków umożliwiających korzystanie z przestrzeni publicznej zgodnie z jej przeznaczeniem.

W CPTED drugiej generacji skoncentrowano się na tworzeniu środowiska wewnętrznego oraz na budowie relacji między użytkownikami przestrzeni, ponieważ to właśnie użytkownicy mogą tworzyć najlepsze mechanizmy kontroli danego obszaru. Oparto ją na następujących zasadach (tzw. 4C, od pierwszych liter nazw w j. ang.):

- Spójność społeczna (ang. *social cohesion*) – zasada ta odnosi się do budowy i wzmacniania relacji łączących mieszkańców osiedli, sąsiadów, sprzedawców osiedlowych sklepów i innych stałych użytkowników danego terenu. Można to realizować np. poprzez prowadzenie szkoleń wzmacniających społeczne kompetencje, uruchamianie programów skierowanych na twórcze rozwiązywanie problemów, organizowanie sąsiedzkich grup patrolowych (zob. → p a t r o l o b y w a t e l s k i [t. 3]) czy przekazanie części odpowiedzialności za organizację życia osiedla w ręce wspólnot mieszkańców, które decydowałyby o wprowadzaniu zmian, remontów i in.
- Łączność (ang. *connectivity*) – oznacza formalną lub nieformalną drogę wymiany → i n f o r m a c j i [t. 2] pomiędzy głównymi użytkownikami danego terenu w postaci np. tablic ogłoszeniowych, okresowo ukazujących się gazetek, forum internetowego mieszkańców itp.
- Kultura wspólnoty (ang. *community culture*) – to strategia koncentrująca się na tworzeniu poczucia wspólnoty poprzez promowanie lokalnych inicjatyw, takich jak np. wydarzenia kulturalne, organizowanie festiwali, spotkań tematycznych, wspólne uprawianie sportów.
- Próg wydolności (ang. *capacity treshold*) – wydolność oznacza zdolność przystosowania danej przestrzeni do zamierzonego jej wykorzystywania, natomiast próg wydolności to pewien poziom równowagi umożliwiający prawidłowe funkcjonowanie przestrzeni, który w przypadku zachwiania wpływa na tę przestrzeń w negatywny sposób. Przykładem może być opuszczanie mieszkań w wyniku wyprowadzki lokatorów, które może zadziałać jak magnes dla potencjalnych sprawców aktów wandalizmu czy przestępstw i tym samym obniżyć poziom bezpieczeństwa osiedla. Naruszenie równowagi wyrównują tzw. społeczne stabilizatory – funkcję taką mogą pełnić np. miejsca spotkań członków lokalnej społeczności, takie jak świetlice, place zabaw, sale do gier.

W CPTED trzeciej generacji w sposób nowatorski uwzględnione zostały elementy, które równolegle przyczyniają się do kształtowania energooszczędnej i niskoemisyjnej gospodarki, a w konsekwencji prowadzą do → z r ó w n o w a ż o n e g o r o z w o j u [t. 4] miast. Dodatkowo w strategii tej skoncentrowano się na kształtowaniu bezpiecznych przestrzeni z uwzględnieniem adaptowania w mieście rozwiązań biorących pod uwagę postępujące zmiany klimatyczne. CPTED trzeciej generacji opiera się na 4 elementach:

- Miejsce – element ten skupia się na warstwie fizycznej miasta; polega na włączaniu w strukturę miasta odpowiedniej ilości przestrzeni publicznej, która – właściwie zagospodarowana – aktywizuje mieszkańców do działania i wpływa na budowę relacji i łączących ich więzi. Istotną rolę odgrywa tu integracja adekwatnej do potrzeb ilości terenów zielonych (parków, skwerów, zielonych dachów itp.), wspieranie działań rewitalizacyjnych, odpowiednie oświetlenie, precyzyjne określenie odpowiedzialności podmiotów i osób za przestrzeń oraz właściwe prowadzenie gospodarki finansowej umożliwiającej bieżące dokonywanie napraw, konserwacji i utrzymanie budynków oraz ich otoczenia w dobrym stanie.
- Ludzie – element ten skupia się na warstwie społecznej miasta; polega na budowie odpowiedniej infrastruktury pozwalającej na komunikowanie się mieszkańców, zgłaszanie swoich potrzeb, postulatów oraz wyrażanie przez nich opinii.
- Technologie – element ten dotyczy wykorzystywania zielonych technologii w mieście oraz wdrażania ekologicznych rozwiązań przyczyniających się do ochrony środowiska.
- Sieci – element ten spaja ze sobą 3 poprzednie strategie; uwzględnia się tu 3 rodzaje sieci:
  - sieci fizyczne – łączące miejsca i zapewniające racjonalną dystrybucję zasobów (takie jak sieci energetyczne, kanalizacyjne, wodociągowe itp.);
  - sieci społecznościowe – sieci społeczne pozwalające na budowanie wzajemnego zaufania i więzi wspólnoty mieszkańców;
  - sieci cybernetyczne – nowoczesne technologie umożliwiające wzajemną komunikację między mieszkańcami i władzami miasta.

Specjaliści podkreślają, iż zasady CPTED pierwszej, drugiej i trzeciej generacji powinny ze sobą współistnieć i być w takiej samej mierze uwzględniane przy tworzeniu lub rewitalizacji przestrzeni jako wieloaspektowy, kompleksowy program prewencyjny (zob. → p r o g r a m y p r o f i l a k t y c z n e i p r e w e n c y j n e [t. 3]).

Agnieszka Polończyk

R.I. Atlas, 2*1st Century Security and CPTED: Designing for Critical Infrastructure Protection and Crime Prevention*, CRC Press, Boca Raton 2013; C. Casteel, C. Peek-Asa, *Effectiveness of Crime Prevention Through Environmental Deisgn (CPTED) in Reducing Robberies*, „American Journal of Preventive Medicine" 2000, vol. 18, iss. 4; G. Cleveland, G. Saville, *2nd Generation CPTED: An Introduction to 2nd Generation CPTED – part 1*, „CPTED Perspective: The International CPTED Association Newsletter" 2003, vol. 6, iss. 1; T.D. Crowe, *Crime Prevention Through Environmental Design: Applications of Architectural Design and Space Management Concepts*, Butterworth-Heinemann, Boston 1991; R. Głowacki i in., *CPTED jako strategia zapewniania bezpieczeństwa społeczności lokalnej*, Wydawnictwo Archidiecezji Lubelskiej Gaudium, Szczytno 2010; J. Jacobs, *The Death and Life of Great American Cities*, Vintage Books, New York 1992; C.R. Jeffery, *Crime Prevention Through Environmental Design*, Sage, Beverly Hills 1971; K. Łojek, *Zapobieganie przestępczości przez kształtowanie bezpiecznej przestrzeni, cz. 1*, „Przegląd Policyjny" 2004, nr 1–2; tenże, *Zapobieganie przestępczości przez kształtowanie bezpiecznej przestrzeni, cz. 2*, „Przegląd Policyjny" 2004, nr 3; Mesa Police Department,

Crime Prevention Through Environmental Design, Mesa Police Department, Mesa 2015; O. Newman, *Defensible Space: Crime Prevention Through Urban Design*, Macmillan, New York 1972; *Zapobieganie przestępczości przez kształtowanie przestrzeni*, J. Czapska (red.), Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2012.

CYBERATAKI – → z a g r o ż e n i a [t. 4] związane z użytkowaniem sieci komputerowych w ramach różnego rodzaju działalności przestępczej – nielegalnego osiągania korzyści materialnych i niematerialnych – oraz cyberatakami, czyli oddziaływaniem na możliwości polityczne, obronne i inne. W przeszłości cyberataki stanowiły próbę wykazania niedoskonałości sieci lub po prostu były formą zabawy, dziś jest to już odmiana → c y b e r w o j n y, → c y b e r t e r r o r y z m u, cyberrewolucji, zastraszania, szantażu albo kradzieży (mienia lub danych). Cyberatak jest szczególnym zagrożeniem dla krajów, których sieci komputerowe są mało odporne na działania związane z atakami informatycznymi (przestarzałe, niedoinwestowane, bez wystarczających zabezpieczeń i pozbawione nadzoru). Największym ułatwieniem dla crackerów jest występowanie łatwej do penetracji i mało odpornej na atak sieci oraz powszechna niska świadomość społeczna wobec takiego zagrożenia i jego skutków w każdej możliwej postaci. → Cy b e r p r z e s t r z e ń w ogólnym znaczeniu to przestrzeń komunikacyjna tworzona przez system powiązań internetowych. Jest przestrzenią otwartego komunikowania się za pośrednictwem połączonych komputerów i systemów informatycznych na całym świecie. Powszechne używanie sieci komputerowych w systemach zarządzania, przesyłania i nadzorowania/gromadzenia danych w niemal wszystkich dziedzinach funkcjonowania państwa/człowieka jest powszechnie akceptowane i podlega ciągłemu rozwojowi. Nikt obecnie nie wyobraża sobie życia bez systemów komputerowych, internetu czy chociażby elektronicznych form obrotu pieniędzmi. Informatyczne ataki są zagrożeniem dla krajów, których sieci komputerowe są mało odporne na działania związane z atakami informatycznymi. Przyczyn, które powodują, że zagrożenie cyberatakiem jest duże i stale rośnie, jest wiele. Do najczęściej wymienianych zalicza się: silne powiązania ekonomiczno-biznesowe między różnymi firmami/koncernami, powiązania polityczno-ekonomiczne oraz militarne między różnymi krajami, słabą odporność i nikłą ochronę systemów przekazywania danych w kontekście tych zagrożeń, ubogą infrastrukturę techniczną i słabość systemów wykrywania, przeciwdziałania i neutralizacji, niską świadomość i wiedzę użytkowników o wspomnianych zagrożeniach i ich skutkach, brak odpowiednich struktur (instytucji, ośrodków czy biur) zajmujących się analizą, zapobieganiem cyberatakom i udoskonalaniem systemu przeciwdziałania, brak uregulowań prawnych – zarówno krajowych, jak i międzynarodowych – zapobiegających i skutecznie odstraszających (zob. → o d s t r a s z a n i e [t. 3]). Z jednej strony → c y b e r p r z e s t ę p c z o ś ć stanowi więc raczej pośrednie zagrożenie dla → b e z p i e c z e ń s t w a n a r o d o w e g o i → b e z p i e c z e ń s t w a m i ę d z y n a r o d o w e g o. Jednostki i grupy zajmujące się tym procederem niezwykle rzadko biorą na cel elementy systemu obronnego lub

→ i n f r a s t r u k t u r y k r y t y c z n e j [t. 2] kraju. Z drugiej jednak strony współczesna skala cyberprzestępczości sprawia, że mimo wszystko może ona negatywnie wpływać m.in. na rozwój gospodarczy czy funkcjonowanie administracji publicznej.

Nawet pomimo nowoczesnego systemu zabezpieczeń w krajach o wysoko rozwiniętej technologii (jak Japonia, Australia, USA, Niemcy, Francja, Kanada, Wielka Brytania) powiązania polityczne, ekonomiczne czy społeczne z krajami o uboższej i mniej zaawansowanej infrastrukturze techniczno-informatycznej narażają te pierwsze na atak oraz powodują utrzymanie wysokich nakładów na przeciwdziałanie im i ochronę własnych sieci. Należy pamiętać, że ataki w sieci odbywają się z użyciem coraz bardziej zaawansowanych technik i metod przenikania, a także są poprzedzone głęboką analizą wrażliwych punktów i obszarów zarówno samej sieci, jak i całego jej otoczenia i obsługujących ją osób. Według specjalistów firmy → K a s p e r s k y L a b [t. 2] zajmującej się przeciwdziałaniem zagrożeniom w sieci i ich analizą ryzyko związane z cyberatakiem jest praktycznie tak samo prawdopodobne w każdym miejscu na świecie, ale skala ataków może już być różna.

W 2002 r. podczas szczytu → N A T O [t. 3] w Pradze po raz pierwszy otwarcie zaczęto mówić o zagrożeniach związanych z atakami w cyberprzestrzeni oraz o sposobach zapobiegania im. W 2010 r. podczas szczytu w Lizbonie jedno z przyjętych założeń nowego programu strategicznego określało ramy współpracy i możliwości poszczególnych członków paktu w zwalczaniu ataków tego typu. W 2004 r. utworzono NATO Computer Incident Response Capability (NCIRC), które na mocy kontraktu z Finmeccanica i Northrop Grumman za 50 mln EUR zostało w maju 2014 r. zmodernizowane do prowadzenia operacji przez 24 godz. na dobę przez 7 dni w tygodniu. Powstałe w 2010 r. w NATO Emerging Security Challenges Division (ESCD) ma w swej strukturze sekcję obrony przed cyberatakami. W 2012 r. utworzono NATO Communications and Information Agency (NCIA), która przewodniczy programowi Multinational Cyber Defence Capability Development (MN CD2). Założycielami MN CD2 były Finlandia, Kanada, Rumunia, Norwegia i Holandia, a głównym powodem jego utworzenia było zwiększenie własnych zdolności w zakresie rozpoznania i zwalczania zagrożeń w sieci. NATO Industry Advisory Group (NIAG) zajmuje się organizowaniem szkoleń i badań w zakresie bieżących i przyszłych problemów związanych z użytkowaniem sieci komputerowych. Zgodnie z zapisem art. 5 traktatu również cyberatak jest obecnie traktowany jako → a g r e s j a i podlega zapisom tego postanowienia. NATO traktuje wojnę w cyberprzestrzeni jako jedną z form ataku i obrony na równi z konwencjonalnymi działaniami sił zbrojnych. Jednym z założeń szczytu walijskiego z 2014 r. było ustalenie tzw.

NATO Industry Cyber Partnership (NICP) określającego 2 zasadnicze programy – środków zapobiegania zagrożeniom i ochrony sieci NATO z uwzględnieniem identycznych potrzeb w ramach wewnętrznych sieci narodowych poszczególnych członków sojuszu. W 2013 r. Komisja Europejska opublikowała dokument *Cyber Security*

Strategy. Jest to wstępny projekt dyrektywy UE dotyczący przeciwdziałania zagrożeniom i ochrony sieci komputerowych. Dokument precyzuje również podstawowe poziomy ochrony zabezpieczeń w elektronicznych systemach przesyłania i analizy danych. Inne poruszane w nim kwestie są związane z elastycznością działań w sieci (i jej skutkami), wzrostem świadomości o zagrożeniach i działaniami badawczo-rozwojowymi w tym obszarze, a także z rozwojem rynku produktów dających ochronę systemom komputerowym na różnych poziomach wykorzystania.

Dyrektywa UE nakłada obowiązki na poszczególnych członków, ale również przekazuje pewne mechanizmy działania dla prywatnego i publicznego sektora.

W listopadzie 2014 r. Rada Europy zaaprobowała Cyber Defence Policy Framework. Dokument opiera się na 5 obszarach: wsparcia rozwoju zdolności zapobiegania naruszeniom w sieci dla poszczególnych członków UE, zwiększenia ochrony sieci komputerowych używanych w krajach UE, wsparcia cywilno-militarnego, rozwoju systemu edukacji oraz współpracy z partnerami spoza UE.

Niektóre → r e ż i m y [t. 3] w sposób mniej lub bardziej oficjalny dokonują ataków w sieci, agencje rządowe i → w y w i a d y [t. 4] wielu państw z kolei, posługując się crackerami na całym świecie, całkowicie nieoficjalnie atakują obszary ważne pod względem prowadzonej przez nich działalności, a przede wszystkim własnego → b e z p i e c z e ń s t w a . Takie działania są prowadzone w oderwaniu od międzynarodowych i wewnętrznych uregulowań prawnych. W przypadku ich wykrycia konsekwencje z tego powodu są dla strony atakującej znikome.

Nie należy też zapominać, że sieć komputerowa jest doskonałym miejscem do działania dla wszelkich radykalnych grup i organizacji (w tym terrorystycznych), które również w sposób oficjalny, za pośrednictwem swoich stron i for internetowych, wpływają na szereg osób, oddziałują na ich poglądy, opinie i zachowanie. Dla struktur militarnych takich jak NATO zagrożenia płynące z ataków w sieci komputerowej mają charakter militarnego zakłócania lub wręcz osłabiania potencjału sojuszu na różnych poziomach działalności (administracyjnym, logistycznym, szkoleniowym, operacyjnym itp.). Natomiast problem cyberataku w obszarach narodowych czy politycznych, np. wobec krajów UE, jest rozpatrywany w 2 aspektach: przeciwko realizowanej polityce i przeciwko pewnym obszarom (takim jak bezpieczeństwo, energia czy transport).

Należy jednak podkreślić konieczność zapewnienia ścisłej współpracy w tym zakresie między militarnymi i cywilnymi strukturami na różnych poziomach wzajemnych relacji. Brak takiej współpracy i skutecznych mechanizmów ochrony/obrony może bowiem doprowadzić do użycia elementów sieci do ataku na inne struktury i obszary.

Dostęp do sieci jest otwarty (pomijając mniejsze lub większe ograniczenia w niektórych krajach), ale nie oznacza to, że nie należy rozwijać mechanizmów i sposobów analiz czy zabezpieczeń przed cyberatakiem oraz zwiększać świadomości społecznej o związanych z tym zagrożeniach. Ważnym i nadal niedostatecznie rozwiązanym

problemem są krajowe i międzynarodowe uregulowania prawne związane nie tylko z analizą i wykrywaniem zagrożeń w cyberprzestrzeni oraz zapobieganiem im, lecz także z ich skutecznym eliminowaniem i karaniem ich wykonawców. Analizy i programy badawcze w zakresie ochrony cyberprzestrzeni pozwolą w przyszłości na stworzenie mechanizmów zapobiegających skutkom ataków lub redukujących ich skutki w różnych obszarach funkcjonowania państw, organizacji, przemysłu czy dla zwykłych obywateli.

Łukasz Czekaj

A. Adamski, *Media w analogowym i cyfrowym świecie. Wpływ cyfrowej rewolucji na rekonfigurację komunikacji społecznej*, Dom Wydawniczy Elipsa, Warszawa 2012; tenże, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy*, Wydawnictwo Dom Organizatora, Toruń 2001; A. Bógdoł-Brzezińska, M. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjne we współczesnym świecie*, ASPRA-JR, Warszawa 2003; A.M. Colarik, *Cyber Terrorism: Political and Economic Implications*, Idea Group, London 2006; Ł. Czekaj, *Cyberatak*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2015; P. Rutkowski, *Strategia cyberbezpieczeństwa Unii Europejskiej – pilne wyzwania, nieśpieszna debata*, [w:] *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*, K. Liedel, P. Piasecka, T.R. Aleksandrowicz (red.), Difin, Warszawa 2014.

CYBERBEZPIECZEŃSTWO – koncepcja kompleksowej formy reakcji podejmowanych za pomocą środków technicznych i nietechnicznych w celu ochrony przed → c y b e r z a g r o ż e n i a m i. Wykształciła się na poziomie strategicznym państw, organizacji rządowych, a także przy projektowaniu systemów IT w sektorze prywatnym. Z racji specyfiki → c y b e r p r z e s t r z e n i i dynamicznego rozwoju branży IT cyberbezpieczeństwo w tego typu → s t r a t e g i a c h [t. 4] czy dokumentach → b e z p i e c z e ń s t w a jest ujmowane z perspektywy stanu końcowego, który dana instytucja planuje osiągnąć.

W literaturze wskazuje się 3 podstawowe cele zapewnienia bezpieczeństwa w cyberprzestrzeni:

- poufność – zachowanie prywatności, objęcie tajemnicą poprzez narzucenie kontroli i limitowanie dostępu do danych przy użyciu odpowiednich rozwiązań technicznych i prawnych;
- integralność – ochrona przed dokonywaniem zmian przez nieuprawnione podmioty lub przed dokonywaniem zmian bez koniecznej autoryzacji;
- dostępność – możliwość korzystania z zasobów zgodnie z oczekiwaniami i potrzebami.

Do tej triady celów dodaje się także odporność. Przyjmując za nieuchronne i niemożliwe do wyeliminowania istnienie → z a g r o ż e ń [t. 4] w cyberprzestrzeni, za wartość należy uznać takie przygotowanie systemów, które pozwala przetrwać → c y b e r a t a k i kontynuować normalne funkcjonowanie.

Same zagrożenia cyberbezpieczeństwa są natomiast klasyfikowane w literaturze jako awarie, wypadki i ataki. Można przyjąć, że wypadki i awarie zależą od czynników technicznych, mają więc charakter losowy, nie są wynikiem celowego działania osoby lub grupy osób. Różnią się tylko pochodzeniem przyczyny względem systemu: zewnętrznej (wypadki) albo wewnętrznej (awarie). Ataki natomiast to wszystkie zdarzenia, których zaistnienie jest powiązane z działaniem człowieka.

Zagrożenia dla cyberbezpieczeństwa można podzielić także w inny sposób, gdy linie podziału przebiegać będą na następujących płaszczyznach:

- podmiotowej – przestępcy, terroryści, podmioty państwowe;
- motywacyjnej – chęć zysku, chęć wywarcia nacisku politycznego, chęć uzyskania → i n f o r m a c j i [t. 2], chęć osiągnięcia przewagi militarnej, forma żartu, chęć zaistnienia w określonym środowisku, zdobycia popularności czy rozgłosu;
- *modus operandi* – działanie doraźne lub długofalowe, działanie z rozgłosem lub ukryte.

Opierając się na powyższych determinantach, w literaturze wymienia się jako zagrożenia w różnych konfiguracjach: → h a k t y w i z m [t. 2], → c y b e r t e r r o r y z m , → c y b e r p r z e s t ę p c z o ś ć , → c y b e r s z p i e g o s t w o (wojskowe, polityczne, ekonomiczne) oraz → c y b e r w o j n ę.

M. Lakomy wyróżnia zagrożenia nieustruktualizowane – haking, haktywizm, haktywizm patriotyczny, cyberprzestępczość – oraz zagrożenia ustrukturalizowane – cyberterroryzm, cyberszpiegostwo, operacje zbrojne w cyberprzestrzeni.

Etap początkowy branży IT nie obejmował równolegle prac nad cyberbezpieczeństwem – informatyka w założeniach miała być domeną elitarnych grup naukowców, zakładającą transparentność: normą było wzajemne zaufanie wszystkich użytkowników, niewielka ilość punktów końcowych, co ułatwiało weryfhację. Dynamiczny rozwój technologii i rosnący poziom funkcjonalności komputerów doprowadził do informatyzacji społeczeństw na skalę globalną, bez uprzedniego uwzględnienia czynników ryzyka. Pierwsze kroki w celu określenia ryzyka zostały podjęte w USA dopiero na zlecenie prezydenta R. Reagana. Została do tego oddelegowana Narodowa Rada Bezpieczeństwa (National Security Agency, NSA), a efektem jej prac była dyrektywa 145 NSA, która jest pierwszym dokumentem podejmującym temat polityki państwa odnośnie do komputerów i systemów informatycznych. Rząd USA następnie przekazał NSA odpowiedzialność za zatwierdzanie norm i urządzeń wykorzystywanych w telekomunikacji i zautomatyzowanych systemach bezpieczeństwa, wraz z uprawnieniami do oceny podatności sieci rządowych. Dopiero w 1987 r. Kongres zatwierdził ustawę o bezpieczeństwie komputerów, która ustanowiła Narodowy Instytut Standardów i Technologii (NIST) i przejęcie przez niego wcześniejszych zadań NSA. Ostatecznie jeszcze przed 1987 r. poziom cyberataków przeprowadzanych przez środowiska hakerskie naruszył → b e z p i e c z e ń s t w o n a r o d o w e USA.

Przyjęte założenia okazały się niewystarczające. W latach 90. XX w. oraz na początku XXI w. doszło do wielu cyberataków, które w sposób znaczący spenetrowały systemy informatyczne państw. Do większych operacji można zaliczyć Moonlight Maze, cyberatak wymierzony w NASA i Departament Energii USA, czy Titan – akt cyberszpiegostwa wobec Departamentu Obrony USA. Zdecydowane kroki zostały podjęte dopiero za prezydentury G.W. Busha. Opracowano 2 dokumenty, które bezpośrednio odnosiły się do cyberbezpieczeństwa w USA. Były to National Security Presidential Directive 38 oraz National Strategy to Secure Cyberspace. Było to pierwsze ujęcie koncepcji cyberbezpieczeństwa, wyznaczało priorytety dla rządu federalnego i przemysłu.

Jednym z kluczowych założeń, które do dziś jest elementem wielu strategii cyberbezpieczeństwa na poziomie krajowym i międzynarodowym, jest zależność poziomu cyberbezpieczeństwa sektora publicznego od sektora prywatnego – który zarządza stosunkowo większą ilością dostępnej cyberprzestrzeni i → infrastruktury krytycznej [t. 2]. Nacisk rynku spowodowany wzrostem cyberprzestępczości oraz działania legislacyjne rządu USA zmusiły twórców oprogramowania, producentów oprogramowania antywirusowego, sprzętów i inżynierów sieci do ulepszenia standardów dotyczących bezpieczeństwa już w fazie planowania projektów oraz wdrożenia systemu aktualizacji do istniejących produktów.

Ogólnoświatowy przełom w podejściu do cyberbezpieczeństwa datuje się na lata 2007–2008. Można przyjąć, że doszło wtedy do poważnych naruszeń cyberbezpieczeństwa, chodzi mianowicie o serię głośnych cyberataków w Estonii w 2007 r. oraz cyberincydent w armii USA, nazywany operacją Buckshoot Yankee. Oba incydenty były swoistym wstrząsem dla kadr zarządzających, nie tylko w USA i w Europie, w konsekwencji na całym świecie rozpoczęto wdrażanie nowych polityk i strategii na rzecz cyberbezpieczeństwa oraz utworzono szereg agencji lub wyspecjalizowanych jednostek – zarówno cywilnych, jak i wojskowych – mających charakter zarówno ofensywny, jak i defensywny, zajmujących się zwalczaniem zagrożeń w cyberprzestrzeni. Jako przykłady należy wymienić: NATO Cooperative Cyber Defence Centre of Excellence, Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (ENISA), Europejskie Centrum ds. Walki z Cyberprzestępczością będące agencją → EUROPOL u [t. 2], Rządowe Zespoły Reagowania na Incydenty Komputerowe w poszczególnych państwach (CERT).

Problematyka cyberbezpieczeństwa jest też przedmiotem niesłabnącego zainteresowania nie tylko ze strony państw, ale także organizacji międzynarodowych. Pod patronatem Rady Europy już w 2001 r. opracowana została konwencja o cyberprzestępczości, ratyfikowana przez Polskę dopiero w 2015 r. Wskazuje ona przede wszystkim, jakie środki powinny przyjąć związane nią państwa w ramach ich prawa wewnętrznego, zarówno materialnego, jak i procesowego, aby zapewnić ściganie i karanie przestępstw przeciwko poufności informacji, integralności i dostępności danych informatycznych, przestępstw komputerowych, przestępstw związanych z pornografią

dziecięcą w cyberprzestrzeni oraz przestępstw związanych z naruszeniem praw autorskich i pokrewnych.

Komisja Europejska w komunikacie z 2007 r. adresowanym do Parlamentu Europejskiego, Rady Europejskiej i Komitetu Regionów odnotowała potrzebę podjęcia na szczeblu unijnym współpracy ukierunkowanej na szeroko rozumiane zwalczanie przestępstw w cyberprzestrzeni. Wskazano na problemy związane z określeniem jurysdykcji krajowej i prawa właściwego, transgranicznym ściganiem przestępstw oraz uznawaniem i stosowaniem dowodów elektronicznych, a także na konieczność usprawnienia koordynacji zwalczania cyberprzestępczości na szczeblu europejskim i międzynarodowym. Za cel Komisja postawiła opracowanie unijnej strategii w sprawie zwalczania i ścigania cyberprzestępczości.

Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń przyjęta została w 2013 r. jako rezolucja Parlamentu Europejskiego. W strategii przedstawiono program działań dotyczący realizacji 5 strategicznych priorytetów:

- osiągnięcia odporności na zagrożenia cybernetyczne,
- ograniczenia cyberprzestępczości,
- opracowania polityki obronnej i rozbudowy zdolności w dziedzinie bezpieczeństwa cybernetycznego w powiązaniu ze wspólną polityką bezpieczeństwa i obrony,
- rozbudowy zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa,
- ustanowienia spójnej międzynarodowej polityki w zakresie cyberprzestrzeni dla UE.

Co istotne, w dokumencie zawarto nawiązanie do art. 222 Traktatu o funkcjonowaniu Unii Europejskiej zawierającego tzw. klauzulę solidarności. Już we wspólnym komunikacie w sprawie przyjęcia strategii cyberbezpieczeństwa, opracowanym uprzednio przez Komisję Europejską i Wysokiego Przedstawiciela Unii ds. zagranicznych i polityki bezpieczeństwa, zaznaczono, że w przypadku „szczególnie poważnego incydentu lub ataku" cybernetycznego państwo członkowskie może powoływać się na klauzulę solidarności UE. W żadnym z tych dokumentów nie wspomina się natomiast o art. 42 ust. 7 Traktatu o Unii Europejskiej, który zawiera „obowiązek udzielenia pomocy i wsparcia wszelkimi dostępnymi środkami, zgodnie z art. 51 Karty Narodów Zjednoczonych w przypadku agresji zbrojnej".

Wspomnieć należy także o dyrektywie dotyczącej ataków na systemy informatyczne mającej na celu ujednolicenie prawa wewnętrznego państw członkowskich poprzez wyznaczenie minimalnych standardów w zakresie definiowania przestępstw popełnianych w cyberprzestrzeni oraz sposobu ich karania, a także ustalenie zasad współpracy w zakresie ich ścigania. W dokumentach Sojuszu Północnoatlantyckiego kwestie cyberbezpieczeństwa ujmowane były wielokrotnie, choć w sposób ogólny. W koncepcji strategicznej → N A T O [t. 3] z 2010 r. wskazano cyberataki jako coraz częściej występujące źródło zagrożeń dla narodowego i euroatlantyckiego dobrobytu, bezpieczeństwa

i stabilności. Kolejna strategia przyjęta została w 2014 r. pod nazwą Wzmocnionej Polityki Cyberobrony (Enhanced Cyber Defence Policy) podczas szczytu w Newport w 2014 r. W deklaracji końcowej szczytu zawarto stwierdzenie: „obrona cybernetyczna należy do podstawowych zadań kolektywnej obrony NATO". Do problematyki tej nawiązano ponownie w końcowym komunikacie, podsumowującym prace szczytu NATO w Warszawie w 2016 r., uznając cyberprzestrzeń za „obszar działań, w którym NATO musi bronić się tak samo skutecznie jak w powietrzu, na lądzie i na morzu". W czasie szczytu przyjęto także zobowiązanie do wzmacniania i rozwijania systemów cyberobrony poszczególnych państw, przedstawiciele NATO i UE wydali zaś wspólną deklarację dotyczącą przyszłej współpracy, m.in. właśnie w zakresie cyberbezpieczeństwa.

Podkreśleniu wagi problemu cyberbezpieczeństwa przez NATO towarzyszyło zaznaczenie, że wobec zagrożeń w cyberprzestrzeni i w reagowaniu na nie państwa NATO kierują się tymi samymi zasadami, co w przypadku zagrożeń w innych obszarach. Wreszcie, dopiero podczas szczytu NATO w Warszawie jednoznacznie zadeklarowano rozciągnięcie możliwości zastosowania art. 5 traktatu północnoatlantyckiego o kolektywnej obronie na przypadki incydentów w cyberprzestrzeni.

Spośród istotnych polskich dokumentów dotyczących cyberbezpieczeństwa oprócz Doktryny Cyberbezpieczeństwa Rzeczypospolitej z 2015 r. wymienić należy Politykę Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej z 2013 r. oraz Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016. W doktrynie cyberbezpieczeństwa wyróżniono jako cyberzagrożenia w wymiarze wewnętrznym: cyberprzestępczość, → c y b e r p r z e m o c, cyberprotesty czy cyberdemonstracje; do zagrożeń w wymiarze zewnętrznym zaliczono natomiast: → c y b e r k o n f l i k t y, cyberkryzysy, cyberwojnę, cyberszpiegostwo. Jako źródła zagrożeń w cyberprzestrzeni podano organizacje ekstremistyczne, terrorystyczne oraz zorganizowane transnarodowe grupy przestępcze, których ataki w cyberprzestrzeni mogą mieć podłoże ideologiczne, polityczne, religijne, biznesowe i kryminalne.

Rządowy program ochrony cyberprzestrzeni zakłada osiągnięcie celu strategicznego, czyli zapewnienie ciągłego bezpieczeństwa cyberprzestrzeni państwa poprzez stworzenie ram organizacyjno-prawnych oraz systemu skutecznej koordynacji i wymiany informacji między administracją publiczną oraz innymi podmiotami i użytkownikami cyberprzestrzeni RP, w tym przedsiębiorcami. Program zakłada podział kompetencji w zakresie ochrony cyberbezpieczeństwa pomiędzy poszczególne organy, instytucje i przedsiębiorstwa, a także zasady nadzorowania i koordynowania ich prac. W programie wiele miejsca poświęcono szeroko rozumianej edukacji wielu różnych grup, od młodzieży szkolnej po kadry urzędnicze.

W ramach działań zmierzających do zapewnienia cyberbezpieczeństwa prowadzone są ćwiczenia obejmujące symulację cyberataków i obrony, odpowiedzi na nie. UE organizuje tego rodzaju ćwiczenia od 2010 r., NATO od 2008 r., USA od 1997 r.

Wojciech Cendrowski

M.D. Cavelty, *Cyber – Security*, [w:] *The Routledge Handbook of New Security Studies*, J.P. Burgees (ed.), Routledge, London–New York, 2010; W. Cendrowski, *Cyberbezpieczeństwo*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; Deklaracja szczytu walijskiego Złożona przez Szefów Państw i Rządów uczestniczących w posiedzeniu Rady Północnoatlantyckiej w Walii 5 września 2014 r.; Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW, Dz. Urz. UE L 218/8 z 14.08.2013 r.; Komunikat ze szczytu NATO w Warszawie Wydany przez Szefów Państw i Rządów uczestniczących w posiedzeniu Rady Północnoatlantyckiej w Warszawie w dniach 8 i 9 lipca 2016 r.; *Koncepcja strategiczna obrony i bezpieczeństwa członków Organizacji Traktatu Północnoatlantyckiego, przyjęta przez szefów państw i rządów w Lizbonie*, tłum. A. Juszczak, „Bezpieczeństwo Narodowe" 2014, nr 1; Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r., Dz. U. 2015, poz. 728; Rezolucja Parlamentu Europejskiego z dnia 12 września 2013 r. w sprawie strategii bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń (2013/2606(RSP)), Dz. Urz. UE C 93/112 z 9.03.2016 r.; M. Roscini, *Cyber Operations and the Use of Force in International Law*, Oxford University Press, Oxford, 2014; Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016 r., Warszawa 2010; P.W. Singer, A. Friedman, *Cybersecurity and Cyberwar, What Everyone Needs to Know*, Oxford University Press, New York 2014.

CYBERBROŃ (BROŃ CYBERNETYCZNA) – to środki walki o charakterze cybernetycznym, które zostały zaprojektowane lub wykorzystane do zadania ran lub śmierci ludziom oraz zniszczenia lub destrukcji obiektów, sprzętów i systemów. To także → złośliwe oprogramowanie [t. 4], które może zakłócić, nawet pośrednio, działanie komponentów systemów broni i zabezpieczeń nieprzyjaciela.

Aby dane narzędzie uznać za broń, musi ono spełniać 2 kryteria:

- pierwotnego przeznaczenia – określone narzędzie jest zaprojektowane i wytworzone w celu wyrządzenia szkody ludziom lub zniszczenia sprzętu;
- intencji użycia – podmiot używa narzędzia w celu wyrządzenia szkody ludziom lub niszczenia sprzętu, nawet jeśli nie było to pierwotnym przeznaczeniem danego narzędzia.

Cyberbroń postrzega się przez pryzmat 2 ujęć:

- w ujęciu węższym cyberbroń jest narzędziem o charakterze ofensywnym;
- w ujęciu szerszym cyberbroń to różnorodne narzędzia cybernetyczne – od nieskomplikowanych programów szpiegowskich i wirusów komputerowych po programy mogące wywołać katastrofalne skutki w świecie fizycznym, porównywalne do ataków konwencjonalnych, takie jak utrata życia lub zdrowia ludzi, uszkodzenie znacznej wartości mienia.

Narzędzia wykorzystane w cyberincydencie klasyfikujemy za pomocą kryterium intencji sprawcy i wpływu, jaki zastosowane narzędzie wywiera na obiekt (zarówno fizyczny, jak i niematerialny – wirtualny). Według pierwszego kryterium, aby dane narzędzie mogło być sklasyfikowane jako cyberbroń, musi spełniać warunek, jakim jest jego przeznaczenie (cel, motyw atakującego). Określenie, czy dane narzędzie spełnia

te przesłanki, nie jest łatwe. Aby to ustalić, należy dokładnie przeanalizować → c y b e r a t a k . Dla przykładu, jeśli dane firmowe takie jak poufne → i n f o r m a c j e [t. 2] czy dane klientów zostaną wykradzione w następstwie cyberataku, to można założyć, że działanie takie zostało podjęte w celu odniesienia korzyści przestępczych. Z kolei jeśli sieć zostanie zaatakowana, a witryna rządowa zablokowana, ale nie zostaną skradzione dane, to najprawdopodobniej mamy do czynienia z działaniem w imię idei (→ h a k t y w i z m [t. 2]), a celem ataku nie było niszczenie – stąd wniosek, że narzędzie, które zostało użyte do wywołania tego incydentu, nie powinno zostać oznaczone jako cyberbroń.

Drugie z wymienionych kryteriów, czyli wpływ, odnosi się do niszczycielskich lub śmiercionośnych zdolności cyberbroni. Może się on różnić w perspektywie krótkoi długoterminowej. Jeśli zniszczenie obiektu lub śmierć człowieka jest skutkiem działania w → c y b e r p r z e s t r z e n i, to narzędzie, które do tego doprowadziło, można nazwać cyberbronią. Żadne z tych kryteriów nie powinno być stosowane osobno. Aby decyzja o klasyfikacji danego narzędzia jako broni była właściwa, konieczne jest wykorzystanie różnych kryteriów i dogłębna analiza incydentu. R. Dewar wskazuje, że w podjęciu decyzji może pomóc dwustopniowy test, który polega na odpowiedzi na poniższe pytania:

- Jaki był motyw zastosowanego narzędzia?
- Jaki był wpływ narzędzia na atakowany obiekt?

Należy pamiętać, że te same narzędzia mogą być cyberbronią lub mogą nie zostać za nią uznane. Wszystko zależy od celu, w jakim zostały wykorzystane. Dodatkowo należy zaznaczyć, że to, czy dane narzędzie zostało uznane za cyberbroń, jest decyzją polityczną.

Aby zakwalifikować operację cybernetyczną jako atak, zwraca się także uwagę na konsekwencje wykorzystania cyberbroni. Cyberbroń ma kilka charakterystycznych cech, które przemawiają za wysoką częstotliwością jej wykorzystania. Są to: niskie koszty wyprodukowania i wykorzystania, elastyczność czasowo-przestrzenna (cyberbroń zapewnia możliwość wyboru odpowiedniego czasu i miejsca oddziaływania na wybrany cel), wysoka skuteczność (ze względu na precyzję), znaczna anonimowość i → b e z p i e c z e ń s t w o atakującego. Broń cybernetyczna chroni atakujące osoby fizyczne przed narażeniem utraty zdrowia lub życia. Ponadto cyberbroń ma globalny zasięg. Podobny obszar oddziaływania mogą zapewnić wyłącznie systemy kosmiczne, jednak w kategoriach mobilności i szybkości cyberbroń ma nad nimi przewagę.

Cyberbroń ma także wiele wad. Dla przykładu raz wykorzystana cyberbroń najprawdopodobniej zostanie rozpoznana i nie będzie już więcej użyteczna. Innymi wadami są jej krótki czas przydatności oraz wąska specjalizacja.

Aby danej broni nadać charakter cybernetyczny, muszą zostać spełnione następujące przesłanki:

- jest używana w kontekście → c y b e r w o j n y rozumianej jako konflikt aktorów zarówno państwowych, jak i niepaństwowych, charakteryzujący się wykorzystaniem cyberprzestrzeni w celu osiągnięcia, utrzymania i obrony przewagi operacyjnej i/lub taktycznej;
- narzędzie może powodować uszkodzenie ludzi albo sprzętu pośrednio lub bezpośrednio;
- atak przeprowadzony zostaje przy wykorzystaniu technologii informatycznych, internetu.

Zgodnie z tymi kryteriami za cyberbroń może być uznany Stuxnet, czyli wirus zaprojektowany w celu dokonania blokady rozwoju irańskiego programu nuklearnego. Jego pierwsze wykorzystanie datuje się na 2010 r., jednak prace nad pierwszą wersją wirusa, wg danych z raportu opublikowanego przez firmę Symantec, zaczęły się już w 2005 r. Celem było zaburzenie działania oprogramowania odpowiedzialnego za monitorowanie pracy wirówek do wzbogacania uranu w ośrodkach atomowych w Natanz i Fordo. Stuxnet paraliżował pracę w ww. placówkach i wybierał losowo kilka maszyn, które w porze nocnej, z maksymalną głośnością, odtwarzały utwory zespołu muzycznego AC/DC.

Międzynarodowi eksperci nie mają wątpliwości, że za wykorzystaniem wirusa przeciwko Iranowi stały USA i Izrael. Miało się to odbywać w ramach tajnej operacji pod kryptonimem Olympic Games. Program rozwoju cyberbroni był wdrażany już w 2006 r. przez administrację G.W. Busha, a kontynuowany od 2009 r. przez B. Obamę.

Inne przykłady wykorzystania cyberbroni:

- 1988 r. – robak Morrisa,
- 2007 r. – DDoS – atak na Estonię,
- 2008 r. – DDoS – atak na Gruzję,
- 2012 r. – Shamoon.

Obecnie tworzone są programy mające na celu rozwój cyberbroni. Przykładowo w USA realizowany jest tzw. Plan X. Jest to program prowadzony przez Defense Advanced Research Projects Agency (DARPA), amerykańską agencję rządową, która zajmuje się rozwojem technologii wojskowych i działa w strukturach Departamentu Obrony. Plan X służy do opracowania platform dla Departamentu Obrony w celu planowania, prowadzenia i oceny zdolności w cyberwojnie. Program łączy środowiska akademickie, przemysł obronny, komercyjny przemysł technologiczny i ekspertów ds. → c y b e r b e z p i e c z e ń s t w a .

Międzynarodowy Związek Telekomunikacyjny (International Telecommunication Union, ITU), jedna z organizacji wyspecjalizowanych ONZ, stworzył ranking Global Cybersecurity Index. Jest to klasyfikacja przedstawiająca poszczególne państwa pod względem ich przygotowania na ataki cyfrowe. Państwa oceniane są w kilku kategoriach, takich jak środki prawne, środki techniczne, środki organizacyjne, budowanie zdolności oraz współpraca. Poniższa tabela ukazuje pierwsze 10 państw w rankingu z 2018 r. Polska zajęła w nim 29. miejsce.

Tab. 1. Ranking Global Cybersecurity Index z 2018 r.

Miejsce w rankingu	Państwo
1.	Wielka Brytania
2.	USA
3.	Francja
4.	Litwa
5.	Estonia
6.	Singapur
7.	Hiszpania
8.	Malezja
9.	Kanada
10.	Norwegia

Źródło: *Global Security Index (GCI) 2018*, ITU.int (dostęp 1.01.2020).

Głównym miejscem opracowywania norm dotyczących broni cybernetycznej jest Cooperative Cyber Defence Centre of Excellence (CCD CoE) w Estonii. Centrum zostało założone 14 maja 2008 r. To międzynarodowa organizacja działająca pod auspicjami → NAT O [t. 3], której misją jest zwiększenie zdolności, współpraca i wymiana informacji między państwami członkowskimi NATO oraz między NATO a partnerami zewnętrznymi w zakresie cyberobrony na podstawie edukacji, badań, rozwoju, zdobytych doświadczeń i konsultacji. T. Stevens wymienia kilka czynników, które powodują problem z ustanowieniem odpowiednich regulacji prawnych na gruncie prawa międzynarodowego w zakresie broni cybernetycznych:

- brak porozumienia podmiotów w zakresie norm tworzenia, posiadania i użycia cyberbroni,
- fizyczna natura broni cybernetycznych a wirtualne środowisko,
- relacje wielkich mocarstw,
- czynniki rynkowe.

Represyjne wykorzystanie przez rządy technologii cybernetycznych w 2010 r. podczas arabskiej wiosny było bodźcem do rozszerzenia ram kontroli eksportu o narzędzia cyberbezpieczeństwa, w tym służących do przeprowadzania testów penetracyjnych. Jednym z dokumentów, który dotyczy broni cybernetycznej, a konkretnie ram kontroli jej eksportu, jest Porozumienie Wassenaar. Jest to pierwsze globalne wielostronne porozumienie w sprawie kontroli eksportu broni konwencjonalnej oraz produktów i technologii podwójnego zastosowania. Zostało zawarte w 1994 r., zaczęło zaś obowiązywać we wrześniu 1996 r. W 2017 r. na corocznym grudniowym spotkaniu przedstawicieli 41 członków porozumienia w Wiedniu do dokumentu wprowadzono wyjątki w zakresie kontroli eksportu wskazanych środków. Zwolnienia te stwierdzają m.in., że kontrole nie mają zastosowania do ujawniania luk w zabezpieczeniach ani do działań związanych z reagowaniem na incydenty cybernetyczne.

W 2013 r. rząd brytyjski i francuski wynegocjowały dodanie 2 elementów do listy technologii podwójnego zastosowania – oprogramowania penetracyjnego i systemów nadzoru komunikacji sieci IP. Nieprecyzyjne zapisy, w tym definicje zawarte w porozumieniu, miały także tworzyć bariery w globalnej współpracy. Widoczne były różnice w procedurach i licencjach występujących w poszczególnych państwach. Eksperci wskazywali, że kontrole znacznie utrudnią badania nad bezpieczeństwem cybernetycznym i wymianę informacji o podatności na → z a g r o ż e n i a [t. 4]. W przypadku broni cybernetycznych ich kreatorami mogą być zwykli użytkownicy internetu, mający sprzęt i umiejętności. Funkcjonują już rynki cyberbroni, o różnym stopniu legalności, a wielkie mocarstwa tylko wzmagają zbrojenia w tym zakresie. Administracja D. Trumpa już w 2017 r. wyraziła wolę przyspieszenia rozwoju broni cybernetycznej, m.in. inwestując głównie w rozwój potencjału ofensywnego, co z kolei może przyspieszać wyścig zbrojeń i destabilizować stosunki międzynarodowe w tym zakresie.

Agnieszka Warchoł

T. Cross, *New Changes to Wassenaar Arrangement Export Controls Will Benefit Cybersecurity*, 16.01.2018, Forbes.com (dostęp 30.08.2019); R. Dewar, *Cyberweapons: Capability, Intent and Context in Cyberdefense*, Center for Security Studies Cyber Defense Trend Analysis 2017; K. Dymanowski, *Broń cybernetyczna jako uzbrojenie strategiczne nowej generacji*, „Kwartalnik Bellona" 2016, nr 2; F.-S. Gady, *Trump and Offensive Cyber Warfare*, 16.01.2017, TheDiplomat.com (dostęp 30.08.2019); G. Hinck, *Wassenaar Export Controls on Surveillance Tools: New Exemptions for Vulnerability Researc*h, 5.01.2018, LawfareBlog.com (dostęp 30.08.2019); A. Kozłowski, *Porozumienie Wassenaar zagraża sektorowi IT*, 22.07.2016, CyberDefence24.pl (dostęp 30.08.2019); S. Mele, *Cyber-Weapons: Legal and Strategic Aspects*, Italian Institute of Strategic Studies, Rome 2013; J. Roberts, *Plan X*, DARPA.mil (dostęp 12.09.2019); J. Ruohonen, K.K. Kimppa, *Updating the Wassenaar Debate Once Again: Surveillance, Intrusion Software, and Ambiguity*, „Journal of Information Technology & Politics" 2019, vol. 16, iss. 2; T. Stevens, *Cyberweapons: Power and the Governance of the Invisible*, „International Politics" 2018, vol. 55, iss. 3–4, https://ccdcoe.org/ (dostęp 30.08.2019); *Tallinn Manual on the International Law Apllicable to Cyber Warfare*, M.N. Schmitt (red.), NATO Cooperative Cyber Defence Centre of Excellence 2013; A. Warchoł, *Cyberbroń*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; taż, *Wpływ cyberprzestrzeni na bezpieczeństwo państwa na początku XXI wieku* [rozprawa doktorska], Kraków 2017; Wassenaar Arrangement, *List of Dual-Use Goods and Technologies and Munitions List*, Wassenaar Arrangement Secretariat, 2018; Wassenaar.org (dostęp 30.08.2019).

CYBERCENZURA – pierwszy człon terminu odnosi się do pojęć związanych z wykorzystaniem elektroniki do komunikacji między podmiotami lub określenia zjawisk dotyczących środowiska komputerowego, internetu, czy mówiąc szerzej → c y b e r p r z e s t r z e n i . → C e n z u r a z kolei to:

> kontrola publicznego przekazywania informacji, stanowiąca ograniczenie wolności wyrażania poglądów oraz rozpowszechniania informacji. Polega na weryfikacji m.in.: publikacji, widowisk, audycji radiowych, telewizyjnych,

dokonywanej głównie przez organy państwowe lub kościelne z punktu widzenia zgodności ich treści z prawem, polityką państwa, obronnością, moralnością czy zasadami wiary.

Cybercenzura to działalność mająca na celu ograniczenie lub zablokowanie dostępu do pewnych treści zawartych w cyberprzestrzeni (konkretnie w jej komponencie – internecie) obywatelom lub grupom obywateli. Prowadzona jest przez władze państwowe lub dostawców usług internetowych. Cybercenzurą nazywamy kontrolę treści pod względem politycznym lub obyczajowym. Może naruszać prawa jednostki, ale także być dozwolona na gruncie prawa, jeśli ma chronić → b e z p i e c z e ń s t w o i porządek publiczny.

Ograniczenie treści w internecie następuje za pośrednictwem działań takich jak:

- techniczne blokady – ograniczenia są stosowane poprzez blokowanie adresu IP, manipulowanie DNS i blokowanie adresów URL z wykorzystaniem proxy; władze państwowe nie mają bezpośredniej kontroli lub jurysdykcji nad daną stroną internetową;
- autocenzura – zachęcanie autorów do autocenzury; może się to odbywać poprzez groźby zastosowania działań prawnych, nieformalne metody zastraszania, promowanie norm społecznych lub próby przekupstwa;
- usuwanie wyników wyszukiwania – współpraca dostawców usług internetowych z władzami państwowymi w celu usunięcia nielegalnych lub niepożądanych stron z wyników wyszukiwania;
- usuwanie treści – cenzorzy mają bezpośrednią możliwość wyegzekwowania żądania usunięcia spornych lub niepoprawnych ich zdaniem treści internetowych.

Totalna cybercenzura jest trudna w realizacji z uwagi na specyfikę cyberprzestrzeni i jej cechy takie jak transnarodowość, zasięg oddziaływania czy anonimowość. Władze państwowe stoją przed wyborem stopnia cenzury, jej zakresu, a także stopnia interwencji – od nieograniczonego przepływu → i n f o r m a c j i [t. 2] po całkowity zakaz dostępu do treści, a nawet do globalnej sieci.

Istnieje wiele powodów, dla których treści umieszczane w internecie są cenzurowane, np.:

- treści zagrażają wizerunkowi państwa,
- treści zaburzają porządek publiczny i bezpieczeństwo państwa,
- dokonuje się kontroli o charakterze religijnym,
- cenzurę wprowadza się w celu ochrony własności intelektualnej,
- cenzura ma na uwadze ograniczenia kulturowe i dotyczące mniejszości,
- celem cenzury jest ochrona moralna,
- zwalczanie → p r z e s t ę p c z o ś c i [t. 3].

E. Schmidt i J. Cohen wyróżniają 3 modele cybercenzury, które wykorzystują władze państwowe:

- model jawny,

- model mieszany,
- model politycznie i kulturowo akceptowalny.

Model jawny cybercenzury stosuje Chińska Republika Ludowa. Treści zawarte w internecie kontrolowane są przez kilka instytucji, są to: Narodowy Urząd Publikacji i Prasy, Główny Urząd Radia i Telewizji, Ministerstwo Technologii, Informacji i Przemysłu, Państwowa Rada Informacji, Centralny Departament Propagandy, Biuro Państwowej Rady Propagandy Internetu, Biuro Informacji i Opinii Publicznej oraz Biuro Internetu. Te instytucje zajmują się m.in.: nadawaniem licencji witrynom internetowym, wydawaniem wytycznych dla właścicieli największych serwisów internetowych w zakresie treści, obsługą systemu ostrzegania SMS o wydarzeniach i wymaganym sposobie ich przedstawienia, wspomaganiem i kontrolą wewnętrznej cenzury portali internetowych, której dokonują specjalnie zatrudnieni cenzorzy oraz administratorzy sieci filtrujący przepływ informacji. Chiński rząd blokuje całe platformy społecznościowe, np. Facebook czy Instagram. Model mieszany, wg Schmidta i Cohena, stosuje Turcja, model politycznie i kulturowo akceptowalny – Korea Południowa, Niemcy czy Malezja.

Można także wskazać inny podział, wyróżniający 2 rodzaje cybercenzury. Pierwszy dotyczy cybercenzury występującej w zamkniętym systemie internetowym, np. w Chinach, i charakteryzuje się ograniczaniem treści, które mogą zaszkodzić wizerunkowi władzy. Drugi odnosi się do systemu otwartego, np. w Europie, dotyczy likwidacji szkodliwych treści, np. mowy nienawiści czy pornografii dziecięcej. W tym przypadku cybercenzura może być dopuszczalna pod warunkiem, że szkoda spowodowana przez udostępnione treści przewyższa szkodę spowodowaną naruszeniem ogólnego zakazu cenzury.

Cybercenzura jest również jednym ze wskaźników potęgi cybernetycznej w modelu CPI (Cyber Power Index) opracowanym przez zespół → w y w i a d u [t. 4] ekonomicznego czasopisma „The Economist" we współpracy z konsorcjum Booz Allen Hamilton. Celem CPI jest tworzenie rankingów zdolności cybernetycznej państw grupy G20 w zakresie zapobiegania i przeciwdziałania atakom cybernetycznym oraz promowanie problematyki cyberbezpieczeństwa w środowisku międzynarodowym.

W 2014 r. Reporterzy bez Granic (ang. Reporters Without Borders) wydali raport z serii *Wrogowie internetu* (ang. *Enemies of the Internet*), w którym wskazano jednostki lub agencje rządowe, które ograniczają wolność internetu. Wśród wymienionych podmiotów znalazły się: Centre for Development of Telematics (Indie), Government Communications Headquarters (Wielka Brytania), National Security Agency (USA). Autorzy wskazali także firmy z sektora prywatnego, np. Hacking Team (Włochy).

Agnieszka Warchoł

I. Baggili i in., *Cybercrime, Censorship, Perception and Bypassing Controls: An Exploratory Study*, [w:] *Digital Forensics and Cyber Crime*, M. Rogers, K.C. Seigfried-Spellar (eds.),

Springer, New York 2012; R. Białoskórski, *Potęga cybernetyczna państw – pomiar i zastosowanie*, „Zeszyty Naukowe AON" 2015, nr 2 (99); M. Olędzki, *Udział wyszukiwarek internetowych w realizacji idei swobodnego przepływu informacji. Analiza działalności wyszukiwarki Google* [rozprawa doktorska], Warszawa 2016; S. Perry, C. Roda, *Human Rights and Digital Technology. Digital Tightrope*, Palgrave, Paris 2017; Reporters Without Borders, *Enemies of the Internet*, 2014; A. Warchoł, *Cybercenzura*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; B. Warf, *Global Geographies of the Internet*, Springer, London 2013; J. Żdżarski, *Cybercenzura w państwie środka*, 7.02.2010, Polityka.pl (dostęp 12.04.2019).

CYBERDYPLOMACJA – termin składa się z przedrostka „cyber-" oraz rzeczownika „dyplomacja". Prefiks „cyber-" nie występuje jako samodzielne słowo, zazwyczaj używa się go do tworzenia określeń nazywających wykorzystanie elektroniki do komunikacji między podmiotami lub zjawisk nawiązujących do środowiska komputerowego oraz internetu. Po raz pierwszy przedrostek został wykorzystany w terminie „cybernetyka".

„Dyplomacja" (od gr. *diploma*) oznaczała akt urzędowy gwarantujący przywileje nadane przez suwerena, sporządzany na 2 glinianych tabliczkach. W literaturze przedmiotu nie ma jednej akceptowalnej definicji terminu „dyplomacja", jednak występuje konsensus co do badania zjawiska dyplomacji na 3 płaszczyznach. Pierwsza obejmuje dyplomację jako narzędzie polityki zagranicznej państwa, jego urzędową działalność mającą na celu prowadzenie rozmów, korespondencji, rokowań oraz zawieranie umów międzynarodowych. Druga określa dyplomację jako „zespół metod, środków oraz umiejętności z zastosowaniem taktu, ostrożności, argumentacji, a więc sztukę uprawiania zawodu dyplomaty". W trzecim ujęciu bierze się pod uwagę rolę korpusu służby zagranicznej w ministerstwach spraw zagranicznych oraz przedstawicielstwach dyplomatyczno-konsularnych.

Słownik języka polskiego nie uwzględnia terminu „cyberdyplomacja". Występuje on w literaturze przedmiotu, jest jednak – podobnie jak inne pojęcia z przedrostkiem „cyber-" – problematyczny do zdefiniowania. Cyberdyplomacją najczęściej nazywa się wykorzystanie nowych →technologii informacyjno-komunikacyjnych [t. 4] oraz sieci w celu osiągania celów dyplomatycznych, wspierania →interesów narodowych [t. 2], wzmacniania i rozszerzania relacji na arenie międzynarodowej oraz zwiększania →bezpieczeństwa narodowego [t. 1]. Główną jej cechą jest zastosowanie nowoczesnych technologii komunikacyjnych w celu interakcji z szerszą grupą odbiorców.

W literaturze przedmiotu występuje wiele terminów, które odmiennie nazywają zjawisko dyplomacji prowadzonej w →cyberprzestrzeni [t. 1]. Oprócz cyberdyplomacji są to także: dyplomacja elektroniczna, e-dyplomacja oraz dyplomacja cyfrowa. Co do zasady te terminy nie są synonimami, jednak biorąc pod uwagę cechy wspólne ich definiensów, często są używane zamiennie.

W dyplomacji elektronicznej wykorzystywane są narzędzia elektroniczne. Według Justyny Arendarskiej obejmuje ona wszelkie formy praktyki dyplomatycznej, w której wykorzystywane są narzędzia i techniki cyfrowe – nie tylko narzędzia internetowe. W terminie „e-dyplomacja" człon „e-" wskazuje na związek znaczeniowy z internetem. Pierwsze zastosowanie tego przedrostka pojawiło się w handlu elektronicznym jako przejaw wczesnej komercjalizacji sieci. Z kolei termin „dyplomacja cyfrowa" (*digital diplomacy*) eksponuje treści zakodowane cyfrowo, które odczytywane są za pomocą urządzeń elektronicznych. Według definicji Fergusa Hansona dyplomacja cyfrowa to wykorzystanie internetu i nowych technologii komunikacji informacyjnej do osiągnięcia celów dyplomatycznych. Badacz opisał, jak zmieniła się dyplomacja dzięki nowym możliwościom technologicznym. Wśród jej cech charakterystycznych wymienił:

- docieranie z przekazem do szerokiego grona odbiorców, co zwiększa wpływy polityczne nadawcy;
- skierowanie komunikatu do konkretnych grup odbiorców;
- zwiększenie świadomości dyplomatów na temat ruchów społecznych i politycznych, zwłaszcza tych napędzanych oddolnie;
- nieprzerwany dostęp do → i n f o r m a c j i [t. 2] i opinii społeczeństwa;
- walka o głosy i konkurowanie z innymi osobami w tych samych warunkach przy braku barier komunikacyjnych, w tym także z osobami fizycznymi i organizacjami, które odnoszą większe sukcesy w kontrolowaniu polityki zagranicznej niż władze państwowe.

Hanson podkreślił, że dyplomacja cyfrowa jest ważnym elementem wspierania polityki zagranicznej kraju, ponieważ umożliwia bezpośrednią interakcję zagraniczną publicznością i jej zaangażowanie. Natalia Chaban, Serena Kelly i Anne-Marie Brady zdefiniowały dyplomację cyfrową jako formę dyplomacji publicznej, która obejmuje wykorzystanie technologii cyfrowych i → m e d i ó w s p o ł e c z n o ś c i o w y c h [t. 3] przez państwa w celu nawiązania komunikacji z zagranicznymi odbiorcami przy niskich kosztach.

Dyplomacja prowadzona za pośrednictwem cyberprzestrzeni bez wątpienia jest dyplomacją publiczną. Jej celem jest kształtowanie pozytywnego wizerunku państwa nadawcy oraz pożądanych postaw wobec niego. Ilan Manor i Elad Segev wyróżnili 2 poziomy dyplomacji cyfrowej: ministerstwa spraw zagranicznych i ambasady. Według autorów podmioty państwowe działając na tych poziomach, mogą dostosować politykę zagraniczną oraz branding narodowy do konkretnych odbiorców z uwzględnieniem historii, kultury i tradycji. Podobnie opisuje dyplomację cyfrową Dev Lewis, wskazując, że jest to wykorzystanie cyfrowych narzędzi komunikacji (mediów społecznościowych) przez dyplomatów w celu komunikowania się ze sobą oraz z ogółem społeczeństwa.

W dyplomacji cyfrowej kluczową rolę odgrywają narzędzia internetowe, takie jak: portale instytucji państwowych prowadzone w różnych językach; konta na X (dawniej

Twittter), Facebooku, Instagramie, TikToku, Snapchacie; internetowe transmisje na żywo; Google+ itd., nazywane narzędziami typu 2.0. Cechy nowych narzędzi, które wykorzystują dyplomaci, pozwalają na użycie terminu „dyplomacja 2.0", który coraz częściej pojawia się w literaturze przedmiotu. Popularne stało się także określenie „dyplomacja wahadłowa" (*shuttle diplomacy*), której prowadzenie znacznie ułatwiają nowoczesne technologie i cyberprzestrzeń.

Wykorzystanie nowoczesnych technologii w dyplomacji sięga lat 90. XX w. Podczas Konferencji Narodów Zjednoczonych na temat Środowiska i Rozwoju w 1992 r. uczestnicy po raz pierwszy korzystali z poczty elektronicznej i list mailingowych w celu koordynacji stanowisk w negocjacjach. Kolejnym wydarzeniem, które wpłynęło na rozwój zjawiska, było powstanie pierwszego Wydziału ds. Zastosowań Komputerowych w Dyplomacji (Establishment of the Unit for Computer Applications in Diplomacy) przy MEDAC (The Mediterranean Academy of Diplomatic Studies) na Malcie. W 2002 r. jednostka przekształciła się w Diplo Foundation, organizację non profit, której celem jest rozwój zdolności w zakresie dyplomacji i stosunków międzynarodowych, w tym dyplomacji publicznej, dyplomacji elektronicznej i zarządzania internetem.

Poszczególne etapy rozwoju cyberdyplomacji obejmowały korzystanie przez dyplomatów z komputerów, internetu, w tym z poczty elektronicznej i stron internetowych, powstanie i zastosowanie mediów społecznościowych, takich jak: Facebook czy X, oraz blogów. Pojawienie się każdego nowego e-narzędzia to wyzwanie dla służb dyplomatycznych, a jego wykorzystanie wiąże się z modyfikacją tradycyjnego wykonywania zadańw polityce zagranicznej.

Wyróżnia się 3 aspekty oddziaływania nowoczesnych technologii na dyplomację:

- zmieniają środowisko, w którym podejmowane są działania dyplomatyczne;
- generują nowe instrumenty do pełnienia funkcji dyplomatycznych;
- są przedmiotem działań dyplomatycznych.

Cyberprzestrzeń umożliwia dyplomatom i przedstawicielom władz państwowych realizację codziennych czynności komunikacyjnych, np. wysyłanie wiadomości, dostęp do informacji, rozpowszechnianie informacji, obsługę konsularną, wirtualną współpracę czy prowadzenie negocjacji.

Cyberdyplomacja to przede wszystkim możliwość realizacji polityki zagranicznej „na odległość". Dzięki cyberprzestrzeni dyplomaci mogą wykonywać swój zawód w czasie, gdy nie mogą podróżować czy spotykać się osobiście. Kiedy pandemia → C O V I D 1 9 [t. 5] objęła znaczną część świata, przywódcy państw i dyplomaci musieli przystosować się do pracy w domu przez odbywanie dwustronnych i wielostronnych spotkań w trybie online za pośrednictwem aplikacji na urządzeniach mobilnych. 6 lutego 2020 r. odbyła się pierwsza nieformalna wideokonferencja ministrów zdrowia państw członkowskich Unii Europejskiej w celu omówienia spraw związanych z wybuchem → p a n d e m i i [t. 5] COVID-19. Kolejne stały się już powszechną praktyką. Media społecznościowe są łącznikiem między nadawcą – dyplomatą

– a odbiorcami z całego świata, co umożliwia szybką wymianę informacji między stronami. Placówki dyplomatyczne zintegrowane z centralą tworzą model sieciocentryczny, przez co synchronizacja zadań jest szybka i efektywna. Przepływ informacji następuje nie tylko na linii centrala – placówki, lecz także między placówkami, co pozwala na lepszą koordynację zadań i szybkie uzupełnianie danych. Platformy społecznościowe pozwalają obywatelom na realny udział w kształtowaniu polityki zagranicznej państwa. Kontakt z politykami czy dyplomatami stał się możliwy w każdej chwili i z każdego miejsca na świecie, zwiększyła się także kontrola społeczna.

Zgodnie z rankingiem tworzonym przez firmę Burson-Marsteller, dostępnym na stronie internetowej www.twiplomacy.com, X (dawniej Twitter) jest obecnie najbardziej popularnym e-narzędziem wśród przedstawicieli władz państwowych, dziennikarzy, publicystów oraz instytucji międzynarodowych. Ten serwis społecznościowy z usługą mikroblogowania nazywany jest nawet „dyplomatycznym barometrem".

Jednym z niebezpieczeństw, jakie stoją przed cyberdyplomacją, jest bez wątpienia problem wiarygodności zamieszczanych informacji, a także brak pewności ze strony odbiorców co do nadawcy wiadomości. Na platformach społecznościowych jest wiele fikcyjnych kont, a część użytkowników nie weryfikuje ich legalności i autentyczności. Fake newsy są powszechną praktyką i często powodują napięcia w stosunkach dyplomatycznych. Niewłaściwe wykorzystanie nowych mediów przez dyplomatów może powodować spadek skuteczności komunikowania, upraszczanie przekazu oraz spłycenie języka dyplomacji do języka mediów. Zagrożeniem dla pozycji dyplomatów jest także rosnąca rola innych aktorów publicznych, np. liderów państwowych, ministerstw, agencji i fundacji rządowych, a także organizacji pozarządowych oraz korporacji, którzy z cyberprzestrzeni korzystają za pomocą tych samych narzędzi, stosując te same metody i kanały komunikacji co zawodowi dyplomaci. Dodatkowo zagrożeniem dla bezpieczeństwa państwa, związanym z wykonywaniem zadań dyplomatycznych w cyberprzestrzeni, jest wyciek informacji. Przykładem jest WikiLeaks, czyli witryna internetowa, na której anonimowoopublikowane zostały dokumenty rządowe i korporacyjne, z których część miała klauzulę tajności. Dotyczyły one m.in.: → w o j n y [t. 4] w Iraku,wojny w Afganistanie czy więźniów z bazy Guantanamo. Za pośrednictwem witryny internetowej WikiLeaks opublikowano także kilkaset tysięcy depesz dyplomatycznych z amerykańskich ambasad na całym świecie. Ponadto haking (hakerstwo), haktywizm, → c y b e r p r z e s t ę p c z o ś ć[t. 1], → c y b e r s z p i e g o s t w o [t. 1], → c y b e r t e r r o r y z m [t. 1] oraz wiele innych → c y b e r z a g r o ż e ń [t. 1], które występują na wszystkich płaszczyznach funkcjonowania państwa, dotyczą również polityki zagranicznej prowadzonej w cyberprzestrzeni.

Józef Bátora określił 3 potencjalne scenariusze zmian, jakie powstają w wyniku oddziaływania nowoczesnych technologii na dyplomację:

- tzw. eksport ryzyka – nowoczesne technologie wpływają na transformację zasad organizacyjnych dyplomacji i jej roli w środowisku międzynarodowym. Powstają

horyzontalne struktury sieciowe, społeczeństwa zyskują wpływ na państwową politykę zagraniczną a ministerstwa spraw zagranicznych tracą monopol na prowadzenie działań dyplomatycznych;

- utrzymanie *status quo* w dyplomacji, czyli nowoczesne technologie nie przyczyniają się do zmian na gruncie działań dyplomatycznych. Postęp technologiczny ułatwia komunikację, ale nie zmienia struktury hierarchicznej w dyplomacji;
- nowoczesne technologie jako „nośnik rewitalizacji" dotychczasowych procedur, norm oraz zasad w dyplomacji. Technologie powodują zmiany, które odnoszą się do praktyki dyplomacji, ale nie dokonują transformacji w samej instytucji dyplomacji i jej roli w stosunkach międzynarodowych.

Dyplomację prowadzoną w cyberprzestrzeni cechuje również możliwość zawierania interakcji i sojuszy, a także udział → społeczeństwa obywatelskiego [t. 4] w pracach rządu. Odnosząc się do tych cech, Antonio Casado Rigalt wyodrębnił termin „dyplomacja 3.0". Olaf Osica rozwinął go i wskazał, że dyplomacja 3.0 jest „oparta na dostępie do zasobów informacyjnych i zarządzaniu wiedzą w zdecentralizowanym środowisku polityki międzynarodowej, w którym państwa i aktorzy niepaństwowi wchodzą w poziome interakcje ze sobą, części sieci współpracują z innymi częściami sieci, włączając w to agencje rządowe, jednostki samorządów lokalnych". Zdaniem Osicy dyplomacja 3.0. dopiero powstaje i w przyszłości będzie ona w pełni cyfrowa. Tym, co odróżnia ją od poprzednich typów, jest „ewolucja polityki zagranicznej w stronę usieciowionego środowiska". Osica trafnie zauważa, że „prawdziwym testem dla polityki zagranicznej w przyszłości będzie zdolność integracji dyplomacji tradycyjnej i cyfrowej".

Agnieszka Warchoł

O.S. Adesina, *Foreign policy in an era of digital diplomacy*, „Cogent Social Sciences" 2017, vol. 3, no. 1; J. Arendarska, *Elektroniczna dyplomacja – nowe narzędzia komunikowania w dyplomacji*, Kwartalnik Naukowy OAP UW „e-Politikon" 2012, nr 4; N. Broś, *Edukacja w dyplomacji publicznej. Cyberdyplomatyczne rozwiązania w międzynarodowym nauczaniu*, „Ogrody Nauk i Sztuk" 2016, t. 6; taż, *Znaczenie nowych technologii dla współczesnej dyplomacji*, „Journal of Political Theory" 2017, nr 22, https://apcz.umk.pl/czasopisma/index.php/DP/article/view/DP.2017.010 (dostęp 25.04.2023); N. Chaban, S. Kelly, A.M. Brady, *Small States in a New Era of Public Diplomacy: New Zealand and Digital Diplomacy*, [w:] *Small States and the Changing Global Order. New Zealand Faces the Future*, A.M. Brady (ed.), Springer, London 2019; F. Hanson, *A Digital DFAT: Joining the 21st Century*, Lowy Institute for International Policy 2010, https://www.files.ethz.ch/isn/124574/ A_digital_DFAT.pdf (dostęp 25.04.2023); tenże, *Baked In and Wired: eDiplomacy@ State*, 25.10.2012, https://www.brookings.edu/wp-content/uploads/2016/06/bakedin-hansonf-5.pdf (dostęp 25.04.2023); B.B. Hocking i in., *Futures for diplomacy. Integrative diplomacy in the 21st century*, Clingendael: Netherlands Institute of International Relations, The Hague 2012; H. Katzan, *Cybersecurity Service Model*, „Journal of Service Science" 2012, vol. 5, no. 2; A. Kusztykiewicz, *Dyplomacja cyfrowa – nowa forma polityki zagranicznej Unii Europejskiej*, „Studia z Polityki Publicznej" 2017, nr 2(14); D. Lewis, *Digital Diplomacy*, 19.12.2014, https://www. gatewayhouse.in/digital-diplomacy-2/ (dostęp 25.04.2023); I. Manor, E. Segev, *America's Selfie: How the US Portrays Itself on Its Social Media Accounts*, [w:] *Digital Diplomacy. Theory and Practice*, C. Bjola, M. Holmes (eds.), Routledge, New York 2015; E. Molendowski, W. Polan, *Dyplomacja gospodarcza. Rola i znaczenie*

w polityce zagranicznej państwa, Wolters Kluwer, Warszawa 2007; O. Osica, *Zmierzch dyplomacji? Polityka zagraniczna w dobie cyfrowej rewolucji*, Klub Jagielloński, Warszawa 2019; A.C. Rigalt, „*Diplomacy 3.0": From Digital Communication to Digital Diplomacy*, http://www.exteriores.gob.es/Portal/es/SalaDePrensa/Multimedia/Publicaciones/Documents/2017_%20ANALISIS_9%20ENG.pdf (dostęp 25.04.2023); J. Siekiera, *Nawiązywanie i utrzymywanie stosunków dyplomatycznych między państwami na przykładzie Rzeczypospolitej Polskiej i Nowej Zelandii*, praca licencjacka, Uniwersytet Wrocławski, Wrocław 2011, http://www.biblioteka-cyfrowa. pl/Content/38808/002.pdf (dostęp 25.04.2023); B. Surmacz, *Ewolucja współczesnej dyplomacji. Aktorzy, struktury, funkcje*, Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, Lublin 2015; A. Warchoł, *Wpływ cyberprzestrzeni na bezpieczeństwo państwa na początku XXI wieku*, praca doktorska, Uniwersytet Pedagogiczny im. KEN w Krakowie, Kraków 2017.

CYBERGRUPY – grupy wyspecjalizowanych informatyków, → h a k e r ó w [t. 2] typu *whitehat*, *blackhat*, *greyhat* itp., przygotowujące i przeprowadzające → c y b e r a t a k i na systemy infrastruktury sieciowej, wykorzystując istniejące luki zabezpieczeń w celu uzyskania nieautoryzowanego dostępu do sieci komputerowej i pozostające niewykryte przez dłuższy czas, najczęściej poprzez cyberataki typu typu APT (ang. *advanced persistent threat*, zaawansowane trwałe zagrożenie). We wczesnych latach 90. XX w. terminem tym określano każdą grupę osób komunikujących się przez sieć, którą łączyło jakieś zainteresowanie, hobby.

Motywacje takich → z a g r o ż e ń [t. 4] mają zazwyczaj charakter polityczny lub gospodarczy. Do tej pory w każdym dużym sektorze biznesowym odnotowano przypadki zaawansowanych technicznie ataków przeprowadzanych przez zorganizowane podmioty, które przeważnie kończyły się kradzieżą danych, szpiegostwem lub zakłóceniem porządku. Newralgicznym celem ataków cybergrup jest zwłaszcza sektor publiczny (w tym rząd), sektor obronny, usługi finansowe, usługi prawne, przemysł, telekomunikacja i wiele innych. Niektóre grupy nie ograniczają się tylko do cyberataków, wykorzystują też metody → i n ż y n i e r i i s p o ł e c z n e j [t. 2], infiltracji bezpośredniej, aby uzyskać dostęp do fizycznej lokalizacji w celu umożliwienia ataków sieciowych.

W krajach rozwiniętych i rozwijających się poziom zabezpieczeń infrastruktury sieciowej (zarówno fizycznej, jak i logicznej) w przypadku dużych podmiotów sektora prywatnego i państwowego przeważnie stoi na wysokim poziomie. Jest to z jednej strony spowodowane określonymi wymaganiami prawnymi, m.in. wskazanymi przez Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), oraz poprzez narzucenie odpowiednich standardów i norm, takich jak np. PN-ISO/IEC 17799:2003.

W związku z tym dokonanie skutecznego złamania zabezpieczeń systemu wymaga:

- eksperckiej wiedzy z wielu wąskich dziedzin bezpieczeństwa IT,

- odpowiedniego przygotowania sprzętu,
- zapewnienia anonimowości,
- poświęcenia znacznego nakładu czasu na przeprowadzenie m.in. tzw. *footprintingu* (czyli zbierania wszelkiego rodzaju wskazówek, → i n f o r m a c j i [t. 2] o infrastrukturze logicznej, fizycznej, pracownikach, procedurach – jest to forma wieloaspektowego → w y w i a d u [t. 4]),
- opracowania oraz przeprowadzenia ataku,
- skutecznego zatarcia śladów naruszenia bezpieczeństwa. Przeprowadzenie całej tej operacji przekracza możliwości pojedynczego człowieka, co jest główną przyczyną stale utrzymującego się trendu wśród hakerów do nawiązywania współpracy.

Cele operacji przeprowadzanych przez cybergrupy są kompleksowe, sprowadzają się w ujęciu definicyjnym do kombinacji → c y b e r s z p i e g o s t w a, sabotażu, rozpoznania i osiągnięcia korzyści finansowych. W praktyce terminologii ochrony danych może być to naruszenie poufności, nienaruszalności, niezaprzeczalności, utraty kontroli dostępu, dostępności.

Wyniki badań instytucji FireEye wskazują, że mediana nieautoryzowanego przebywania w sieci, w której atak APT pozostaje niewykryty, różni się znacznie między regionami – średni czas przebywania w 2018 r. w obu Amerykach wynosił 71 dni, w Europie, Afryce i krajach Bliskiego Wschodu 177 dni, a w krajach rejonu Azji i Pacyfiku nawet 204 dni.

Istotnym zagadnieniem definiującym podmiotowość cybergrup jest aspekt wiążący je z aktorami państwowymi. Z perspektywy prawa międzynarodowego odpowiedzialność za cyberatak można przypisać danemu państwu, jeśli operacje cybernetyczne są prowadzone przez organy państwa, osoby lub podmioty uprawnione na mocy prawa wewnętrznego do wykonywania władzy państwowej. Państwo ponosi odpowiedzialność także za inne podmioty – określane zbiorczo jako aktorzy niepaństwowi – w przypadku, gdy pomiędzy nimi a państwem występuje konkretny związek wynikający z zaangażowania ich przez dane państwo lub działania zgodnie z instrukcjami pochodzącymi od władz państwowych albo pod jego kontrolą.

Tego typu podział ma ścisły związek z prawną kwalifikacją działań podejmowanych w → c y b e r p r z e s t r z e n i przez podmioty niebędące państwami z perspektywy dziedziny prawa międzynarodowego, ponieważ nie stosuje się do nich umów międzynarodowych. W przypadku cyberataku, bez względu na jego skalę i skutki, przeprowadzonego przez podmiot niepaństwowy, kluczowe znaczenie ma naruszenie → s u w e r e n n o ś c i [t. 4] zaatakowanego państwa. Jeśli do niego nie doszło, państwo zaatakowane nie ma prawa do interwencji oraz do użycia siły, nie można bowiem stosować działań odwetowych wobec aktorów niepaństwowych na warunkach i zasadach dotyczących państw. Państwo zaatakowane może natomiast skorzystać z prawa do samoobrony oraz ma możliwość pociągnięcia do odpowiedzialności prawnej kraju,

z którego terytorium przeprowadzono cyberatak, w związku z niezachowaniem staranności w nadzorze nad jego infrastrukturą cybernetyczną.

Do niedawna istniały rozbieżności zdań wobec statusu osób biorących udział bezpośrednio w cyberatakach czy pracujących nad systemami → cyberbezpieczeństwa państwa. Początkowo powoływano instytucje o szerokim spektrum zadań w strukturach organów państw lub osobne piony w agencjach wywiadowczych (np. amerykańska cybergrupa Tailored Access Operations (TAO) wchodziła początkowo w skład NSA), zatem wątpliwe było, czy wobec osób w nich pracujących można stosować regulacje → międzynarodowego prawa humanitarnego [t. 3]. Odpowiedź przyniósł szczyt → NATO [t. 3] w Warszawie w 2016 r., podczas którego rozszerzono zadania kolektywnej obrony o sferę cyberprzestrzeni, w tym także uznając samą cyberprzestrzeń za obszar działań militarnych. Przykładem instytucji oraz tego typu sił zbrojnych w NATO jest Cyberund Informationsraum w Republice Federalnej Niemiec czy United States Cyber Command w USA. W przypadku polskich sił zbrojnych powołano program Cyber.mil.pl, w którego skład wchodzi Narodowe Centrum Bezpieczeństwa, Centrum Operacji Cybernetycznych, Inspektorat Informatyki, → Służba Kontrwywiadu Wojskowego [t. 4], Wojska Obrony Terytorialnej, Wojskowy Instytut Łączności, Akademia Marynarki Wojennej oraz Wojskowa Akademia Techniczna. Nie jest możliwe ustalenie jednoznacznego rankingu państw pod względem siły rażenia w cyberprzestrzeni – mimo że np. NATO uznało cyberprzestrzeń za piąty teatr działań wojennych, do dziś w poważanych ośrodkach badawczych jak Global Firepower czy SIPRI (Stockholm International Peace Research Institute) nie ma żadnych danych wskazujących, który z aktorów państwowych ma przewagę na tym polu. Przyczyn tej sytuacji można doszukiwać się w braku wypracowanych i zaakceptowanych powszechnie narzędzi pomiaru, co uniemożliwia zbudowanie wiarygodnej metody badań. Dużym utrudnieniem w przypadku wielu państw jest brak jakichkolwiek danych, nawet stwierdzających istnienie ew. funkcjonujących grup w strukturach armii. Z racji dużej wagi cyberbezpieczeństwa w sektorze prywatnym firma CrowdStrike zasugerowała badanie czasu, jaki jest potrzebny określonym cybergrupom państwowym na przełamanie systemów zabezpieczeń – wg ich testów najszybsze były cybergupy pracujące dla Federacji Rosyjskiej (18 min, 49 sek.), kolejne miejsce zajęła cybergrupa Korei Północnej (2 godz., 20 min, 14 sek.), na trzecim miejscu byli reprezentanci Chińskiej Republiki Ludowej (4 godz., 26 sek.), na czwartym hakerzy z Islamskiej Republiki Iranu (5 godz., 9 min i 4 sek.).

Obecnie trudno jednoznacznie określić pozycję armii USA w cyberprzestrzeni, jednakże biorąc pod uwagę nakłady finansowe przeznaczane na siły zbrojne, zaawansowanie pod względem technologicznym, udział w znaczących cyberoperacjach ofensywnych i defensywnych, nadal trzeba zakładać, że USA są jednym z najważniejszych aktorów w cyberprzestrzeni. USA w ramach swoich struktur tylko w 2018 r. powołały 133 cybergrupy w 5 kategoriach: 13 cybergrup miało na celu obronę bezpośrednią

USA i ich interesów przed cyberatakami o znaczących konsekwencjach, 68 cybergrup miało chronić krytyczne sieci i systemy należące do Departamentu Obrony, 27 cybergrup było odpowiedzialnych za zintegrowanie cyberataków wspierających plany operacyjne i operacje awaryjne, 25 cybergrup miało zapewniać wsparcie dla procesu planowania i analizy. W samym

U.S. Cyber Command pracuje ok. 16,5 tys. → ż o ł n i e r z y [t. 4], nie licząc pracowników cywilnych. Najsłynniejszą jednostką, której istnienie zostało ujawnione podczas tzw. afery Snowdena, jest Tailored Access Operations (TAO) w Fort Mead w stanie Maryland, zatrudnia ona ok. 600 specjalistów. TAO specjalizuje się w działaniach ofensywnych i defensywnych w cyberprzestrzeni, aktywnie brała udział w → i n w a z j i [t. 2] USA w 2003 r. na Irak, neutralizując cywilne i militarne systemy informatyczne. Ściśle współpracuje z CIA oraz dysponuje najwyższej jakości technologią, jednakże jej największą przewagę stanowi możliwość przeprowadzenia bardzo skutecznych cyberataków typu Quantum.

Na półkuli wschodniej najbardziej znane grupy hakerskie, działające prawdopodobnie pod egidą Chińskiej Republiki Ludowej, to Elderwood Group, Putter Panda, Unit 61398, Comment Crew, Hidden Lynx, Axiom, istnieje też wiele innych. W głównej mierze ich działanie sprowadza się do cyberszpiegostwa. Wyróżnia je wysoki poziom specjalizacji w precyzyjnych atakach na konkretne branże, np. Hidden Lynx atakuje tylko obiekty przemysłu obronnego. Wszystkie istniejące grupy w 2010 r. zjednoczyły się pod nazwą Elderwood Group i przeprowadziły skoordynowany cyberatak nazwany operacją Aurora – zaatakowały ośrodki przemysłowe, instytucje → p r a w c z ł o w i e k a [t. 3] oraz infrastrukturę logistyczną.

Wśród najgroźniejszych grup można także wymienić te mające prawdopodobne wsparcie Federacji Rosyjskiej: APT28 oraz Dragonfly 2.0. APT28 jest odpowiedzialne za cyberataki na oficjalne witryny NATO, OBWE, rządu polskiego i gruzińskiego. Celami Dragonfly są natomiast obiekty przemysłowe oraz energetyczne na całym świecie. Grupa ta najczęściej stosuje zaawansowane techniki ataków typu *watering hole* lub *spear-phishing*, a także infekowanie wirusami o wielopoziomowej strukturze (np. trojany Heriplor, Karagany, Listrix). Dragonfly 2.0 jest także odpowiedzialna za 2 poważne blackouty energetyczne w Ukrainie w 2015 i 2016 r. Istnieje duże prawdopodobieństwo, że hakerzy z tych grup byli odpowiedzialni za cyberataki przy użyciu wirusów: Quasar RAT, Vermin; wirusów typu → r a n s o m w a r e [t. 3]: Petya, WannaCry, NotPetya; czy ransomware typu TeleBots (zob. → z ł o ś l i w e o p r o g r a m o w a n i e [t. 4]).

Skomplikowana sytuacja geopolityczna na Bliskim Wschodzie spowodowała powstanie cybergrup bezpośrednio odwołujących się do państw, które wspierają, np. Iranian Cyber Army (ICA) czy Syrian Electronic Army (SEA). Ich działanie można sklasyfikować jako przejawy → w a l k i i n f o r m a c y j n e j [t. 4], rozpowszechnianie → p r o p a g a n d y [t. 3] poprzez prezentowanie określonych treści na zhakowanych

stronach internetowych, walkę z niezależnymi mediami czy jednostkowe, niewyszukane cyberataki na osoby powiązane ze środowiskiem opozycji. P.J. Springer określa SEA jako czołową arabską grupę hakerską, która przeprowadzała cyberataki także na cele izraelskie. Autor ten uważa, że istnieją przesłanki, iż grupa jest finansowana przez syryjski rząd.

Cybergrupy, które nie są powiązane z żadnymi strukturami państwowymi, przeważnie wywodzą swoje motywacje z idei wolnego dostępu do informacji oraz ochrony praw człowieka. Pierwszą tego typu cybergrupą była Cult of the Dead Cow, która poprzez przeprowadzanie cyberataków oraz działalność haktywistyczną (→ h a k t y w i z m [t. 2]) koncentrowała swoje wysiłki na wyrażaniu sprzeciwu wobec proliferacji → b r o n i m a s o w e g o r a ż e n i a w latach 80. XX w. Na początku drugiego tysiąclecia na forum 4chan.org podobne idee legły u podstaw ruchu Anonymous, słynnego z ataków na strony i bazy danych rządów, korporacji i podmiotów sektora prywatnego, które naraziły się moralnie → o p i n i i p u b l i c z n e j [t. 3]. Grupie przypisywane są akcje przeciwko Kościołowi scjentologicznemu, wspieranie operacyjne wycieków WikiLeaks, przeprowadzanie cyberataków oraz kontrkampanii informacyjnych przeciwko ISIS (zob. → P a ń s t w o I s l a m s k i e [t. 3]), a także działania o wyraźnie politycznym zabarwieniu, jak pośrednie wspieranie opozycji w Rosji (kampania OpRussia) i Iranie w 2009 r., udzielanie instrukcji protestującym przeciwko → r e ż i m o m [t. 3] rządowym podczas arabskiej wiosny czy ataki na strony rządu chińskiego. Z ruchu Anonymous w okolicach 2011 r. odłączyła się grupa hakerów typu *black hat*, która nadała sobie nazwę Lulzsec i zdobyła popularność, zwalczając Anonymous oraz dokonując szeregu włamań na bardzo dobrze zabezpieczone systemy i witryny, ich ofiarą padło m.in. CIA, Sony Pictures oraz wiele innych.

Wojciech Cendrowski

J. Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld*, O'Reilly, Newton 2010; W. Cendrowski, *Cybergrupy*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; *Law of international responsibility*, [w:] *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations*, M.N. Schmitt (red.), Cambridge University Press, Cambridge 2017; P. Shakarian, J. Shakarian, A. Ruef, *Introduction to Cyber-Warfare: A Multidisciplinary Approach*, Elsevier, Waltham 2013; P.J. Springer, *Cyber Warfare: A Reference Handbook*, ABC-CLIO, Santa Barbara–Denver–Oxford 2015.

CYBERKONFLIKT – to każdy konflikt w → c y b e r p r z e s t r z e n i, który obejmuje interakcje między aktorami zaangażowanymi w aktywizm cyfrowy, podmiotami rządowymi, firmami sektora prywatnego. Celem aktorów jest podniesienie świadomości społecznej odnośnie do konkretnego problemu. Zjawisko samo w sobie ma zdecydowanie wymiar oddziaływania politycznego.

Terminem cyberkonfliktu określa się także elementy interakcji członków → c y b e r g r u p – zwłaszcza związanych z ruchami promującymi tzw. wolne

oprogramowanie, związane z hakingiem, *script kiddies*. W takich przypadkach konflikt i → k r y z y s [t. 2] mogą działać jako katalizator lub mechanizm obronny, który prowadzi do ustanowienia struktur, formy zarządzania lub, w przypadku braku zaistnienia wcześniej wymienionych form, dezintegracji grupy. Konflikt jest katalizatorem dla utworzenia tzw. kryptohierarchii i mechanizmów obronnych na zasadzie wymuszania na społeczności rozdzielenia zadań. Poprzez negocjacje i miękką kontrolę społeczność/cybergrupa może rozwijać nowe struktury w celu radzenia sobie z konfliktem, tworzą się wówczas grupy rdzeniowe i peryferyjne oraz kryptohierarchie.

Wyżej opisany scenariusz nie zawsze jest osiągalny – ze względu na ekstremalną polaryzację grup społeczność może nie być w stanie tworzyć nowych struktur, ale rozgałęzia się i poprzez konflikt tworzy mechanizm obronny, pozwalający uniknąć centralizacji. W najgorszym wypadku społeczność dzieli się na 2 części, zanika współpraca między częścią pierwotną a nowo utworzoną. Taka sytuacja może wywołać konflikt konstruktywny lub destrukcyjny, w zależności od poziomu zintegrowania społeczności i zaangażowania grupy.

W tych społecznościach internetowych konflikt i samoorganizacja odgrywają kluczową rolę w powstaniu struktur. Wewnątrzkomunowy konflikt cybernetyczny przebiega w określonych etapach, są to: pojawienie się przywódcy, rozdzielenie na grupy główne i peryferyjne, utworzenie struktur łagodnej kontroli poprzez kryptohierarchiczność. Drugim typem jest cyberkonflikt między społecznościami – występujący w przypadku istnienia zróżnicowania pod względem polaryzacji grupy oraz konfliktu między społecznościami negocjującymi swoją tożsamość, → s t r a t e g i ę [t. 4].

Z perspektywy stosunków międzynarodowych oraz → b e z p i e c z e ń s t w a n a r o d o w e g o cyberkonflikt stał się szerzej analizowanym zagadnieniem po krytyce zawartej w serii artykułów prof. Ch. Demchaka, wykładowcy na U.S. Naval War College, w reakcji na uznanie przez dowództwo armii USA cyberprzestrzeni za kolejną, 5. sferę działań wojennych. Demchak zwraca uwagę, że jest to ujmowanie zjawiska w sposób jednowymiarowy, co w konsekwencji ogranicza ujmowanie → z a g r o ż e ń [t. 4] cyberprzestrzeni do jednej dziedziny oscylującej wokół zagadnień → b e z p i e c z e ń s t w a narodowego, naruszeń → s u w e r e n n o ś c i p a ń s t w a [t. 4] i może prowadzić do źle rozumianego zjawiska → c y b e r w o j n y, która jego zdaniem jest także zbyt wąskim ujęciem w perspektywie zagrożenia bezpieczeństwa narodowego państw, biorąc pod uwagę zjawisko globalizacji. Autor wskazuje, że obecne konflikty, wykraczające zdecydowanie poza ramy związane z cyberprzestrzenią, nabierają charakteru hybrydowego. Nie wszystkie konflikty obejmują także aktorów wyłącznie państwowych, wręcz można zaobserwować trend kontraktowania cybergrup przez podmioty państwowe w sposób uniemożliwiający powiązanie ich z państwem zlecającym w celu uniknięcia odpowiedzialności wynikającej z reguł interpretacji prawa międzynarodowego.

Demchak nie precyzuje także dylematów bezpieczeństwa, jakie są następstwem tego typu incydentów. Sprowadza ich ujmowanie do cyberkonfliktu, by podkreślić

najszersze spektrum zagrożeń cyberprzestrzeni, wykraczające poza powszechne rozumienie zagadnień bezpieczeństwa związanego z informatyzacją różnego rodzaju systemów komputerowych. Rozszerza termin cyberkonfliktu o aspekt dotkniętych nim osób, rzeczy, procesów oraz skutków, takich jak zmiana percepcji oraz internalizacja rzeczywistości grup społecznych.

Dobrym przykładem jest tu → p h i s h i n g [t. 3] – może być → c y b e r a t a k i e m , nawet jeśli jego ofiarą stają się przypadkowe osoby, i wówczas jest traktowany jako przestępstwo, ale może być też częścią cyberoperacji, pierwszym elementem jej fazy przygotowawczej, częścią głównego ataku, elementem centralnym kampanii informacyjnej, → c y b e r s z p i e g o s t w a itp. lub kompleksowym połączeniem wszystkich wymienionych czynników.

W dziedzinie nauk o bezpieczeństwie → i n f o r m a c j i [t. 2] w środowisku naukowym zagadnienie cyberkonfliktu szerzej rozwinęli K. Liedel oraz P. Piasecka, rozróżniając 3 podstawowe formy aktywności:

- aktywizm, rozumiany jako działalność niepowodująca szkód w cyberprzestrzeni, mająca na celu głównie spełnianie funkcji informacyjnych, zwrócenie uwagi społeczności na określone problemy, realizowany głównie poprzez działalność na forach, w mediach i na happeningach;
- → h a k t y w i z m [t. 2], który jest wykorzystaniem hakowania w sposób nie destrukcyjny, ale zakłócający poprawne działanie baz danych, stron internetowych, mający często charakter humorystyczny, jego głównym celem jest zwrócenie uwagi szerszego grona odbiorców na określony problem społeczny, jest to częste działanie podgrup hakerskich typu *script kiddies*, realizowane na zasadzie mało skomplikowanych cyberataków, takich jak wstrzykiwanie kodu MySQL do baz danych czy kodu stron internetowych albo organizacja ataków DDoS;
- → c y b e r t e r r o r y z m, definiowany jako cyberatak lub groźba cyberatatku na sieci i jednostki komputerowe, mająca zastraszyć określone instytucje czy organy władz w celu uzyskania konkretnych działań politycznych, społecznych.

Tego typu ujmowanie podejścia do zagrożeń cyberprzestrzeni zwraca uwagę na subtelne elementy systemu → c y b e r b e z p i e c z e ń s t w a narodowego, który poza posiadaniem niezbędnej ilości środków i możliwości zdominowania działań podczas ewentualnej cyberwojny musi być równocześnie odporny w każdym innym aspekcie na zakłócenia wywołane incydentami bezpieczeństwa w skali pospolitych cyberprzestępstw lub spowodowane przez wykorzystanie cyberprzestrzeni w inny, nowatorski sposób.

Z biegiem lat sprawdza się hipoteza wypracowana w środowisku teoretyków nauk społecznych, która przewidywała dalszy rozwój zjawiska wraz z postępującą transformacją cyfrową, co prowadzi do wykroczenia znaczenia cyberkonfliktu poza aspekty symboliczne i mobilizacyjne. Cyberkonflikt wkracza – obecnie w niewielkim stopniu – do głównego nurtu mediów informacyjnych poprzez współpracę z korporacjami,

kooperację organizacji pozarządowych i działalność nowych formacji społeczno-politycznych, zaczyna być stałym elementem struktury sceny politycznej. Zjawisko nabrało cech → w o j n y i n f o r m a c y j n e j [t. 4] wysokiego poziomu, poza symbolicznymi cyberatakami o wymiarze społecznym o niskim poziomie dochodzi także do ataków na infrastrukturę IT. Przy dalszym nasilaniu się cyberkonfliktu hipotetycznie tego typu działania mogą stracić na znaczeniu.

Wojciech Cendrowski

W. Cendrowski, *Cyberbezpieczeństwo*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; P. Domrowski, Ch.C. Demchak, *Cyber War, Cybered Conflict, and the Maritime Domain*, „Naval War College Review" 2014, vol. 67, nr 2; A. Karatzogianni, *Firebrand Waves of Digital Activism 1994–2014. The Rise and Spread of Hactivism and Cyberconfict*, Palgrave Macmillan, Hampshire 2015; taż, *The Politics of Cyberconflict*, Routledge, New York 2006; M. Libicki, *What Is Information Warfare?*, National Defense University, Washington 1995; K. Liedel, P. Piasecka, *Wojna cybernetyczna – wyzwanie XXI wieku*, „Bezpieczeństwo Narodowe" 2011, nr 1 (17); O. Wasiuta, S. Wasiuta, *Wojna hybrydowa Rosji przeciwko Ukrainie*, Wydawnictwo Arcana, Kraków 2017.

CYBEROPERACJE – (ang. *cyberoperations*, CO) według Departamentu Obrony USA operacje prowadzone w → c y b e r p r z e s t r z e n i [t. 1], z wykorzystaniem wszelkich dostępnych narzędzi. W trakcie cyberoparacji głównym zadaniem sił zbrojnych jest osiągnięcie precyzyjnych celów w cyberprzestrzeni lub za jej pośrednictwem. Te działania prowadzi się za pomocą łączy i węzłów znajdujących się w domenie fizycznej, a następnie wykorzystuje funkcje logiczne do tworzenia efektów – w pierwszej kolejności – w cyberdomenie, jak również (w razie potrzeby) w domenie fizycznej. Cyberoperacje mogą być realizowane przez wojsko lub służby specjalne jako samodzielne operacje bez zaangażowania regularnych sił zbrojnych lub jako – zsynchronizowana z innymi operacjami wojskowymi – misja koordynowana przez dowództwo sił połączonych.

Wyróżnia się 3 rodzaje operacji (misji) prowadzonych w cyberprzestrzeni:

- operacje sieci informacyjnych Departamentu Obrony (ang. *DoD information network operations*; DODIN);
- ofensywne operacje w cyberprzestrzeni (ang. *offensive cyberoperations*; OCO);
- defensywne operacje w cyberprzestrzeni (ang. *defensive cyberspace operations*; DCO);

Sieć informacyjną Departamentu Obrony USA (lub innych państw) rozumie się jako zestaw możliwości informacyjnych i procesów polegających na gromadzeniu, przetwarzaniu, przechowywaniu, rozpowszechnianiu i zarządzaniu → i n f o r m a c j a m i [t. 2] na potrzeby decydentów politycznych lub dowódców wojskowych, jak również systemy łączności, oprogramowania, dane oraz dostępne systemy → b e z p i e c z e ń s t w a [t. 1]. Operacja typu DODIN obejmuje więc działania polegające

na zabezpieczeniu, konfigurowaniu, obsłudze, rozszerzaniu oraz utrzymywaniu infrastruktury Departamentu Obrony (instytucji wojskowych) oraz na zachowaniu jej poufności, dostępności dla użytkowników oraz integralności. Operacje defensywne koncentrują się na obronie DODIN lub innych sieci informacyjnych przed → c y b e r a t a k a m i [t. 1], na powstrzymywaniu potencjalnych przeciwników przez podjęciem decyzji o ataku lub na odbudowywaniu zabezpieczeń, które zostały naruszone. Są one również prowadzone jako odpowiedź na atak agresora. W takiej sytuacji obejmują działania realizowane w obcej cyberprzestrzeni i skutkujące fizycznym uszkodzeniem lub zniszczeniem systemów wroga. Z kolei operacje ofensywne polegają na projekcji siły w cyberprzestrzeni w ramach realizacji celów wyznaczonych przez dowództwo wojskowe lub kierownictwo polityczne państwa. Są skierowane przeciwko systemom uzbrojenia, systemom C2, węzłom logistycznym i innym ważnym obiektom przeciwnika. Podobnie jak operacje obronne będące odpowiedzią na atak, mogą powodować uszkodzenie bądź fizyczne zniszczenia.

Oprócz USA, zdolności do prowadzenia cyberoperacji posiada szereg państw. Do grona tego zalicza się m.in.: Federacja Rosyjska, Chińska Republika Ludowa, Izrael i Iran. W Federacji Rosyjskiej prowadzeniem operacji w cyberprzestrzeni zajmują się jednostki znajdujące się w strukturach Federalnej Służby Bezpieczeństwa (FSB), Służby Wywiadu Zagranicznego (SWR), Głównym Zarządzie Wywiadu (GRU), jak również grupy funkcjonujące poza tajnymi służbami motywowane „względami patriotycznymi". Podobnie jak w pozostałych państwach określane są one jako APT (Advanced Persistent Threat) – podmioty, które uzyskały nieautoryzowany dostęp do sieci komputerowej i pozostają niewykryte przez dłuższy czas, celem przeprowadzenia cyberataku bądź wykradzenia określonych informacji. Do grona APT w Rosji są zaliczane:

- Turla APT (działająca w ramach FSB),
- Jednostka 26165 określana również jako APT28 (działająca w ramach GRU),
- Jednostka 74455 (działająca w ramach GRU),
- Jednostka APT 29 (działająca w ramach SWR).

Jednostka 26165 miała odpowiadać za ingerencję w wybory w Ukrainie w 2014 r., w wybory prezydenckie w Stanach Zjednoczonych, za ataki na Bundestag w 2015 r., na francuską telewizję TV5 Monde, a także na Czarnogórę w latach 2016–2017 (w związku z trwającym procesem akcesyjnym do → NAT O [t. 3]). Jednostka 74455 jest zaliczana do grona najbardziej destruktywnych grup hakerskich na świecie. Jej członkowiemieli realizować głośne operacje, takie jak „NotPetya" i „Olimpic Destroyer". W pierwszej z nich celem agresora stało się pogłębienie destabilizacji Ukrainy oraz zaognienie relacji między Kijowem a Moskwą. Operacja polegała na zainfekowaniu najpopularniejszego w Ukrainie programu służącego do rozliczeń podatkowych (MeDoc) → z ł o ś l i w y m o p r o g r a m o w a n i e m [t. 4]. Jednak operacja wymknęła się spod kontroli i łącznie zostało zaatakowanych ponad 200 tys. komputerów

na świecie,co spowodowało miliardowe straty. Największe miały miejsce w kilku międzynarodowych korporacjach (Maersk, FedEx oraz Merck).

Operacja „Olimpic Destroyer" miała miejsce w 2018 r. w czasie zimowych igrzysk olimpijskich w Korei Południowej. Powodem ataku było odrzucenie udziału sportowców zgłoszonych przez Rosyjski Komitet Olimpijski i Rosyjski Komitet Paraolimpijski. W ramach przygotowań GRU stworzyło sieć fałszywych wersji popularnych południowokoreańskich aplikacji. Spodziewano się, że skłonią one mieszkańców do ich pobierania. Równocześnie wysyłano nieprawdziwe informacje ostrzegające o anomaliach pogodowych. Podczas rozpoczęcia olimpiady złośliwe oprogramowanie zostało aktywowane, co doprowadziło do jej chwilowego paraliżu.

Kibice nie mogli okazywać biletów za pomocą aplikacji MKOl-u, a na stadionie, na którym odbywała się ceremonia otwarcia, stracono połączenie z Wi-Fi. Organizatorom udało się uniknąć poważniejszych konsekwencji dzięki szybkiej reakcji zespołu ds. → c y b e r b e z p i e c z e ń s t w a [t. 1] z Pjongczang, który naprawił wadliwą sieć w ciągu jednej nocy. Rosyjska jednostka 74455 przeprowadziła również cyberataki w 2019 r. na Gruzję. Były one związane z wizytą sekretarza generalnego NATO Jensa Stoltenberga oraz z perspektywą przystąpienia Gruzji do NATO. Cyberatak skierowano w internetowe strony rządowe, biznesowe oraz prasę. Łącznie zhakowano ponad 2 tys. państwowych i prywatnych stron internetowych oraz 2 stacje telewizyjne Imedi i Maestro. Kolejna jednostka – APT29, funkcjonująca w ramach Służby Wywiadu Zagranicznego – była odpowiedzialna m.in. za cyberatak przeprowadzony w 2020 r. na amerykańską firmę SolarWinds, zajmującą się dostarczaniem na rynek systemów służących do zarządzania infrastrukturą IT oraz do jej monitorowania. Dokładnym obiektem ataku stał się system Orion, wykorzystywany przez ponad 30 tys. podmiotów publicznych i prywatnych w USA. Jednostka APT29 wykorzystała wtedy metodę określaną jako atak za pomocą łańcucha dostaw: wprowadziła złośliwy kod Sunburst do systemu Orion. Nieświadomi administratorzy SolarWinds przesłali następnie aktualizację oprogramowania ze zhakowanym kodem do klientów. Poszkodowanych zostało wiele firm i organizacji rządowych funkcjonujących w takich sektorach jak: bezpieczeństwo wewnętrzne, handel, czy finanse, w tym FireEye, Microsoft, Intel, Cisco czy Deloitte.

Równie dynamiczny rozwój grup hakerskich zajmujących się prowadzeniem operacji w cyberprzestrzeni obserwujemy w Chińskiej Republice Ludowej. Jak przyznała U.S. – China Economic and Security Commission, w Państwie Środka funkcjonowało ponad 250 grup hakerskich, zagrażających ekonomicznym interesom Stanów Zjednoczonych. Sandra Watson-Parcels w raporcie pt. *Chinese Hacker Groups*, opublikowanym przez International Institute for Counter-Terrorism w 2018 r., zidentyfikowała 24 grupy hakerskie składające się z jednej lub kilku organizacji. Wśród nich znalazły m.in. APT1, APT3, Honker Union of China, APT10, KeyBoy, DragonOK, APT16, EvilPost, Danti, SVCMONDR, China Girls Security Team, APT27, APT17 czy APT18.

Jedną z najsłynniejszych grup jest APT1, znana również jako jednostka 61398. Funkcjonuje ona w 2. Biurze 3. Departamentu Sztabu Generalnego PLA (→ w y w i a d [t. 4] radiowyi elektroniczny). Podstawowym zadaniem APT1 są operacje typu NCO (ang. *Computer Network Operation*), polegające na włamywaniu się do obcych sieci komputerowych i wykradaniu danych użytecznych z punktu widzenia PLA. Celem → h a k e r ó w [t. 2] stały się organizacje polityczne, przedsiębiorstwa państwowe i prywatne, instytucje akademickie, organizacje międzynarodowe oraz rządowe bazy danych funkcjonujące w branżach takich jak: informatyka, lotnictwo, telekomunikacja, przemysł satelitarny, transport, budownictwo, media, nawigacja, usługi finansowe, żywność,rolnictwo, górnictwo, czy opieka zdrowotna. Od 2005 r., czyli momentu założenia APT1, grupa przeprowadzała głównie operacje przeciwko Stanom Zjednoczonym, Kanadzie, Korei Południowej, Tajwanowi, Wietnamowi i Izraelowi, najczęściej z użyciem → z ł o ś l i w e g o o p r o g r a m o w a n i a [t. 4] typu TROJAN czy ECLYTS. Pierwsze przypadki cyberoperacji miały miejsce w 1999 r., po omyłkowym ostrzelaniu ambasady ChRL w Sarajewie. Kolejne miały miejsce w 2001 r., po przekroczeniu chińskiej przestrzeni powietrznej przez amerykański samolot szpiegowski. W następnych latach wyspecjalizowane jednostki chińskiej Armii Ludowo-Wyzwoleńczej przeprowadzały regularne cyberataki na amerykańskie instytucje państwowej i prywatne korporacje. Do dzisiaj chińskie grupy hakerskie funkcjonujące w ramach wojska lub współpracujące z rządem w Pekinie przeprowadziły setki różnych operacji i cyberataków. Do najbardziej znanych zaliczają się m.in.:

- operacja „Nitro" (2009),
- operacja „Aurora" (2009–2010),
- peracja „Nocny Smok (2006–2011),
- atak na RAS (2011).

Operacja „Nitro" polegała na przeprowadzeniu kilku ataków na cele znajdujące się na terenie Chińskiej Republiki Ludowej lub poza nią. Obiektem zainteresowań stały się organizacje pozarządowe zajmujące się ochroną → p r a w c z ł o w i e k a [t. 3] w ChRL oraz prywatne korporacje sektora R&D, motoryzacyjne, zbrojeniowe i chemiczne. Łącznie zainfekowano ponad 100 komputerów podmiotów mających swoją siedzibę w Stanach Zjednoczonych, Bangladeszu i Wielkiej Brytanii. Operacja „Aurora" była wymierzona w prywatne przedsiębiorstwa, m.in. w Google, Adobe i McAfee. W przypadku Google celem ataku stały się konta chińskich dysydentów zamieszkałych w USA lub w Europie. Z kolei w przypadku McAfee chodziło o oprogramowanie Periscope, wykorzystywane przez duże przedsiębiorstwa programistyczne. Hakerzy przeprowadzający operację skorzystali z tzw. luki dnia zerowego (ang. *zero-day vulnerability*), czyli luki w zabezpieczeniach programu lub przeglądarki, o której to luce właściciel nie miał świadomości. Operacja „Nocny Smok" była jednym z najdłużej trwających ataków, ale pod względem metod i doboru celów okazała się zbliżona do poprzednich. Zaatakowano 21 amerykańskich organizacji rządowych, 6 spółek przemysłowych i energetycznych, 13 firm komunikacyjnych,

komputerowych i elektronicznych, 13 firm ochroniarskich i 6 spółek finansowych. Atak na firmę RAS jest zaliczany do najbardziej spektakularnych i bolesnych dla USA chińskich sukcesów. RAS był jednym z dominujących przedsiębiorstw w Stanach Zjednoczonych zajmujących się analizą ryzyka i usługami związanymi z zapewnieniem bezpieczeństwa w sieci. Pierwszy etap ataku polegał na gromadzeniu informacji o infrastrukturze informatycznej RAS – jej słabych stronach oraz personelu. Następnie do biura firmy w ciągu 2 dni hakerzy wysłali 2 różne wiadomości, które dotarły do zespołów składających się z mniej doświadczonych pracowników. Jeden z nich otworzył wiadomość sugerującą, że znajduje się w niej „plan rekrutacji" na 2011 r. Pozwoliło to napastnikom na eksport informacji z tego komputera oraz zdobycie nad nim kontroli. Kolejno uzyskiwali oni dostęp do serwerów firmy, komputera, na którym znajdowały się dane poufne, a następnie – do baz danych innych firm, z którymi współpracowała firma RAS.

Tomasz Wójtowicz

Ch. Bing, *APT28 Targeted Montenegro's Government Before It Joined NATO, Researchers Say*, https://www.cyberscoop.com/apt28-targeted-montenegros-governmentjoined-nato-researchers-say/ (dostęp 22.11.2021); K. Collier, *A Favourite Target of Russian Hackers, the Olympics Are on Guard*, https://www.nbcnews.com/tech/security/olympics-are-guard-favorite-target-russian-hackers-rcna1422 (dostęp 23.11.2021); *U.S., U.K. Blame Russia For 2019 Cyberattack On Georgian Websites*, https://www.rferl. org/a/tbilisi-washington-blame-russia--cyberattack-georgian-websites/30445595. html (dostęp 23.11.2021); J. Hakala, J. Melnychuk, *Russia's Strategy in Cyberspace*, StratCom COE and NATO Cooperative Cyber Defence COE, Riga 2021; C.R. Knake, *Cyber War. The Next National Security and What to Do About it*, An Imprint of HarperCollins Publishers 2012; A. Ng, *US. Russia's NotPetya the Most Destructive Cyberattack Ever*, https:// www.cnet.com/tech/services-and-software/uk-said-russia-isbehind-destructive-2017-cyberattack-in-ukraine/ (dostęp 23.11.2021); S. Oladimejj, S. Kerner, *SolarWinds Hack Explained. Everything You Need to Know*, https:// whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-needto-know (dostęp 23.11.2021); G. Siboni, *What Lies behind Chinese Cyber Warfare*, „Military & Strategic Warfare" 2012, vol. 4; tenże, *What Lies behind Chinese Cyber Warfare*, https://www.inss.org.il/wp-content/uploads/sites/2/systemfiles/MASA42Eng%204%20(2)_Siboni.pdf (dostęp 23.11.2021); S. Watson Parcels, *Chinese Hacker Groups*, International Institute for Counter-Terrorism, June 2018; B.T. Williams, *TheJoint Force Commander's Guide to Cyberspace Operations*, https://ndupress.ndu.edu/Publications/Article/577499/the-joint-force-commanders-guide-to-cyberspaceoperations/ (dostęp 22.11.2021).

CYBERPOLITYKA – określenie sposobu uprawiania polityki, który dzięki zastosowaniu nowych, powszechnie dostępnych narzędzi technologicznych pozwala usprawniać procesy polityczne w zmiennym i dynamicznym środowisku, charakteryzującym się nowymi rodzajami konfliktów, ale także nowymi możliwościami kooperacji. To pojęcie powszechnie utożsamiane z działaniami państwa masowo wykorzystującego nowe formykomunikowania się. W takim znaczeniu państwo nie rządzi i nie ingeruje w stosunki panujące między ludźmi, ale ogranicza się do wyznaczania podstawowych ram (m.in. prawnych) do ich funkcjonowania, jak również dostarcza narzędzi (urządzenia, internet) i zapewnia możliwości komunikacji (dostęp do internetu oraz do sieci komórkowych), a tym samym zwiększa poziom partycypacji

obywateli w życiu politycznym. Cyberpolityka to zatem realizacja określonych celów za pomocą konkretnychśrodków przez przedstawicieli mających prawo decydowania nadane im przez społeczeństwo. Przy czym realizacja tych celów odbywa się dzięki powszechnemu wykorzystaniu nowych technologii informacyjnych i komunikacyjnych (ang. *Information and Communication Technologies*, ICT).

Termin *cyberpolityka* jest neologizmem złożonym z przedrostka *cyber*(od wyrazu *cybernetyka*) i rzeczownika *polityka*. Jak wskazuje źródłosłów, w cyberpolityce istotne jest koordynowanie i nadzorowanie społeczności oraz relacji międzyludzkich za pomocą sieci informatycznych i technologii komunikacyjnych. Te relacje obejmują sferę polityki i charakteryzują się zastosowaniem mnogości środków technicznych w tym obszarze: od mikrofonu, przez telewizję, aż po internet. Takie rozumienie cyberpolityki prezentuje Philip Howard – amerykański socjolog i badacz komunikacji, który twierdzi, że cyberpolityka określa rolę nowych technologii informacyjnych we współczesnym życiu politycznym. Analizowanie cyberpolityki to także odkrywanie jej sekretnych i mniej chlubnych odsłon, które dotyczą ustanawiania standardów telekomunikacyjnych oraz podejmowania decyzji dotyczących infrastruktury informatycznej. Ustalanie standardów prywatności w świetle prawa, budowanie powszechnego dostępu szerokopasmowego lub decydowanie, które pakiety informacyjne okażą się potencjalnie ważniejsze od innych – to wszystko może istotnie wpływać na kształtowanie życia politycznego.

Asumpt do stworzenia nowej odsłony polityki, czyli właśnie cyberpolityki, dał sukcesywny wzrost poziomu wykorzystania internetu i innych technologii informacyjno-komunikacyjnych w działalności politycznej, a także – stale powiększający się obszar funkcjonowania polityki. Obok tradycyjnych działań komunikacyjnych i marketingowych stopniowo w sferze polityki następuje przeniesienie debaty publicznej oraz organizowania się politycznego do sfery wirtualnej. Potencjał nowych technologii, dostrzeżony przez polityków, sprawił, że świat polityki przeniknął do → c y b e r p r z e s t r z e n i [t. 1], która zaczęła pełnić funkcję areny dla procesów politycznych. Nowe media i nowe technologie funkcjonują w polityce na tych samych zasadach co w życiu codziennym – pełnią przede wszystkim funkcję praktyczną. Wykorzystuje się je z myślą o przyśpieszeniu, usprawnieniu i ulepszeniu procesów politycznych i administracyjnych oraz w celach marketingowych i komunikacyjnych.

Funkcje nowych technologii w sferze polityki obejmują m.in. dostarczanie → i n f o r m a c j i [t. 2], szybkie i łatwe komunikowanie się, konsolidację zwolenników i aktywizację wyborców. Przyczyn tak chętnego wykorzystywania internetu i nowych technologii w działalności politycznej należy upatrywać w zmianach cywilizacyjno-pokoleniowych. Z jednej strony – obserwowany spadek aktywności wyborczej obywateli i potrzeba dotarcia do niszowego lub biernego elektoratu uzupełniają się z popularnością internetu wśród młodego pokolenia, dostępnością i powszechnością tego medium. Aspekt zmiany pokoleniowej stał się ważnym bodźcem przeniesienia

debaty politycznej do sieci, ponieważ to w użytkownikach mediów widzi się nowe pokolenie wyborców, urodzonych w erze internetu i określanych jako *millenium kids, echo boomers* lub generacja „Y". Dla ubiegających się o władzę to oni stali się potencjalnym elektoratem. Istotną rolę odgrywa także lobby technologiczne i teleinformacyjne, które tworzy infrastrukturę internetową. Sieć pozwala odbiorcom dotrzeć do informacji alternatywnych, które nie są eksponowane w mediach dominujących. Daje ponadto wiele możliwości technicznych pomocnych w tworzeniu treści przez samych odbiorców –otwarta architektura tego medium ma wpływ na tworzenie nowej jakości przekazu i nowego sposobu komunikowania się w polityce. Ponieważ użytkowników internetu ciągle przybywa, a sama sieć – w powszechnym przekonaniu – jest bardziej atrakcyjnym medium dla młodszego pokolenia niż telewizja czy radio, skorzystanie z jego atutów może z pewnością pomóc politykom w dotarciu do tej grupy docelowej.

Jeżeli cyberpolitykę postrzega się jako wykorzystanie środków cyfrowych w rozmaitych aspektach działalności politycznej, należy mieć świadomość faktu, że obejmuje ona zarówno systemy demokratyczne, jak i niedemokratyczne. Bez wątpienia nadaje to nową jakość zjawiskom o charakterze politycznym i wiąże się bezpośrednio ze zmianami systemu politycznego. Cyfrowe technologie informacyjne od początku swojego istnienia postrzegano z zasady jako demokratyczne, z uwagi na ich interaktywność, wymienność ról nadawcy i odbiorcy, synchroniczność komunikacji, dostęp do wszelkiej zawartości zawsze i wszędzie, przenośnośćterminali czy wyeliminowanie pośredników. Rozwój internetu – będącyrezultatem wspólnych działań rządów, instytucji naukowych, firm komercyjnych i pojedynczych obywateli – jest efektem przedsiębiorczości, swobodnego przepływu idei, współpracy międzynarodowej na skalę globalną. Ze swej natury ta sieć ma zatem charakter demokratyczny. W systemach demokratycznych nierzadko służy realizacji idei pluralizmu politycznego, wolności słowa, ułatwia komunikację elit politycznych z obywatelami. Można zatem powiedzieć, że internet służy demokracji przez to, że umożliwia obywatelom łatwiejszy dostęp do różnorodnej informacji oraz pozwala rządom, partiom politycznym i innym organizacjom zajmującym się polityką i samym politykom na kontakt z obywatelem, na prezentowanie swojego punktu widzenia. Generuje również coraz nowsze sposoby aktywności politycznej polegające już nie tylko na pozyskiwaniu informacji i wyrażaniu opinii, lecz także na korzystaniu z usług publicznych, na udziale w podejmowaniu decyzji politycznych oraz w tworzeniu prawa. Co więcej, z uwagi na swój wszechstronny pluralizm, pozwala na spotkaniesię w nim i na wymianę poglądów wszystkich zainteresowanych stron. Pozwala także na kreowanie nowych form realizowania zasad ustroju demokratycznego – na głosowanie elektroniczne czy na wykorzystywanie nowych kanałów komunikacji z wyborcami. Ogromny demokratyczny potencjał internetu oraz innych technologii informacyjnych i komunikacyjnych umożliwia odbudowę różnych społeczności i uczynienia z nich przeciwwagi dla dominujących scentralizowanych

struktur władzy. Nie oznacza to jednak, że w państwach niedemokratycznych internet nie istnieje i nie jest potrzebny. Często bywa cenzurowany i ograniczany, a nawet blokowany. Nierzadko jest używany jako tuba propagandowa panujących rządów autorytarnych. W systemach niedemokratycznych stanowi jednak niezastąpione narzędzie walki o wolność słowa. W wielu krajach pełni zatem funkcję okna na świat i okazuje się jedyną szansą dla opozycji demokratycznej walczącej o zmianę ustroju politycznego. Może być wykorzystywany w walce o → p r a w a c z ł o w i e k a [t. 3], swobody polityczne, wolne wybory itp. Sprzyja więc rozpowszechnianiu idei demokratycznych, a być może – także narodzinom ruchów społecznych, → s p o ł e c z e ń s t w a o b y w a t e l s k i e g o [t. 4] i samej demokracji. Staje się więc niezbędny dla walczących o zmianę.

Jak powszechnie wiadomo, nowe media odgrywają w dużym stopniu rolę kreatora polityki, a wykorzystywanie internetu w działalności politycznej może wpływać na wzrost lub spadek poparcia kandydata czy polityka oraz na poziom aktywności politycznej internautów. Mogą oni, oprócz dostarczania informacji politycznej wyborcom, kształtować postawy polityczne elektoratu oraz stanowić narzędzie kontroli. Ponadto uzupełniają, przyśpieszają i usprawniają różne typy aktywności społecznej związanej z zaangażowaniem w debatę polityczną oraz z uczestnictwem w podejmowaniu politycznych decyzji. Stwarzają przez to rządzącym i obywatelom nową perspektywę dla kształtowania dialogu demokratycznego oraz pozwalają przeciwdziałać takim zjawiskom, jak → k r y z y s [t. 2] demokracji, brak zaufania do rządzących, nikłe zainteresowanie polityką czy spadek aktywności obywatelskiej.

Współczesna cyberpolityka koncentruje się na wykorzystaniu nowych mediów przede wszystkim jako platformy prezentacji ofert politycznych, poszczególnych kandydatów-polityków, na potrzeby marketingu politycznego. Internet jest także doskonałym medium do kreowania wizerunku polityka i partii politycznej, do budowania wokół nich społeczności i lojalności oraz do aktywizowania elektoratu. Sieć stała się także swoistą płaszczyzną walki o elektorat: często służy polaryzacji zwolenników i przeciwników i staje się narzędziem → p r o p a g a n d y [t. 3] głównie poprzez kampanie negatywne.

Formy, w których realizuje się cyberpolityka, to m.in.:

- działania promocyjno-marketingowe:
  - strony internetowe polityków i partii politycznych oraz witryny skoncentrowane wokół określonych poglądów,
  - kampanie elektroniczne (np. wyborcze) z wykorzystaniem poczty elektronicznej, banerów reklamowych, grup dyskusyjnych, czatów, debat online itp.,
  - blogosfera polityczna,
  - aktywność na portalach społecznościowych typu Facebook, Twitter, Instagram, Blip, Flickr, TikTok;

- działania podejmowane w celu usprawnienia procesów politycznych, np. rządzenia i procesów wyborczych:
  - e-demokracja, m.in.: sieciowe referenda, wybory (tzw. e-voting), inicjatywa ustawodawcza wyrażona w formie elektronicznej, sieciowe sondaże → o p i n i i p u b l i c z n e j [t. 3], dyskusje polityczne między obywatelami a politykami, a także – organizacjami społecznymi,
  - e-administracja, czyli realizacja usług publicznych z wykorzystaniem sieci,
  - e-dyplomacja, czyli instrument soft power, stosowany we współczesnych stosunkach międzynarodowych;
- stymulowanie aktywności obywatelskiej:
  - elektroniczne przesyłanie indywidualnego stanowiska poszczególnych obywateli w trakcie procesu legislacyjnego czy elektronicznego aplikowania na stanowiska publiczne,
  - poprawa dialogu na linii obywatel – władza dzięki szybkiej i łatwej komunikacji,
  - narzędzie propagowania głoszonych idei oraz sposób → m o b i l i z a c j i [t. 3] członków i pozyskiwania zwolenników,
  - platforma wspierająca powstawanie inicjatyw obywatelskich oraz ruchów społecznych.

Praktyczne zastosowanie technologii ICT w aktywności politycznej przybiera zatem różne formy: od wykorzystania ich w działalności marketingowej (zarówno w czasie kampanii wyborczej, jak i poza nią), przez uproszczenie procedur administracyjnych oraz wyborczych czy próby mobilizacji społeczeństwa do większej aktywności w ramach społeczeństwa obywatelskiego i ruchów społecznych, aż po tworzenie wirtualnych systemów czy instytucji politycznych, a nawet państw (demokracja sieciowa, wirtualne państwo, internetowe partie polityczne). Wszystkie te aktywności przenoszące działania społeczne i polityczne do sieci mają – w opinii inicjatorów – na celu mobilizowanie obywateli do zwiększenia partycypacji politycznej oraz udziału w inicjatywach społecznych. Celem jest stworzenie nowocześniejszego i sprawniejszego modelu demokracji bezpośredniej. Cyberpolityka zmienia oblicze demokratycznej formy rządzenia. Debata polityczna, stanowiąca niezbywalny element systemu demokratycznego, nie może funkcjonować bez pośrednictwa mediów, które we współczesnym świecie nie tylko są czynnikami stymulującymi wymianę poglądów, lecz także pełnią funkcję kontrolną. Współczesny odbiorca preferuje przecież takie sposoby komunikacji, które pozwalają na bardziej aktywny udział w dyskursie politycznym, a przy tym eliminują jednokierunkowość relacji nadawczo-odbiorczych i asymetrię komunikacyjną.

Sabina Olszyk

P. Howard, *Cyberpolitics*, http://www.oxfordbibliographies.com/view/document/ obo-9780199756841/obo-9780199756841 0049.xml (dostęp 31.07.2021); M. Majorek, S. Olszyk, M. Winiarska-Brodowska, *Cyberpolityka. Internet jako przestrzeń aktywności politycznej*,

Texter, Warszawa 2018; M. Nowina-Konopka, *Rola Internetu w rozwoju demokracji w Polsce*, „Biblioteka Myśli Politycznej – Ośrodek Myśli Politycznej", Kraków–Nowy Sącz 2008; S. Olszyk, *Współczesne oblicza cyberpolityki*, [w:] *Kultura pokoju. Kultura sieci*, A. Kurkiewicz, A. Kołodziej (red.), Wydawnictwo Wyższej Szkoły Bezpieczeństwa, Poznań 2019; L. Porębski, *Elektroniczne oblicze polityki. Demokracja, państwo, instytucje polityczne w okresie rewolucji informacyjnej*, AGH Uczelniane Wydawnictwa Naukowo-Dydaktyczne Kraków 2004.

CYBER POWER (POTĘGA CYBERNETYCZNA) – podobnie jak w wypadku innych terminów z przedrostkiem „cyber-" *cyber power* nie ma jednej akceptowalnej definicji w naukach społecznych. Aby dokładnie zrozumieć istotę pojęcia, należy przyjrzeć się jego częściom składowym: *cyber* oraz *power* (potęga). Przedrostka „cyber-" zazwyczaj używa się do tworzenia pojęć dotyczących elektroniki lub środowiska komputerowego.

„Potęga" to termin wieloznaczny i interdyscyplinarny. Wraz z rozwojem nowoczesnych technologii, → g l o b a l i z a c j ą [t. 5], zmianami na arenie międzynarodowej czy powszechną informatyzacją życia społecznego definiens pojęcia wciąż ewoluuje. Nie jest to nowy termin, o czym świadczy fakt, że o potędze pisali już Platon, Arystoteles czy Niccolò Machiavelli. W naukach społecznych pojęcie potęgi to jedna z kluczowych kategorii takich dyscyplin jak: nauka o stosunkach międzynarodowych, nauki o polityce oraz nauki o → b e z p i e c z e ń s t w i e [t. 1].

„Potęga" odpowiadająca angielskiemu *power* powiązana jest z władzą i interesem. Robert A. Dahl określał potęgę jako zdolność skłonienia innych do zrobienia czegoś, czego nie zrobiliby w innych okolicznościach. John G. Stoessinger w definicji potęgi podkreślił umiejętność państwa do wykorzystania swoich materialnych i niematerialnych zasobów w sposób, który wpłynie na zachowanie innych podmiotów (państw). Raymond Aron postrzegał ją jako zdolność do czynienia, tworzenia czy niszczenia. Mirosław Sułek wskazał, że przy charakterystyce potęgi używamy określeń takich jak „zdolność" i „możliwość", które dodatkowo zwracają uwagę na wolę, będącą czynnikiem psychologicznym. Potęga wyraża także możliwości i skalę sprawowania przez państwo władzy nad terytorium bądź środowiskiem, w którym funkcjonuje. W tym ujęciu siła określana jest jako zdolność do realnego i skutecznego stosowania potęgi. John Mearsheimer pisał, że potęgę realizuje się za pomocą zasobów, które są w posiadaniu państwa. Dzielił ją na potencjalną i realną, opartą na sile ekonomicznej i zbrojnej.

Warto zwrócić uwagę także na klasyfikację pojęcia potęgi autorstwa Marie-Claude Smouts, która wyróżniła 3 grupy definicji: tradycyjne, neorealistyczne i strukturalne. W ujęciu pierwszym – tradycyjnym – siła państwa zależy od posiadanych zasobów. Podejście neorealistyczne pozwala postrzegać potęgę jako zdolność ustalania reguł gry i określania ostatecznego wyniku negocjacji. Zgodnie z ostatnim z wymienionych, czyli podejściem strukturalnym, potęgę definiuje się jako możliwość kształtowania

struktur gospodarki światowej, narzucania dominujących wartości i zasad działania, które mają być obligatoryjnie respektowane przez państwa.

Podsumowując krótkie rozważania terminologiczne, można przyjąć, że potęga stanowi zdolność rzeczywistego lub potencjalnego oddziaływania państwa na inne podmioty oraz osiągania własnych celów. W ten sposób ten termin definiuje m.in. Joseph S. Nye, który w swoim dziele *The Changing Nature of World Power* wskazał, że „potęga to zdolność osiągania własnych celów". Dodatkowo wyodrębnił 2 składowe potęgi: tzw. twardą i miękką. → *S o f t p o w e r* [t. 4] wyrasta z ideałów politycznych, sposobu prowadzenia polityki oraz kultury danego kraju. → C y b e r p r z e s t r z e ń [t. 1] jest obecnie płaszczyzną, która w znaczący sposób pozwala zbudować zdolność uzyskiwania tego, co się chce, bardziej dzięki atrakcyjności niż przymusowi czy pieniądzom. *Hard power* to potencjał danego podmiotu, który wynika głównie z czynników militarnych i ekonomicznych, stąd często utożsamia się go z tradycyjną → g e o p o l i t y k ą [t. 2]. Twarda siła państwa oparta jest na przymusie, groźbach oraz sankcjach ekonomicznych. Colin S. Gray definiuje *hard power* jako zdolność celowego zadawania bólu lub nagradzania w pogoni za wpływami. Głównym narzędziem działania na tej płaszczyźnie są siły zbrojne. Strategie twardej siły koncentrują się na takich działaniach, jak interwencja wojskowa czy sankcje gospodarcze, w celu egzekwowania → i n t e r e s ó w n a r o d o w y c h [t. 2]. W porównaniu z *soft power* twarda siła jest trudniejsza w wykorzystaniu, angażuje znacznie więcej środków, a także demaskuje intencje sprawcy, jego narzędzia i metody działania. Zasoby twardej siły mają charakter głównie gospodarczy i militarny. W przeciwieństwie do zasobów *soft power* są one najczęściej przechowywane w rezerwie i wykorzystywane w określonym miejscu i czasie z uwzględnieniem konkretnych celów strategicznych i taktycznych. Państwo nie musi wykorzystywać zasobów twardej siły, ale może zagrozić ich wykorzystaniem, co z kolei jest częścią tzw. strategii odstraszania. Jest ona aktem zniechęcenia przeciwnika do podjęcia nieprzyjaznych działań ze względu na niekorzystne dla niego konsekwencje tychże działań.

Cyberprzestrzeń może być instrumentem zarówno „miękkiej", jak i „twardej siły" państwa. Umiejętność osiągania przez państwo zakładanych celów za pomocą sprzężonych w cyberprzestrzeni elektronicznych zasobów informacyjnych nazywana jest potęgą cybernetyczną (*cyber power*). Zdaniem Nye'a c*yber power* może być rozpatrywana w wymiarach wewnętrznych i zewnętrznych oddziaływań informacyjnych, generujących „miękką" oraz „twardą" siłę państwa. Problematykę potęgi cybernetycznej obrazuje tabela 1.

Tabela 1. Wymiary fizyczny i wirtualny potęgi cybernetycznej

	Aspekt wewnętrzny	Aspekt zewnętrzny
Instrumenty informacyjne	*Hard*: ataki DoS / DDoS *Soft*: system norm i standardów	*Hard:* ataki na systemy SCADA*Soft:* działania dyplomatyczne wpływające na →opinię publiczną [t. 3]
Instrumenty fizyczne	*Hard:* rządowa kontrola przedsiębiorstw *Soft:* działania wspierające ruchy obrońców →prawa człowieka [t. 3]	*Hard:* ataki na routery lub magistrale sieciowe *Soft:* działania szkalujące cyberdostawców

Źródło: J.S. Nye, Jr., *Cyber power*, Belfer Center for Science and International Affairs, Harvard Kennedy School 2010, http://www.belfercenter.org/sites/default/files/legacy/ files/cyber-power.pdf (dostęp 11.05.2023).

Zdaniem Nye'a *cyber power* opiera się na zestawie zasobów związanych z tworzeniem, kontrolą i komunikowaniem informacji elektronicznych, są to: infrastruktura, sieci, oprogramowanie, umiejętności ludzkie. Składa się na nie internet sieci komputerowych, ale są to także intranety, technologie komórkowe i komunikacja kosmiczna. Zdefiniowana behawioralnie cyberpotęga to zdolność do uzyskania preferowanych rezultatów przez wykorzystanie elektronicznie połączonych zasobów informacyjnych w domenie cybernetycznej.

Jak pisze Robert Białoskórski, „potęga cybernetyczna może być rozpatrywana w sensie defensywnym i wówczas mamy do czynienia z defensywną potęgą cybernetyczną (ang. *defensive cyber power*, DCP) oraz w sensie ofensywnym w postaci – ofensywnej potęgi cybernetycznej (ang. *offensive cyber power*, OCP)".

Według innych definicji *cyber power* to zdolność wykorzystania cyberprzestrzeni do tworzenia przewagi i wpływania na wydarzenia w innych środowiskach operacyjnych i na wszystkich instrumentach władzy.

To umiejętność wykorzystania cyberprzestrzeni do opracowania i przeprowadzenia nowatorskich, ukierunkowanych działań, które wpływają na zachowanie innych osób lub urządzeń. Cybersiły można użyć do wypracowania preferowanych wyników wewnątrz cyberprzestrzeni lub poza nią. Potęgą cybernetyczną określane są także umiejętności zmiany zachowania podmiotu docelowego za pośrednictwem cyberprzestrzeni w kontekście →bezpieczeństwa narodowego [t. 1] i konfliktu.

Podmioty państwowe lub niepaństwowe wykorzystują tę siłę poprzez kampanie cybernetyczne, które obejmują pojedyncze ukierunkowane wydarzenie (lub serię wydarzeń) z wykorzystaniem środków przymusu, perswazji lub środków technicznych, aby osiągnąć określony efekt w ramach celu strategicznego.

Badacze Adrian Venables, Siraj Ahmed Shaikh i James Shuttleworth wskazują, że na *cyber power* składają się następujące zdolności:

- zaangażowanie i wywieranie wpływu mające na celu zrozumienie i kształtowanie opinii w celu kierowania polityką i dyskursem w domenie cybernetycznej przy użyciu narzędzi *soft power*;
- ukierunkowane i ewentualnie ofensywne środki mające na celu odmowę, degradację, zniszczenie, zakłócenie lub przekierowanie usług czy danych do określonych urządzeń lub komponentów, aby osiągnąć określone cele;
- odporność infrastruktury cybernetycznej poprzez skuteczne przewidywanie, absorpcję, adaptację i odbudowę po kampanii cybernetycznej. Kampania może składać się z twardych, miękkich lub inteligentnych technik siłowych dostępnych dla podmiotu państwowego lub niepaństwowego i może być realizowana poprzez połączenie mechanizmów technicznych i politycznych w celu wzmocnienia, dostosowania i obrony infrastruktury;
- zasoby i środki pozwalające na uzyskanie atrybucji pełnego zakresu kampanii cybernetycznych w celu przeciwdziałania określonym działaniom, a w razie potrzeby podjęcia czynności odwetowych;
- umiejętności techniczne i potencjał stanowiące podstawę skutecznego i trwałego zapewnienia wszystkich powyższych elementów.

W naukach społecznych pojawiają się koncepcje modeli pomiaru potęgi cybernetycznej. Jednym z nich jest National Cyber Power Index (NCPI) opracowany przez zespół wywiadu ekonomicznego (The Economist Intelligence Unit, EIU) czasopisma „The Economist" we współpracy z konsorcjum Booz Allen Hamilton. National Cyber Power Index mierzy zdolności cybernetyczne z wykorzystaniem 29 wskaźników dla 30 krajów w ramach 8 celów narodowych. Cele wymienione przez autorów raportu to:

1) Inwigilacja i monitorowanie grup wewnątrz państwa.
2) Wzmocnienie i poprawa krajowej obrony cybernetycznej.
3) Kontrolowanie → ś r o d o w i s k a i n f o r m a c y j n e g o [t. 4] i manipulowanie nim.
4) Zbieranie danych wywiadowczych w innych krajach.
5) Rozwijanie krajowych cybernetycznych i komercyjnych kompetencji technologicznych.
6) Zniszczenie lub wyłączenie infrastruktury i zdolności przeciwnika.
7) Definiowanie międzynarodowych norm cybernetycznych i standardów technicznych.
8) Gromadzenie bogactwa i (lub) wydobywanie kryptowaluty.

NCPI składa się z wielu komponentów. W jego ramach mierzone sąstrategie rządowe, zdolności w zakresie działań obronnych i ofensywnych, sposób alokacji zasobów, sektor prywatny, siła robocza oraz innowacje. Autorzy rankingu (por. tabela 2) zwracają także uwagę na trudności w jegotworzeniu, np. → i n f o r m a c j e [t. 2], które obrazują potęgę cybernetyczną państwa, bardzo często są wrażliwe i utajnione, a państwa celowo ukrywają dane na temat swoich zdolności cybernetycznych.

Tabela 2. Ranking NCPI 2022

Miejsce w rankingu	2022 r.
1	Stany Zjednoczone
2	Chiny
3	Federacja Rosyjska
4	Wielka Brytania
5	Australia
6	Holandia
7	Korea Południowa
8	Wietnam
9	Francja
10	Iran

Źródło: J. Voo, I. Hemani, D. Cassidy, *National Cyber Power Index 2022*, Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2022, https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf (dostęp 11.05.2023).

Inną znaną koncepcją pomiaru potęgi cybernetycznej państw jest np. koncepcja zaproponowana przez Alberto Miguela Gómeza.

Agnieszka Warchoł

I. Albrycht i in., *Three Seas United in Cyber Power*, Instytut Kościuszki, Kraków 2022, https://ik.org.pl/wp-content/uploads/RAPORT-3Seas-United-in-Cyberpower-PL. pdf (dostęp 11.05.2023); R. Białoskórski, *Potęga cybernetyczna państw – pomiar i zastosowanie*, „Zeszyty Naukowe AON" 2015, nr 2(99); R.A. Dahl, *The Concept of Power*, „Behavioral Science" 1957, vol. 2, no. 3; C.S. Gray, *Hard Power and SoftPower. The Utility of Military Force as an Instrument Of Policy in the 21st Century*,Strategic Studies Institute, U.S. Army War College, Carlisle 2011; D. Kondrakiewicz, *Metody pomiaru siły państwa w stosunkach międzynarodowych*, http://ptsm.edu.pl/ wp-content/uploads/publikacje/poziomy-analizy-stosunkow-miedzynarodowych/Kondrakiewicz.pdf (dostęp 1.05.2023); R. Łoś, *Potęga – ujęcie teoretyczne: definicja, struktura i oddziaływanie*, [w:] *Międzynarodowe studia polityczne i kulturowe wobec wyzwań współczesności*, T. Domański (red.), Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2016; J. Mearsheimer, *The Tragedy of Great Power Politics*, Norton, New York 2001; J.S. Nye, Jr., *Cyber power*, Belfer Center for Science and International Affairs, Harvard Kennedy School 2010, http://www.belfercenter.org/sites/ default/files/legacy/files/cyber-power.pdf (dostęp 11.05.2023); tenże, *The Changing Nature of World Power*, „Political Science Quarterly*"* 1990, vol. 105, no. 2; P. Pacak, *«Soft power» jako środek realizacji celów polityki zagranicznej państwa w systemie postwestfalskim*, https://ptsm.edu.pl/wp-content/uploads/publikacje/poziomyanalizy-stosunkow-miedzynarodowych/Pacak.pdf (dostęp 1.05.2023); J. Sadłocha, *Pomiędzy miękką a twardą siłą:* smart power, „Wrocławskie Studia Politologiczne"2012, nr 13; M.C. Smouts, *International Organizations and Inequality among States*, „International Social Science Journal" 1995, vol. XLVII, no. 2; J.G. Stoessinger, *TheMight of Nation. World Politics in Our Times*, Random House, New York 1969; M. Sułek, *Modelowanie i pomiar potęgi państw w stosunkach międzynarodowych*, „Stosunki Międzynarodowe" 2003, nr 3–4; A. Venables, S.A. Shaikh, J. Shuttleworth, *A Model for Characterizing Cyberpower*, [w:] *Critical Infrastructure Protection IX. 9th IFIP 11.10 International Conference, ICCIP 2015 Arlington, VA, USA, March 16–18, 2015. Revised*

Selected Papers, M. Rice, S. Shenoi (eds.), Springer, London 2015; J. Voo, I. Hemani, D. Cassidy, *National Cyber Power Index 2022*, Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2022, https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf, [dostęp 11.05.2023]; M.A. Gomez, *Identifying Cyber Strategies vis-a-vis Cyber Power*, https://www.academia.edu/6544932/Identifying_Cyber_Strategies_vis-a-vis_Cyber_Power (dostęp 11.05.2023); L.M. Zerini, *Odstraszanie: analiza pojęcia*, http://www.geopolityka.org/ analizy/matteo-zerini-odstraszanie-analiza-pojecia (dostęp 9.05.2023).

CYBERPRZEMOC (*cyberbullying*) – zjawisko często utożsamiane z cyberbullyingiem (jedną z jego odmian), polegające na wykorzystywaniu dostępnych technik i elektronicznych narzędzi informacyjno-komunikacyjnych do permanentnego, świadomego i wrogiego zachowania względem innej osoby (grupy osób), zmierzające do wyrządzenia tej osobie (grupie osób) krzywdy. W znaczeniu ogólnym cyberprzemoc jest → p r z e m o c ą [t. 3] z wykorzystaniem technologii informacyjnych i komunikacyjnych, tj. portali społecznościowych, czatów, stron internetowych, platform dyskusyjnych, serwisów komunikacyjnych (komunikatorów), blogów, wiadomości e-mail, SMS-ów, MMS-ów itp.

Najczęściej cyberprzemoc przejawia się w postaci wykorzystującego możliwości nowych mediów nękania, zastraszania, upokarzania, szantażowania, kompromitowania, zamieszczania w sieci poniżających i/lub ośmieszających → i n f o r m a c j i [t. 2], zdjęć, filmów czy nagrań odnoszących się do nękanej w ten sposób osoby (lub grupy osób) oraz podszywania się pod kogoś wbrew jego woli (zmieniając swoją tożsamość w internecie). Sprawcy cyberprzemocy w stosunku do ofiar stosują coraz to nowsze jej formy. W zależności od przyjętej systematyki do faz, etapów, form czy rodzajów cyberprzemocy zalicza się najczęściej m.in.:

- zapłon – wzniecanie kłótni będące często zapowiedzią, wstępem do kolejnego etapu rozwoju sytuacji przemocowej w sieci, np. początkowa faza *flamingu*;
- *flaming* – celowe i emocjonalne bądź cyniczne podnoszenie napięcia wypowiedzi w sieci pomiędzy użytkownikami serwisów społecznościowych i dyskusyjnych, którego konsekwencją jest eskalacja → a g r e s j i i odejście od początkowego tematu rozmowy;
- molestowanie – permanentne wysyłanie nękających, poniżających wiadomości powodujące u ofiary poczucie dyskomfortu lub osaczenia;
- oczernianie – publikowanie w sieci kompromitujących, szkalujących, nieprawdziwych informacji wymierzonych w dobre imię i reputację danej osoby;
- wykluczanie – antyspołeczna praktyka pozbawiania członkostwa lub uczestnictwa w grupie online, np. na forum lub w grupie na portalu społecznościowym;
- personifikacja – podawanie się w sieci za kogoś innego;
- → p h i s h i n g [t. 3] – wyłudzanie i gromadzenie ważnych informacji osobistych i poufnych danych;

- plotkowanie – dzielenie się personalnymi informacjami o osobach trzecich oraz tworzenie nieprawdziwego obrazu lub wizerunku danej osoby;
- przechytrzanie – tzw. zjawisko Rudego Lisa – np. uzyskiwanie szkodliwych informacji, które są później ujawniane, udostępniane;
- → t r o l l i n g [t. 4] – przeszkadzanie w prowadzonej w sieci dyskusji poprzez stosowanie pogardliwych wypowiedzi o innych użytkownikach, obsesyjne zwracanie uwagi itp.;
- cyberstalking – cyberdręczenie, obsesyjne kontrolowanie, nagabywanie, zastraszanie, znieważanie i niepokojenie osób online;
- cybergróźby – rozważanie skrzywdzenia kogoś innego, siebie lub odbiorcy komunikatu albo grożenie popełnieniem samobójstwa;
- cyberprześladowanie – uporczywe śledzenie i kontrolowanie aktywności osób w → c y b e r p r z e s t r z e n i ;
- cyberagresja – rodzaj cyberprzemocy łączący w sobie elementy charakterystyczne dla innych form, np. wulgarne i złośliwe komentowanie zdjęć i wpisów internetowych, publikowanie ośmieszających ofiarę → c y b e r a t a k u zdjęć i filmów, ujawnianie na forum sekretów danej osoby, zastraszanie, szantażowanie, przesadne zgłaszanie wydumanych nadużyć administratorom serwisów itd.;
- *grooming* – doświadczenie dziecka: bycie uwiedzionym przez osobę dorosłą w sieci objawiające się prezentowaniem dziecku materiałów pornograficznych, wyłudzaniem intymnych zdjęć, krzywdzeniem dziecka w trakcie spotkania w realnej rzeczywistości;
- → s e k s t i n g [t. 4] – wysyłanie prowokacyjnych seksualnie filmów, obrazów lub tekstów o wyraźnie seksualnej tematyce;
- cyberprostytucja – uzyskiwanie korzyści materialnych w zamian za tworzenie, udostępnianie bądź przekazywanie drogą internetową materiałów erotycznych lub pornograficznych z udziałem osoby, która takie materiały wytworzyła i udostępniła.

Jak zauważa J. Barlińska, przyczyn występowania zachowań przemocowych w sieci (cyberprzemocy) jest wiele i wynikają one po pierwsze z indywidualnych właściwości i predyspozycji osób będących w okresie adolescencji (dojrzewania); po drugie z cech komunikacji za pośrednictwem internetu. W pierwszym przypadku nasilanie się przemocy w sieci może być spowodowane m.in.: ograniczoną zdolnością osób do decentracji (uwzględniania wszystkich okoliczności towarzyszących określonym działaniom; przeciwnie do koncentracji), brakiem lub ograniczoną zdolnością do refleksji nad sobą i swoim zachowaniem, relatywizmem moralnym, brakiem ukształtowanej tożsamości osobistej oraz zdecydowanie większym wpływem grupy rówieśniczej na daną jednostkę niż osób dorosłych, których reprezentacja w internecie jest znacznie niższa. Natomiast w drugim przypadku przyczyn cyberprzemocy należy doszukiwać się w: sile wpływu internetu na modyfikację zachowań społecznych; różnicach występujących między porządkiem wirtualnym a realnym; anonimowości oferowanej przez

nowe media; braku możliwości pełnej identyfikacji uczestnika wirtualnego komunikowania; braku ograniczeń i barier w procesie komunikowania, które kształtują charakter relacji; częstym braku informacji zwrotnej odnośnie do konkretnego, aspołecznego zachowania w sieci (co sprzyja fałszywemu przekonaniu o bezkarności); „efekcie odhamowania", który polega na braku odczuwania naturalnych ograniczeń werbalnych występujących w tradycyjnych kontaktach międzyludzkich (chodzi tu o stosunkową łatwość w „wypowiadaniu się" i obrażaniu innych za pośrednictwem nowoczesnych narzędzi komunikacyjnych). Cyberprzemoc stanowi poważne → z a g r o ż e n i e [t. 4] dla → c y b e r b e z p i e c z e ń s t w a jednostek, grup społecznych i całych społeczeństw, a edukacja informacyjno-medialna w tym zakresie powinna skupiać się na prezentacji precyzyjnego katalogu zasad prawidłowego poruszania się w wirtualnym świecie oraz treningu pożądanych zachowań w tej materii. Cyberbullying (określany także jako mobbing elektroniczny) to z kolei specyficzna forma przemocy występująca w przestrzeni wirtualnej, która ma na celu wyzwolenie u jednostki poczucia dyskomfortu lub zagrożenia poprzez jej uporczywe nękanie, molestowanie, upokarzanie, poniżanie, dręczenie, szykanowanie, znęcanie się czy szantażowanie, stwarzająca poważne zagrożenie dla → b e z p i e c z e ń s t w a jednostki w sieci. Cyberbullying często utożsamiany bywa ze zjawiskiem cyberprzemocy, co jest zgodne z prawdą jedynie częściowo, ponieważ cyberprzemoc jest pojęciem zdecydowanie szerszym, obejmującym wszelkie formy działania zmierzającego do wyrządzenia innym krzywdy, niezależnie od stopnia znajomości między osobą nękającą (sprawcą) a nękaną (ofiarą). Natomiast cyberbullying dotyczy wyłącznie osób znających się wzajemnie, grupy rówieśniczej, klasy szkolnej, uczniów danej placówki oświatowej, więc przypadkowość w wyborze ofiary tu nie występuje.

Jak podają K. Knol i J. Pyżalski, cyberbullying (mobbing elektroniczny) odnosi się do najpoważniejszych przypadków agresji uskutecznianej za pomocą tzw. nowych mediów (głownie internetu lub telefonów komórkowych), które będą charakteryzowały się triadą cech mobbingu tradycyjnego (bullyingu), czyli intencjonalnością działania sprawcy w stosunku do ofiary, regularnością i powtarzalnością określonych form molestowania i nierównowagą sił występującą pomiędzy sprawcą a ofiarą, wynikającą z przewagi fizycznej, liczebnej, potencjałowej, emocjonalnej lub umiejętności obsługi narzędzi informatycznych. Nowoczesne podejście do definiowania cyberbullyingu odzwierciedla jednak potrzebę oraz dążenie do rozszerzenia wspomnianego katalogu cech charakterystycznych dla tego elektronicznego zjawiska o dodatkowe elementy, a nawet chęć przedefiniowania powyższych cech w kierunku bardziej odpowiadającym przestrzeni wirtualnej (w odniesieniu do wiktymizacji i sprawstwa online). Cyberbullying nierzadko łączony jest, a nawet utożsamiany, z pojęciami takimi jak cyberstalking (cyberdręczenie), cyberprześladowanie czy cyberagresja, z tym że cyberbullyingowi przypisuje się stosowanie przemocy wobec dzieci i młodzieży, a pozostałym określeniom – przemocy wobec dorosłych. Ponadto wskazane terminy charakteryzują się

różnym zakresem znaczeniowym – technicznym zakresem aspektu działania i podejściem do kryteriów tradycyjnego bullyingu (czyli kwestii celowości, powtarzalności, nierównowagi sił oraz relacji sprawca – ofiara wewnątrz grupy społecznej). Biorąc pod uwagę powyższe, Pyżalski skonstruował definicję mobbingu elektronicznego (cyberbullyingu), któremu nadał znaczenie „rówieśniczej agresji elektronicznej realizowanej przez dzieci i młodzież w ramach tej samej grupy społecznej, w sposób powtarzalny, celowy i w sytuacji znacznej przewagi sprawców nad ofiarą".

Czynnikami wpływającymi na rozszerzanie się grona sprawców i ofiar cyberbullyingu są wg M. Walrave'a i W. Heirmana:

- możliwość zachowania anonimowości w sieci;
- możliwość ingerencji w życie rówieśnicze 24 godziny na dobę przez 7 dni w tygodniu;
- przekonanie o nieuchwytności bądź niezauważeniu podejrzanego działania przez rodziców, nauczycieli i wychowawców;
- fakt nieodbierania przez sprawcę cyberbullyingu niewerbalnych sygnałów wysyłanych przez ofiarę;
- możliwość elektronicznego przekazania informacji w dużym tempie i nieograniczonej liczbie użytkowników internetu czy telefonii komórkowej.

Skutkami cyberbullyingu mogą być dla ofiary:

- wzmożone poczucie lęku, osamotnienia, zagrożenia, upokorzenia, frustracji, gniewu, smutku;
- niski poziom samooceny, poczucie beznadziei i wycofanie społeczne;
- depresja, zaburzenia emocjonalne, śmierć.

Ważną → s t r a t e g i ą [t. 4] w przypadku podejmowanych działań mających na celu profilaktykę zachowań problemowych dotyczących zjawiska cyberbullyingu jest strategia informacyjna, której zamiarem jest przekazanie odbiorcy wiarygodnych informacji o naturze, istocie i zasadzie działania cyberbullyingu oraz o zagrożeniach z tym związanych. Profilaktykę tę należy oprzeć na wynikach aktualnych badań naukowych, dostosować treść i formę przekazu do odpowiedniej grupy odbiorców, a jej prowadzenie w tym zakresie zlecić osobom zajmującym się przeciwdziałaniem mobbingowi elektronicznemu (cyberbullyingowi).

Paweł Łubiński

J. Barlińska, *Wpływ kontaktu zapośredniczonego przez komputer na nasilenie zachowań antyspołecznych i cyberprzemocy*, „Dziecko Krzywdzone. Teoria, Badania, Praktyka" 2009, nr 1 (26); J.J. Dooley, J. Pyżalski, D. Cross, *Cyberbullying Versus Face-to-Face Bullying: A Theoretical and Conceptual Review*, „Journal of Psychology" 2009, vol. 217 (4); K. Dyrla-Mularczyk, M. Pluciński, *Cyberbullying i agresja elektroniczna jako współczesne zagrożenia dla komunikacji w sieci*, „Teraźniejszość – Człowiek – Edukacja" 2017, t. 20, nr 4 (80); B. Jankowiak, *Cyberprzemoc (cyberbyllying) wśród młodzieży jako zachowanie ryzykowne*, [w:] *Zanurzeni w mediach. Konteksty edukacji medialnej*, N. Walter (red.), Wydawnictwo Naukowe UAM, Poznań 2016; A. Kaczmarek, *Edukacja medialna wobec zagrożeń*

cyberprzemocy i cyfrowego wykluczenia, „Kultura – Media – Teologia" 2013, nr 13; K. Knol, J. Pyżalski, *Mobbing elektroniczny: analiza rozwiązań profilaktycznych i interwencyjnych*, „Dziecko Krzywdzone. Teoria, Badania, Praktyka" 2011, nr 1 (34); E. Krzyżak-Szymańska, J. Kowalkowska, A. Szymański, *Zagrożenia dzieci i młodzieży w sieci – cyberproblemy, diagnoza i profilaktyka. Vademecum nauczyciela*, Górnośląska Wyższa Szkoła Handlowa im. Wojciecha Korfantego w Katowicach, Katowice 2016; R. Lew-Starowicz, *Profilaktyka cyberprzemocy w szkole*, [w:] *Człowiek w świecie rzeczywistym i wirtualnym. Wybrane patologie społeczno-wychowawcze w cyberprzestrzeni*, A. Andrzejewska, J. Bednarek, S. Ćmiel (red.), Wydawnictwo WSGE, Józefów 2013; P. Łubiński, *Cyberprzemoc*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; C.P. Monks i in., *Bullying in Different Contexts: Commonalities, Differences and The Role of Theory*, „Aggression and Violent Behavior" 2009, no. 14; W. Poleszak, *Profilaktyka zachowań agresywnych w internecie. Propozycja działań profilaktycznych*, [w:] *Cyberbullying: zjawisko, konteksty, przeciwdziałanie*, J. Pyżalski (red.), Wydawnictwo Naukowe WSP, Łódź 2012; J. Pyżalski, *Agresja elektroniczna dzieci i młodzieży – różne wymiary zjawiska*, „Dziecko Krzywdzone. Teoria, Badania, Praktyka" 2009, nr 1 (26); tenże, *Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży*, Oficyna Wydawnicza Impuls, Kraków 2012; tenże, *Gimnazjaliści online: dobre i złe wiadomości z polskiej części wyników European Cyberbullying Intervention Project*, [w:] *Cyberbullying: zjawisko, konteksty, przeciwdziałanie*, J. Pyżalski (red.), Wydawnictwo Naukowe WSP, Łódź 2012; M. Walrave, W. Heirman, *Skutki cyberbullyingu – oskarżenie czy obrona technologii?*, „Dziecko Krzywdzone. Teoria, Badania, Praktyka" 2009, nr 1 (26); Ł. Wojtasik, *Przemoc rówieśnicza z użyciem mediów elektronicznych – wprowadzenie do problematyki*, „Dziecko Krzywdzone. Teoria, Badania, Praktyka" 2009, nr 1 (26); P. Ziółkowski, *Zagrożenie cyberprzemocy wśród młodzieży szkolnej*, [w:] *Bezpieczna i przyjazna szkoła*, P. Ziółkowski (red.), Wydawnictwo Wyższej Szkoły Gospodarki w Bydgoszczy, Bydgoszcz 2016.

CYBERPRZESTĘPCZOŚĆ – wszelkie nielegalne działania prowadzone przez osoby wykorzystujące technologię informacyjną i sieci telekomunikacyjne w sposób, który narusza dobra chronione prawnie. Jest to termin niejednoznaczny, nie został dotychczas ujęty w sposób jednolity w obowiązujących systemach prawa karnego, wśród specjalistów prawa istnieje spór co do identyfikacji tego typu przestępstw oraz określenia jego ram. Innym problematycznym aspektem jest chaos terminologiczny, w literaturze można zetknąć się z takimi określeniami jak przestępstwa informacyjne, przestępczość wirtualna, przestępstwa związane z technologią cyfrową, przestępstwa internetowe, e-przestępczość itp.

Z perspektywy prawa międzynarodowego można się odwoływać do ogólnej definicji wypracowanej przez ONZ, która wyróżnia wąską oraz szeroką perspektywę ujęcia tego zjawiska:

- wąska – sprowadza cyberprzestępczość do wszelkich działań przeprowadzonych na zasadzie operacji informatycznych, których celem jest system bezpieczeństwa informatycznego;
- szeroka – zalicza do cyberprzestępstw wszystkie działania popełnione za pomocą albo dotyczące systemów lub sieci komputerowych.

Jedyną umową międzynarodową dotyczącą cyberprzestępczości jest Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r., która dzieli ją na 5 grup:

- przestępstwa komputerowe, skierowane przeciwko poufności, integralności i dostępności danych i systemów komputerowych; należą do nich: nielegalny dostęp, nielegalne przechwytywanie, zakłócanie danych, zakłócanie działania systemu itp.;
- nielegalne działania związane z użyciem narzędzi komputerowych: fałszowanie przy użyciu technologii komputerowej, oszustwo w celu nielegalnego wydobycia korzyści ekonomicznych dla siebie lub osób trzecich;
- okrucieństwa związane z treścią, głównie z pornografią dziecięcą;
- naruszenia praw autorskich i praw pokrewnych;
- rozpowszechnianie → i n f o r m a c j i [t. 2] o rasistowskiej i innej naturze podżegającej do → p r z e m o c y [t. 3], nienawiści lub dyskryminacji osoby lub grupy obywateli ze względu na pochodzenie rasowe, narodowe, religijne lub etniczne. Ta grupa została dołączona na początku 2002 r., kiedy do konwencji przyjęto protokół dodatkowy.

Choć jest to akt o charakterze regionalnym, ma on istotny wpływ na prawo międzynarodowe, wskazuje na potrzebę penalizacji → c y b e r a t a k ó w, na obowiązek ścigania i karania ich sprawców. Zawiera on wzorcowe normy prawne, które powinny zostać inkorporowane do prawa wewnętrznego, i tworzy ramy współpracy między państwami dotkniętymi cyberprzestępczością zgodnie z zasadą, że jedyną metodą zapobiegania cyberprzestępczości jest restrykcyjne egzekwowanie prawa, do czego niezbędna jest ścisła współpraca międzynarodowa.

W innym ważnym dokumencie – Tallinn Manual 2.0 – zwrócono uwagę na konieczność odróżnienia cyberprzestępstw, do których ma zastosowanie konwencja budapeszteńska, od innych form konfliktów w → c y b e r p r z e s t r z e n i, takich jak szpiegostwo państwowe i gospodarcze, sabotaż i inne akty wywołujące efekty podobne do konwencjonalnego ataku zbrojnego, a zatem znacznie wykraczające poza tradycyjne ramy pojęcia przestępstwa.

Istnieją 3 podejścia do kryminalizacji społecznie niebezpiecznych ingerencji popełnianych z wykorzystaniem możliwości i środków technologii komputerowej, uważanych za przestępstwo:

- nieautoryzowany dostęp do systemów komputerowych, rozprzestrzenianie wirusów komputerowych (zob. → z ł o ś l i w e o p r o g r a m o w a n i e [t. 4]) i niezgodne z prawem korzystanie z systemów komputerowych i informacji (Norwegia, Singapur, Słowacja, Filipiny, Republika Korei);
- uznanie za przestępstwa komputerowe tylko tych czynów, których popełnienie powoduje szkody majątkowe i w obrębie komputerowego przetwarzania informacji (Dania, Szwecja, Szwajcaria, Japonia);

- sklasyfikowanie nie tylko czynów, które powodują szkody majątkowe, ale także naruszają prawa osobiste lub zagrażają → bezpieczeństwu narodowemu (USA, Francja, Niemcy, Wielka Brytania, Holandia).

W polskiej literaturze prawniczej nie ma oddzielnych rozdziałów odnoszących się do cyberprzestępstw. Najnowsze opracowania prawne dotyczące zagadnień → cyberbezpieczeństwa sugerują podział na:

- przestępstwa *stricte* komputerowe, w tym nieautoryzowany dostęp do systemu komputerowego oraz nielegalny → podsłuch [t. 3] komputerowy (naruszenie tajemnicy komunikacji) – art. 267 kk;
- naruszenie integralności danych komputerowych – art. 268 kk, art. 268a kk;
- naruszenie integralności systemu komputerowego – art. 269 kk, art. 269a kk, art. 269b kk;
- przestępstwa związane z wykorzystaniem sieci i systemów teleinformatycznych oraz nowych technologii (np. oszustwo – art. 286 kk, nielegalne pozyskanie programu komputerowego – art. 278 § 2 kk, oszustwo komputerowe – art. 287 kk, oszustwo telekomunikacyjne – art. 285 kk, przeciwko wiarygodności dokumentów, jak np. fałszerstwo komputerowe – art. 270 § 1 kk, zniszczenie lub pozbawienie mocy dowodowej dokumentu elektronicznego – art. 276 kk). Szerzej ten temat rozwija w literaturze naukowej J. Clough, który wydziela 5 typów: nielegalne transakcje online, zaawansowane oszustwa z opłatami, przestępstwa związane z elektronicznym transferem środków, oszustwa inwestycyjne, → kradzież tożsamości [t. 2];
- przestępstwa popełnione z wykorzystaniem komputera i sieci teleinformatycznych (stalking – art. 190a § 1 kk, w tym także kradzież informacji biometrycznych, nadanej tożsamości, biograficznej tożsamości, art. 190a § 2kk, podszywanie się pod inną osobę);
- przestępstwa z wykorzystaniem komputerów skierowane przeciwko wolności seksualnej popełnione na szkodę małoletniego (*grooming* – art. 200a § 1 i 2 kk, posiadanie treści pornograficznych z udziałem małoletniego poniżej 15 lat – art. 202 kk);
- przestępstwa przeciwko czci (zniesławienie – art. 212 kk, zniewaga – art. 216 kk).

Wymienić można wiele rodzajów cyberprzestępstw, zaliczanych najczęściej do jednej z 4 kategorii:

- przestępstw wymierzonych przeciwko osobom indywidualnym,
- przestępstw przeciwko własności,
- przestępstw przeciwko organizacjom,
- przestępstw wymierzonych przeciwko społeczeństwu.

Literatura kryminalistyczna wymienia następujące motywacje kierujące cyberprzestępcami:

- Zemsta – atakujący może popełnić przestępstwo przeciwko firmie po tym, gdy został niesprawiedliwie potraktowany. Może być to były lub aktualny pracownik,

konkurencja lub grupa osób o wspólnym interesie. W tym przypadku często przewija się archetyp pracownika, który nie dostał awansu mimo przeświadczenia o dobrze spełnianych obowiązkach i wysokiej wydajności pracy. Forma ataku w tym przypadku będzie zróżnicowana ze względu na umiejętności i zasoby dostępne atakującemu.

- Okazja – w przypadku pracownika wewnętrznego nie musi istnieć ściśle określona motywacja do popełnienia jakiejkolwiek formy przestępstwa przeciwko swojemu pracodawcy. Nowy pracownik może podczas wykonywania obowiązków trafnie zidentyfikować podatność na → z a g r o ż e n i a [t. 4] wewnętrzne w systemach, z których pieniądze lub dane mogłyby zostać pozyskane bez udziału innych osób. Następnie zapada decyzja o wykorzystaniu luki na swoją korzyść i dochodzi do kradzieży pieniędzy lub danych. Może być ona rozciągnięta w czasie, a nawet może dojść do niej po usunięciu podatności w systemie. Typowym przykładem są osoby pracujące w finansach, księgowości – dodają one najczęściej fikcyjnych pracowników do systemu, płacą im pensje na konto, równolegle prowadząc drugą księgę wydatków dla ukrycia swoich działań.
- Chciwość – to motywacja zarówno pracowników wewnętrznych, zewnętrznych, jak i przestępców, szansa wzbogacenia się kosztem innego podmiotu jest atrakcyjną możliwością pozwalającą usprawiedliwić swoje postępowanie poprzez wykluczenie czynienia bezpośrednich szkód innym ludziom. Często indykatorem takiej motywacji jest ulokowanie dochodów pozyskanych z przestępstwa na złagodzenie potencjalnych szkód.
- Test umiejętności – cyberprzestępcy w ramach zdobywania doświadczenia mogą przeprowadzać ataki na różnego rodzaju instytucje zarówno z sektora prywatnego, jak i publicznego. Celem takich pobocznych ataków jest często zdobycie sławy w środowisku, udowodnienie wysokiego poziomu swoich umiejętności. Zostawianie tego typu znaków często wskazuje na działalność tzw. *script kiddies*, czyli osób mniej zaawansowanych pod względem technicznej wiedzy i umiejętności, które do ataków wykorzystują najczęściej udostępnione im wirusy, programy i metody cyberataków.
- Konkurencja z branży – cechą szczególną niektórych rynków jest nacisk na uzyskanie przewagi strategicznej, a przeprowadzenie cyberataku na konkurencyjną firmę jest sprawdzonym sposobem na osiągnięcie tego celu. Efektem ubocznym jest podważenie jej reputacji w oczach obecnych i potencjalnych klientów, którzy mogą ulec obawom o stan swoich interesów w związku z kłopotami firmy czy kontrahentów.
- Zysk dla profesjonalnych cyberkryminalistów lub → c y b e r g r u p cyberprzestępczych – ich motywacją (obecnie właściwie niespotykane jest działanie jednostki na większą skalę) jest uzyskanie finansowej korzyści. Atak w tym przypadku nie jest osobisty, często jest zlecony przez osobę trzecią. Usługi tego typu

cyberprzestępców można zazwyczaj zamówić poprzez fora i strony w → d a r k - n e c i e [t. 2].

- Względy polityczne, → h a k t y w i z m [t. 2] – są to cyberataki motywowane politycznym → r a d y k a l i z m e m [t. 3], niekiedy celem jest głoszenie politycznych i/lub religijnych haseł oraz zniechęcanie ludzi do innych poglądów. Przykładem może być cyberatak na podmiot bojkotu konsumenckiego lub na firmę dostarczającą produkt bądź usługę, która u atakującego wzbudza nienawiść.
- Względy geopolityczne – to cyberataki przeprowadzane przez agencje rządowe innych państw bądź wynajęte przez nie cybergrupy. Motywacją w tym przypadku jest najczęściej przeprowadzenie aktów → c y b e r s z p i e g o s t w a wobec infrastruktury firmy w celu uzyskania przewagi technologicznej, politycznej, ekonomicznej – uzyskiwane są tajne informacje o projektach wojskowych lub sytuacji w określonym państwie. Niektóre pozyskane dane są następnie wykorzystywane przez służby wywiadowcze, z których część może zdobyć zainteresowana (np. konkurencyjna) firma. Drugim opcjonalnym celem może być spowodowanie znaczących szkód. Szczególnym przypadkiem tego typu działań jest wirus Stuxnet z 2006 r., stworzony przy udziale amerykańskich i izraelskich służb wywiadowczych, którego wprowadzenie do oprogramowania wirówek wzbogacających uran wstrzymało irański program nuklearny. Odnotowano także próby złamania systemów ochrony w elektrowniach jądrowych i innych przedmiotach → i n f r a - s t r u k t u r y k r y t y c z n e j [t. 2] w USA. Niektórzy w ten sposób odnoszą zyski, jednocześnie szkodząc biznesowi (np. Korea Północna zakłóciła większość komputerów w Sony Pictures).

Działania cybergrup państwowych związane są także z podejmowaniem tzw. → w a l k i i n f o r m a c y j n e j [t. 4], np. poprzez przyjmowanie roli „nieznanych haktywistów", narażając prywatne informacje na publiczny dostęp, aby mieć na nie wpływ (w ten sposób → r o s y j s k i e s ł u ż b y w y w i a d o w c z e [t. 3] wpłynęły na wyniki wyborów w USA, publikując korespondencję Partii Demokratycznej). Dlatego aktywność „państwowych" → h a k e r ó w [t. 2] jest dość zróżnicowana, zapewnienie ochrony przed ich działaniami jest dużym wyzwaniem.

Członkowie grup zorganizowanych mogą korzystać z oprogramowania hakerów „państwowych", a hakerzy „państwowi" mogą również kraść pieniądze z banków państwa, przeciwko któremu odbywa się specjalna operacja. Jeśli stosowny zestaw narzędzi zostanie umieszczony w sieci, z pewnością zacznie być szeroko wykorzystywany. Wszystko to podnosi cenę cyberbezpieczeństwa dla biznesu – podobnie jak w przypadku innych przestępstw, przezwyciężenie konsekwencji włamań jest znacznie droższe niż ich ochrona przed nimi.

Według IBM Security i Ponemon Institute średnia cena nawet stosunkowo niewielkiego wycieku informacji (z 2,5 tys. do 100 tys. kont) to 3,87 mln USD, większego wynosi zaś co najmniej 40 mln USD. Należy podkreślić, że wartości te obecnie wzrastają

z uwagi na zachodzące zmiany w prawodawstwie. Dlatego globalne koszty bezpieczeństwa cybernetycznego przekroczą w 2021 r. 60 mld USD, przewiduje się również, że rynek cyberbezpieczeństwa będzie wart 300 mld USD do 2024 r. Cyberprzestępcy będą nadal poprawiać swoje umiejętności.

Podczas IV spotkania Międzyrządowej grupy ekspertów w celu przygotowania kompleksowej analizy problemu cyberprzestępczości, które odbyło się w Wiedniu w kwietniu 2018 r., odnotowano bieżące globalne trendy w legislacyjnej regulacji przeciwdziałania cyberprzestępczości. Stwierdzono, że w wielu rozwijających się państwach członkowskich ONZ (Ameryka Łacińska, Afryka, Azja) nadal brakuje podstawowych aktów prawnych regulujących cyberprzestępczość lub są one dopiero opracowywane. Z kolei w wielu państwach, w których takie dokumenty zostały przyjęte, nie zawsze jest możliwe ich wykorzystanie z powodu poważnych rozbieżności z przepisami dotyczącymi postępowania karnego. Badania wykazały, że nawet przy odpowiednich ramach prawnych konieczna jest ich dalsza reforma. To jedyny sposób, aby nadążyć za zmianami.

Niektórzy autorzy do cyberprzestępstw zaliczają haking, cyberszpiegostwo oraz działania wykorzystujące techniki psychologiczno-socjologiczne. W takim ujęciu wskazuje się, że cechą wspólną przestępstw opartych na hakingu jest wykorzystywanie słabości w systemach docelowych, aby uzyskać dostęp do nich lub spowodować zakłócenia ich działania. Natomiast do grupy czynów popełnianych za pomocą technik psychologiczno-społecznych zalicza się najczęściej oszustwa i wyłudzenia dokonywane dzięki poufnym informacjom uzyskanym przez szeroko rozumiane wprowadzanie w błąd użytkowników internetu. Wszystkie cyberprzestępstwa wykorzystujące dostęp do poufnych danych – osiągnięty jednak w inny sposób niż poprzez zdobycie i wykorzystanie zaufania ich dysponentów – kwalifikowane są jako cyberszpiegostwo.

Badanie Clark School na University of Maryland jest jednym z pierwszych, które określiło niemal stałą liczbę ataków hakerów na komputery z dostępem do internetu – występują one średnio co 39 sekund.

Cyberprzestępczość jest znaczącym problemem w skali globalnej. W 2017 r. cyberprzestępcom udało się ukraść łącznie 146,3 mld EUR w 20 krajach świata. Z raportu *Norton Cyber Security Insight 2017* wynika, że w 2016 r. w 20 biorących udział w badaniu krajach hakerzy okradli łącznie 978 mln osób. Tylko w 7 krajach Europy (Francji, Niemczech, Włoszech, Holandii, Hiszpanii, Szwecji i Wielkiej Brytanii) cyberprzestępcy okradli 98,2 mln ludzi. Zabrali im 23,3 mld EUR.

Usługi cyberprzestępców na rok 2018 na czarnym rynku są stosunkowo tanie: usługa ataku DDoS kosztuje od 30 do 70 USD za dzień, w pakiecie za cały miesiąc 1200 USD, → b o t n e t wraz z siecią 2 tys. komputerów zombie to koszt 200 USD, cena za zhakowanie konta na portalach Facebook lub Twitter wynosi 130 USD, zhakowanie konta Gmail kosztuje natomiast 162 USD.

Specjaliści ds. cyberbezpieczeństwa z firmy Cisco Talos wykryli na Facebooku 74 grupy cyberprzestępcze, zrzeszające łącznie 385 tys. członków, jak podał serwis ArsTechnica.com. Użytkownicy oferowali tam m.in. usługi hakerskie oraz rozsiewanie spamu. Na forach tych grup oferowane były dane ze zhakowanych kart bankowych, informacje finansowe, dane uwierzytelniające, narzędzia i usługi spamowania poczty elektronicznej. Można również było zamówić kampanie phishingowe (zob. → p h i - s h i n g [t. 3]) oraz podrobione dokumenty tożsamości. Eksperci Cisco zgłosili Facebookowi istnienie grup, co poskutkowało ich usunięciem z portalu. Zwrócono jednak uwagę, że nie minęło wiele czasu, a kolejne grupy tego rodzaju zaczęły pojawiać się w tym samym serwisie społecznościowym. Facebook obecnie współpracuje z Cisco nad rozwiązaniem problemu.

Według raportu KPMG *Barometr cyberbezpieczeństwa. W obronie przed cyberatakami* z kwietnia 2019 r., który powstał na podstawie ankiety wśród 100 firm w Polsce, szeroko rozumiana cyberprzestępczość została uznana za zagrożenie przez 96% z nich, co oznacza wzrost o 12 punktów procentowych wobec badania z poprzedniego roku. W ramach cyberprzestępczości organizacje wskazują najczęściej na zagrożenie ze strony pojedynczych hakerów (84%), zorganizowane grupy cyberprzestępcze (58%) oraz cyberterrorystów (54%). Skutki cyberprzestępczości dotknęły 68% ankietowanych przedsiębiorstw, a 25% z nich zanotowało wzrost liczby cyberataków. Globalne straty spowodowane działalnością cyberprzestępców wyniosły ok. 1% światowego PKB. Jak wskazuje M. Kurek z KPMG, cyberprzestępczość rozwija się dziś niezwykle dynamicznie, a jej transgraniczny charakter sprawia, że hakerzy są coraz lepiej zorganizowani, bezkarni i dysponują ogromnym zapleczem kapitałowym. Część grup wspierana jest przez obce państwa.

Cyberatak na światową skalę, skoordynowany i z użyciem złośliwych wiadomości e-mail, może spowodować straty gospodarcze w wysokości nawet 193 mld USD – są to szacunki ekspertów ds. analizy ryzyka z firm ubezpieczeniowych Aon i Lloyd's of London. W tej kwocie zawierałyby się m.in. same wypłaty odszkodowań, które mogłyby osiągnąć kwoty od 10 do 27 mld USD, w zależności od limitów zapisanych w polisach, które mogą wynosić od 500 tys. do 200 mln USD. Globalny cyberatak może jednocześnie dotknąć podmioty z wielu sektorów gospodarki na całym świecie. Na największe straty narażone są jednak handel, → o c h r o n a z d r o w i a [t. 3], przemysł wytwórczy i branża finansowa.

W perspektywie najbliższych kilkunastu lat każde dotychczas znane nam przestępstwo stanie się cyberprzestępstwem – to teza najnowszego raportu opublikowanego przez Infuture Hatalska Foresight Institute *Future of Crime*, opracowanego z udziałem ekspertów m.in. Atende oraz Cisco Poland. W raporcie prezentowane są zagrożenia „dzisiaj", „jutro" i „pojutrze" – od ataków na infrastrukturę krytyczną po hakowanie genów i tzw. *mindreading*.

Group-IB, międzynarodowa firma specjalizująca się w zapobieganiu cyberatakom, zaprezentowała nowy paradygmat bezpieczeństwa informacji podczas globalnej

międzynarodowej konferencji CyberCrimeCon 2018. Koncepcja została ujęta w raporcie rocznym *Hi-Tech Crime Trends 2018*, w którym analizowane są globalne trendy w rozwoju cyberprzestępczości i przewidywane przyszłe cele prorządowych grup hakerów i hakerów o motywacjach finansowych. Przejście z pozycji defensywnej do polowania na cyberprzestępców jest obecnie głównym trendem na rynku bezpieczeństwa informacji.

Wojciech Cendrowski, Olga Wasiuta

W. Cendrowski, O. Wasiuta, *Cyberprzestępczość*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; CyberDefence24, *Przyszłość cyberprzestępczości*, 25.04.2018, CyberDefence24.pl (dostęp 24.04.2019); FutureOfCrime. Atende.pl (dostęp 24.04.2019); Group-IB, *Hi-Tech Crime Trends 2017*; W. Gogołek, *Komunikacja sieciowa. Uwarunkowania, kategorie i paradoksy*, ASPRA-JR, Warszawa 2010; *Groups*, Attack.Mitre.org (dostęp 24.04.2019); *Hackers Attack Every 39 Seconds*, 10.02.2017, SecurityMagazine.com (dostęp 24.04.2019); B. Hołyst, T. Pomykała, *Cyberprzestępczość, ochrona informacji i kryptologia*, „Prokuratura i Prawo" 2011, nr 1; D. Jagiełło, *Karnoprawne ramy odpowiedzialności za przestępstwa popełniane w cyberprzestrzeni*, [w:] *Cyberbezpieczeństwo. Zarys wykładu*, C. Banasiński (red.), Wolters Kluwer, Warszawa 2018; A. Kopciuch, *Grupy cyberprzestępcze*, 12.02.2019, CyberSecurity.org (dostęp 24.04.2019); KPMG, *Barometr cyberbezpieczeństwa. W obronie przed cyberatakami*, 2019, KPMG.pl (dostęp 24.04.2019); *Law of International Responsibility*, [w:] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, M.N. Schmitt (red.), Cambridge University Press, Cambridge 2017; Norton by Symantec, *2017. Norton Cyber Security Insights Report: Global Results*, 2018; PAP, *Eksperci policzyli, ile kosztowałyby straty gospodarcze spowodowane cyberatakiem na światową skalę*, 3.02.2019, BusinessInsider.com.pl (dostęp 24.04.2019); PAP/BAD, *Na Facebooku wykryto 74 grupy cyberprzestępcze, zrzeszały 385 tys. członków*, 6.04.2019, WNP.pl (dostęp 24.04.2019); F. Rodniewicz, *Postanowienia decyzji ramowej Rady w sprawie ataków na systemy informatyczne a ujęcie cyberprzestępstw w kodeksie karnym*, „Ius Novum" 2009, nr 1; J.A. Shamsi, S. Zeadally, F. Sheikh i i in., *Attribution in Cyberspace: Techniques and Legal Implications*, „Security and Communication Networks" 2016, no. 9; M. Siwicki, *Cyberprzestępczość*, C.H.Beck, Warszawa 2013; M. Smarzewski, *Cyberterroryzm a cyberprzestępstwa o charakterze terrorystycznym*, „Ius Novum" 2017, nr 1.

CYBERPRZESTRZEŃ – mimo wielu prób nie została ustalona jej powszechnie akceptowana definicja. Wynika to m.in. z różnych podejść do fenomenu cyberprzestrzeni, np. techniczno-technologicznego, społecznego, kulturowego, pragmatycznego, metaforycznego itp. Niesamodzielna cząstka cyberpochodzi od stgr. κῠβερνάω, kubernáō (sterować, nawigować), J. Unold sugeruje koncepcję z jednej strony nawigowania w oceanie danych cyfrowych, a z drugiej „kontroli" osiąganej poprzez odpowiednią manipulację tymi danymi. Przestrzeń w kontekście cyberprzestrzeni oznacza system współzależności między użytkownikami, komputerami, serwerami itp. wewnątrz sieci.

Pojęcie cyberprzestrzeni spopularyzował W. Gibson, amerykański pisarz science fiction, który posłużył się tym terminem w opowiadaniu *Burning Chrome* w 1982 r. 2 lata później w powieści *Neuromancer* cyberprzestrzeń określał jako:

> konsensualną halucynację doświadczaną każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach, przez dzieci nauczane pojęć matematycznych… Graficzne odwzorowanie banków danych wszystkich komputerów świata. Niewyobrażalną złożoność.

Koncepcję cyberprzestrzeni opisał już wcześniej V. Vinge w powieści pt. *True Names* w 1981 r.

Stopniowo nienaukowe rozumienie cyberprzestrzeni jako wytworu ludzkiej wyobraźni i niezidentyfikowanego zjawiska zmieniało się na rzecz niematerialnej sfery ludzkiej działalności, w której skład wchodzą komputery i sieci. Pojęcie zaczęło być wykorzystywane przez naukowców jako określenie powiązań o charakterze wirtualnym, powstałych i funkcjonujących poprzez ich fizyczne manifestacje – komputery oraz infrastrukturę telekomunikacyjną.

W potocznym rozumieniu cyberprzestrzeń traktowana jest jako przestrzeń społeczna, w której spotykają się (komunikują) internauci za pośrednictwem komputerów przyłączonych do globalnej sieci WWW. Stanowi ona sieć powiązań jednostek w celu wymiany → i n f o r m a c j i [t. 2] prowadzenia biznesu, kreowania sztuki, prowadzenia polityki. Określa się nią kompleks zjawisk związanych z szeroko pojętą → t e c h n o l o g i ą i n f o r m a c y j n o - k o m u n i k a c y j n ą [t. 4] (TIK), rozpatrywanych w perspektywie kulturowej, socjologicznej, psychologicznej, pedagogicznej, aksjologicznej, politycznej, ekonomicznej, medycznej, informatologicznej itp. W każdym z tych obszarów rodzą się dylematy wynikające z relacji i zależności będących konsekwencją zderzenia świata realnego z wirtualnym. Podmioty (społeczności wirtualne) funkcjonujące w cyberprzestrzeni tworzą jej szerszy kontekst, nazywany cyberkulturą. W kulturze tej mamy do czynienia zarówno z rzeczywistością rozszerzoną, jak i rzeczywistością wirtualną. Istotą rozszerzonej rzeczywistości jest łączenie obrazu świata rzeczywistego z elementami stworzonymi przy wykorzystaniu technologii informatycznych, natomiast idea rzeczywistości wirtualnej opiera się na tworzeniu sztucznego, całkowicie wygenerowanego komputerowo środowiska, które może naśladować wygląd świata rzeczywistego. Obie rzeczywistości (wirtualna i rozszerzona) mieszczą się w kategorii światów wygenerowanych przez człowieka dzięki TIK, a więc sztucznych. Badacze twierdzą, że na obecnym etapie rozwoju technologii wirtualnej i rozszerzonej rzeczywistości ich użytkownicy mają problemy z oddzieleniem doświadczeń zdobytych w świecie fizycznym od doświadczeń związanych z wirtualną lub rozszerzoną rzeczywistością. Oznacza to, że środowisko wirtualne może nie być odróżnialne w percepcji człowieka od rzeczywistości, a granice między doświadczeniem zdobytym w świecie fizycznym i wirtualnym zacierają się coraz bardziej. Zapewne rewizji trzeba będzie poddać te koncepcje cyberprzestrzeni, które całkowicie przeciwstawiają ją „światu realnemu". Analiza pojęć związanych z funkcjonowaniem cyberprzestrzeni dokonana przez Unolda sugeruje konieczność poszerzenia refleksji w tym obszarze. Zakresy pojęć takich jak autostrada informacyjna, przestrzeń cyfrowa, → i n f o s f e r a [t. 2],

„myślące rzeczy", „otaczająca inteligencja", wirtualna rzeczywistość czy symulowana rzeczywistość zmuszają do szukania odpowiedzi na pytanie o różnice między światem realnym a rzeczywistością symulowaną, a także o sposób zachowania się człowieka, który ma świadomość „zanurzenia się" w rzeczywistości symulowanej.

Cyberprzestrzeń staje się pojęciem, które coraz częściej jest nie tylko utożsamiane z internetem, lecz także łączone z różnymi mediami, takimi jak telewizja, klasyczne sieci telefoniczne, telefonia komórkowa, a szczególnie z internetem rzeczy, czyli wszechobecnym, niewidocznym przetwarzaniem informacji, niezwiązanym z konkretnym komputerem, lecz dokonującym się wszędzie, dzięki podłączonym do sieci przedmiotom codziennego użytku. Cyberprzestrzeń stanowi zatem podstawowy kanał wymiany informacji, obejmuje wszystkie systemy komunikacji elektronicznej, które przesyłają informacje pochodzące ze źródeł cyfrowych lub są przeznaczone do digitalizacji.

Cyberprzestrzeń może być analizowana w 2 aspektach – materialnym i niematerialnym. Perspektywa materialna określa sferę fizyczną cyberprzestrzeni, czyli infrastrukturę teleinformatyczną, w której skład wchodzą urządzenia takie jak komputery, kable, routery. W aspekcie niematerialnym cyberprzestrzeń jest odrębnym środowiskiem i nie powinna być traktowana jako suma urządzeń. Podkreśla się tu możliwość budowy interakcji międzyludzkich.

J. Bednarek wyróżnił następujące funkcje cyberprzestrzeni:

- informacyjna – cyberprzestrzeń jako przestrzeń wymiany informacji,
- ludyczna – cyberprzestrzeń pozwala człowiekowi na zaspokajanie potrzeby rozrywki,
- stymulująca – użytkownik cyberprzestrzeni aktywnie odbiera treści, które się w niej znajdują,
- wzorotwórcza – w cyberprzestrzeni tworzą się nowe wzorce, idee, standardy życia,
- interpersonalna – w cyberprzestrzeni powstają relacje. Jest kanałem komunikacji między podmiotami. Funkcja ta wynika z wszechobecnej telewizji i komputerów łączących się z całym światem przez internet.

P. Sienkiewicz opisuje cyberprzestrzeń z perspektywy badań systemowych, szczególnie analizy systemowej, którą definiuje jako zbiór metod i technik analitycznych, ocenowych i decyzyjnych służących racjonalnemu rozwiązywaniu systemowych sytuacji decyzyjnych, a zarazem będących czynnościami wspomagającymi działania osób odpowiedzialnych za decyzje podejmowane w warunkach niepewności i ryzyka. Przestrzeń cybernetyczna („galaktyka Wienera") jest dla autora konwergencją technologii informatycznych, telekomunikacyjnych i mediów, charakteryzujących się cechami takimi jak: sieciowość, wirtualność, interaktywność, multimedialność, hipertekstowość. Z perspektywy analizy systemowej duże znaczenie mają cechy strukturalne i funkcjonalne cyberprzestrzeni jako „złożonego systemu o strukturze «sieci sieci». System ten ewoluuje, jest zdolny do zachowań chaotycznych związanych z nieliniowym

charakterem reakcji (stosunków i sprzężeń) między elementami: powstającymi i znikającymi sieciami składowymi". Przyczyn tego stanu rzeczy Sienkiewicz upatruje w społecznym charakterze relacji wewnątrzi międzysieciowych.

J. Wasilewski zebrał najczęściej cytowane w literaturze definicje cyberprzestrzeni, są to mianowicie:

- globalna domena → ś r o d o w i s k a i n f o r m a c y j n e g o [t. 4] składająca się ze współzależnych sieci tworzonych przez infrastrukturę technologii informacyjnej oraz zawartych w nich danych, włączając internet, sieci telekomunikacyjne, systemy komputerowe, a także osadzone w nich procesory oraz kontrolery;
- wirtualna przestrzeń, w której krążą elektroniczne dane przetwarzane przez komputery PC z całego świata;
- interaktywna domena stworzona z cyfrowych sieci, która jest wykorzystywana do przechowywania, modyfikowania oraz przekazywania informacji; jej częścią jest internet, ale zawierają się w niej także inne systemy informacyjne, które obsługują biznes, infrastrukturę oraz wspomagają świadczenie usług;
- wirtualna przestrzeń wszystkich systemów technologii informacyjnej powiązanych na poziomie danych w skali globalnej, której fundament stanowi internet; systemy IT działające w wyizolowanej przestrzeni wirtualnej nie stanowią części cyberprzestrzeni;
- przestrzeń komunikacyjna utworzona przez globalne połączenie sprzętu służącego do automatycznego przetwarzania cyfrowych danych.

Interpretując te definicje, badacz stawia pytanie, w jaki sposób poprawne rozumienie tego, czym jest cyberprzestrzeń, wpływa na postrzeganie → b e z p i e c z e ń s t w a państwa. Położenie w definicji cyberprzestrzeni akcentu na elementy → i n f r a s t r u k t u r y i n f o r m a c y j n e j [t. 2] sprawia, że bezpieczeństwo tak ujętej cyberprzestrzeni skupiać się będzie na zapewnieniu ochrony tylko tym elementom, natomiast włączenie do definicji użytkowników i relacji występujących między nimi wymaga rozumienia bezpieczeństwa w tym obszarze w sposób dynamiczny i wieloaspektowy. Definicja cyberprzestrzeni przyjęta w → D o k t r y n i e c y b e r b e z p i e c z e ń s t w a RP [t. 2] uwzględnia oba te elementy. Stanowi ją:

> przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniające przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończeń sieci) wraz z powiązaniami między nimi oraz relacjami z użytkownikami.

W ujęciu socjologicznym cyberprzestrzeń określana jest jako nowa przestrzeń umożliwiająca interakcje, komunikację, kontakty towarzyskie, organizowanie się oraz prowadzenie transakcji. Takie rozumienie cyberprzestrzeni zostało zaprezentowane

m.in. w dokumencie pt. *Information Systems Defence and Security: France's Strategy*. Cyberprzestrzeń została nazwana przez Francuzów Nową Wieżą Babel, co oznacza, że umożliwia ona mieszanie się języków, kultur, informacji i idei na poziomie globalnym. Podobne znaczenie terminu cyberprzestrzeni zostało zamieszczone w austriackiej → s t r a t e g i i [t. 4] → c y b e r b e z p i e c z e ń s t w a (Österreichische Strategie für Cyber Sicherheit, ÖSCS, ang. Austrian Cyber Security Strategy). W dokumencie czytamy, że cyberprzestrzeń jest przestrzenią ogólnej interakcji społecznej i jest wykorzystywana przez ludzi do socjalizowania się, prowadzenia życia towarzyskiego.

W ujęciu psychologicznym cyberprzestrzeń uznawana jest za stan umysłu. Zdaniem J.P. Barlowa cyberprzestrzeń to „każda przestrzeń, w której ludzie mogą gromadzić swoje umysły bez zabierania tam swoich ciał". W latach 90. XX w., w czasie I → w o j n y [t. 4] w Zatoce Perskiej, która uważana jest za pierwszą wojnę ery informacyjnej, cyberprzestrzeń uzyskała miano kolejnego pola walki. W 1995 r. płk J.A. Warden w publikacji pt. *The Enemy as a System* zaprezentował model (tzw. model Wardena), w którym cyberprzestrzeń została umieszczona obok lądu, morza, powietrza i przestrzeni kosmicznej. Wojskowy określił ją jako jedną ze strategicznych płaszczyzn walki z wrogiem. Zdeterminowało to zmiany w państwowych dokumentach dotyczących bezpieczeństwa.

W 2017 r., w czasie szczytu → N A T O [t. 3] w Warszawie, sygnatariusze uznali cyberprzestrzeń za kolejny obszar prowadzenia działań zbrojnych. W oficjalnym komunikacie wskazano, że cyberprzestrzeń jest obszarem działań, w którym NATO musi bronić się tak samo skutecznie jak na lądzie, w powietrzu i na morzu. To, co różni cyberprzestrzeń od pozostałych sfer działalności państwa, to fakt, że jest ona płaszczyzną sztucznie wykreowaną przez człowieka.

Cyberprzestrzeń stała się obecnie nowym polem walki o wpływy i dominację pomiędzy narodami, państwami i korporacjami, co pociąga za sobą konieczność dokonania licznych zmian zarówno w pragmatyce, jak i w prawno-organizacyjnym wymiarze funkcjonowania systemów bezpieczeństwa w skali globalnej i lokalnej. W przestrzeni tej prowadzi się wiele form walki, takich jak:

- *warfare* – której celem jest uzyskanie przewagi w dowodzeniu,
- *intelligence-based warfare* – bazująca na wiedzy rozpoznawczej,
- *electronic warfare* – nakierowana na techniki radioelektroniczne i kryptograficzne,
- *psychological warfare* – związana z walką psychologiczną,
- *hacker warfare* – będąca atakiem na systemy informacyjne,
- *economic information warfare* – związana z blokowaniem informacji w celu osiągnięcia przewagi ekonomicznej,
- *cyberwarfare* – będąca wojną w rzeczywistości wirtualnej.

Dlatego, jak stwierdza A. Nowak, „sieciowość, zarówno w wymiarze społecznym, jak i technologicznym, wraz z jej wszystkimi konsekwencjami, stanowi jedno z najważniejszych pojęć nowego paradygmatu bezpieczeństwa na poziomie krajowym i międzynarodowym". W związku z tym przestrzeń wirtualna, cyfrowa zaczyna być

traktowana także jak terytorium danego państwa, co skutkuje wprowadzeniem do tezaurusa pojęciowego nowego terminu – cyberprzestrzeni państwa. W *Doktrynie Cyberbezpieczeństwa RP* definiowana jest ona jako:

> cyberprzestrzeń w obrębie terytorium państwa polskiego i poza jego terytorium w miejscach, gdzie funkcjonują przedstawiciele RP, tj. placówki dyplomatyczne, kontyngenty wojskowe, jednostki pływające oraz statki powietrzne poza przestrzenią RP, podlegające polskiej jurysdykcji.

Na potrzeby polityki ochrony cyberprzestrzeni przyjęto, że pojęcie bezpieczeństwa cyberprzestrzeni stanowi „zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mający na celu zapewnienie niezakłóconego funkcjonowania cyberprzestrzeni".

Cyberprzestrzeń jest, jak podkreśla T.R. Aleksandrowicz, „przestrzenią operacyjną, w której wykonywane są przez ludzi działania mające przynieść określony cel, ze swej strony mają wywołać efekty w samej cyberprzestrzeni, jak i poza nią". W przestrzeni tej prowadzona jest → w a l k a i n f o r m a c y j n a [t. 4], której celem jest: uzyskanie wpływu na zachowanie podmiotów będących celem ataku; zakłócanie lub uniemożliwienie funkcjonowania zaatakowanego systemu informatycznego; fizyczne niszczenie infrastruktury informatycznej przeciwnika. Za pośrednictwem sieci teleinformatycznych wchodzących w skład cyberprzestrzeni można wpływać na → i n f r a s t r u k t u r ę k r y t y c z n ą [t. 2] państwa obejmującą systemy zaopatrzenia w energię, surowce energetyczne i paliwa, systemy łączności, sieci teleinformatyczne, systemy finansowe, zaopatrzenia w żywność, wodę, systemy ochrony zdrowia, transportowe, ratownicze, zapewniające ciągłość działania administracji publicznej, systemy produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

Oznacza to, że cyberprzestrzeń ma także wymiar militarny. → R e w o l u c j a w s p r a w a c h w o j s k o w y c h [t. 3] (ang. *revolution in military affairs*, RMA) spowodowała, że dotychczasowe działania sił zbrojnych zostały wsparte nowoczesnymi technologiami informatycznymi, które polegają na:

> użyciu przewagi informacyjnej nad przeciwnikiem (wywiad i rozpoznanie elektroniczne, precyzyjna lokalizacja pozycji własnych za pomocą urządzeń systemu nawigacji satelitarnej GPS) oraz wykorzystaniu broni precyzyjnego rażenia, pozwalającej na dokładną lokalizację celu i jego precyzyjne zniszczenie przy minimalizacji ofiar.

W związku z tym cyberprzestrzeń określa się 5. środowiskiem walki, poza lądem, morzem, przestrzenią powietrzną i kosmosem.

Ochrona cyberprzestrzeni staje się priorytetowym zadaniem rządów ze względu na powstałe → z a g r o ż e n i a [t. 4] o wymiarze globalnym, do których M. Lakomy zalicza:

- → c y b e r t e r r o r y z m – politycznie motywowany atak lub groźba ataku na komputery, sieci lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie i ludziach daleko idących celów politycznych,
- działalność wywiadowczą – próby wyprowadzania → i n f o r m a c j i n i e j a w n y c h [t. 2] z serwerów należących do instytucji rządowych, korporacji lub komputerów osobistych,
- wykorzystanie cyberprzestrzeni do prowadzenia działań zbrojnych mających na celu uzyskanie przewagi informacyjnej, „niewidzialność" przeciwnika, terenem działań jest cyberprzestrzeń, a czynnikiem krytycznym – czas.

W ramach sieciowego paradygmatu bezpieczeństwa opisanego przez Aleksandrowicza państwa traktowane są jako węzły w sieci stosunków międzynarodowych, których obowiązkiem jest dostrzeganie szans i zagrożeń wynikających z funkcjonowania w cyberprzestrzeni i równocześnie reagowanie na generowane w tym środowisku zagrożenia oraz przeciwdziałanie im.

Współcześnie cyberprzestrzeń jest narzędziem polityki, przestrzenią konfliktów oraz sferą realizacji interesów poszczególnych państw. Do głównych zagrożeń dla polityki bezpieczeństwa państwa w cyberprzestrzeni zalicza się m.in.: cyberterroryzm, → c y b e r s z p i e g o s t w o , → c y b e r w o j n ę , → c y b e r p r z e s t ę p c z o ś ć .

Hanna Batorowska, Katarzyna Batorowska, Agnieszka Warchoł

T.R. Aleksandrowicz, *Podstawy walki informacyjnej*, Wydawnictwo Spotkania, Warszawa 2016; tenże, *Świat w sieci. Państwa Społeczeństwa Ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego*, Difin, Warszawa 2014; *Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Biuro Bezpieczeństwa Narodowego, Warszawa 2015; J. Kulesza, *Ius internet. Między prawem a etyką*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2010; A. Kura, *Zagrożenia dla bezpieczeństwa informacyjnego państwa u progu XXI wieku*, Wydawnictwo Sztafeta, Stalowa Wola 2016; M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2015; tenże, *Znaczenie cyberprzestrzeni dla bezpieczeństwa państw na początku XXI wieku*, „Stosunki Międzynarodowe – International Relations" 2010, nr 3–4 (42); M. Marczuk, *Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru*, „Przegląd Teleinformatyczny" 2018, nr 1–2; A. Nowak, *Cyberprzestrzeń jako nowa jakość zagrożeń*, „Zeszyty Naukowe AON" 2013, nr 3 (92); P. Sienkiewicz, *Analiza systemowa zagrożeń dla bezpieczeństwa cyberprzestrzeni*, „Automatyka" 2009, t. 13, z. 2; tenże, *Ontologia cyberprzestrzeni*, „Zeszyty Naukowe WWSI" 2015, nr 13, vol. 9; J. Skrzypczak, *Polityka ochrony cyberprzestrzeni RP*, „Przegląd Strategiczny" 2014, nr 7; J. Unlod, *Zarządzanie informacją w cyberprzestrzeni*, Wydawnictwo Naukowe PWN, Warszawa 2015; A. Warchoł, *Wpływ cyberprzestrzeni na bezpieczeństwo państwa na początku XXI wieku* [rozprawa doktorska], Kraków 2017; J.A. Warden, *The Enemy as a System*, „Airpower Journal" 1995, vol. 9, no. 5; J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9; S. Wojciechowska-Filipek, Z. Ciekanowski, *Bezpieczeństwo funkcjonowania w cyberprzestrzeni. Jednostki – Organizacje – Państwa*, CeDeWu, Warszawa 2019; M. Wójcik, *Rozszerzona rzeczywistość w usługach informacyjnych bibliotek*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2018.

CYBERSTALKING – zjawisko uporczywego nękania z wykorzystaniem technologii informacyjno-komunikacyjnych (głównie internetu). Na gruncie polszczyzny nie powstała jedna obowiązująca nazwa tego zjawiska, dlatego powszechnie używa się zapożyczonego terminu angielskiego (ang. *cyberstalking*) lub – rzadziej – spolszczonej hybrydy *cybernękanie*. Angielski czasownik *stalk* oznacza tutaj ‘prześladować, śledzić’, natomiast przedrostek *cyber*odnosi się do zjawisk zachodzących w → c y b e r p r z e s t r z e n i [t. 1], w komunikacji elektronicznej lub w internecie. Można zatem stwierdzić, że cyberstalking to prześladowanie lub nękanie kogoś w cyberprzestrzeni, z wykorzystaniem komunikacji elektronicznej lub internetu. Osobę popełniającą przestępstwo cyberstalkingu nazywa się cyberstalkerem.

Internet może być wykorzystywany przez cyberstalkera jako a) źródło → i n f o r m a c j i [t. 2] (w tym – prywatnych lub ogólnodostępnych) na temat ofiary, dzięki czemu śledzenie i nękanie staje się jest bardziej efektywne oraz b) narzędzie komunikacji z ofiarą. Jarosław Groth wskazuje, że w literaturze przedmiotu wśród najczęściej spotykanych działań cyberstalkera wymienia się:

- **uporczywe przesyłanie niechcianych wiadomości** – cyberstalker wysyła do ofiary liczne e-maile, SMS-y lub wiadomości w → m e d i a c h s p o ł e c z n o ś c i o w y c h [t. 3], mające zróżnicowaną treść;
- **nękanie za pośrednictwem serwisów czatowych lub innych komunikatorów** – prześladowca może próbować wielokrotnie kontaktować się z ofiarą lub przyjąć tożsamość ofiary w takich serwisach i wysyłać wiadomości do innych użytkowników;
- **ataki na komputer (lub inne urządzenie) ofiary** – przeprowadzanie takich ataków obejmuje np. rozpowszechnianie → złośliwego o p r o g r a m o w a n i a [t. 4] w celu uszkodzenia sprzętu lub uzyskania dostępu do prywatnych informacji ofiary;
- **poszukiwanie informacji o ofierze w internecie** – cyberstalker przeszukuje zasoby internetowe (w tym – konta w serwisach społecznościowych) w celu zdobycia informacji o ofierze (np. adresu, numeru telefonu, zdjęć, danych o zatrudnieniu lub informacji
  o zainteresowaniach), które następnie może wykorzystać do nękania;
- **publikowanie informacji na temat ofiary w internecie** – prześladowca może udostępniać w internecie zdjęcia, korespondencję lub inne treści na temat ofiary bez jej zgody, rozpowszechniać nieprawdziwe informacje o ofierze lub publikować jej zmodyfikowane lub kompromitujące zdjęcia czy obraźliwe komentarze na temat ofiary, zwłaszcza w mediach społecznościowych;
- **zamawianie towarów lub usług w imieniu ofiary** – prześladowca kupuje na koszt ofiary towary lub usługi – często są to produkty mające wywołać u ofiary emocje (np. zamówienie na nazwisko ofiary subskrypcji czasopism pornograficznych);
- **kradzież tożsamości** – stalker może podszywać się pod ofiarę, przejmować jej tożsamość w celu np. nawiązywania kontaktów z innymi osobami lub zamawiania produktów;

- **prowokowanie innych osób do dręczenia ofiary** – prześladowca może skłaniać innych użytkowników internetu do dręczenie swojej ofiary poprzez m.in. tworzenie fałszywych profili ofiary w serwisach randkowych lub pornograficznych i umieszczanie na nich danych kontaktowych do ofiary, umieszczanie kontrowersyjnych wpisów na czatach, grupach dyskusyjnych lub w mediach społecznościowych w imieniu ofiary, które mają skłonić innych użytkowników do wszczęcia dyskusji.

W literaturze przedmiotu są dostępne liczne typologie prześladowców. Stalkerów (w tym także cyberstalkerów) można podzielić na (według P. Mullen i in.):

1) osoby odrzucone (ang. *rejected stalker*) przez ofiarę – ten typ prześladowcy miał bliski związek z ofiarą (np. związek romantyczny lub przyjacielski) i nie akceptuje zakończenia danej relacji. Działania stalkerów odrzuconych charakteryzują się jednocześnie chęcią zemsty oraz pojednania z ofiarą;
2) osoby poszukujące intymności lub związku z ofiarą (ang. *intimacy seekers*) – prześladowca próbuje nawiązać relację ze swoją ofiarą, a swoje działania tłumaczy głównie tym, że ofiara odwzajemnia uczucia;
3) osoby naruszające normy społeczne (ang. *incompetent suitors*) – prześladowca próbuje nawiązać kontakt z ofiarą (np. umówić się na spotkanie) lub stworzyć związek, ale podczas tych prób narusza akceptowalne społecznie normy zachowania (np. nie akceptuje odpowiedzi „nie" uzyskanej od ofiary);
4) osoby urażone lub rozgoryczone (ang. *resentful stalkers*) – ten typ stalkera nęka ofiarę z intencją wywołania u niej emocji, głównie strachu, z powodu zemsty za rzeczywistą lub domniemaną krzywdę lub upokorzenie;
5) tzw. drapieżnicy (ang. *predatory stalkers*) – stalker zbiera informacje o ofierze lub ją śledzi w celu przeprowadzenia rzeczywistego ataku (np. na tle seksualnym).

W innej typologii stalkerów wyróżnić można:

1) typ erotomana albo erotomanki (ang. *the erotomaniac / the erotomanic*) – prześladowca ma urojenia o charakterze seksualnym i fałszywe przekonanie, że ofiara jest osobą mu przeznaczoną;
2) typ obsesyjnie zakochany (ang. *the love obsessional*) – prześladowca często zna ofiarę osobiście i przejawia obsesję na jej punkcie;
3) typ z tendencjami do obsesji (ang. *the simple obsessional*) – stalker najczęściej zna ofiarę lub jest albo był z nią w związku i prześladuje ofiarę w kontekście tej relacji.

Cyberstalkerów można także przyporządkować do jednej z grup, które wydzielili Leroy McFarlane i Paul Bocij:

1) cyberstalkerzy mściwi (ang. *vindictive cyberstalkers*) – charakteryzujący się dużą intensywnością kontaktów ze swoimi ofiarami, dążący do wywołania negatywnych odczuć u ofiary (głównie strachu) poprzez m.in. przesyłanie niepokojących zdjęć (np. czaszek lub zwłok), infekowanie urządzeń ofiary złośliwym oprogramowaniem, prowadzenie obraźliwych dyskusji;

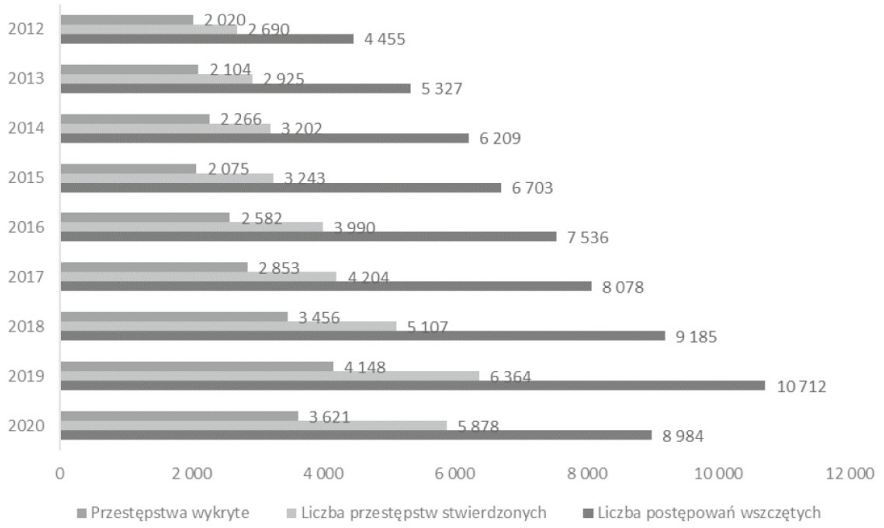
2) cyberstalkerzy opanowani (ang. *composed cyberstalkers*) – prześladowcy mający na celu wyłącznie rozdrażnienie lub zirytowanie ofiary, a nie – nawiązanie z nią relacji;
3) cyberstalkerzy romantyczni (ang. *intimate cyberstalkers*) – prześladowcy próbujący zdobyć uczucia ofiary lub zwrócić jej uwagę,np. byli partnerzy lub znajomi ofiary oraz osoby aktualnie „zakochane" w ofierze, chcące nawiązać z nią romantyczne relacje;
4) cyberstalkerzy zbiorowi (ang. *collective cyberstalkers*) – kilku cyberstalkerów połączonych w grupę i wspólnie prześladujących ofiarę: konkretną osobę lub nawet organizację czy firmę.

Wyniki badań nad stalkingiem wskazują, że prześladowcami są najczęściej mężczyźni (głównie byli partnerzy lub znajomi ofiar, rzadziej –osoby powiązane z ofiarą kontaktami zawodowymi lub osoby obce dla ofiary). Stalkerzy często przejawiają zaburzenia urojeniowe i zaburzenia osobowości, cechują się niskim poziomem empatii oraz trudnościami w nawiązywaniu relacji interpersonalnych. Większość ofiar to kobiety. Nękania często doświadczają także osoby publiczne oraz osoby, których praca jest związana z kontaktem z ludźmi (np. nauczyciele lub lekarze). Działania prześladowcy wywołują u ofiary liczne negatywne skutki, m.in. odczuwanie niepokoju i strachu, skrępowania i wstydu, bezsilności, osamotnienia, mogą pojawić się poczucie izolacji społecznej oraz dolegliwości zdrowotne (fizyczne i psychiczne). Ofiary nękania doświadczają skutków psychologicznych porównywalnych z objawami zespołu stresu pourazowego. Cyberstalking jest rodzajem → p r z e m o c y [t. 3] psychicznej. Nie wszystkie ofiary zgłaszają organom ścigania, że doświadczyły nękania. Wśród sposobów radzenia sobie z prześladowaniem można wskazać m.in. bezpośrednią konfrontację z prześladowcą (np. polegającą na próbach nawiązania rozmowy lub grożeniu sprawcy), unikanie prześladowcy i niereagowanie na jego działania, wzmacnianie pewności siebie (np. udział w psychoterapii, zajęciach samoobrony, stosowanie technik relaksacyjnych) lub szukanie pomocy na zewnątrz. Uporczywe nękanie jest jednak przestępstwem i powinno zostać zgłoszone policji.

W polskim kodeksie karnym regulacje dotyczące zjawiska stalkingu (w tym – jego odmiany, czyli cyberstalkingu) dodano w 2011 r. Artykuł 190a kk wprowadza definicję stalkingu oraz kradzieży tożsamości. Zgodnie z art. 190a § 1. kk „Kto przez uporczywe nękanie innej osoby lub osoby jej najbliższej wzbudza u niej uzasadnione okolicznościami poczucie → z a g r o ż e n i a [t. 4], poniżenia lub udręczenia lub istotnie narusza jej prywatność, podlega karze pozbawienia wolności od 6 miesięcy do lat 8". Zatem stalking zdefiniowano w kk jako „uporczywe nękanie". W § 2 art. 190a wskazano natomiast definicję kradzieży tożsamości, która może być traktowana jako odrębne przestępstwo lub jeden ze sposobów nękania. Zgodnie z art. 190a § 2: „Tej samej karze podlega, kto, podszywając się pod inną osobę, wykorzystuje jej wizerunek, inne jej dane osobowe lub inne dane, za pomocą których jest ona publicznie identyfikowana, w celu wyrządzenia jej szkody majątkowej lub osobistej". W przypadku, gdy efektem

uporczywego nękania lub podszywania się pod inną osobę jesttargnięcie się pokrzywdzonego na własne życie, kara dla sprawcy wynosi od 2 do 12 lat pozbawienia wolności (art. 190a kk § 3). Ściganie przestępstwa określonego w § 1 (uporczywe nękanie) lub w § 2 (podszywanie się pod inną osobę) następuje na wniosek pokrzywdzonego (art. 190a kk § 4). Należy zwrócić uwagę na to, że w kk nie określono metody działania sprawcy w zakresie nękania lub podszywania się, zatem uznaje się, że art. 190a kk penalizuje zarówno działania realizowane w świecie rzeczywistym (stalking), jak i w wirtualnym (cyberstalking). Uporczywe nękanie i podszywanie się pod inną osobę należą do grupy przestępstw przeciwko wolności. Według statystyk dostępnych na stronie Policji w 2020 r. liczba postępowań wszczętych z art. 190a kk wyniosła 8984, liczba przestępstw stwierdzonych – 5878, a liczba przestępstw wykrytych – 3621.

Wykres 1. Postępowania wszczęte i przestępstwa stwierdzone z art. 190a kk za lata2012–2020



Źródło: Policja, *Statystyka – Kodeks karny, przestępstwa przeciwko wolności (189–193), Uporczywe nękanie i wykorzystanie wizerunku (art. 190a)*, https://statystyka.policja. pl/st/kodeks-karny/przestepstwa-przeciwko-4/76586,Uporczywe-nekanie-i-wykorzystanie-wizerunku-art-190a.html (dostęp 08.11.2021).

W razie doświadczenia zjawiska cyberstalkingu zaleca się:

1) gromadzenie dowodów – należy zarejestrować, zapisać i przechowywać wiadomości otrzymywane od prześladowcy;
2) wyrażenie sprzeciwu – jeśli jest to możliwe, to należy wyrazić sprzeciw wobec działań stalkera oraz zażądać ich zaprzestania oraz udokumentować sprzeciw (np. zapisać wiadomość przesłaną do stalkera);

3) kontrolowanie emocji – ofiara nie powinna podejmować żadnych rozmów, dyskusji i kłótni z prześladowcą;
4) sprawdzenie wykorzystywanych urządzeń (np. komputera) – ze względu na to, że stalker mógł zainstalować na urządzeniu ofiarynp. oprogramowanie szpiegujące;
5) poinformowanie bliskiej osoby o sytuacji – wsparcie osób bliskich jest istotne dla m.in. zwiększenia poczucia → b e z p i e c z e ń s t w a[t. 1] ofiary;
6) zawiadomienie organów ścigania – ofiara powinna złożyć zawiadomienie na najbliższym komisariacie policji o uporczywym nękaniu. Przeciwdziałanie zjawiskom stalkingu i cyberstalkingu (oraz ogólnie → c y b e r p r z e m o c y [t. 1]) obejmuje głównie działania edukacyjne. Umiejętności rozpoznania i szybkiego zareagowania na cybernękanie sąniezbędne do skutecznego zakończenia prześladowania.

Paulina Motylińska

M. Cyrklaff-Gorczyca, *Cyberstalking jako forma przemocy z wykorzystaniem technologii informacyjno-komunikacyjnych*, [w:] *Ekologia informacji a zasoby informacyjne w bibliotekach i cyberprzestrzeni*, K. Materska, B. Taraszkiewicz (red.), Stowarzyszenie Bibliotekarzy Polskich, Słupsk 2017; K. Gorazdowski, *Penalizacja zjawisk stalkingu, cyberstalkingu i mowy nienawiści – próba oceny przyjętych rozwiązań prawnych na płaszczyźnie prawnokarnej*, „Studia Administracji i Bezpieczeństwa" 2017, nr 3(3); J. Groth, *Cyberstalking – perspektywa psychologiczna*, „Forum Oświatowe" 2010, nr 2(43); P. Kaur et al., *A Systematic Literature Review on Cyberstalking. An Analysis of Past Achievements and Future Promises*, „Technological Forecasting and Social Change" 2021, vol. 163; L. McFarlane, P. Bocij, *An Exploration of Predatory Behaviour in Cyberspace: Towards a Typology of Cyberstalkers*, „First Monday – Journal on The Internet" 2003, vol. 8, iss. 9; P. Mullen i in., *Study of Stalkers*, „The American Journal of Psychiatry" 1999, vol. 156, iss. 8; E. Short i in., *The Impact of Cyberstalking*, „Studies in Media and Communication" 2015, vol. 3, iss. 27; D. Siemieniecka, M. Skibińska, K. Majewska, *Cyberagresja – zjawisko, skutki, zapobieganie*, Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika, Toruń 2020; Ustawa z dnia 6 czerwca 1997 r. Kodeks karny, Dz.U. 1997, nr 88, poz. 553 z późn. zm.

CYBERSZPIEGOSTWO – aktywność ofensywna w sieci aktorów państwowych i niepaństwowych, które obejmuje kopiowanie bez zgody → i n f o r m a c j i [t. 2] tajnych, poufnych, zapisanych w systemach informatycznych lub przesyłanych w → c y b e r p r z e s t r z e n i . Najczęściej celem jest zdobycie informacji takich jak plany przemysłowe, projekty technologiczne, tajemnice wojskowe, korespondencja dyplomatyczna oraz informacje cenne ze względów ekonomicznych. Jest to najbardziej uniwersalne ujęcie tego terminu, warto jednak odnotować, że choć większość podmiotów państwowych dzieli w swym prawie wymienione znamiona tego działania, to w szczegółowym ujęciu różnią się znacznie: np. *U.S. Cyber Operations Policy* określa cyberszpiegostwo jako:

> operacje i powiązane z nimi programy lub działania prowadzone […] w cyberprzestrzeni lub za jej pośrednictwem, głównie w celu gromadzenia danych wywiadowczych […] z komputerów, systemów łączności bądź informacji, z zamiarem pozostania niewykrytym.

W Wielkiej Brytanii z kolei w *National Cyber Security Strategy 2016–2021* definiuje się ją jako „wykorzystanie sieci komputerowej do infiltracji określonej sieci komputerowej i gromadzenie danych wywiadowczych".

Utrzymanie → b e z p i e c z e ń s t w a n a r o d o w e g o jest jednym z najważniejszych celów każdego podmiotu państwowego, a zdobywanie informacji (ciągłe bądź jednorazowe) dotyczące podmiotów zagranicznych, potencjalnych adwersarzy, jest jednym z wielu środków, które pozwalają na rzeczywiste uzyskanie przewagi politycznej, ekonomicznej, technologicznej – w przypadku cyberszpiegostwa inna jest tylko płaszczyzna działań. Przykład wzorowego cyklu wywiadowczego, stosowanego przez Wspólnotę Wywiadowczą (Intelligence Community – federacja 16 agencji wywiadowczych w USA) składa się z 5 etapów, są to: 1) planowanie i kierowanie; 2) zbiór; 3) analiza i przetwarzanie; 4) produkcja;

5) rozpowszechnianie. Można to podzielić na 2 podstawowe kategorie: gromadzenie i analizę – te 2 etapy odróżniają informację od danych wywiadowczych. Informacje zebrane stają się informacjami wywiadowczymi dopiero po ich przeanalizowaniu.

Informacje pozyskane przez → w y w i a d [t. 4] można podzielić na 2 rodzaje ze względu na ich źródło:

- osobowe (ang. *human intelligence*, HUMINT),
- uzyskane poprzez przechwytywanie sygnałów elektronicznych (ang. *signals intelligence*, SIGINT).

Ponadto wywiad klasyfikuje je jako zamknięte lub otwarte. HUMINT przez prawie cały XX w. był głównym źródłem pozyskiwania informacji wywiadowczych – w miarę rozwoju ochrony poufnych informacji przez podmioty państwowe oraz wzrostu nakładów na instytucje kontrwywiadowcze dostęp do źródeł osobowych stawał się coraz trudniejszy. Ponadto problemem była niewiarygodność i jakość pozyskiwanych informacji – źródła osobowe często działały jako tzw. podwójni agenci, którzy celowo podawali fałszywe informacje, duże znaczenie mają także zwykłe nieporozumienia i przekazywanie niedokładnych informacji. W miarę postępu cywilizacyjnego dużej wagi nabrały metody typu SIGINT, które umożliwiają bezpośredni dostęp do informacji, minimalizując możliwość celowego lub przypadkowego wprowadzenia w błąd. W SIGINT można wyróżnić 2 subdyscypliny:

- wywiad komunikacyjny (ang. *communications intelligence*, COMMINT), który ma na celu przejęcie z zagranicy komunikacji radiowej, przewodowej czy z użyciem innych środków elektromagnetycznych, czyli upraszczając, zbiór sygnałów elektronicznych, które obejmują mowę lub tekst;
- wywiad elektroniczny (ang. *electronic intelligence*, ELINT), którego celem jest zbieranie sygnałów elektronicznych z zagranicy, niezwiązanych z komunikacją osobistą, w czym zawiera się zbiór emitujących promieniowanie elektromagnetyczne, z wykluczeniem źródła detonacji atomowej.

Wraz z rozwojem technologii telekomunikacyjnej powstają kolejne, nowe subdyscypliny SIGINT-u, jak np. rozpoznanie obrazowe (ang. *imagery intelligence*, IMINT), czyli analiza na podstawie danych zgromadzonych za pomocą fotografii wizualnej, podczerwieni, laserów, czujników wielospektralnych i radaru. Od czasu, gdy dominacja w cyberprzestrzeni zyskała na znaczeniu, spowodowała ukształtowanie się kolejnej subdyscypliny – CYINT (ang. *cyber intelligence*), której celem jest pozyskiwanie informacji z cyberprzestrzeni.

Klasyfikacja źródeł na otwarte i zamknięte zależy od poziomu dostępności informacji – otwarte źródło jest terminem opisującym informacje publicznie dostępne, zawarte m.in. w oficjalnych przemówieniach, doniesieniach prasowych, technicznych, profesjonalnych czasopismach naukowych, internetowych bazach danych. U podmiotów państwowych, które funkcjonują na zasadzie liberalnej demokracji, dopiero dążenie do osiągnięcia uzasadnionego celu zwalnia państwo z obowiązku upubliczniania tego typu informacji, nadając im status → i n f o r m a c j i n i e j a w n y c h [t. 2]. W związku z tym aktorzy państwowi podejmują próby pozyskania tego typu informacji (określanych jako zamknięte) od innych aktorów, co jest potocznie określane szpiegostwem – aspektem wysiłków służb wywiadowczych, w którego skład wchodzą wysiłki rządu mające na celu uzyskanie informacji niejawnych lub chronionych – publicznie niedostępnych.

Ważnym elementem podanej definicji cyberszpiegostwa, wymagającym szczegółowego wyjaśnienia, jest zagadnienie kopiowania – trzeba podkreślić, że tego typu działanie nie wpływa na takie czynniki bezpieczeństwa informacji jak dostępność czy integralność danych oraz sieci i systemy, w których dane się znajdują. Natomiast operacja, której skutkiem jest zakłócenie funkcjonowania komputera, systemu komputerowego, sieci i pokrewnej infrastruktury sieciowej, dokonania zmiany, usunięcia, uszkodzenia lub wejścia w posiadanie danych albo oprogramowania, jest definiowana jako → c y b e r a t a k. W takim wypadku stosowane są inne przepisy prawa międzynarodowego. Jednakże nie rozstrzyga to ostatecznie pytania o relację między tymi pojęciami. Cel, jakim jest uzyskanie informacji wywiadowczych o przeciwniku, zakłada przenikanie do systemów, ich monitorowanie czy kradzież informacji, więc muszą być to działania prowadzone w taki sposób, aby pozostały niewidoczne – bez zmiany danych czy naruszenia sposobu działania systemów, co jest cechą charakterystyczną cyberszpiegostwa.

Należy rozróżnić akty cyberszpiegostwa ze względu na dostęp fizyczny, bezpośredni oraz zdalny. W sytuacji bezpośredniej dostęp odbywa się poprzez lokalną instalację sprzętu lub poprzez jego ukrytą funkcjonalność wprowadzoną w pobliżu komputera albo docelowo do systemu, sieci oprogramowania. Praktycznym przykładem może być działanie → a g e n t a w y w i a d u , który uzyskuje dostęp do pomieszczenia z elementem infrastruktury sieciowej i pobiera informacje z sieci, dysku twardego komputera do pamięci przenośnej. Cyberszpiegostwo zdalne sprowadza się do

przeprowadzania operacji, które są uruchamiane z pewnej odległości od komputera, sieci, infrastruktury docelowej, zazwyczaj po uzyskaniu dostępu przez internet. Jako przykłady takiego działania można podać bezpośrednie włamanie do sieci i systemów komputerowych, manipulację za pomocą → p h i s h i n g u [t. 3] w celu uzyskania hasła i nieautoryzowanego wejścia do sieci, rozpowszechnianie → z ł o ś l i w e g o o p r o g r a m o w a n i a [t. 4] w celu zlokalizowania podatności w systemie operacyjnym i utworzenie tzw. backdoora. Cyberszpiegostwo zdalne, z racji swojego fenomenu, ma priorytetowe znaczenie dla aktualnej analizy prawnej z perspektywy prawa międzynarodowego z 2 powodów: po pierwsze z uwagi na niski poziom trudności i kosztów przeprowadzenia tego typu operacji, współcześnie jest to wiodąca metoda gromadzenia danych; po drugie prawo międzynarodowe jest systemem opartym na terytorium, ustawodawcy regulowali prawo na podstawie jurysdykcji fizycznych granic państw, co implikuje pytania i wątpliwości dotyczące wykładni prawa w aspekcie cyberszpiegostwa i samej cyberprzestrzeni.

Pierwszy znany przypadek cyberszpiegostwa jest datowany na 1986 r., była to działalność prowadzona przez niemieckiego → h a k e r a [t. 2] M. Hessa, który został zwerbowany przez KGB. Hess naruszył integralność systemów komputerowych Lawrence Berkeley National Laboratory. Ostatecznie, dzięki wsparciu FBI, został złapany dzięki metodzie tzw. *honeypot*. Działalność związaną z cyberszpiegostwem prowadzą także podmioty pozapaństwowe, odnosi się to do zjawiska szpiegostwa gospodarczego. Odnotować należy zmiany, które zaszły od lat 80. XX w.: obecnie nie ma już hakerów działających w pojedynkę, haking stał się elementem wysoko wyspecjalizowanej gry, w której przeciwnikiem są instytucje, w ramach realizacji swoich → s t r a t e g i i [t. 4] → c y b e r b e z p i e c z e ń s t w a dysponujące szeregiem zabezpieczeń na poziomie systemowym oraz zespołami wyszkolonych specjalistów. Obecnie hakerzy łączą się w swoiste → c y b e r g r u p y, działają zarówno na rzecz stałego zleceniodawcy, jak i na własną rękę, kierują się celami ideologicznymi czy chęcią zysku.

Ze względu na cel ataku można wyszczególnić 2 rodzaje ataków, jakie przeprowadzają hakerzy. Pierwszy jest swoistym, możliwie najszerzej przeprowadzanym skanowaniem sieci, ukierunkowanym na znalezienie systemów z lukami bezpieczeństwa. W tego typu działaniach często wykorzystuje się złośliwe oprogramowanie, które automatyzuje ten proces, wyszukując sieci i systemy wg ich podatności na atak. Drugi typ uderza w czynnik ludzki, są to najczęściej działania phishingowe. Cyberataki na sektor rządowy i militarny, z racji ich wysokiego poziomu zabezpieczeń, są stosunkowo wysublimowane i precyzyjne, w literaturze określa się je jako APT (ang. *advanced persistent threat*, zaawansowane trwałe zagrożenie).

Cyberszpiegostwo może zostać uznane za nowy sposób prowadzenia → w o j n y [t. 4], lecz nie każdy jego przypadek jest równoznaczny z → c y b e r w o j n ą. D. Ventre zwraca uwagę, że chociaż akty cyberszpiegostwa są znacznie bardziej powszechne niż akty cyberwojny, to tej ostatniej nie można traktować tylko jako częstszych czy

bardziej rozbudowanych aktów cyberszpiegostwa, tak samo jak pojęcia wojny tradycyjnej i konwencjonalnego szpiegostwa nie są tożsame.

W swoich publikacjach T. Rid stawia tezę, że cyberszpiegostwo nie jest aktem wojny ani przestępstwem, a jedynie przeniesieniem działań wywiadowczych do cyberprzestrzeni, determinowanym stale rosnącym poziomem informatyzacji państw i społeczeństw. Dotychczas odnotowane czy ujawnione cyberataki kwalifikuje on m.in. właśnie jako akty cyberszpiegostwa (obok cybersabotażu i działalności wywrotowej). Pod względem wymaganego poziomu technicznego zaawansowania lokuje on cyberszpiegostwo pomiędzy akcjami sabotażowymi – jako reprezentującymi poziom najwyższy – a działalnością wywrotową na najniższym poziomie. Podobnie ocenia społeczne zaangażowanie towarzyszące każdej z tych form cyberataków – w odniesieniu do cyberszpiegostwa jest ono mniejsze niż w przypadku działalności wywrotowej, lecz większe niż w odniesieniu do sabotażu.

Powszechnie traktowane w czasie pokoju jako przestępstwo, w czasie konfliktu zbrojnego szpiegostwo jako gromadzenie informacji o wrogu staje się akceptowaną i niezbędną częścią każdej kampanii wojskowej. Jak wynika z art. 24 IV konwencji haskiej dotyczącej praw i zwyczajów wojny lądowej z 1907 r., „stosowanie środków niezbędnych do uzyskania informacji o wrogu uważa się za dozwolone". W przypadku prowadzenia działań w cyberprzestrzeni ustalenie granicy między zgodnym z prawem gromadzeniem informacji a szpiegostwem, skutkującym utratą statusu członka sił zbrojnych, jest jeszcze trudniejsze niż w odniesieniu do wojny tradycyjnej.

Pomimo wspomnianych rozbieżności interpretacyjnych w literaturze jako przykłady akcji cyberszpiegowskich wymieniane są Titan Rain, GhostNet, Shady RAT czy operacja Aurora.

Wojciech Cendrowski

R. Buchan, C*yber Espionage and International Law*, Hart Publishing, Oxford 2019; J. Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld*, O'Reilly, Newton 2010; W. Cendrowski, *Cyberszpiegostwo*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; tenże, *Cyberwojna i jej znaczenie dla bezpieczeństwa NATO w kontekście przypadków i dokumentów strategicznych*, [w:] *Walka informacyjna. Uwarunkowania – Incydenty – Wyzwania*, H. Batorowska (red.), Uniwersytet Pedagogiczny im. KEN w Krakowie, Kraków 2017; J. Green, *Introduction*, [w:] *Cyber Warfare: A Multidisciplinary Analysis*, J. Green (ed.), Routledge, London– New York 2015; Konwencja haska o prawach i zwyczajach wojny lądowej, Dz. U. 1927, nr 21, poz. 161; P. Shakarian, J. Shakarian, A. Ruef, *Introduction to Cyber-Warfare: A Multidisciplinary Approach*, Elsevier, Waltham 2013; T. Rid, *Cyber War Will Not Take Place*, „Journal of Strategic Studies" 2012, vol. 35, no. 1; D. Ventre, *Cyberconflict: Stakes of Power*, [w:] *Cyberwar and Information Warfare*, D. Ventre (ed.), Wiley, London–New York 2011.

CYBERTERRORYZM (ang. *cyberterrorism*) – metoda walki politycznej, która łączy klasyczny → t e r r o r y z m [t. 4] z → c y b e r a t a k a m i, mającymi realizować cele polityczne.

Termin powstał z połączenia 2 pojęć – → c y b e r p r z e s t r z e n i i terroryzmu. Wspólną cechą terroryzmu i cyberterroryzmu jest użycie → p r z e m o c y [t. 3] (lub groźba jej użycia) przeciw → l u d n o ś c i c y w i l n e j [t. 3]. Po raz pierwszy pojęciem posłużył się w 1997 r. B. Collin, pracownik Institute for Security and Intelligence w Kalifornii. Określił on cyberterroryzm jako przejście terroryzmu ze świata realnego do wirtualnego i jako „świadome wykorzystanie systemu teleinformatycznego, sieci komputerowej lub jej części składowych w celu wsparcia bądź też ułatwienia przeprowadzenia akcji terrorystycznej".

W 1979 r. w szwedzkim raporcie dotyczącym → z a g r o ż e ń [t. 4] komputerowych cyberterroryzmem została określona aktywność związana z komputerami i prowadząca do zniszczenia systemów teleinformatycznych, nadzoru i kontroli, a także programów, danych i in. w celu zastraszenia rządów i społeczeństw, wywarcia na nich psychologicznej presji. W literaturze przedmiotu występuje wiele definicji cyberterroryzmu.

Jedną z najczęściej cytowanych jest definicja D.E. Denning z Uniwersytetu Georgetown:

> cyberterroryzm to połączenie terroryzmu i cyberprzestrzeni. Potocznie rozumie się, że są to bezprawne ataki i groźby ataku na komputery, sieci i informacje tam zgromadzone w celu zastraszenia lub zmuszenia rządu lub jego ludzi do realizacji celów politycznych lub społecznych. Ponadto, aby atak zakwalifikować jako cyberterroryzm, powinien skutkować przemocą wobec osób, mienia lub spowodować strach.

Narodowe Centrum Ochrony Infrastruktury USA zdefiniowało cyberterroryzm jako:

> atak kryminalny, popełniony przy użyciu komputera oraz sieci telekomunikacyjnych, powodujący użycie siły, zniszczenie bądź też przerwanie usług w celu wywołania poczucia strachu, poprzez wytworzenie zamieszania i wywołania niepewności w określonej części populacji, w celu wpływania na rządy oraz ludność w sposób mogący wykorzystać ich reakcje dla osiągnięcia z góry określonych celów politycznych, społecznych, ideologicznych bądź też głoszonego przez terrorystów programu.

V.A. Vasenin i O.V. Kazarin definiują „akt cyberterroryzmu" jako czyn popełniony za pomocą komputerów i innych środków komunikacji, który może powodować zagrożenie dla ludzkiego zdrowia i życia, przyczynić się do niszczenia obiektów materialnych, wywoływać negatywne konsekwencje dla społeczeństwa lub mieć na celu zwrócenie uwagi na polityczne żądania terrorystów. Autorzy wskazują, że aby zakwalifikować dany atak jako cyberterrorystyczny, należy wziąć pod uwagę jego charakter, skutki i intencje sprawcy.

J. Lewis za cyberterroryzm uznaje wykorzystanie sieci komputerowych jako narzędzi do sparaliżowania lub poważnego ograniczenia możliwości efektywnego wykorzystania struktur narodowych, np. energetyki, transportu, instytucji rządowych, bądź do zastraszenia czy wymuszenia na rządzie lub populacji określonych działań.

M. Pollitt, agent specjalny FBI, cyberterroryzmem nazwał

> zorganizowany z premedytacją, z przyczyn politycznych, atak na informacyjne systemy komputerowe, programy komputerowe i dane. Jego wynikiem jest przemoc grup lub tajnych agentów wobec niewalczących celów.

Zjawisko cyberterroryzmu może występować na wielu wirtualnych płaszczyznach, np.: danych osobowych, regulacji prawnych narodowych i międzynarodowych, → b e z p i e c z e ń s t w a t e l e i n f o r m a t y c z n e g o , technologii teleinformacyjnej i teleinformatycznej, → b e z p i e c z e ń s t w a osobowego.

Zdaniem R. Kołodziejczyka cyberterroryzm to:

> wykorzystywanie cyberprzestrzeni w działaniach terrorystycznych. Narzędziem do wykonywania aktów terroru jest sieć komputerowa, a celem związane z infrastrukturą krytyczną państw zasoby, do których należą m.in.: energia, woda oraz transport, telekomunikacja, bankowość i finanse. Przejęcie kontroli nad tymi zasobami, które sterowane są za pomocą komputerów i internetu, powoduje chaos i panikę oraz brak stabilizacji w działaniach państwa.

Terroryści często wykorzystują metody działania oparte na nowoczesnych technologiach, gdyż generują one niższe koszty, a także mogą być używane na odległość, co pozwala uniknąć bezpośredniego kontaktu z przeciwnikiem oraz np. z materiałami wybuchowymi. Internet zapewnia terrorystom dostęp do → i n f o r m a c j i [t. 2] i predyspozycji w zakresie nowych technik i metod działania. Tabela 1 przedstawia przykładowe metody działania, które są wykorzystywane do ataków cyberterrorystycznych. Rozwój nowoczesnych technologii oraz powszechna informatyzacja życia społecznego mają wpływ na ciągłe rozszerzanie katalogu.

Tab. 1. Metody ataków cyberterrorystycznych

Metoda ataku	**Cel działania, rodzaje ataków**
Komputerowe wirusy, robaki i bakterie	Wirus to samoreprodukujący się kod, który uszkadza programy lub dane, zmieniając sposób działania zainfekowanego sprzętu. Robak (ang. *worm*) to rodzaj samoreplikującego się wirusa komputerowego, który nie zmienia zawartości plików, ale rozmnaża się w pamięci komputera. Cel działania robaka jest taki sam jak w przypadku wirusa – niszczenie danych i komputerów. Różnica polega na tym, że robak nie potrzebuje programu nosiciela, gdyż rozmnaża się samoistnie, zazwyczaj jako załącznik do poczty elektronicznej lub poprzez obecność na stronach internetowych, np. pornograficznych lub z nielegalnym oprogramowaniem. Bakteria to program, który wprost nie powoduje uszkodzenia plików, ale blokuje możliwość korzystania z nich przez użytkownika. Celem bakterii jest rozmnażanie się. Bakterie reprodukują się wykładniczo i zajmują dużą część pamięci procesora, dysku i innych zasobów.

Koń trojański	Rodzaj → z ł o ś l i w e g o o p r o g r a m o w a n i a [t. 4] dołączany jako tajny element funkcjonalnych programów i narzędzi komputerowych. Może on wykonywać niepożądane działanie, nieprzewidziane przez użytkownika programu, np. usuwanie plików, formatowanie dysku, przesyłanie danych do swojego twórcy bez zgody i wiedzy użytkownika. Trojana od wirusa odróżnia to, że ten pierwszy jest częścią funkcjonalnego programu, natomiast drugi z wymienionych zastępuje go całkowicie. Ukryty kod umożliwia atakującemu przejęcie kontroli nad zainfekowanym komputerem i dostanie się za jego pośrednictwem do sieci.
Złośliwe podzespoły (ang. *chipping*)	To działanie polega na umieszczeniu w komputerach chipów, które zawierają programy dające dostęp do systemów lub tworzenie wad konstrukcyjnych umożliwiających zniszczenie sprzętu komputerowego.
„Tylne drzwi" (ang. *backdoor*)	Celowo umieszczony przez programistę fragment kodu, który pozwala mu na dostęp do komputera lub systemu informatycznego bez znajomości loginu lub hasła użytkownika.
Podszywanie się (ang. IP *spoofing*)	Działanie polega na podszyciu się przez atakującego pod użytkownika systemu, który ma własny adres IP, poprzez sfałszowanie źródłowego adresu IP w pakiecie przesyłanym drogą internetową. Aby osiągnąć prawo dostępu do zasobów, podszywający może dokonać np. modyfikacji pakietów w trakcie połączenia. Metoda ta używana jest w trakcie ataków DDoS.
Przechwycenie transmisji (ang. *hijacking)*	Przechwycenie transmisji pomiędzy dwoma komputerami lub systemami umożliwiające dostęp do chronionych informacji lub programów. Najbardziej znana odmiana IP spoofingu.
Podsłuchiwanie (ang. *sniffing*)	Jedna z metod penetracji systemów komputerowych. Przechwytywanie pakietów danych przesyłanych w sieci TCP/IP, m.in. tych nieadresowanych do komputera, na którym działa przestępca. Za pomocą tej metody można przechwycić wszystkie hasła, które nie są przekazywane zakodowanym kanałem. Atak tego typu jest bardzo trudny do wykrycia, gdyż nie wprowadza zmian w sieci. *Sniffing* występuje najczęściej w sieciach lokalnych LAN. Włamywacz, chcąc przeprowadzić proces przechwytywania pakietów, musi jedynie uruchomić program sniffujący.
Phishing	Polega na tworzeniu fałszywych wiadomości e-mail i witryn WWW, które wyglądają identycznie jak serwisy internetowe znanych firm, aby skłonić klientów tych firm do podania swoich danych osobowych, numeru karty kredytowej lub informacji o elektronicznym rachunku bankowym – kodów i haseł potrzebnych do zalogowania i autoryzacji transakcji. Jednym z najbardziej spektakularnych ataków typu → p h i s h i n g [t. 3] była operacja Aurora przeprowadzona w 2009 r. wobec Google, konkretnie jej celem były konta pocztowe osób zaangażowanych w obronę → p r a w c z ł o w i e k a [t. 3]. Amerykanie podejrzewają, że za atakiem stoi rząd Chińskiej Republiki Ludowej, a koncern Google zapowiedział, że zerwie z Chinami umowę co do cenzurowania (→ c e n z u r a) w tym kraju wyników wyszukiwania.

Pharming	Odmiana *phishingu*. Przestępcy wykorzystują dodatkowo serwer DNS w celu ukrycia prawdziwego adresu IP spreparowanej strony internetowej.
Receptor van Eycka (ang. *electromagnetic radiation*, EMR)	Atakujący, który dysponuje odpowiednim sprzętem, może oglądać na swoim monitorze repliki obrazów wyświetlanych na ekranie atakowanego urządzenia.
DoS (ang. *denialof service*) DDoS (ang. *distributed denial of service*)	Działania mające na celu zablokowanie konkretnego serwisu sieciowego lub zawieszenie urządzenia poprzez przesłanie licznych żądań, zapytań, pakietu danych z różnych źródeł, znacznie przewyższających ilość, którą ów serwis można obsłużyć. Ataki mogą doprowadzić do awarii sieci teleinformatycznej lub teleinformacyjnej. DoS różni się od DDoS tym, że drugi z wymienionych najczęściej poprzedzony jest penetracją przez atakującego wielu komputerów i zmienieniem ich w tzw. zombie. W ten sposób atak na jeden cel następuje z wielu źródeł jednocześnie.
Broń częstotliwości radiowej (ang.*electromagnetic pulse*, EMP)	Celowe użycie energii elektromagnetycznej o dużej mocy. Urządzenie emitujące promieniowanie elektromagnetyczne należące do widma radiowego stosowane w celu zniszczenia technicznych urządzeń elektronicznych orazzbiorów informatycznych.
Zalewanie (ang. *flooding)*	Atak, którego celem jest zablokowanie usług danego serwera poprzez wysłanie do serwera dużej ilości pakietów. Jest to również jeden ze sposobów ataku DoS, a także technika blokowania serwerów IRC polegająca na przesyłaniu do określonego kanału dużej ilości tekstu, co powoduje trudności w prowadzeniu konwersacji między użytkownikami kanału.
Spam	Anonimowa, nieoczekiwana, masowo rozsyłana wiadomość tekstowa. Spam może przeciążyć sieci dostawców usług sieciowych, serwery pocztowe oraz komputery użytkowników. Powoduje blokadę miejsca na dyskach twardych, przeciążenia serwerów, wyłudzanie danych, zainfekowanie urządzeń złośliwym oprogramowaniem, emisję materiałów niepożądanych przez użytkownika itp.
Bomby logiczne (ang. *logic bomb*)	Ich działanie polega na aktywizacji nowych funkcji elementów logicznych urządzenia, co prowadzi do zniszczenia lub uszkodzenia sprzętu i oprogramowania. W odróżnieniu od konia trojańskiego nie uruchamia złośliwego oprogramowania od razu, ale w określonym czasie, np. po uruchomieniu określonej aplikacji lub po zajściu danego zdarzenia.

Źródło: oprac. aut.

Jedną z najbardziej niebezpiecznych metod działania cyberterrorystów jest tzw. *swarming attack.* Tego typu atak polega na spiętrzeniu oraz nałożeniu się na siebie ataków przeciwko → i n f r a s t r u k t u r z e k r y t y c z n e j [t. 2] państwa w cyberprzestrzeni oraz w świecie fizycznym, tj. przeciwko jej materialnym nośnikom. H. Schmidt wskazuje, że cyberprzestrzeń stworzyła zależności, które permanentnie

zmieniają swoją naturę w sposób nieprzewidywalny, a tym, czego należy się najbardziej obawiać odnośnie do ataków fizycznych, aktów kryminalnych i kataklizmów naturalnych, jest właśnie *swarming attack*.

Sprawcami cyberataków mogą być → h a k e r z y [t. 2], crackerzy, aktywiści, wandale, szpiedzy, działacze ruchów narodowowyzwoleńczych, sfrustrowani pracownicy, podmioty gospodarcze, resorty siłowe państwa oraz terroryści.

Tabela 2 zawiera przykłady korzyści działania w sieci organizacji terrorystycznych.

Tab. 2. Powody, które skłaniają terrorystów do ataków w cyberprzestrzeni

Powód terrorystycznego ataku w cyberprzestrzeni	**Wpływ ataku terrorystycznego w cyberprzestrzenina bezpieczeństwo informacyjne**
Niskie koszty przeprowadzenia ataku	Cyberterrorystą może zostać niemal każdy. Potrzebne narzędzia: komputer, odpowiedni program, wiedza i umiejętności (które za sprawą specjalnych forów internetowych można szybko przyswoić).
Transnarodowy charakter	Trudno zidentyfikować atakującego. Cyberterroryzm wykracza poza granice państw. Cyberterroryści z różnych stron świata, dzięki dostępowi do sieci internet, mogą działać wspólnie.
Przewidywanie zagrożeń ataków	Nie wiadomo, które zagrożenie jest realne, a które pozorne.
Cel ataku	Nie wiadomo, co jest dokładnym celem ataku ani w jaki sposób będzie on przeprowadzony, by ten cel zrealizować.
Budowa koalicji	Nie wiadomo, kto jest sprzymierzeńcem, a kto nieprzyjacielem.

Źródło: oprac. aut.

Podobnie jak inne pojęcia z przedrostkiem cyber-, cyberterroryzm nie ma jednej, powszechnie akceptowanej definicji. Ich wielość prowadzi do problemów interpretacyjnych, a o *definiens* terminu spierają się naukowcy z całego świata. Podstawowy problem związany z brakiem jednolitości przy definiowaniu zjawiska wpływa na to, że nie możemy jednoznacznie określić, czy świat miał lub ma obecnie do czynienia z cyberterroryzmem czy jest to na razie element futurologii.

Agnieszka Warchoł

J.T. Caruso, *Combating Terrorism: Protecting the United States*, 21.02.2002, FBI.gov (dostęp 21.02.2019); D.E. Denning, *Cyberterrorism*, CS.Georgetown.edu (dostęp 25.02.2019); taż, *Wojna informacyjna i bezpieczeństwo informacji*, tłum. J. Bloch, Wydawnictwa Naukowo-Techniczne, Warszawa 2002; R. Kołodziejczyk, *Nowa odsłona terroryzmu – cyberterroryzm*, „Rocznik Bezpieczeństwa Międzynarodowego" 2017, vol. 11, nr 2; E. Lichocki, *Cyberterroryzm*

państwowy i niepaństwowy – początki, skutki i formy, [w:] *Ewolucja terroryzmu na przełomie XX i XXI wieku*, M.J. Malinowski, R. Ożarowski, W. Grabowski (red.), Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2009; A. Podraza, *Cyberterroryzm jako wzrastające zagrożenie dla bezpieczeństwa międzynarodowego w XXI wieku*, [w:] *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna*, A. Podraza, P. Potakowski, K. Wiak (red.), Difin, Warszawa 2013; D. Verton, *Black Ice. Niewidzialna groźba cyberterroryzmu*, tłum. K. Masłowski, Helion, Gliwice 2004; A. Warchoł, *Cyberterroryzm*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; taż, *Terroryści w sieci*, [w:] *Współczesne aspekty bezpieczeństwa państwa*, A. Piędel, J. Pomiankiewicz, A. Żebrowski (red.), Wyższa Szkoła Bezpieczeństwa i Ochrony im. Marszałka Józefa Piłsudskiego, Nisko 2016; taż, *Zagrożenia dla bezpieczeństwa informacyjnego państwa u progu XXI wieku*, Wydawnictwo Sztafeta, Stalowa Wola 2016.

CYBERWOJNA (ang. *cyberwar*) – konfrontacja w → c y b e r p r z e s t r z e n i , w tym konfrontacja komputerowa w internecie, jedna z odmian → w o j n y i n f o r m a c y j n e j [t. 4]. Ma na celu destabilizację systemów komputerowych i dostępu do internetu przez agencje rządowe, centra finansowe i biznesowe oraz tworzenie nieporządku i chaosu w życiu państw. Stosunki międzypaństwowe i konfrontacja polityczna często znajdują kontynuację w internecie w postaci cyberwojny i jej elementów: wandalizmu, → p r o p a g a n d y [t. 3], szpiegostwa, bezpośrednich ataków na systemy komputerowe i serwery itd.

Cyberwojna jest terminem budzącym duże naukowe zainteresowanie, o czym świadczy znaczna liczba publikacji, w których podejmowano próby zgłębienia jego istoty, co utrudnia jednak przedstawienie definicji. Właściwie każdy badacz w inny sposób próbuje określić, co jest istotą cyberwojny, często nie podejmują oni trudu określenia systemowej definicji, lecz tłumaczą zjawisko poprzez podanie przykładów, znaczenia oraz liczby cyberataków, ewentualnie wskazują na brak terminologicznego konsensusu i powszechnie akceptowanej definicji.

B. Schneier, specjalista ds. → c y b e r b e z p i e c z e ń s t w a, uważa, że w wielu przypadkach definicja cyberobrony nie jest dobrze stosowana, ponieważ nie wiadomo jeszcze, jak wygląda → w o j n a [t. 4] w cyberprzestrzeni, gdzie wybuchnie cyberwojna oraz w jaki sposób cyberprzestrzeń będzie się rozwijała podczas wojny. Według G. Sandroni cyberwojna jest kształtowana zgodnie z charakterystyką cyberprzestrzeni, jej głównymi aktorami są państwa i charakteryzuje ją motywacja polityczna. Można ją również zdefiniować jako zestaw działań przeprowadzanych w celu wprowadzenia zmian w → i n f o r m a c j a c h [t. 2] i systemach wroga, jednocześnie chroniąc informacje przed systemami atakującego. R. Clarke, specjalista ds. bezpieczeństwa w rządzie USA, definiuje cyberwojnę jako zbiór działań podjętych przez państwo, aby przeniknąć do komputerów lub sieci w innym kraju w celu spowodowania szkód lub zmian.

Definicje, które mają wartość merytoryczną, można podzielić na 2 grupy. Pierwsza koncentruje się na określeniu wskaźników zjawiska cyberwojny (np. R. Stiennon

wyróżnił 4 filary istotne dla cyberwojny: inteligencję, technologię, logistykę, dowództwo), druga grupa opiera formułowanie teorii na aspekcie powiązania cyberprzestrzeni, wojny i cyberataku (np. S. Winterferd i J. Andress). Tego typu ujęcie, choć nie jest wyczerpujące, wnosi wartościowe uwagi, wskazuje np. brak wypowiedzenia cyberwojny w międzynarodowych stosunkach politycznych, ewentualne zgłaszanie incydentów cyberbezpieczeństwa na arenie międzynarodowej, jak w przypadku cyberataku na Estonię w 2007 r. czy podczas konfliktu zbrojnego w Gruzji w 2008 r., co w sposób znaczący dewaluuje poziom incydentu do kategorii cyberprzestępstwa.

Zasadniczym problemem związanym z rozumieniem istoty cyberwojny pozostaje trudność wskazania granic analizowanego zjawiska. F.-B. Huyghe podkreśla, że w prawdziwym znaczeniu cyberwojna pozbawiona jest realnego miejsca, gdyż nie można z całą pewnością nadać jej określonej lokalizacji. Zrozumienie cyberwojny utrudnia istnienie podwójnej granicy:

- ontologicznej: czy to naprawdę wojna? jakie są granice między tą kategorią a innymi, takimi jak → p r z e s t ę p c z o ś ć [t. 3], konflikt, → a g r e s j a, sabotaż itp.?
- topologicznej: wojna ma miejsce i odbywa się w zasadzie na terytorium takiego lub innego państwa, w jaki sposób można transponować lub zreinterpretować pojęcie wojny do epoki cyfrowej? Podkreślić należy, że nigdy nie było cyberwojny z jawnym otwarciem i zamknięciem działań wojennych, powiązaniem → s t r a t e g i i [t. 4] własnej i strategii przeciwnika, odwrotu i ofensywy, śmierci, terytoriów okupowanych, zawieszenia broni i pokoju, rozbrojenia itp. Ta odmienność działań w cyberprzestrzeni sprawia, że cyberwojna wg części badaczy nie kwalifikuje się do miana wojny. T. Rid w artykule *Cyber War Will Not Take Place*, a następnie w książce pod tym samym tytułem stawia tezę, że konflikt, w którym brak ofiar w ludziach, nie sformułowano jasnego celu i nie da się udowodnić politycznych motywacji atakujących, nie może być określany jako wojna. Kluczową przeszkodą dla zrozumienia istoty cyberwojny, jej rzeczywistego stanu i potencjalnych implikacji jest brak niezbędnego interdyscyplinarnego spojrzenia, które posłużyłoby do analizy problemu o najbardziej złożonym charakterze. Trudności te trafnie określił J.A. Green, wskazując, że prawnicy nie mają pojęcia o technologii, której uwarunkowania powinni regulować, stratedzy nie zwracają uwagi na szerzej rozumiane kwestie etyczne i prawne, informatycy zaś koncentrują się na technicznych uwarunkowaniach cyberagresji bez głębszej analizy implikacji politycznych czy strategicznych.

Za szczególnie cenną i mogącą stanowić punkt dalszych dyskusji i odniesień uznać można definicję cyberwojny zaproponowaną przez P. Shakariana, J. Shakarian i A. Ruefa. Wskazują oni, że cyberwojna jest rozszerzeniem polityki na działania podejmowane w cyberprzestrzeni przez podmioty państwowe (lub przez podmioty niepaństwowe o znacznym ukierunkowaniu lub wsparciu państwa), które stanowią poważne

→ z a g r o ż e n i e [t. 4] dla → b e z p i e c z e ń s t w a innego państwa, lub działanie o takim samym charakterze podejmowane w odpowiedzi na poważne zagrożenie dla bezpieczeństwa państwa (rzeczywiste lub postrzegane).

Analiza relacji zachodzących między podmiotami uczestniczącymi w cyberatakach jest istotna odnośnie do postrzegania zjawiska cyberwojny i stanowi możliwość określenia jej cech charakterystycznych. Na ich podstawie wyróżniono modele 4 dominujących form cyberataków, aktualnie stosowane w symulacjach teoretycznych gier, pozwalające na stworzenie obrazu dynamiki aktorów „cyberareny politycznej", są to:

- wojna → m e d i ó w s p o ł e c z n o ś c i o w y c h [t. 3], ukierunkowana na wywołanie niepokojów i rozłamów w społeczeństwie, ma wpłynąć na wewnętrzną sytuację polityczną danego państwa;
- wojna strategiczna, którą można zdefiniować jako akt fizycznego niszczenia, grabieży danych, a także nabywanie i rozwijanie umiejętności ofensywnych i defensywnych w celu przeprowadzenia ataku na →i n f r a s t r u k t u r ę k r y t y c z n ą [t. 2] aktorów państwowych;
- → b i t w a ideologiczna, polegająca na wykorzystaniu cyberprzestrzeni przez organizacje radykalne czy fundamentalistyczne do popularyzowania swoich ideologii i rekrutowania nowych członków;
- wojna inicjowana przez obywateli, w której ramach ataki osób cywilnych na inne osoby cywilne w danym państwie oraz na instytucje innego państwa są częścią konfliktu o większym wymiarze ideologicznym lub kinetycznym.

Kolejnym problemem, oprócz definicyjnego, jest odróżnienie cyberwojny od innych zagrożeń występujących w cyberprzestrzeni, takich jak → c y b e r t e r r o r y z m , → c y b e r p r z e s t ę p c z o ś ć , → c y b e r s z p i e g o s t w o .

Brak aktów prawa międzynarodowego znajdujących zastosowanie bezpośrednio do cyberwojny nie oznacza jednak, że działania w cyberprzestrzeni nie wywołują żadnych prawnych konsekwencji lub że nie mogą być oceniane z perspektywy prawa. Niektórzy autorzy nie traktują braku regulacji prawnej jako mankamentu obecnej sytuacji, wskazując, że wystarczające są obecnie obowiązujące umowy międzynarodowe.

S. Shackleford wymienia kilka dokumentów użytecznych do prawnej oceny cyberataków: Układ o nierozprzestrzenianiu broni jądrowej, Układ Antarktyczny, międzynarodowe prawo kosmiczne, Konwencję Narodów Zjednoczonych o prawie morza, międzypaństwowe układy o wzajemnej pomocy prawnej (MALT lub MLAT).

Próba udzielenia kompleksowej odpowiedzi na pytania, jakie rodzi prawna kwalifikacja cyberwojen, została podjęta przez ekspertów z NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE), międzynarodową instytucję badawczą stworzoną przez państwa → NAT O [t. 3] w celu badania zagrożeń cyberprzestrzeni (nie jest to oficjalna placówka należąca do NATO – ma ona charakter naukowo-szkoleniowy). Efektem ich prac jest dwukrotnie już wydawany *Tallinn Manual on the International Law Applicable to Cyber Operations*. Książka nie odzwierciedla oficjalnej doktryny

NATO, jest jednak czymś więcej niż próbą odniesienia zasad wyrażonych w umowach międzynarodowych do cyberwojny, zawiera szerokie odwołania do orzecznictwa.

Najczęściej prawne implikacje cyberwojny analizowane są na płaszczyznach *ius ad bellum*, *ius in bellum*, prawa do → n e u t r a l n o ś c i [t. 3] czy prawa do samoobrony. Odpowiadając na pytanie o prawną kwalifikację cyberwojny, wskazuje się na możliwość stosowania do cyberwojny regulacji prawnych odnoszących się do → m i ę d z y n a r o d o w e g o p r a w a h u m a i t a r n e g o k o n f l i k t ó w z b r o j n y c h [t. 3], → p r a w c z ł o w i e k a [t. 3], umów międzynarodowych składających się na prawo dyplomatyczne i konsularne, prawa morskiego, prawa lotniczego, prawa przestrzeni kosmicznej, międzynarodowego prawa telekomunikacyjnego, w drodze analogii czy też przy zastosowaniu wykładni dynamicznej. Innym rozwiązaniem problemu braku regulacji jest odwołanie się do zwyczaju międzynarodowego, przy czym wątpliwości w literaturze budzi to, czy w odniesieniu do cyberwojny ukształtowały się już takie zwyczaje, które można byłoby uznać za źródło norm. Z jednej strony podkreśla się niewielką ilość ujawnianych informacji dotyczących praktyki przyjmowanej przez państwa w odniesieniu do przypadków cyberataków i informacji o reakcjach na nie, z drugiej jednak liczba rozmaitych dokumentów dotyczących szeroko rozumianego cyberbezpieczeństwa stale rośnie, co daje podstawy, by oczekiwać, że w niedalekiej przyszłości będzie można mówić o ukształtowaniu się takich norm zwyczajowych.

Odrębnym zagadnieniem jest problem prawnej kwalifikacji działań podejmowanych w cyberprzestrzeni przez podmioty niebędące państwami, ponieważ co do zasady nie stosuje się do nich umów międzynarodowych. Przyjmuje się, że operacje w cyberprzestrzeni, jeśli są przeprowadzane przez podmioty niepaństwowe, a nie naruszają → s u w e r e n n o ś c i p a ń s t w a [t. 4] zaatakowanego, nie stanowią realizacji prawa do interwencji ani prawa do użycia siły, ponieważ te dotyczyć mogą tylko państw, niezależnie od potencjalnych następstw cyberataków. Jeśli cyberataku nie można w sposób jednoznaczny przypisać państwu, nie można stosować działań odwetowych na warunkach i zasadach dotyczących państw. Państwo zaatakowane może natomiast skorzystać z prawa do samoobrony, może postawić państwu, z którego terytorium przeprowadzono cyberatak, zarzut niezachowania należytej staranności w nadzorze nad infrastrukturą cybernetyczną znajdującą się na jego terenie. Wątpliwości budzi status osób biorących udział w cyberatakach i możliwość stosowania względem nich regulacji → m i ę d z y n a r o d o w e g o p r a w a h u m a n i t a r n e g o [t. 3].

Cyberwojna, mimo etymologii pojęcia sugerującej ścisły związek z wojną, istotnie różni się od wojny tradycyjnej. Środki służące do prowadzenia ataku w cyberprzestrzeni cechują się znacznie większą różnorodnością niż broń konwencjonalna, nie pozostawiają trwałych śladów materialnych, a dane cyfrowe stosunkowo łatwo jest sfałszować czy odpowiednio zmodyfikować, by utrudnić lub uniemożliwić identyfikację atakującego. Dlatego też jednym z najbardziej istotnych zagadnień dotyczących

cyberataków jest ustalenie podmiotów odpowiedzialnych za nie, co zwykle wyznacza dalszy tok postępowania i ma decydujące znaczenie dla podjęcia działań odwetowych w cyberprzestrzeni lub poza nią. Prowadzenie cyberwojny nie wymusza konieczności tworzenia organizacji zdolnej do zorganizowania ataku – może go bowiem przeprowadzić zarówno pojedynczy człowiek, jak i niesformalizowana grupa. Ponieważ sztuką staje się ukrywanie tożsamości w cyberprzestrzeni, rację bytu straciły, tak istotne w tradycyjnej wojskowości, sposoby uzewnętrzniania przynależności do organizacji militarnej. W przypadku cyberwojny zawodzi tradycyjne rozumienie pojęć takich jak wróg, strony zaangażowane w wojnę i neutralne czy zwycięstwo. Ustalone przez prawo międzynarodowe formy prowadzenia działań odwetowych, negocjacji, zawarcia pokoju czy poddania się są niemożliwe do zastosowania. Prymarnym celem cyberwojny nie jest fizyczne unicestwienie przeciwnika. W porównaniu z wojną tradycyjną cyberwojna charakteryzuje się bardziej zróżnicowaną plejadą potencjalnych uczestników, przy czym stale wzrasta znaczenie aktorów niepaństwowych.

Wojciech Cendrowski

J. Carr, *Inside Cyber Warfare. Mapping the Cyber Underworld*, O'Reilly, Newton 2010; W. Cendrowski, *Cyberwojna*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; tenże, *Cyberwojna i jej znaczenie dla bezpieczeństwa NATO w kontekście przypadków i dokumentów strategicznych*, [w:] *Walka informacyjna. Uwarunkowania – Incydenty – Wyzwania*, H. Batorowska (red.), Uniwersytet Pedagogiczny im. KEN w Krakowie, Kraków 2017; S. Goel, Y. Hong, *Cyber War Games: Strategic Jostling Among Traditional Adversaries*, [w:] *Cyber-Warfare: Building the Scientific Foundation*, S. Jajodia (ed.), Springer, London 2015; J. Green, *Introduction*, [w:] *Cyber Warfare: A Multidisciplinary Analysis*, J. Green (ed.), Routledge, London–New York 2015; F. Huyghe, *Cyberwar and its Borders*, [w:] *Cyberwar and Information Warfare*, D. Ventre (ed.), Wiley, London–New York 2011; P. Parks, *Cyberwarfare*, Reference Point Press, San Diego 2013; P. Shakarian, J. Shakarian, A. Ruef, *Introduction to Cyber-Warfare: A Multidisciplinary Approach*, Elsevier, Waltham 2013; M. Roscini, *Cyber Operations and the Use of Force in International Law*, Oxford University Press, Oxford, 2014; R. Stiennon, *Surviving Cyberwar*, Government Institutes, Lanham–Toronto–Plymouth 2010; S. Winterfeld, J. Andress, *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice*, Elsevier, Waltham 2013.

CYBERWOJSKA – rodzaje lub specjalistyczne komponenty sił zbrojnych odpowiedzialne za zapewnienie → b e z p i e c z e ń s t w a [t. 1] podmiotu (państwowego) w → c y b e r p r z e s t r z e n i [t. 1], a także prowadzące operacje wojskowe w domenie cybernetycznej. Cyberwojska to wysoko wykwalifikowane grupy ekspertów z zakresu nowoczesnych technologii, czyli „cyberwojownicy", którzy posiadają rozległą wiedzę na temat → c y b e r b e z p i e c z e ń s t w a [t. 1], są w stanie bronić wojskowej i strategicznej rządowej → i n f r a s t r u k t u r y k r y t y c z n e j [t. 2] oraz mogą przeprowadzać ataki cybernetyczne. To cyfrowe jednostki wojskowe, których → ż o ł n i e r z e [t. 4] i dowódcy są wyposażeni w najnowsze narzędziai techniki, w tym technologie informacyjne.

Działalność cyberwojsk może przybierać formę defensywną, która zapewnia, że wojskowe sieci komputerowe są zabezpieczone i nie są zagrożone ze strony wewnętrznej lub zewnętrznej. Można wyodrębnić także formę ofensywną, która obejmuje przeprowadzanie ataków cybernetycznych z wykorzystaniem broni cybernetycznej przeciwko przeciwnikom w celu zniszczenia, wykorzystania, uszkodzenia infrastruktury przeciwnika lub zebrania → i n f o r m a c j i [t. 2] dla celów wywiadowczych. Podobnie jak tradycyjna walka operacje wojskowe w cyberprzestrzeni wymagają inteligencji, planowania i przywództwa zaangażowanych ludzi.

Wojsko, podobnie jak inne sektory funkcjonowania państwa, jest obecnie zależne od systemów informatycznych. Zmiany w siłach zbrojnych państw spowodowane informatyzacją, miniaturyzacją, usieciowieniem, robotyzacją czy wirtualizacją sprowadzają się m.in. do zmniejszenia stanów liczebnych wojsk, a w zamian za to wyposażania ich w technologie informacyjne. Obserwujemy stałe unowocześnianie sił zbrojnych, co jest wynikiem rewolucji w dziedzinie wojskowości, tzw. RMA (*revolution in military affairs*).

Alexis Bautzmann stwierdził, że przejawem procesu militaryzacji internetu jest powstawanie cyberwojsk wyspecjalizowanych w walce w środowisku teleinformatycznym. Bogusław Pacek oraz Romuald Hoffmann wskazują, że „współczesne siły zbrojne zmieniają swój charakter w związku z postępem technologicznym i wejściem w tzw. erę informacyjną". Tworzenie nowego rodzaju sił zbrojnych jest dla państw procesem długotrwałym, złożonym i kosztownym. Wymaga inwestycji zarówno w ludzi, jak i nowoczesne technologie. Formowanie cyberarmii jest jednak konieczne, by zapewnić obywatelom pełne bezpieczeństwo. Współcześnie powstają nowe jednostki wojskowe żołnierzy na odległość, których zadaniem jest walka w cyberprzestrzeni. Swoje umiejętności ulepszają na cybernetycznych poligonach, posługując się wirtualną bronią i zaawansowanymi zabezpieczeniami.

Podczas szczytu → N A T O [t. 3] w Warszawie, który odbył się w dniach 8–9 lipca 2016 r., cyberprzestrzeń uznana została za „domenę operacji". Członkowie Sojuszu Północnoatlantyckiego uznali cyberprzestrzeń za obszar działań, w którym NATO musi bronić się tak samo skutecznie, jak w powietrzu, na lądzie i na morzu. Wzmocnienie cyberobrony krajowych sieci i infrastruktury zostało potraktowane jako priorytet. Zgodnie z pkt 71 Deklaracji końcowej szczytu NATO w Warszawie: „Każdy sojusznik deklaruje wywiązywanie się z obowiązku doskonalenia swojej odporności i zdolności do szybkiego i skutecznego reagowania na ataki cybernetyczne, w tym w sytuacjach hybrydowych".

Już w latach 90. XX w. John A. Warden pisał, że na każdą organizację należy patrzeć jako na strukturę składającą się z 5 wzajemnie powiązanych kręgów, tworzących jedną całość, takich jak: elity polityczne, instytucje państwowe, infrastruktura, społeczeństwo i systemy obronne. Każdy z kręgów funkcjonuje w 5 wymiarach – na morzu, lądzie, w powietrzu, przestrzeni kosmicznej i przestrzeni cybernetycznej. W modelu Wardena zostały stworzone podwaliny pod współczesne rozważania dotyczące

cyberbezpieczeństwa państwa, gdyż cyberprzestrzeń została postawiona obok innych domen: lądu, morza, powietrza i kosmosu.

Bezsprzecznie warunkiem walki zbrojnej w cyberprzestrzeni jest posiadanie sił zdolnych do jej prowadzenia. Jak wskazują Łukasz Olejnik i Artur Kurasiński:

> rywalizacja międzypaństwowa to od wielu stuleci domena wojska. Za pomocą wojsk państwa dokonują tzw. projekcji siły. Teraz te interakcje przenoszą się także do cyberprzestrzeni. Zatem cyberoperacje mogą być narzędziem projekcji siły, a państwa budują zdolności działania w cyberprzestrzeni zarówno w ramach swych jednostek cywilnych, jak i wojskowych (cyberwojska).

Współcześnie większość państw ma cyberwojska. Niekiedy są to wymogi wynikające z obowiązków związanych z członkostwem w organizacjach międzynarodowych.

Według rankingu National Cyber Power Index (NCPI), opracowanego przez zespół wywiadu ekonomicznego (The Economist Intelligence Unit, EIU) czasopisma „The Economist" we współpracy z konsorcjum Booz Allen Hamilton, który mierzy zdolności cybernetyczne z wykorzystaniem 29 wskaźników dla 30 krajów w ramach 8 celów narodowych, największą potęgą cybernetyczną wykazują się USA, Chiny i Rosja. Działania o charakterze defensywnym i ofensywnym, brane pod uwagę w ww. rankingu, są domeną m.in. cyberwojsk danych państw.

Amerykanie posiadają jedną z pierwszych na świecie oficjalnych cyberarmii. Od 21 maja 2010 r. istnieje United States Cyber Command (USCYBERCOM), która planuje, koordynuje, integruje, synchronizuje operacje prowadzone w cyberprzestrzeni, i kieruje nimi oraz ochrania wojskowe sieci informacyjne. Stany Zjednoczone są w grupie podmiotów, które za pomocą swoich wykwalifikowanych specjalistów dokonują → c y b e r a t a k ó w [t. 1] na systemy informatyczne innych państw, głównie w celach wywiadowczych. USCYBERCOM ma zdolnośćoperacyjną do → o c h r o n y i n f r a s t r u k t u r y k r y t y c z n e j [t. 5] Stanów Zjednoczonych. Niektóre z oddziałów mają przypisane swoje role wspierające, broniące lub przeprowadzające analizę zagrożeń sieciowych i planowanie strategiczne.

W 2015 r. Chiny utworzyły Siły Wsparcia Strategicznego Chińskiej Armii Ludowo-Wyzwoleńczej (ALW). Reforma miała na celu poprawę zdolności ALW do walki w konfliktach informacyjnych oraz wzmocnienie wspólnych operacji i zdolności, aby wspierać strategiczne cele Chin. Niektóre źródła wskazują, że jest to armia rozwoju technologii wojskowej i ewolucji działań wojennych skoncentrowana na wykorzystaniu zdolności kosmicznych, elektromagnetycznych i sieciowych jako kluczowych czynników umożliwiających zintegrowane operacje w wielu domenach konfliktów na lądzie, w morzu, powietrzu, kosmosie i cyberprzestrzeni. Znana jest jednostka 61398 Chińskiej Armii Ludowo-Wyzwoleńczej słynąca z → c y b e r s z p i e g o s t w a [t. 1] i → c y b e r p r z e s t ę p c z o ś c i [t. 1].

W Federacji Rosyjskiej w strukturach państwowych – siłach zbrojnych i → s ł u ż b a c h s p e c j a l n y c h [t. 4] – znajdują się rozbudowane jednostki do działań

w cyberprzestrzeni. W Rosji istnieje również szeroko rozwinięte podziemie cyberprzestępców wspierające Kreml w operacjach prowadzonych w cyberprzestrzeni. Na terenie Federacji Rosyjskiej od dawna działa już kilka instytucji, których zadaniem jest monitorowanie cyberataków z zewnątrz, m.in.: „biuro K" należące do Ministerstwa Spraw Wewnętrznych, Centrum Bezpieczeństwa Informacji, które podlega Federalnej Służbie Bezpieczeństwa, oraz Kolegium Federalnej Łączności i Informacji, które zajmuje się przeprowadzaniem operacji w cyberprzestrzeni. Pierwsze informacje o utworzeniu rosyjskiej cyberjednostki powiązanej z resortem obrony pojawiły się w 2013 r. Kilka lat temu w mediach ukazały się informacje o tym, że Federacja Rosyjska nie ma oficjalnej cyberarmii, ale Ministerstwo Obrony zamierza do 2017 r. utworzyć odpowiednią strukturę do ochrony sił zbrojnych w cyberprzestrzeni. Te informacje były dementowane przez rosyjskie władze. Okazało się jednak, że doniesienia medialne opierały się na prawdziwych danych, bo na początku 2017 r. Rosjanie utworzyli oddziały informacyjne w sektorze obronnym. Wojskowi podkreślają, że ich celem jest ochrona →interesów narodowych [t. 2] i →walka informacyjna [t. 4]. Oddziały mają prowadzić szeroko pojęte działania informacyjne, w tym zwalczać zachodnią →propagandę [t. 3] oraz chronić systemy teleinformatyczne. Będą one zarówno realizować zadania w wymiarze defensywnym, jak i przeprowadzać ofensywne operacje w cyberprzestrzeni.

Aktorzy niepaństwowi są nierzadko także klasyfikowani jako cyberarmie. Są oni wynajmowani przez rządy, wojsko lub sektor prywatny i otrzymują za takie działania wynagrodzenie finansowe. Istnieją również cyberwojska ochotników, a za przykład może posłużyć powołana w Estonii Liga Obrony Cybernetycznej (LOC). Ta cyberarmia składa się z oddziału ochotników, którymi są głównie specjaliści z zakresu bezpieczeństwa cybernetycznego, ale także wszyscy ci, którzy chcą się przyczynić do zwiększenia →bezpieczeństwa w sieci [t. 1], w tym prawnicy, ekonomiści, studenci. Zapewnienie cyberbezpieczeństwa ma być realizowane przez współpracę między członkami LOC, rozpowszechnianie wiedzy na temat →bezpieczeństwa informacyjnego [t. 1] oraz udział w międzynarodowych szkoleniach w zakresie cyberbezpieczeństwa. Cyberarmię powołała do życia ochotnicza Estońska Liga Obrony (Eesti Kaitseliit), która wspiera państwowe siły zbrojne. Celem organizacji jest ochrona estońskiej cyberprzestrzeni, a pokłosiem jej utworzenia były cyberataki na Estonię w 2007 r.

W Polsce funkcjonują Wojska Obrony Cyberprzestrzeni – specjalistyczny komponent →Sił Zbrojnych Rzeczypospolitej Polskiej [t. 4] powołany 8 lutego 2022 r. o godz. 11.00 podczas uroczystości w Klubie Wojskowej Akademii Technicznej (WAT) w Warszawie, z udziałem ministra obrony narodowej Mariusza Błaszczaka. Formalnie Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni funkcjonuje na mocy Ustawy z dnia 11 marca 2022 r. o obronie Ojczyzny, która weszła w życie 23 kwietnia 2022 r. Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni

(DKWOC) powstało na bazie Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni i jednostek bezpośrednio podporządkowanych. Wojska Obrony Cyberprzestrzeni są właściwe do realizacji pełnego zakresu działań w cyberprzestrzeni, szczególnie w ramach proaktywnej ochrony oraz aktywnej obrony elementów i zasobów cyberprzestrzeni kluczowych z punktu widzenia Sił Zbrojnych Rzeczypospolitej Polskiej. Dowódcą został gen. bryg. Karol Molenda.

Agnieszka Warchoł

M. Aschmann, J.J. van Vuuren, L. Leenen, *Cyber Armies: The Unseen Military in the Grid*, International Conference on Cyber Warfare and Security 2015, https:// www.proquest.com/openview/dad1bd4d21a8d5ca7f9f3704a78b6d4b/1?pq-origsite= gscholar&cbl=396500 (dostęp 10.05.2023); Deklaracja końcowa szczytu NATO w Warszawie, wydana przez szefów państw i rządów uczestniczących w posiedzeniu Rady Północnoatlantyckiej w Warszawie w dniach 8 i 9 lipca 2016 r., „Bezpieczeństwo Narodowe" 2016, nr 37–40, https://www.bbn.gov.pl/ftp/dok/03/37-40_ KBN_Deklaracja_szczytu.pdf (dostęp 6.05.2023); P. Dela, *Elementy systemu walki w cyberprzestrzeni*, „Bellona" 2020, t. 702, nr 3, https://kwartalnikbellona.com/api/ files/view/1540923.pdf (dostęp 5.05.2023); K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Wydawnictwo Adam Marszałek, Toruń 2008; K. Liedel, P. Piasecka, *Wojna cybernetyczna – wyzwanie XXI wieku*, „Bezpieczeństwo Narodowe" 2011, nr 17; G. Masters, *No secret anymore: Russia touts cyber force*, https://www.scmagazineuk.com/no-secretanymore-russia-touts-cyber-force/article/640288/ (dostęp 15.05.2023); T. Minárik, *NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit*, https:// ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/(dostęp 5.05.2023); A. Ni, B. Gill, *The People's Liberation Army Strategic Support Force: Update 2019*, 29.05.2019, https://jamestown. org/program/the-peoples-liberation-army-strategic-support-force-update-2019/ (dostęp 5.05.2023); Ł. Olejnik, A. Kurasiński, *Filozofia cyberbezpieczeństwa*, Wydawnictwo Naukowe PWN, Warszawa 2022; B. Pacek, R. Hoffmann, *Działania sił zbrojnych w cyberprzestrzeni*, Akademia Obrony Narodowej, Warszawa 2013; *Russia Creates a Cyber Army*, https://www.youtube.com/watch?v=bgkr8nmooo8 (dostęp 15.05.2023); *The Estonian Defence League's Cyber Unit*, https://www.kaitseliit.ee/en/ cyber-unit (dostęp 12.05.2023); *U.S. Cyber Command*, http://www.arcyber.army.mil/org-uscc.html (dostęp 16.05.2023); Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny, Dz.U. 2022, poz. 655.

CYBERZAGROŻENIA – zakłócenie pracy systemów kontroli sieci komputerowej oraz systemów operacyjnych komputerów przez osoby, które podejmują próby nieautoryzowanego dostępu do urządzenia i/lub sieci systemu sterowania, przy użyciu ścieżki transmisji danych.

Uzyskanie dostępu może być przeprowadzone z wewnętrznych struktur organizacji, przez zaufanych użytkowników lub przez nieznane podmioty, pojedyncze osoby, grupy, warunkiem jest posiadanie eksperckiej wiedzy z zakresu → b e z p i e c z e ń s t w a . Źródła cyberzagrożeń są zróżnicowane, można m.in. wymienić wrogie rządy podmiotów państwowych, grupy terrorystyczne, niezadowolonych pracowników itp. W celu ochrony przed tego typu → z a g r o ż e n i a m i [t. 4] konieczne jest stworzenie odpowiedniego systemu bezpieczeństwa, polityki bezpieczeństwa, procedur, które w adekwatny sposób zabezpieczałyby systemy teleinformatyczne w danej instytucji.

Względnie dobry podział cyberzagrożeń oddaje propozycja ich kategoryzacji w protokole dla Wspólnego Komitetu Ekonomicznego w USA, autorstwa L.K. Gershwina, oficera → w y w i a d u [t. 4] CIA, związanego z działem nauki i technologii. Wymienia on rządy państw, terrorystów, szpiegów przemysłowych, grupy → p r z e s t ę p c z o ś c i z o r g a n i z o w a n e j [t. 3], haktywistów (→ h a k t y w i z m [t. 2]), → h a k e r ó w [t. 2]. W przypadku ochrony przed cyberzagrożeniami ze strony rządów innych państw powoływane są programy walki cybernetycznej, → s t r a t e g i e [t. 4], doktryny → c y b e r b e z p i e c z e ń s t w a, w których definiuje się ważne dla państwa → i n t e r e s y n a r o d o w e [t. 2] w kontekście → c y b e r p r z e s t r z e n i, których naruszenie spowodowałoby reakcję ofensywną w wielu aspektach. Przykładem działań rządów innych państw może być np. → p r o p a g a n d a [t. 3], uciążliwe niszczenie rządowych stron internetowych, szpiegostwo czy spowodowanie poważnych zakłóceń, w następstwie których mogłoby dojść do straty życia ludzkiego i rozległych zniszczeń strukturalnych. Warto przy tym zaznaczyć, że w sferze cyberzagrożeń tylko → c y b e r a t a k i przeprowadzone przez inne podmioty państwowe mogą spowodować długotrwałe szkody w infrastrukturze, która krytycznie zagroziłaby → b e z p i e c z e ń s t w u n a r o d o w e m u zaatakowanego państwa. Wiedza ekspercka, zaplecze szkoleniowe, technologie, czas i możliwość ich wytworzenia do tej pory wciąż są ważnym czynnikiem ograniczającym wystąpienie tego typu incydentów, jednakże znaczenie cyberbezpieczeństwa wzrasta. Przewiduje się, że w ciągu 5–10 lat wszyscy aktorzy państwowi będą dysponować znacznymi środkami, które w pełni pozwolą rozwinąć zdolności do przeprowadzania cyberataków na infrastrukturę innych państw. Celem działań aktorów państwowych jest przeważnie osłabienie, zakłócenie działania infrastruktury zaatakowanego państwa. W zakres celów pobocznych wchodzą takie działania jak → c y b e r s z p i e g o s t w o, szpiegostwo oraz kradzież w zakresie rozwoju technologii, zakłócenie funkcjonowania gospodarki.

Drugorzędnym cyberzagrożeniem są terroryści, którzy – z racji bardziej ograniczonych środków niż podmioty państwowe – chcąc uniemożliwić realizację interesów narodowych danego państwa, zdecydowanie rzadziej posuwają się do wykorzystania środków ofensywnych w cyberprzestrzeni. Nie bez znaczenia pozostaje popularność wykorzystywania środków konwencjonalnych, o niższym stopniu skomplikowania, a także psychologiczny efekt fizycznych zamachów terrorystycznych. Specjaliści przewidują, że w związku z wymianą pokoleniową w szeregach terrorystów cyberzagrożenia ze strony tego typu ugrupowań wzrosną. Celem cyberterrorystów jest szerzenie terroru wśród → l u d n o ś c i c y w i l n e j oraz podważenie międzynarodowej polityki globalnej → w o j n y [t. 4] z → t e r r o r y z m e m [t. 4].

Trzecim z kolei cyberzagrożeniem jest działalność szpiegów przemysłowych oraz zorganizowanych → c y b e r g r u p. Stopień szkodliwości ich działań jest średni, motywacja działań sprowadza się do zysku finansowego poprzez działanie na zlecenie konkurencji, sprzedaż tajemnic handlowych, szantaż firm sektora prywatnego.

Poziom cyberzagrożenia, jakim są działania tzw. haktywistów, także został oceniony jako średni – można go zdefiniować jako cyberataki przeprowadzane przez cybergrupy motywowane chęcią działania politycznego. Charakter międzynarodowych cybergrup haktywistycznych jest bardziej nastawiony na działanie propagandowe, informacyjne niż zniszczenie systemów i sieci informatycznych. Celem pobocznym jest uzyskanie rozgłosu głoszonych postulatów przez dane ugrupowanie.

Za najmniejsze zagrożenie są uznawani, mimo wylansowanego przez media mitu, hakerzy działający w pojedynkę. Nie dysponują oni środkami, wyspecjalizowaną wiedzą, technologią i czasem, by przeprowadzić cyberatak, który w sposób krytyczny zagroziłby bez konsekwencji cyberbezpieczeństwu instytucji rządowej, infrastruktury rządowej oraz krytycznej. Niemniej jednak duża liczba hakerów na całym świecie specjalizujących się w określonych technologiach i środowiskach sprzętowych jest w stanie doprowadzić w krótkim czasie do znacznych szkód materialnych oraz spowodować pośrednie zagrożenie dla życia. Także pojedyncze działania hakerów mogą doprowadzić do niezamierzonego zakłócenia funkcjonowania → i n f r a s t r u k t u r y k r y t y c z n e j [t. 2].

Istnieje spór dotyczący podziału cyberzagrożeń. Opierając się na powyższych kryteriach, literatura przedmiotu wyróżnia wśród najważniejszych: haktywizm, → c y b e r p r z e s t ę p c z o ś ć , → c y b e r t e r r o r y z m, cyberszpiegostwo oraz → c y b e r w o j n ę . Z racji sporów teoretycznych co do natury określonych zjawisk w cyberprzestrzeni część autorów wymienia tylko: szpiegostwo wojskowe, polityczne, ekonomiczne, cyberprzestępczość oraz → c y b e r k o n f l i k t.

Na poziomie codziennego użytkowania internetu statystycznie najczęściej spotykanymi cyberzagrożeniami są: *malware* typu trojan, wykorzystujące → i n ż y n i e r i ę s p o ł e c z n ą [t. 2], luki bezpieczeństwa w oprogramowaniu i strukturach języków programowania (np. Acrobat Reader, Java, Flash), → p h i s h i n g [t. 3], wirusy typu *worm* oraz precyzyjne ataki typu APT (ang. *advanced persistent threat*, zaawansowane trwałe zagrożenie). Wśród innych zagrożeń można wymienić występujące pojedynczo lub w kombinacji zjawiska takie jak → b o t n e t y , → r a n s o m w a r e [t. 3], ataki typu DDoS (ang. *distributed denial od service*), ataki typu *wiper*, → k r a d z i e ż t o ż s a m o ś c i [t. 2] intelektualnej, kradzież środków pieniężnych, manipulacja danymi, niszczenie danych, rozpowszechnianie *spyware* oraz → z ł o ś l i w e g o o p r o g r a m o w a n i a [t. 4], ataki typu *man in the middle* (MITM), *drive-by downloads*, *malvertising*, rozpowszechnianie fałszywego lub niezaktualizowanego oprogramowania. Prognozy eksperckie wskazują możliwe zagrożenia dla nowych technologii takich jak *Internet of Things* (IoT) oraz dla rozwoju → b i g d a t a i algorytmów sztucznej inteligencji.

Mimo że prawie wszystkie cyberzagrożenia odnoszą się do sfery technologii informatycznych, przez co znacznej wartości nabiera wiedza i znajomość systemów, do naruszeń cyberbezpieczeństwa dochodzi najczęściej na skutek błędu ludzkiego.

Informatyzacja sfery militarnej i politycznej państw, zarówno rozwiniętych, jak i rozwijających się, brak skutecznych rozwiązań prawnych na poziomie krajowym i międzynarodowym oraz wysoki poziom skomplikowania incydentów w cyberprzestrzeni czynią cyberzagrożenia wyzwaniem dla bezpieczeństwa narodowego, a także czynnikiem, który daje możliwość oddziaływania różnym podmiotom (także niepaństwowym) na sprawy wewnętrzne państw.

Wojciech Cendrowski

R. Białoskórski, *Cyberthreats in the Security Environment of the 21st Century: Attempt of the Conceptual Analysis*, „Journal of Security & Sustainability Issues" 2012, vol. 1 (4); S. Brenner, *Cyber Threats The Emerging Fault Lines of the Nation State*, Oxford University Press, New York 2009; W. Cendrowski, *Cyberzagrożenia*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; J.I. Duffany, *Computer Security*, [w:] *Computer and Network Security Essentials*, K. Daimi (ed.), Springer, Detroit 2018; R.A. Grimes, *Hacking the Hacker: Learn from the Experts Who Take Down Hackers*, Wiley, Indianapolis 2017; B. Olszewski, *Cyberprzestrzeń w perspektywie bezpieczeństwa międzynarodowego*, [w:] *Bezpieczeństwo wielorakie perspektywy. Bezpieczeństwo z perspektywy środowisk i obszarów*, W. Horyń, N.A. Fechner (red.), Wydawnictwo Wyższej Szkoły Bezpieczeństwa w Poznaniu, Poznań 2015; M. Roscini, *Cyber Operations and the Use of Force in International Law*, Oxford University Press, Oxford, 2014; P.W. Singer, A. Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, New York 2014; B. Surmak, *Bezpieczeństwo cybernetyczne państwa*, [w:] *Trzy wymiary współczesnego bezpieczeństwa*, S. Sulowski, M. Brzeziński (red.), Dom Wydawniczy Elipsa, Warszawa 2014; A. Tarabasz, *Cybersecurity and Internet of Threats – New Challenges in Customer Behavior*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2018, nr 360.

CYBORG – organizm cybernetyczny, istota złożona z organicznych i technicznych (biomechatronicznych) części ciała. Jej procesy życiowe są wspomagane bądź realizowane przez urządzenia techniczne. Termin ten powstał przez kontaminację anglojęzycznych słów *cybernetic* (cybernetyczny) oraz *organism* (organizm). W szerszym ujęciu cyborgiem będzie każdy organizm posiadający w swoim ciele urządzenie techniczny. Oznacza to, że miano to należy się np. człowiekowi z rozrusznikiem serca lub wszczepionym kardiowerterem-defibrylatorem. Częściej więc stosowane jest ujęcie węższe, ale adekwatniej odnoszące się do terminu „cybernetyczny".

Skoro cybernetyka traktuje o systemach sterowania i przekazywania → i n f o r m a c j i [t. 2], to cyborgiem określimy taki organizm, w którym doszło do inwazyjnej ingerencji w układ nerwowy przez połączenie go z urządzeniami technicznymi, zazwyczaj elektronicznymi lub mechanicznymi. Między częściami organicznymi a technicznymi dochodzi do cybernetycznego sprzężenia zwrotnego. Techniczna ingerencja w tkankę organiczną ma na celu albo przewrócenie zdolności, która została utracona (np. wskutek choroby lub wypadku), albo wzmocnienie zdolności. To drugie podejście współgra z dążeniem do tzw. wzmocnienia człowieka (*human enhancement*), które jest jednym z nurtów w ruchu transhumanistycznym. Termin

„cyborg" został ukuty w 1960 r. przez Manfreda Clynesa i Nathana Kline'a. Został on użyty w artykule *Cyborgs and Space* opublikowanym w czasopiśmie „Astronautics", postulującym biochemiczne, fizjologiczne i elektroniczne dostosowanie człowieka do warunków panujących w przestrzeni kosmicznej. Koncepcja zespolenia człowieka (rzadziej zwierzęcia) z maszyną obecna była już wcześniej w literaturze science fiction. Postać człowieka z licznymi protezami pojawiła się w opowiadaniu Edgara Allana Poe *Człowiek, który się zużył* (*The Man That Was Used Up*) z 1843 r. Prawdopodobnie pierwszym literackim cyborgiem był Nyctalope z cyklu opowiadań francuskiego autora Jeana de la Hire'a, z których pierwsze ukazało się w 1911 r. Bohater miał sztuczne serce i wiele innych sztucznych bądź wzmocnionych organów, co dawało mu ogromne możliwości, m.in. zdolność do widzenia w ciemności. Sam cykl był prekursorski dla nurtu popkultury koncentrującego się wokół superbohaterów. Wśród innych kulturowych przedstawień cyborgów, które pojawiły się w ostatnich latach, można wymienić: Molly z powieści *Neuromancer* Williama Gibsona, replikantów z filmu *Łowca androidów*, Terminatora z cyklu filmów o tym tytule,

Dartha Vadera oraz generał Greviousa z sagi *Gwiezdne wojny*, RoboCopa z filmu o tym tytule, → ż o ł n i e r z y [t. 4] z filmu *Uniwersalny żołnierz* (kilka z tych postaci tylko częściowo odpowiada definicji cyborga, będąc biologicznie wzmocnionymi maszynami, czyli tworami z pogranicza cyborgów i androidów – humanoidalnych robotów).

Łukasz Kamieński wymienia 3 główne kierunki sztucznego wzmocnienia możliwości człowieka, które mogą być użyteczne w zastosowaniach militarnych: wspomaganie farmakologiczne (zażywanie substancji pochodzenia chemicznego i biologicznego, które oddziałują przede wszystkim na psychikę żołnierza), wspomaganie genetyczne (modyfikacje genetyczne za pomocą terapii genowych, służące poprawie zdolności i zachowania żołnierzy, a także genetyczna medycyna regeneracyjna) oraz właśnie wspomaganie cybernetyczne. W ramach tego ostatniego możemy wyróżnić następujące kierunki:

- tworzenie interfejsu mózg – maszyna, czyli wykorzystanie mózgu do bezpośredniego kontrolowania urządzeń (impuls przekazywany jest z mózgu do urządzenia);
- wzmocnienie zdolności kognitywnych przez stymulację mózgu (impuls przekazywany jest z urządzenia do mózgu), może mieć ona charakter inwazyjny i nieinwazyjny;
- wzmocnienie możliwości fizycznych żołnierza przez egzoszkielety, które w przyszłości mogą być nie tylko noszone, ale w sposób inwazyjny częściowo implantowane do układu mięśniowego i systemu nerwowego;
- budowa bionicznych protez kończyn, wykorzystujących biologiczne sterowanie sztuczną kończyną (opierają się one na wykorzystaniu czynności elektrycznej nerwów i mięśni w kikucie, elektromiograficznym wzmocnieniu tych sygnałów i używaniu ich w celu kontrolowania ruchów protezy);

- zarządzanie personelem przez chipowanie w celu lokalizacji i dowodzenia oraz monitorowania stanu psychofizycznego, a także przez technologie obrazowania mózgu użyteczne na etapie rekrutacji.

Prowadzone są również prace nad militarnym wykorzystaniem zwierząt cyborgów. →Agencja Zaawansowanych Badań i Rozwoju Departamentu Obrony USA (DARPA) [t. 5] prowadzi prace nad owadami cyborgami, które wyposażone byłyby w czujniki oraz systemy przesyłania danych wszczepione w fazie poczwarki. Program Hybrid Insect Micro-Electro-Mechanical-Systems (HI-MEMS) został zainspirowany pracami naukowców z Uniwersytetu Cornella. W 2013 r. ujawniono z kolei prowadzone eksperymenty z obiecującymi wynikami, polegające na wprowadzaniu implantów w ciało owadów, co pozwalało na zdalne sterowanie ich lotem za pomocą elektronicznego systemu przekaźnikowego zamocowanego na grzbiecie owada. Agencja DARPA opracowuje również implant neuronowy do zdalnego kontrolowania ruchu rekinów, dzięki czemu można będzie wykorzystywać ich zmysły do monitorowania ruchu jednostek pływających.

Rafał Kopeć

P. Emanuel i in., *Cyborg Soldier 2050. Human/Machine Fusion and the Implicationsfor the Future of the DOD*, U.S. Army Combat Capabilities Development Command, Chemical Biological Center, Aberdeen 2019; Ł. Kamieński, *Nowy wspaniały żołnierz. Rewolucja biotechnologiczna i wojna w XXI wieku*, Wydawnictwo UJ, Kraków 2014; K. Nørgaard, M. Linden-Vørnle, *Cyborgs, Neuroweapons, and Network Command*, „Scandinavian Journal of Military Studies" 2021, vol. 4, no. 1; H. Siljak, P.H.J. Nardelli, R.C. Moioli, *Cyborg Insects: Bug or a Feature?*, „IEEEAccess" 2022, vol. 10; E.P. Zehr, *Inventing Iron Man. The Possibility of a HumanMachine*, Johns Hopkins University Press, Baltimore 2011.

CYFROWA DEMENCJA – (ang. *digital dementia*) termin wprowadzony w 2012 r. przez Manfreda Spitzera, niemieckiego psychiatrę i neurobiologa, w celu opisania symptomów chorobowych będących skutkiem niekontrolowanego korzystania z mediów cyfrowych (głównie urządzeń z dostępem do internetu). Mowa tu o zaburzeniach funkcji poznawczych (zmniejszona uwaga, skrócony czasu zapamiętywania, zdolność koncentracji), a nawet o przyśpieszonym wystąpieniu wczesnej demencji. Warto podkreślić za badaczami z dziedziny neurobiologii, że obniżenie zdolności poznawczych jest dalece nieporównywalne z szerszą dewastacją poznawczą, jaką jest demencja, czyli utrata funkcji poznawczych oraz zdolności behawioralnych w takim stopniu, że zakłóca to codzienne życie i czynności danej osoby. Zazwyczaj objawy demencji obserwuje się u osób starszych, jednak obecnie – jak twierdzi M. Spitzer – są one coraz bardziej zauważalne u przedstawicieli pokolenia ludzi, którzy dorastali w erze wszechobecnej technologii, czyli także komputerów i internetu. Przedstawiciele tego pokolenia powszechnie nazywani są cyfrowymi tubylcami (ang. *digital natives*), czyli – jak zauważa Marc Prensky – „native speakerami" cyfrowego języka komputerów, gier wideo i internetu.

Według Spitzera bezrefleksyjne zanurzenie się w świecie mediów cyfrowych może znacząco zaszkodzić zdrowiu naszego mózgu. Ten organ, plastyczny i podatny na zmiany, kiedy pracuje, podlega stałym zmianom, natomiast gdy go nie używamy, to nie powstają w nim ślady pamięciowe, czyli nie zachodzi proces uczenia się, a przez to maleje nasz potencjał umysłowy (jeśli np. czegoś nie robimy, ponieważ używamy komputera, to w naszych mózgach nie powstają połączenia neuronalne będące skutkiem wykonywania określonych czynności). Ta cudowna zdolność naszego mózgu oznacza, że wpływ na jego strukturę ma zarówno to wszystko, co robimy, jak i to, czego nie robimy lub co robimy zbyt rzadko, a największą gotowość do zmian mózg wykazuje w dzieciństwie. Od rodzaju stymulacji, czyli od tego, co będziemy robić i czego robić nie będziemy (głównie dotyczy to dzieci i ludzi młodych), zależy, w jakim stopniu mózg rozwinie swój potencjał.

Zatem warto zwrócić uwagę na sposoby w jakich – zdaniem Spitzera – pozbywamy siebie rozumu na skutek niekontrolowanego obchodzenia się z różnymi formami mediów cyfrowych:

- Odbieramy sobie możliwość samodzielnego myślenia oraz korzystania z własnej pamięci, gdyż pozwalamy technice wyręczać nas w pracy umysłowej – np. nadużywanie funkcji „zapisz" wpływa niekorzystnie na proces zapamiętywania, gdyż – zgodnie z efektem *Zeigarnik* – lepiej pamiętamy zadanie niedokończone (mózg nie chce tej sprawy „wypuścić" i ciągle o tym myśli), stały dostęp do internetu nie ułatwia pamiętania, a jedynie – przypominanie sobie, sięganie do zewnętrznego banku pamięci (coraz częściej wiemy,gdzie daną → i n f o r m a c j ę [t. 2] znaleźć, a nie jest nam wiadome to, czego ona dotyczy), a jeżeli korzystamy z systemu nawigacji satelitarnej, osłabiamy naszą zdolność orientacji przestrzennej.
- Utrudniamy lub wręcz uniemożliwiamy głębokie przetwarzanie treści docierających do naszego mózgu – np. człowiek poznający świat za pomocą myszy komputerowej zastanawia się nad nim mniej dogłębnie niż wtedy, gdy wszystkimi zmysłami pojmuje otaczającą rzeczywistość.
- Z procesu uczenia się eliminujemy czynności manualne i motorykę. Przykładowo: poznawanie przez dziecko świata za pomocą myszy komputerowej, skutkuje spowolnieniem zdolności refleksji nad nim, gdyż ruchy ciała stają się elementem konkretnych śladów pamięciowych, wpływających na sprawność operowania w myślach wyuczonymi treściami – ręce odgrywają istotną rolę podczas nabywania wiedzy ogólnej czy też uczenia się abstrakcyjnych pojęć.
- Wpływamy na nasze zachowania społeczne. Przykładowo: portale społecznościowe oferujące podejrzanej jakości kontakty społeczne wpędzają młodych użytkowników w depresję i w samotność, a zatem w czynniki stresujące, które prowadzą do obumierania komórek nerwowych i w dłuższej perspektywie sprzyjają rozwojowi demencji, zastąpienie – głównie u dzieci – rzeczywistych kontaktów międzyludzkich portalami społecznościowymi może prowadzić na dłuższą metę do

zmniejszania się społecznych modułów w ich mózgach, reklamy promujące niezdrowy tryb życia mogą uzależnić konsumentów – głównie dzieci – od konkretnych form pożywienia bogatych w tłuszcze i węglowodany.

- Bierzemy udział w narastaniu realnej → p r z e m o c y [t. 3] w otaczającym nas świecie – m.in. brutalne gry komputerowe pozostawiają ślady pamięciowe u dzieci i młodzieży w postaci narastającej gotowości do stosowania przemocy, mniejszej wrażliwości wobec realnej → a g r e s j i [t. 1], izolacji społecznej i słabszych szans na zdobycie wykształcenia.
- Wciągamy dzieci w cyfrową narkomanię. Przykładowo: wyposażamy dzieci od najmłodszych lat w smartfony, przez co skazujemy je na możliwość uzależnienia się od nich i izolację społeczną.
- Skazujemy się na stan „trwałego częściowego rozkojarzenia uwagi"lub na stan nieustannego bycia zajętym, czyli zwracania uwagi na wszystko bez skoncentrowania się na czymkolwiek. Cyfrowo „podłączeni", skazujemy mózg na funkcjonowanie w stanie ciągłego → k r y z y s u [t. 2], podczas którego mózg nie ma czasu na refleksję, na kontemplację, na podejmowanie przemyślanych decyzji – funkcjonuje ciągle w stanie pobudzenia w oczekiwaniu na nowy kontakt lub ekscytującą informację, a to prowadzi do stresu psychicznego nazywanego technowypaleniem mózgu (ten organ w takiej sytuacji automatycznie sygnalizuje nadnerczu konieczność wydzielania kortyzolu i adrenaliny, co na dłuższą metę prowadzi do zaburzeń zdolności poznawczych, do depresji, a także zmienia sieć neuronową w hipokampie, czyli w tych obszarach mózgu, które zawiadują nastrojem i myśleniem).
- „Wyćwiczamy" zespół deficytu uwagi – nieustanne wykonywanie wielu czynności jednocześnie (tzw. wielozadaniowość) może skutkować bardziej powierzchownym przetwarzaniem różnorodnych i stale zmieniających się treści.
- Zastępujemy głęboką pracę umysłową, będącą podstawowym warunkiem procesu uczenia się, cyfrowym ślizganiem się po powierzchni: gdy klikamy na oślep i nigdy nie wracamy do rzetelnego źródła danych, szukamy informacji w sposób horyzontalny(poruszając się po powierzchni), a nie – wertykalny. Chodzi o to,żeby całość rozpoznawać przez zrozumienie szczegółów, a szczegóły – przez odwołanie się do całości.
- Osłabiamy zdolności precyzyjnego wyszukiwania danych (ang. *information retrieval*): tendencja do bardziej powierzchownego wyszukiwania danych w sieci – choć nie tylko charakterystyczna dla młodych ludzi – jest wynikiem zbyt ubogiej wiedzy na temat a) struktur informacyjnych, b) logicznych zasad łączenia danych z różnych źródeł oraz c) odróżniania rzeczy ważnych od nieistotnych.

Jeżeli chodzi o dzieci i młodzież, to – według raportu *Nastolatki 3.0* – polski nastolatek w 2020 r. wpatrywał się w ekran komputera lub smartfona ok. 12 godzin na dobę: w wolnym czasie średnio 4 godziny i 50 minut dziennie, w trakcie zdalnych lekcji średnio 7 godzin i 41 minut. Blisko co dziesiąty (11,5%) nastolatek w wolnym czasie

jest aktywny w sieci ponad 8 godzin dziennie, a co piąty (21,3%) spędza tyle czasu przed monitorem w dni wolne od lekcji. Co szósty nastolatek (16,9%) intensywnie korzystaz internetu w godzinach nocnych (po godz. 22).

Oznaki i objawy demencji cyfrowej obejmują zatem: pochyloną postawę, opóźnienia w rozwoju, utratę pamięci krótkotrwałej, odosobnienie społeczne, brak ruchu, niepokój, depresję, złość, zaburzenia równowagii nieprawidłowe wzorce ruchowe.

Problemom, jakie niosą ze sobą cyfrowe media, w tym – rozprzestrzenianiu się cyfrowej demencji, możemy jednak starać się zapobiec poprzez wcielenie odpowiednich pomysłów w życie. Oto ich lista:

- Zrozumienie mechanizmów uczenia się, zapamiętywania, uwagii rozwoju pozwoli dostrzegać → z a g r o ż e n i a [t. 4] wynikającez użytkowania nowych technologii.
- Odsunięcie w czasie pierwszego kontaktu dziecka z cyfrowymi mediami – dzieci, w przeciwieństwie do dorosłych, których mózgi są w miarę uformowane, dużo mniej plastyczne, a tym samym bardziej odporne na negatywne skutki uboczne ze strony nowych technologii, uczą się bardzo szybko, więc prawdopodobieństwo,że przyswajane przez nie treści utrwalą się na całe życie, jest duże.
- Opanowanie nowych technologii i kontrolowanie kryjącej się w niej siły, m.in. umiejętne budowanie wielozadaniowości (np. stopniowanie wielozadaniowości, czyli rozpoczęcie od 2 zadań narazi to tych, w których jesteśmy naprawdę dobrzy), koncentrowanie uwagi (np. świadome zaangażowanie umysłu, czyli skupienie się na kwestiach mających dla nas znaczenie osobiste).
- Wyłączanie gadżetów i zwracanie się ku sobie – skupienie się natym, co nas otacza, na własnych uczuciach, myślach i stanie fizycznym, co zmniejsza stres, pomaga nam słuchać innych i lepiej się z nimi komunikować (m.in. medytacja, joga, autohipnoza wspomagające odprężenie się pomagają w osiąganiu spokoju i zmieniają naszą fizjologię – zwalniają rytm serca, spowalniają oddech, obniżają ciśnienie krwi).
- Zwiększanie kontroli nad technologicznymi pokusami, które – gdy technologia przestaje być użytecznym narzędziem, a staje się sensem życia – mogą być groźne. Przykładowo: w celu ochrony przed uzależniającymi stronami internetowymi można stosować programy i filtry monitorujące zawartość, skontaktować się ze specjalistą lub szukać grup wsparcia.
- Utrzymywanie łączności offline – zwiększenie świadomości znaczenia kontaktów z innymi ludźmi, połączone z ćwiczeniami umiejętności społecznych, może przyczynić m.in. się do pokonania strachu przed kontaktami twarzą w twarz.
- Właściwe „obchodzenie" się z mózgiem (kształcenie mózgu, dbanie o jego jakość), m.in. trening mózgu offline (np. nauka gry w szachy, nauka obcego języka, malowanie obrazów), zadbanie o tzw. kognitywne rezerwy mózgu, z których możemy czerpać w sytuacji, gdy nasz umysłowy potencjał maleje (im wyższy punkt

wyjścia, tym dłuższy przebieg procesu „opadania" – umysłowej degradacji, choć pewną rolę odgrywają tu również predyspozycje genetyczne).

Ponadto aby uniknąć negatywnego wpływu nowych technologii na nasze życie, w tym – osłabiania naszego (a przed wszystkim ludzi młodych i dzieci) potencjału umysłowego, warto mocno zrewidować swój do nich stosunek i poddać się „cyfrowemu detoksowi", czyli dobrowolnej i celowej abstynencji od korzystania z technologii (odłączenia się na pewien czas od telefonu, laptopa i wszystkich urządzeń, za pośrednictwem których stale jesteśmy online). Problem przywiązania do nowych technologii wiąże się też ze zjawiskiem określanym jako FOMO (od ang. *Fear of Missing Out*), oznaczającym wewnętrzny przymus ciągłego sprawdzania e-maili lub pisania postów na portalach społecznościowych w obawie przed utratą kontaktu z potencjalnie ważnymi informacjami. Takim zachowaniom towarzyszy również phubbing (połączenie słów *phone* oraz *snubbing* – 'telefon' oraz 'odtrącanie'), czyli koncentrowanie się na smartfonie kosztem komunikacji interpersonalnej.

Cyfrowy detoks może przynieść korzyści każdemu – może poprawić dobrostan psychiczny i więzi społeczne, zmniejszyć ryzyko kompulsywnego korzystania ze smartfonów (i nie tylko), a także poprawić nastrój, sen i pozbyć się uczucia wewnętrznego niepokoju. Kto staje się zatem bardziej świadomym korzystania z technologii, może uniknąć niekorzystnych i długoterminowych skutków – zmniejszyć ryzyko zaburzeń poznawczych, a także możliwych szkód psychologicznych lub fizycznych.

Wydaje się zatem, że korzystanie z nowoczesnych technologii ma wiele negatywnych skutków dla naszych zdolności poznawczych, choć – oczywiście – ważne staje się dostrzeżenie jej potencjalnych korzyści, aby zrozumieć, jaką rolę odgrywają cyfrowe zachowania poszczególnych osób. Potrzeba jednak więcej badań, aby zrozumieć, czy ten wpływ okazuje się tylko tymczasowy, czy też powoduje długotrwałe, stałe pogarszanie się stanu zdrowia, które dowodzi zasadności nazwania tego zjawiska demencją cyfrową.

Emilia Musiał

Digital Dementia Is on the Rise, „Korea JoongAng Daily*",* June 24, 2013, http:// koreajoongangdaily.joins.com/news/article/article.aspx?aid=2973527 (dostęp 20.10.2021); A. Jupowicz-Ginalska i in., *Polacy a lęk przed odłączeniem – raport z badań*, https://www.wdib.uw.edu.pl/ attachments/article/1992/FOMO.%20 Polacy%20a%20l%C4%99k%20przed%20od%C5%82%C4%85czeniem%20-%20raport%20z%20bada%C5%84.pdf(dostęp20.10.2021); *Nastolatki 3.0, Raport z ogólnopolskiego badania uczniów – 2021* r., https://thinkstat.pl/publikacje/nastolatki-3-0-raport-z-ogolnopolskiego-badania-uczniow-2021-r (dostęp 20.10.2021); A. Ogonowska, *Psychologia mediów i komunikowania. Wprowadzeni*e, Impuls, Kraków 2018; E. Petlák, J. Zajacová, *Rola mózgu w uczeniu si*ę, Petrus, Kraków 2010; M. Prensky, *Digital Natives, Digital Immigrants*, „On the Horizon" 2001, vol. 9, iss. 5, https://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20 Digital%20Immigrants%20-%20Part1.pdf (dostęp 10.10.2021); G. Small, G. Vorgan,*iMózg. Jak przetrwać technologiczną przemianę współczesnej umysłowości*, tłum. S. Borg, Vesper, Poznań 2011; B. Sparrow, J. Liu, D.M. Wegner, *Google Effects on Memory: Cognitive Consequences of Heaving Information at Our Fingertips*, „Science" 2011, vol. 333, iss. 776, https://citeseerx.ist.psu.edu/viewdoc/download?

doi=10.1.1.405.4868&rep=rep1&type=pdf (dostęp 20.10.2021); M. Spitzer, *Cyfrowa demencja. W jaki sposób pozbawiamy rozumu siebie i nasze dzieci*, tłum. A. Lipiński, Wydawnictwo Dobra Literatura, Słupsk 2013; tenże, *Jak uczy się mózg*, tłum. M. Guzowska-Dąbrowska, PWN, Warszawa 2011; M. Szpunar, *Internet i jego wpływ na procesy pamięciowe*, „Teraźniejszość – Człowiek – Edukacja" 2015, t. 18, nr 2(70); A. Wirtwein, P. Kościelniak, *Wywieźli ich na pustynię i zabrali telefony. Wyniki cyfrowego detoksu dają do myślenia*, https://www.focus.pl/artykul/idz-nacyfrowy-detoks (dostęp 20.10.2021); M. Żylińska, *Neurodydaktyka. Nauczanie i uczenie się przyjazne mózgowi*, Wydawnictwo UMK, Toruń 2013.

CYFROWA KONWENCJA GENEWSKA – od 20 lat na podstawie decyzji sekretarza generalnego ONZ działa grupa ekspertów rządowych zajmująca się zmianami w obszarze informatycznym i telekomunikacyjnym w aspekcie →bezpieczeństwa międzynarodowego (Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, wcześniej jako Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN GGE). Efektem pracy tego zespołu było zaproponowanie w 2015 r. nowych regulacji określających reguły odpowiedzialnych zachowań państw w → cyberprzestrzeni. Ich przestrzeganie ma na razie charakter fakultatywny, ale legislacja międzynarodowa zmierza w kierunku ich pełnej implementacji w krajowych systemach prawnych. W swoim raporcie eksperci wskazali, że regulacje międzynarodowe muszą odnosić się także do cyberprzestrzeni, co zaakceptowało 20 państw uczestniczących w badaniach, w tym te o pozycji mocarstwowej: USA, Rosja i Chiny.

W 2017 r. została utworzona → Światowa Komisja ds. Stabilności w Cyberprzestrzeni [t. 4] (Global Commission for the Stability of Cyberspace). Pracuje ona nad opracowaniem pakietu propozycji norm i zaleceń zmierzających do zapewnienia międzynarodowego bezpieczeństwa, stabilności i przewidywalnych działań w cyberprzestrzeni zarówno ze strony państw, jak i podmiotów komercyjnych. Szczególna rola przypadła firmie Microsoft, która uznała, że konieczna jest poprawa transparentności przy jednoczesnym egzekwowaniu odpowiedzialności za realizowane w cyberprzestrzeni przedsięwzięcia. 9 listopada 2017 r. na forum ONZ B. Smith – prezes, a zarazem główny prawnik Microsoftu – zgłosił pilną potrzebę wspólnego działania celem sprostania stale rosnącej liczbie cyberzamachów, sponsorowanych przez poszczególne państwa. Zwrócił uwagę na konieczność stworzenia międzynarodowej organizacji, którą określił mianem cyfrowej konwencji genewskiej. Według Smitha winno to być porozumienie firm nowoczesnych technologii z całego świata, które podejmą współpracę w obronie swoich klientów. Pierwszy krok należałby jednak do państw, które muszą zobowiązać się do zaniechania → cyberataków przeciw cywilnej infrastrukturze. Natomiast firmy informatyczne przy tworzeniu nowych technologii, pozostając neutralne, powinny przyjąć zakres standardów mających na celu ochronę osób. Takie porozumienie na światową skalę miałoby szansę

skutecznie przeciwdziałać → c y b e r p r z e s t ę p c z o ś c i . Poglądy te podzielane są przez wiele organizacji międzynarodowych, które uważają, że infrastruktura cyfrowa winna być neutralna, przy jednoczesnym zakazie proliferacji → c y b e r b r o n i oraz ograniczeniu zdolności ofensywnych państw w przestrzeni cyfrowej. Ważną misję ma tu do spełnienia Międzynarodowa Organizacja Atrybucji Cyberataków. Ma to być nowy element cyberobrony, gromadzący i analizujący dane oraz identyfikujący sprawców zamachów, narzędzie służące poprawie transparentności działań w sieci, ułatwiające społeczności międzynarodowej podejmowanie właściwych działań, w stosunku do nieprzestrzegających zasad i prawa. Ta organizacja ma identyfikować pośredników, którzy są angażowani przez zainteresowane państwa do ataku na inne kraje. Kolejnym ważnym elementem jest Porozumienie Technologiczne (Tech Accord). Ma ono zapewniać ochronę prywatnych użytkowników w cyberprzestrzeni. Inicjatorzy tego rozwiązania uważają, że konieczna jest budowa zaufania rynku cywilnego do producentów nowych technologii oraz samych urządzeń. To z kolei będzie implikowało pożądane zachowania konsumentów, przyczyniając się do szybszego rozwoju handlu i usług.

Fundamenty porządku cyfrowego są stale naruszane przez prace państw nad cyberbronią i cyberatakami. Współcześnie cyberprzestrzeń jest ściśle powiązana ze sferą informacyjną, której towarzyszy dynamiczny wzrost znaczenia → m e d i ó w s p o ł e c z n o ś c i o w y c h [t. 3] oraz → m e d i ó w a l t e r n a t y w n y c h [t. 3]. Stąd wg analityków nie wszystkie cyberataki będą skierowane jedynie na tzw. sferę twardego → c y b e r b e z p i e c z e ń s t w a . Celem może być – oprócz spowodowania strat fizycznych czy ekonomicznych – także wrogie i manipulacyjne oddziaływanie psychologiczne na społeczeństwo. Takie działania są obecnie z powodzeniem stosowane przez Rosję wobec Ukrainy oraz społeczności międzynarodowej, która otrzymuje nieprawdziwy obraz tego konfliktu poprzez wpływanie na → o p i n i ę p u b l i c z n ą [t. 3]. To ważny element → w o j n y p s y c h o l o g i c z n e j [t. 4].

W Warszawie 6 lutego 2018 r. odbyła się międzynarodowa konferencja „Kształtowanie odpowiedzialnego zachowania państw w cyberprzestrzeni", której organizatorami byli German Marshall Fund of the United States (GMF) oraz Microsoft. Obrady były istotnym krokiem do wypracowania cyfrowej konwencji genewskiej dla ochrony cyberprzestrzeni w czasie pokoju. Będąca w procesie tworzenia i konsultacji cyfrowa konwencja genewska przyjęła następujące założenia dotyczące powstrzymywania się państw od:

- zamachów na systemy, których zniszczenie wpłynęłoby na → b e z p i e c z e ń s t w o o b y w a t e l i (obiekty → i n f r a s t r u k t u r y k r y t y c z n e j [t. 2]);
- atakowania systemów, których destrukcja godziłaby w globalną gospodarkę (integralność systemów finansowych) lub mogłaby skutkować poważnymi zakłóceniami (atak na usługi oparte na chmurach);

- atakowania prywatnych kont lub danych będących w posiadaniu dziennikarzy oraz osób prywatnych, zwłaszcza związanych z procesami wyborczymi;
- wykorzystania → i n f o r m a c j i [t. 2] i technologii komunikacyjnych do przywłaszczania własności intelektualnej podmiotów komercyjnych, w tym tajemnic handlowych;
- instalowania lub wymagania backdoorów w komercyjnych wytworach masowej produkcji;
- budowy polityki związanej z aspektami zapobiegania, zabezpieczania, wykorzystywania czy raportowania podatności, zwłaszcza w obszarze produktów masowej produkcji i usług komercyjnych.

Jednocześnie konwencja ma powstrzymywać rozwój cyberbroni oraz wprowadzać limity, w tym jej rozwoju, i zapewniać utrzymanie nad nią kontroli w bezpiecznym środowisku. Ma służyć ograniczeniu proliferacji cyberbroni oraz zaangażowaniu w cybernetyczne operacje ofensywne, tak by zredukować masowe uszkodzenia cywilnej infrastruktury krytycznej. Przepisy konwencji mają wspierać prywatny sektor w przedsięwzięciach służących wykrywaniu i ograniczaniu cyberataków oraz odpowiadaniu na nie, a także w prowadzeniu działań naprawczych. Ma w tym pomagać wspieranie zdolności i mechanizmów odpowiedzialnych za odpowiedź oraz regenerację, szczególnie tzw. Computer Emergency Response Teams (CERT), przy założeniu, że zamach na instytucje wsparcia traktowany byłby jako równoznaczny z atakowaniem personelu medycznego w szpitalach wojskowych.

Obserwujemy, że państwa stale podnoszą zdolności ofensywne w cyberprzestrzeni i wzrasta liczba dokonywanych przez nie cyberataków na podmioty cywilne i obiekty infrastruktury krytycznej. W Europie nadal jednak istnieje postrzeganie cyberbezpieczeństwa wyłącznie przez pryzmat twardej sfery bezpieczeństwa. W tym czasie celem → s t r a t e g i i [t. 4] Rosji staje się rozszerzenie kontroli nad własnym internetem przy jednoczesnym zastępowaniu zachodnich rozwiązań informatycznych rodzimymi zamiennikami. Kolejnym etapem jest wzmacnianie tzw. suwerenności cyfrowej, by uniezależnić się od wpływów zewnętrznych, głównie w przestrzeni informacyjnej. Dla Rosji dostęp do informacji i ich selekcja stały się składową szerszej koncepcji bezpieczeństwa. Kreml i Chiny podnoszą bezpieczeństwo swoich cyberprzestrzeni, rozwijając działania w zakresie bezpieczeństwa informatycznego. Aktywność → h a k e r ó w [t. 2] i cyberataki są skoordynowane z działaniami politycznymi, ekonomicznymi oraz informacyjnymi prowadzonymi przez te mocarstwa. Przykładem takich działań jest rosyjska ingerencja i oddziaływanie w trakcie wyborów prezydenckich w USA, Francji, Czechach i w Hiszpanii podczas referendum w Katalonii. Współczesnym → z a g r o ż e n i e m [t. 4] jest zaburzanie procesów demokratycznych poprzez oddziaływanie psychologiczne i informacyjne na społeczeństwa określonych państw. Ich celem jest podważanie wiarygodności państwa i jego organów, niszczenie wizerunku oraz poczucia zaufania do przywódców politycznych, instytucji

międzynarodowych czy sojuszników. Dzieje się to w wyniku tworzenia chaosu informacyjnego destabilizującego sytuację społeczno-polityczną i tworzącego napięcia społeczne. Użytkownicy sieci oraz mediów społecznościowych odchodzą od uzyskiwania wiedzy z → m e d i ó w t r a d y c y j n y c h [t. 3], stąd to właśnie internet staje się frontem walki o ich umysły, emocje i poglądy. Rośnie też wykorzystanie zautomatyzowanych kont w mediach społecznościowych, ściśle skorelowanych z innymi działaniami hakerów i służb specjalnych. Prowadzone przy ich użyciu operacje informacyjne i psychologiczne były realizowane na podstawie danych skradzionych z kont politycznych liderów, partii politycznych, organów państwowych lub międzynarodowych. Cyberprzestrzeń nierozerwalnie łączy się obecnie ze sferą informacyjną. W epoce dynamicznego wzrostu znaczenia mediów społecznościowych oraz popularności tzw. → m e d i ó w a l t e r n a t y w n y c h [t. 3] aktorzy państwowi coraz częściej będą wykorzystywali → s ł u ż b y s p e c j a l n e [t. 4] oraz grupy hakerów do przeprowadzania cyberataków nie tylko na twardą sferę cyberbezpieczeństwa, związaną z infrastrukturą krytyczną. Cyberataki mogą być ukierunkowane na wzmocnienie efektu oddziaływania informacyjnego i psychologicznego na społeczeństwo oraz opinię międzynarodową. Mogą zmierzać do zakłócenia procesów istotnych reform lub negocjacji, osłabienia determinacji i oporu przeciwnika czy nieprzychylnych sobie władz państwowych. W efekcie mogą podważać wizerunek i zaufanie do danego państwa i osłabiać jego pozycję we wspólnocie międzynarodowej. Mogą także stworzyć alternatywne tło informacyjne, zakłócając odbiór bądź odwracając uwagę od istotnych wydarzeń wewnętrznych lub międzynarodowych.

W tej sytuacji niezbędne jest osiągnięcie kompromisu ustalającego, gdzie przebiegają granice w polityce oddziaływań informacyjnych i psychologicznych w cyberprzestrzeni, których przekroczenie będzie jednoznaczne z aktem wypowiedzenia wojny i spowoduje podjęcie działań odwetowych lub nałożenie → s a n k c j i [t.4] ze strony organizacji międzynarodowych. Ważnym aspektem będzie zdefiniowanie kategorii ataków informacyjnych oraz rozpoczęcie intensywnej edukacji odbiorców cyberinformacji. Temu właśnie celowi służy wypracowanie uregulowań cyfrowej konwencji genewskiej. Cyberbezpieczeństwo stało się bowiem krytycznym elementem bezpieczeństwa międzynarodowego i warunkiem globalnej stabilizacji gospodarczej. Stąd ambitnym i wymagającym szybkich działań wyzwaniem jest wygenerowanie uniwersalnego zbioru zasad, co do którego będzie panował międzynarodowy konsensus.

Andrzej Czop, Marek Pietrzyk

E. Andruszkiewicz, *Audyt bezpieczeństwa w aplikacjach obsługujących transakcje elektroniczne*, [w:] *Globalne cyberbezpieczeństwo*, Y. Utsumi (red.), Warszawa 2006; O. Czop, M. Pietrzyk, *Cyfrowa konwencja genewska*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; A. Klimczuk, *#MicrosoftMówi: #Trendy2018 – co będzie zajmowało polski biznes w 2018 roku*, 30.01.2018, News.Microsoft.com. pl (dostęp 12.02.2019); A. Lelonek, *Konsultacje dotyczące Cyfrowej konwencji genewskiej w Warszawie*, 8.02.2018, CyberDefence24.pl (dostęp

20.04.2019); T. Rid, P. Buchanan, *Attributing Cyber Attacks*, „The Journal of Strategic Studies" 2015, vol. 38; H. Sommer, G. Zakrzewski, *Problem zaufania klienta w relacji z pracownikiem korzystającym z nowych technologii*, [w:] *Cyberprzestrzeń zagrożenia w sieci*, M. Koziński, S. Kosznik-Biernacka, J. Grubicka (red.), Fundacja Pro Pomerania, Słupsk 2017; G. Świszcz, *Cybernetyczna osłona kluczowych procesów państwa – wyzwania dla infrastruktury krytycznej*, [w:] *Cyberterroryzm i systemy informacyjne w bezpieczeństwie*, B. Szczypta-Kłak, K. Pobuta (red.), Helion, Gliwice 2017; H. Tworek, *Microsoft Is Right: We Need a Digital Geneva Convention*, 5.09.2017, Wired.com (dostęp 20.01.2019); O. Wasiuta, S. Wasiuta, *Wojna hybrydowa Rosji przeciwko Ukrainie*, Wydawnictwo Arcana, Kraków 2017.

CYFROWE PATOLOGIE – nieprawidłowe zjawiska i → z a g r o ż e n i a [t. 4] występujące w → c y b e r p r z e s t r z e n i; „produkt" współczesnej cywilizacji medialnej. To patologie w internecie (patologiczne formy korzystania z mediów, w tym internetu) stanowiące przykład zachowań/działań całkowicie pozbawionych społecznej akceptacji, wywołujących powszechne potępienie (repulsję); negatywne zjawisko społeczne, które uwzględnia następujące warunki: naruszenie norm społecznych, destruktywność zachowania mierzoną skalą potępienia społecznego, występowanie w większej skali zbiorowości lub w skali masowej, konieczność występowania działań profilaktycznych.

Zagrożenia te mogą mieć wielowymiarowy charakter. Z jednej strony możemy mówić o wszelkiego rodzaju → c y b e r p r z e s t ę p c z o ś c i (→ p r z e s t ę p c z o ś c i [t. 3] przy użyciu zaawansowanych technologii, przestępczości internetowej), w obrębie której ogólnie wskazuje się 3 rodzaje przestępstw:

- przestępstwa popełniane przy użyciu elektronicznych sieci informatycznych i systemów informatycznych (np. fałszerstwa i oszustwa komputerowe, → s a b o t a ż k o m p u t e r o w y [t. 4]);
- przestępstwa typowe dla sieci łączności elektronicznej (np. ataki typu odmowa usługi – DoS, haking, cracking);
- przestępstwa kontentowe (związane z treścią), czyli publikacje nielegalnych treści w mediach elektronicznych (np. rozpowszechnianie materiałów związanych z pornografią dzieci, instrukcji przestępczych, ofert popełniania przestępstw, fałszywych → i n f o r m a c j i [t. 2]).

Warto zauważyć, że niezbędna do popełnienia nielegalnych działań – w przypadku dwóch pierwszych rodzajów przestępstw internetowych – jest znajomość technologii komputerowych. W przypadku przestępstw związanych z treścią ten aspekt schodzi na plan dalszy, tu wystarczy obsługa przeglądarki internetowej czy też umiejętność dodawania postów lub komentarzy na stronie internetowej.

Z drugiej zaś strony możemy wskazać na tzw. zagrożenia cyberprzestrzeni i świata wirtualnego, które to oprócz dostępu do nieodpowiednich, patologicznych treści, np. „patostreamów", czyli wulgarnych, poniżających i pełnych → p r z e m o c y [t. 3] materiałów nadawanych na żywo w sieci (osoby transmitujące je, tzw. patostreamerzy,

często w zamian za pieniądze wpłacane przez widzów pokazują w czasie rzeczywistym przemoc np. wobec swojej rodziny), niosą za sobą możliwości wypaczeń psychiki, chorób psychicznych i różnego rodzaju patologii. Szczególnie niepokojące są uzależnienia, a także w coraz większym stopniu nasilające się specyficzne zachowania związane z realizowaniem różnorodnych form przemocy i → a g r e s j i zarówno w świecie wirtualnym, jak i rzeczywistym, zmiany o charakterze społecznym oraz zagrożenia z zakresu etyki, zanik samodzielnego myślenia i pogłębionej refleksji.

Przykłady zachowań ryzykownych/agresywnych w cyberprzestrzeni mogących prowadzić do różnego rodzaju patologii – tzw. patologiczne formy komunikowania się – to:

- → c y b e r p r z e m o c ;
- internetoholizm;
- fonoholizm;
- niemoralne i przestępcze komunikowanie się;
- e-osobowość.

Cyberprzemoc to przemoc z użyciem urządzeń elektronicznych, najczęściej telefonu lub komputera. Bywa określana jako cyberbullying, nękanie (ang. *harassment*), dręczenie, prześladowanie w internecie. Jej celem zawsze jest wyrządzenie krzywdy drugiej osobie. Cyberprzemoc to – podobnie jak przemoc tradycyjna – regularne, podejmowane z premedytacją działanie wobec słabszego, który nie może się bronić.

Najczęstsze formy elektronicznej agresji:

- agresja słowna, np. wyzywanie na czatach internetowych, zamieszczanie komentarzy na forum internetowym w celu ośmieszenia, sprawienia przykrości lub wystraszenia innej osoby (m.in. → t r o l l i n g [t. 4], → h e j t i n g [t. 2]);
- upublicznianie upokarzających, przerobionych zdjęć i filmów (m.in. *happy slapping*);
- zamieszczanie przykrych komentarzy na profilach innych osób w portalach społecznościowych;
- włamanie na konto i podszywanie się pod kogoś w celu zamieszczania w jego imieniu obraźliwych postów i zdjęć na profilach innych użytkowników;
- szantażowanie;
- ujawnianie sekretów;
- wykluczanie z grona „znajomych" w internecie;
- celowe ignorowanie czyjejś działalności w sieci.

Cyfrowy odpowiednik agresji jest tak bardzo popularny m.in. dlatego, że napastnicy (tzw. stalkerzy) czują się często anonimowi i bezkarni, np. zamieszczając witryny na serwerze w kraju, w którym pisemne groźby nie są karalne. W odniesieniu do cyberprzemocy przestaje się liczyć siła fizyczna, chodzi o to, żeby wykorzystać jak najlepiej media elektroniczne, by zdyskredytować ofiarę. Zachowania niemoralne, przestępcze w świecie wirtualnym (tj. mobbing, znęcanie się psychiczne, prześladowanie, zniesławianie czy wymuszanie) są o tyle groźne, że poniżające materiały dostępne w krótkim

czasie dla wielu osób mogą pozostać w sieci (np. w formie kopii na komputerach) po tym, gdy przestępca zostanie już schwytany.

Innym patologicznym zachowaniem osoby (zaburzeniem nawyków i popędów w zachowaniu) jest internetoholizm polegający na uzależnieniu od internetu. To uzależnienie przejawiające się w ustawicznym spędzaniu czasu w internecie, dążeniu do jak najczęstszego używania internetu i odczuwaniu dyskomfortu, nawet złości, kiedy nie można tego robić. Dopóki przebywanie w sieci – niezależnie od ilości spędzonego w niej czasu – nie przeszkadza w codziennym życiu i ma obiektywną oraz uzasadnioną przyczynę, nie możemy mówić o uzależnieniu. Problem pojawia się w chwili utraty kontroli nad czasem i sposobem użytkowania tego medium objawiającym się zaniedbywaniem nauki, pracy, rodziny czy kontaktów społecznych.

Należy zauważyć, że proces powstawania uzależnienia od internetu (ang. *internet addiction disorder*) ma kilka faz:

- faza I: zaangażowanie – zapoznanie się z internetem;
- faza II: zastępowanie – zastępowanie silnych odczuć zwykłą redukcją dyskomfortu;
- faza III: ucieczka – pogłębianie się uzależnienia, całkowita ucieczka od świata realnego.

W przypadku długotrwałego spędzania czasu w sieci możemy mówić m.in. o skutkach psychologicznych (np. fobia społeczna, depresje, zubożenie struktur poznawczych) czy też społecznych (np. zanik więzi emocjonalnych z osobami najbliższymi, zaniedbywanie, pomijanie, zapominanie dotychczasowych obowiązków). Złe i nierozsądne korzystanie z internetu może także doprowadzić do choroby cywilizacyjnej o podłożu społecznym i emocjonalnym – rodzaju depresji – syndromu skrajnego wycofania społecznego. Hikikomori – bo o nim jest mowa – oznacza odizolowanie się od świata zewnętrznego i zamknięcie się w przestrzeni domu czy pokoju. Problem ten nie jest niebezpieczny dla ogółu, ale może doprowadzić do samobójstw lub radykalnych kroków spowodowanych przerażeniem i stresem danej osoby.

Poważne zagrożenie dla zdrowia fizycznego i psychicznego stwarza uzależnienie od telefonu komórkowego – określane mianem fonoholizmu. W uzależnieniu fundamentalne jest działanie jako poddanie się człowieka uzależnionego czynności nałogowej, wokół której koncentruje on coraz bardziej swoje myśli i która zajmuje coraz więcej miejsca w jego życiu, tak że traci on nad nim kontrolę. W uzależnieniu czynność ta przestaje pełnić właściwą sobie funkcję (telefon dla człowieka) i staje się celem samym w sobie (człowiek dla telefonu). W ten sposób człowiek uzależniony psychicznie od określonej czynności traci swoją autonomię, dystans i nie dysponuje sobą w sposób wolny.

Nierozważne używanie telefonów komórkowych nie jest uzależnieniem jednorodnym. Specjaliści wyróżniają:

- uzależnienie od SMS-ów – przymus nieustannego otrzymywania i wysyłania wiadomości tekstowych;

- uzależnienie od nowych modeli – nabywanie coraz to nowszych modeli aparatów komórkowych;
- SWT – syndrom włączonego telefonu – obawa przed wyłączeniem się telefonu choćby na kilka minut po wyładowaniu baterii. Lęk przed niedostępnością telefonu dotyka nas, kiedy niemal panicznie boimy się uszkodzenia bądź zgubienia telefonu, utraty zasięgu albo pakietu danych czy rozładowania baterii. Poważny niepokój przybiera wówczas formę fobii, którą określa się nomofobią (ang. *no mobile phobia*). Nierozerwalnie z nomofobią wiąże się strach przed tym, że coś nas omija – to forma społecznego lęku zwana FOMO (ang. *fear of missing out*). Mechanizm ten oznacza obsesyjne sprawdzanie postów, reagowanie na każdy dźwięk telefonu, nieustanne publikowanie czegoś w → m e d i a c h s p o ł e c z n o ś c i o w y c h [t. 3], przeglądanie non stop nagłówków newsów, mimowolne sięganie po telefon w każdej wolnej chwili, bycie online 24/7. Media społecznościowe są nieodłączną częścią życia „sfomowanych" osób.

Z tymi sytuacjami wiąże się zjawisko nazwane phubbingiem (od ang. *phone*, telefon, i *snubbing*, lekceważenie). Polega ono na skupieniu swojej uwagi na smartfonie kosztem komunikacji interpersonalnej. To nic innego jak wyciągnięcie telefonu i ignorowanie wszystkiego i wszystkich wokół siebie. Chęć sprawdzenia najnowszych wieści w smartfonie staje się ważniejsza niż komunikacja „offline", zasady dobrego wychowania czy → b e z p i e c z e ń s t w a na drodze.

Wiele „sfomowanych" osób dotyka także MOMO (ang. *mystery of missing out*). To rodzaj paranoi związanej z rzeczami, które je omijają. Takie osoby czują niepokój, kiedy ich znajomi nie zamieszczają nowych wpisów w mediach społecznościowych. Zakładają, że wszyscy bawią się wspaniale i robią tak ciekawe rzeczy, że nie mają czasu ich relacjonować. Niektóre osoby boją się nawet, że inni nie chcą im pokazać, co robią, ponieważ ich nie lubią.

FOMO, MOMO i inne związane z nimi zjawiska mogą powodować problemy z relacjami międzyludzkimi w rzeczywistym świecie. Niekontrolowane prowadzą do depresji, a także przyczyniają się do częstszego sięgania po używki wśród niektórych grup wiekowych.

Kolejny rodzaj zachowań patologicznych w cyberprzestrzeni to wszelkiego rodzaju niemoralne i przestępcze komunikowanie się wśród dzieci, młodzieży i dorosłych, do których możemy zaliczyć:

- seksoholizm – nadmierne uzależnienie od czynności seksualnych, które obecnie coraz częściej przybiera formę uzależnienia od internetowej pornografii (stron internetowych umożliwiających oglądanie lub ściąganie filmów pornograficznych i zdjęć), drogą do uzależniania się od seksu jest także cyberseks, czyli rodzaj internetowej aktywności seksualnej, wirtualnej interakcji erotycznej, w trakcie której strony relacji mogą osiągnąć seksualną przyjemność;

- → s e k s t i n g [t. 4] – trend panujący głównie wśród nastolatków, który polega na pisaniu pikantnych wiadomości do innych, a także wysyłaniu im nagich lub półnagich zdjęć, do sekstingu można wykorzystać tradycyjne SMS-y, ale też wszelkie aplikacje do wysyłania wiadomości, media społecznościowe oraz e-maile;
- pedofilia w internecie – *grooming*, czyli aktywność podejmowana po to, aby nawiązać kontakt emocjonalny z określonym dzieckiem, zdobyć jego zaufanie, a następnie wykorzystać je seksualnie; wykorzystanie to może przybrać różne formy – od nakłonienia do przesłania niecenzuralnych zdjęć, zachęcania do prostytucji po zmuszanie do udziału w pornografii dziecięcej czy gwałt, jest to także mechanizm używany, by nakłonić dziecko do prostytucji lub udziału w pornografii dziecięcej;
- prostytucja nieletnich – cyberprostytucja – wirtualny nierząd będący atrakcyjną formą zarobkowania dla nieletnich, polega na uzyskiwaniu korzyści materialnych w zamian za udostępnianie w internecie materiałów erotycznych lub pornograficznych (zdjęcia, filmy, pokazy na żywo, płatne transmisje) z własnym udziałem, cyberprostytucja kwitnie w specjalnie powstałych do tego celu serwisach internetowych, ale osoby prostytuujące się używają także popularnych serwisów społecznościowych, wstępem do cyberprostytucji jest seksting.

Internet sprawia, że unikamy zadumy, rozpraszamy się i mamy obsesję na punkcie gratyfikacji. To tu, gdzie wszystkie chwyty są dozwolone, wielu ludzi tworzy swoje alternatywne ja: bardziej asertywne, bardziej kompetentne, seksowniejsze, śmielsze *alter ego*, czyli e-osobowość. Alternatywna wersja samego siebie (alternatywna tożsamość) z jednej strony może przełamywać pewne zahamowania (np. lęki społeczne), z drugiej popychać i motywować ludzi do czynów patologicznych i przestępczych. W rzeczywistym świecie jesteśmy ostrożniejsi i ważymy swoje słowa, bo jesteśmy obserwowani i rozpoznawani, a gdy tylko przekroczymy granice świata wirtualnego, nasze zachowania ulegają zmianie. Sprzyja temu bowiem wykształcenie się e-osobowości, którą cechują: narcyzm i wyolbrzymione poczucie możliwości, wyniosła postawa wobec innych, nowy zbiór „sieciowych" zasad moralnych, skłonność do impulsywnego zachowania czy regresja do stanów dziecięcych (infantylne formy myślenia, wartościowania, odczuwania i reagowania).

E-osobowość umożliwiająca eksperymentowanie w internecie z naszą tożsamością (ważne staje się to, co o sobie napiszemy, to, czego nie ujawnimy, chcąc wyretuszować obraz samego siebie) – zdawałoby się – daje odskocznię od napięć i stresów prawdziwego życia, pozwala być kimś innym, ale należy pamiętać o tym, aby się w tej inności internetowej nie zatracić.

Wśród patologicznych zjawisk w komunikowaniu się w cyberprzestrzeni warto wymienić cyfrową głupotę oraz demencję cyfrową. Ta pierwsza oznacza irracjonalne zachowania, np. przekazywanie intymnych zdjęć do internetu i poddawanie ich ogólnej ocenie, bezmyślne naśladownictwo np. zachowań z zakresu sekstingu. Demencja

cyfrowa – umysłowa degradacja – to psychiczne i fizyczne symptomy chorobowe, tj. zakłócenia pamięci, uwagi i koncentracji, deficyt emocjonalny, objawy ogólnego otępienia, będące skutkiem niekontrolowanego korzystania z mediów cyfrowych. Na uwagę zasługują też: flaming – celowe zaostrzanie wymiany zdań między internautami w serwisach dyskusyjnych i społecznościowych, co doprowadza do eskalacji agresji słownej między nimi; mowa nienawiści – rozbudzanie nienawiści do konkretnej osoby lub grupy osób, często odwołujące się do negatywnych stereotypów i uprzedzeń związanych z płcią, rasą, pochodzeniem, religią, orientacją seksualną; trolling – nieprzyjazne zachowanie wobec internautów biorących udział w dyskusji, np. pogardliwe wypowiedzi, obsesyjne poprawianie błędów, wygłaszanie opinii niezwiązanych z tematem rozmowy.

Jak zauważa A. Ogonowska, każda patologia użytkowania mediów ma swoją dynamikę i rozciąga się w czasie. Im wcześniej zwróci się uwagę na istniejący problem, tym łatwiej pomóc konkretnej osobie poradzić sobie z nim. A zatem możemy mówić o następujących etapach patologicznego korzystania z mediów i mechanizmach rządzących danym zachowaniem:

- poznawanie nowego zachowania, eksploracja – uczenie się tego zachowania, aby osiągnąć nowy cel (np. zmniejszenie stresu);
- specjalizacja w patologicznym zachowaniu medialnym – doskonalenie form i sposobów korzystania z patologicznego zachowania w różnych sytuacjach;
- dominacja patologicznego zachowania – patologiczne zachowanie medialne staje się centralną wartością w życiu jednostki kosztem innych zachowań, wartości i celów;
- używanie problemowe – uciekanie od problemów i zagłuszanie ich patologicznymi zachowaniami;
- → k r y z y s [t. 2] i próba zerwania z patologicznym zachowaniem – pod wpływem narastających problemów i presji otoczenia chęć wyjścia z cyklu nałogowego.

Odpowiedzią na patologię cyfrową (patologiczne korzystanie z mediów) są podejmowane działania profilaktyczne, interwencyjne i korekcyjne w zakresie zachowań wykraczających poza przyjęte standardy. Wśród nich warto wymienić: działania zapobiegające pojawianiu się zachowań patologicznych (głównie w szkołach), edukację społeczeństwa w celu uwrażliwienia na wczesne oznaki zagrożenia patologią oraz informowanie o dostępnych formach pomocy, prowadzenie lokalnych, dostosowanych do odbiorców programów edukacyjnych i interwencyjnych, szkolenie nauczycieli i osób realizujących programy zapobiegania, informowanie i szkolenie konkretnych osób, bezpośrednie oddziaływanie leczniczo-rehabilitacyjne na jednostkę czy też utworzenie doraźnych struktur i ośrodków. Niezbędna jest edukacja medialna, czyli działalność edukacyjna polegająca na wkroczeniu w przestrzeń użytkowników mediów, której celem jest wykształcenie w nich określonych kompetencji pozwalających na świadome z nich korzystanie.

Emilia Musiał

E. Aboujaoude, *Wirtualna osobowość naszych czasów. Mroczna strona e-osobowości*, tłum. R. Andruszko, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2012; A. Borkowska, *Cyberprzemoc. Włącz blokadę na nękanie. Poradnik dla rodziców*, NASK Państwowy Instytut Badawczy, Warszawa 2019; T. Cantelmi, *Technopłynność. Człowiek w epoce Internetu. Technopłynny umysł*, tłum. A. Laciuga, Wydawnictwo Franciszkanów Bratni Zew, Kraków 2014; J. Kosiński, *Paradygmaty cyberprzestępczości*, Difin, Warszawa 2015; S. Kozak, *Patologia cyfrowego dzieciństwa i młodości. Przyczyny, skutki, zapobieganie w rodzinach i szkołach*, Difin, Warszawa 2014; A. Ogonowska, *Psychologia mediów i komunikowania. Wprowadzenie*, Wydawnictwo „Impuls", Kraków 2018; I. Pospiszyl, *Patologie społeczne*, Wydawnictwo PWN, Warszawa 2009; T. Prymek, *O patologii i zagrożeniach cyfrowego pokolenia*, „Problemy Wczesnej Edukacji" 2014, nr 10/4 (27); P. Siedlanowski, *Homo crudelis? Patostream – kolejna patologia w sieci*, „Biuletyn Edukacji Medialnej" 2018, nr 2; M. Spitzer, *Cyfrowa demencja. W jaki sposób pozbawiamy rozumu siebie i swoje dzieci*, Dobra Literatura, Słupsk 2013; S. Wójcik, *Zagrożenia dzieci i młodzieży w internecie*, „Dziecko Krzywdzone. Teoria, Badania, Praktyka" 2017, vol. 16, no. 1; *Zagrożenia cyberprzestrzeni i świata wirtualnego*, J. Bednarek, A. Andrzejewska (red.), Difin, Warszawa 2014.

CYFROWE PRAWA CZŁOWIEKA →Prawa człowieka [t. 3] to zespół praw i wolności, które przysługują każdemu człowiekowi bez względu na pochodzenie etniczne, płeć, język, wyznanie, przekonania polityczne, pochodzenie narodowe i społeczne, majątek itp. Są one niezbywalne (nie można się ich zrzec) i nienaruszalne. Postulują poszanowanie wartości najcenniejszych dla człowieka, takich jak życie, godność, wolność, swobodny rozwój.

Podstawę prawną ochrony praw człowieka stworzyły dwa dokumenty: Karta Narodów Zjednoczonych uchwalona w 1945 r. i Powszechna Deklaracja Praw Człowieka uchwalona w 1948 r. przez Zgromadzenie Ogólne ONZ. W 1953 r. weszła w życie Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie dnia 4 listopada 1950 r., w skrócie nazywana Europejską Konwencją Praw Człowieka. Jest to umowa międzynarodowa, której stronami są wszystkie państwa członkowskie →Rady Europy.

Wraz z rozwojem technologii w porządku prawnym pojawiła się kategoria tzw. cyfrowych praw człowieka. Zagadnienie to może być analizowane:

- z punktu widzenia wpływu nowych technologii na istniejące już prawa człowieka;
- z punktu widzenia formułowania nowych praw wypływających z potrzeb dostosowania do nowych technologii (będą to np. prawo dozapewnienia dostępności cyfrowej, prawo do bycia zapomnianym, prawo do poufności i integralności systemów informatycznych).

Ważnym dokumentem jest przyjęta przez Radę Praw Człowieka Organizacji Narodów Zjednoczonych rezolucja RES/26/13 „Promocja, ochrona i stosowanie praw człowieka w Internecie". Uchwała stanowi, że te same prawa, które przysługują ludziom poza internetem, muszą być również chronione w sieci, szczególnie dotyczy to wolności słowa, która ma zastosowanie bez względu na granice i za pośrednictwem dowolnych mediów, zgodnie z art. 19 Powszechnej Deklaracji Praw Człowieka

i Międzynarodowym Paktem Praw Obywatelskich i Politycznych. Ponadto w dokumencie tym Rada Praw Człowieka:

- uznaje globalny i otwarty charakter internetu jako siły napędowej przyspieszającej postęp w kierunku rozwoju w różnych formach;
- wzywa wszystkie państwa do upowszechniania i ułatwiania dostępu do internetu oraz międzynarodowej współpracy mającej na celu rozwój mediów, urządzeń i → t e c h n o l o g i i i n f o r m a c y j n o - k o m u n i k a c y j n y c h [t. 4] we wszystkich krajach;
- potwierdza, że wysokiej jakości edukacja odgrywa decydującą rolę w rozwoju, w związku z tym wzywa wszystkie państwa do krzewienia umiejętności cyfrowych i ułatwiania dostępu do → i n f o r m a c j i [t. 2] w internecie, co może być ważnym narzędziem upowszechniającym prawo do edukacji;
- wzywa wszystkie państwa do zajęcia się kwestiami → b e z p i e c z e ń s t w a [t. 1] w internecie, zgodnie z ich międzynarodowymi zobowiązaniami w zakresie praw człowieka, w celu zapewnienia ochrony wolności wypowiedzi, prawa do zrzeszania się, prywatności i innych praw człowieka w internecie, w tym za pośrednictwem krajowych demokratycznych, przejrzystych instytucji, opartych na praworządności w sposób gwarantujący wolność i bezpieczeństwo w internecie, aby mógł on być siłą generującą rozwój gospodarczy, społeczny i kulturalny;
- podkreśla znaczenie zwalczania propagowania nienawiści, którestanowi podżeganie do → d y s k r y m i n a c j i [t. 5] lub → p r z e m o c y [t. 3] w internecie, w tym przez propagowanie tolerancji i dialogu;
- wzywa wszystkie państwa do rozważenia sformułowania, w ramach przejrzystych i integracyjnych procesów z udziałem wszystkich zainteresowanych stron, oraz przyjęcia krajowych przepisów publicznych związanych z internetem, których celem jest powszechne korzystanie z praw człowieka;
- zachęca specjalne komisje do uwzględnienia tych kwestii w ramach ich istniejących mandatów;
- postanawia kontynuować rozważania na temat propagowania, ochrony i stosowania praw człowieka, w tym prawa do wolności wypowiedzi, w internecie i przy użyciu innych technologii, a także na temat tego, w jaki sposób internet może być ważnym narzędziem rozwoju i korzystania z praw człowieka.

Innowacje związane z technologią istotnie wpływają na stosowanie tradycyjnych praw człowieka, w tym m.in. szerokiego zakresu praw osobistych i politycznych, społeczno-ekonomicznych i kulturalnych. Wpływ nowych technologii na dobra osobiste jest szczególnie wyraźny w wypadku korzystania z prawa do prywatności, ochrony danych osobowych, wolności wypowiedzi, nietykalności mieszkania, tajemnicy komunikowania się, prawa do bezpieczeństwa czy domniemania niewinności. Wymienione prawa są najbardziej zagrożone w związku z nieprawidłowym korzystaniem z nowych technologii. Wolność słowa jest prawem, które uległo znacznej przemianie pod wpływem

zastosowania nowych technologii. Otworzyły one zupełnie nowe rodzaje komunikacji. Internet i inne technologie pozwalają na wyrażanie opinii i poglądów, które łatwo można udostępnić milionom ludzi w ułamku sekundy. Platformy typu YouTube, X (dawniej Twitter), Facebook stały się swoistą współczesną agorą. Dzięki zastosowaniu nowych kanałów komunikacyjnych wiadomości o naruszeniach praw człowieka mogą szybko dotrzeć do ogromnej liczby osób, co jednocześnie może podnieść świadomość wagi poszanowania podstawowych praw. Cyfrowe technologie generują też jednak nowe zagrożenia dla praw człowieka, takie jak blokowanie lub ograniczanie przesyłania informacji, monitorowanie i kontrolowanie treści przekazywanych danych oraz bezprawne wykorzystywanie danych osobowych. Podobnie wygląda sytuacja w wypadku prawa do prywatności – nowe technologie mogą pomóc je chronić i jednocześnie stać się źródłem bezpośredniego zagrożenia. Wiele osób nie zdaje sobie sprawy z tego, że dane, które dobrowolnie udostępniają, np. na własnym profilu w portalu społecznościowym, są coraz cenniejsze dla firm oferujących usługi internetowe. Bezkrytyczne zachowanie internautów korzystających z „dobrodziejstw wirtualnych" sprawia, że sfera prywatności staje się sferą przezroczystą. Użytkownicy powinni uważać na różnego rodzaju oszustwa internetowe, jak → p h i s h i n g [t. 3], typosquatting czy oszustwo nigeryjskie.

Ważnym prawem człowieka, które wykształciło się w związku z aktywnością online, jest „prawo do bycia zapomnianym". Reguluje je Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – RODO. W art. 17 zapisano, że osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia tych danych, a administrator ma obowiązek bez zbędnej zwłoki je usunąć, jeżeli zachodzi jedna z następujących okoliczności:

- dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
- osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie, i nie ma innej podstawy prawnej przetwarzania;
- osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania;
- dane osobowe były przetwarzane niezgodnie z prawem;
- dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;
- dane osobowe zostały zebrane w związku z oferowaniem usług → s p o ł e c z e ń s t w a i n f o r m a c y j n e g o [t. 4], o których mowa w art. 8 ust. 1 (warunki wyrażenia zgody przez dziecko w wypadku usług społeczeństwa informacyjnego).

Co więcej, jeżeli administrator upublicznił dane osobowe, a ma obowiązek je usunąć, to – biorąc pod uwagę dostępne technologie i koszt realizacji –podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych,kopie tych danych osobowych lub ich replikacje.

Z coraz większym dostępem do internetu wiąże się również zagadnienie dostępności cyfrowej organów sektora publicznego. W Polsce kwestię tę reguluje Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych. Dokument ten stanowi implementację dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/2102 z dnia 26 października 2016 r. w sprawie dostępności stron internetowych i mobilnych aplikacji organów sektora publicznego (dalej: dyrektywa 2016/2102). Polska ustawa odnosi się do zasobów cyfrowych organów administracji publicznej i określa:

- wymagania dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych;
- wymogi dotyczące treści, przeglądu i aktualizacji deklaracji dostępności stron internetowych i aplikacji mobilnych podmiotówpublicznych oraz ich publikacji;
- kompetencje organu właściwego w sprawach monitorowania tego,czy zapewniona jest dostępność cyfrowa stron internetowych i aplikacji mobilnych podmiotów publicznych, oraz nadzoru nadstosowaniem przepisów ustawy;
- zasady monitorowania zapewniania dostępności cyfrowej stron internetowych lub aplikacji mobilnych oraz prowadzenia sprawozdawczości w zakresie dostępności cyfrowej;
- postępowanie w sprawie zapewniania dostępności cyfrowej strony internetowej, aplikacji mobilnej lub ich elementów.

Podstawowym standardem technicznym, do którego odsyłają przepisy dotyczące dostępności cyfrowej, są wytyczne WCAG 2.1 (Web Content Accessibility Guidelines). Odesłanie do podstawowych 4 zasad tego standardu widoczne jest w art. 5 ust. 2 ustawy o dostępności cyfrowej: dostępność cyfrowa strony internetowej i aplikacji mobilnej polega na zapewnieniu ich funkcjonalności, kompatybilności, postrzegalności i zrozumiałości.

Z prawem dotyczącym dostępności cyfrowej szeroko związany jestteż rozwój tzw. e-administracji, co umożliwia obywatelom korzystanie z praw związanych z różnymi organami administracyjnymi za pośrednictwem sieci. Coraz więcej mówi się o tzw. obywatelstwie cyfrowym.

Przejawia się to również w prawie obywateli do posiadania pełnego dostępu do danych i usług administracji publicznej. Wiele spraw urzędowych można już załatwić bez wychodzenia z domu. W ten sposób można np. złożyć wniosek o wydanie dowodu osobistego lub zgłosić jego utratę, skorzystać z programu „Rodzina 500+", założyć własną działalność gospodarczą, sprawdzić punkty karne lub przejrzeć historię kupowanego pojazdu.

Rozwój nowych technologii wpływa również na społeczne prawa człowieka, jak prawo do edukacji, w tym do bezpłatnej nauki na szczeblu podstawowym, do dostępu do szkolnictwa wyższego oraz do wsparcia w celu ułatwienia dostępu do edukacji. Oddziałuje również na prawa w dziedzinie kultury obejmujące prawo do udziału w życiu kulturalnym i korzystaniaz postępu naukowego. Dzięki zasobom e-bibliotek, zdigitalizowanym zbiorom muzealnym lub chociażby transmisji wykładów i wystąpień publicznych wiedza i nowe odkrycia dużo szybciej i łatwiej docierają do większego grona odbiorców.

E wa Durek

W. Brzozowski, A. Krzywoń, M. Wiącek, *Prawa człowieka*, Wolters Kluwer, Warszawa 2021; Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/2102 z dnia 26 października 2016 r. w sprawie dostępności stron internetowych i mobilnych aplikacji organów sektora publicznego, Dz.Urz. UE L 327 z 2.12.2016; *DziałaniaMinisterstwa Cyfryzacji*, https://www.gov.pl/web/cyfryzacja/dzialania (dostęp 15.04.2023); Karta Narodów Zjednoczonych, Statut Międzynarodowego Trybunału Sprawiedliwości i Porozumienie ustanawiające Komisję Przygotowawczą Narodów Zjednoczonych, Dz.U. 1947, nr 23, poz. 90; Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 4 i 8 oraz uzupełniona Protokołem nr 2, Dz.U. 1993, nr 61, poz. 284; H. Markiewicz, P. Polański, *Dostępność w świetle prawa międzynarodowego. Uwarunkowania rozwoju jednolitego rynku cyfrowego*, [w:] *Prawomiędzynarodowe. Teoria i praktyka*, I. Kraśnicka (red.), C.H. Beck, Warszawa 2020; M. Nastić, *The Impact of the Informational and Communication Technology on the Realization and Protection of Human Rights*, „Balkan Social Science Review" 2021, vol. 17; P. Polański, *Dwa oblicza prawa do dostępności cyfrowej*, „Prawo Mediów Elektronicznych" 2020, nr 4; *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, E. Bielak-Jomaa, D. Lubasz (red.), Wolters Kluwer, Warszawa 2018; Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz.Urz. UE L 119 z 4.05.2016; *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, Resolution adopted by the Human Rights Council, 14.07.2014, UN Doc. A/HRC/RES/26/13, https://www.right-docs.org/doc/a-hrc-res-26-13/ (dostęp 15.04.2023); *Ustawa o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych. Komentarz*, E. Fabian, H. Markiewicz-Hoyda, P. Polański (red.), C.H. Beck, Warszawa 2021; *Ustawa o dostępności cyfrowej stroninternetowych i aplikacji mobilnych podmiotów publicznych. Komentarz*, G. Szpor, K. Czaplicki (red.), Wolters Kluwer, Warszawa 2020; Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych, Dz.U. 2019, poz. 848 z późn. zm.

CYFROWY NARCYZM – (ang. *digital narcissism*) cyfrowe oblicze zachowań skierowanych na własne *ja* – zachowań w →c y b e r p r z e s t r z e n i [t. 1], w których m.in. splatają się – na większą niż dotąd skalę – ekshibicjonizm i voyeuryzm, czego konsekwencją jest prezentowanie różne wersje samych siebie i jednocześnie, z coraz większą ochotą, podglądanie innych. To – jak podaje Magdalena Szpunar – autoprezentacja i odpowiednio spreparowana kreacja samego siebie, stająca się wręcz anomalią immamentnie związaną z naszym stylem życia, sposobem ucieczki

od problemów zewnętrznego świata, formą radzenia sobie z lękiem, poczuciem pustki, uzależnieniem od nieustannej aprobaty innych. Do swoistej erupcji takich zachowań przyczyniło się życie w epoce wizualnej, w której „[…] mamy do czynienia z efektem postpiśmienności przejawiającym się odejściem od form tradycyjnego pisma na rzecz form audiowizualnych i ideograficznych". Warto podkreślić w tym miejscu, że prymat obrazu – czyli dominacja tego, co widzialne, nad tym, co zrozumiałe – prowadzący do patrzenia bezrozumnego, przekształca istotę zwaną *homo sapiens*, wytwór kultury pisanej, w *homo videns*, istotę, która słowo zdetronizowała na rzecz obrazu.

Ten rodzaj współczesnego narcyzmu – jego cyfrowa odsłona – stanowi ponadto swego rodzaju zestaw praktyk komunikacyjnych typowych dla technologii Web 2.0, opartych na egocentryzmie tak uwypuklonym, że aż graniczącym z patologią.

Cyfrowy narcyzm wyraża się poprzez serię „ekstremalnych" działań (w zasadzie codziennie), takich jak robienie dużej ilości selfies (cyfrowych autoportretów stanowiących formę wyrażania siebie, kształtowania własnej tożsamości, afiliowania działań) czy nieskrępowane odsłanianie się (nadmierne ujawnianie → i n f o r m a c j i [t. 2] o sobie) nazywane oversharingiem, który przejawia się w kompulsywnym przeglądaniu się w wirtualnym lustrze, którego odbicie stanowią patrzący inni. Narcissurfing to nie tylko wyszukiwanie online treści na swój temat, lecz także przemożna potrzeba informowania o sobie.

Dzielenie się (a raczej: nadmierne dzielenie się) to sposób, w jaki cyfrowi narcyzi kolekcjonują przejawy swojego „uwielbienia" – czego odzwierciedleniem są tzw. lajki i komentarze zwrotne świadczące o skuteczności wyrażania siebie oraz popularności, ale także (a może – przede wszystkim) będące sposobem na zaistnienie (medialną widoczność stającą się panaceum na odczucie bezsensu własnej egzystencji, remedium na problemy życiowe i brak sukcesów w realnym życiu, znak statusu społecznego i pozycji jednostki) – ponieważ istnieją tylko wtedy, gdy mogą być widziani i rozpoznawani. Można powiedzieć: „Oglądasz mnie, więc istnieję", co może oznaczać, że cyfrowi narcyzi, ponieważ nie mają nic do zaoferowania (ani własnych kompetencji, ani ważnych treści), prezentują swoją fizyczność, która nie wymaga od nich poniesienia niemal żadnych wysiłków. Co więcej – cyfrowy narcyz nie może (a raczej: nie potrafi) żyć bez publiczności, która zapewnia mu społeczną aprobatę: „potrzebuje innych w roli oglądających, słuchających, czy czytających płytkich wynurzeń publikowanych online". Właściwie możemy powiedzieć, że pragnie żyć w środowisku określanym mianem wiecznego lajka – coraz mniej robi dla siebie, a coraz więcej dla innych, aby otrzymać lajkową afirmację.

„Staje się patchworkiem pragnień wielu, tak naprawdę niewiele znaczących dla niego ludzi, których pochwała staje się sposobem na podwyższenie jego samooceny".

Pojmowanie narcyzmu w kontekście cyberprzestrzeni pozwala zauważyć, że zachowania narcystyczne w tej odsłonie wzmacniają i podtrzymują media narcystyczne, takie jak telewizja czy internet (zwłaszcza sieci społecznościowe), oferujące

szansę na zaistnienie niemal wszystkim. Jak pisze Elias Aboujaoude, Facebook stanowi doskonałe forum dla tendencji narcystycznych, ponieważ „osoby narcystyczne, zamiast patrzeć w lustro, mogą spędzać całe dnie w sieci, uaktualniając swoje profile i pławiąc się w swoim blasku". Ponadto zauważa, że internet oferuje wiele możliwości jeszcze większego zachłyśnięcia się sobą i promocji siebie, takich jak dowolna preparacja własnej biografii (kształtowania własnego wizerunku online, określanego mianem trybu Boga), odpowiednio dobrane zdjęcia czy też zamierzona „kolekcja" znajomych – słowem: nieustanne multiplikowanie samego siebie. Liczne badania – w tym przeprowadzone na uniwersytetach w Swansea, w Mediolanie, we Florencji – pokazują, że 2/3 ludzi ma tendencję do korzystania z sieci społecznościowych przede wszystkim w celu publikowania selfies, co dowodzi, że te sieci służą jako multiplikatory pragnienia bycia w centrum uwagi i zaspokojenia tej głębokiej potrzeby podziwu. Ponadto zauważono, że sieci społecznościowe przyciągają głównie narcyzów wrażliwych, tych, którzy czują się bardziej niepewnie i mają niższą samoocenę, ponieważ w środowisku online czują się bardziej pewni siebie niż w rzeczywistych interakcjach. Dlatego używają tej przestrzeni jako środka do uzyskania podziwu, którego pragną. Można by rzec – za B. Świątek – że: „[…] narcystyczne media łechtają ego przeciętnego odbiorcy, wmawiając mu, że jest kimś wartościowym i znaczącym. Pospolitość traktują jak wartość, a walorem staje się brak jakichkolwiek umiejętności".

W kontekście rozważań o narcyzmie cyfrowym warto zauważyć, żeosobnik narcystyczny (*Homo narcissus*) m.in.:

- wykazuje nastawienie wielkościowe, chroniczną potrzebę podziwu i brak empatii (aprobatę samego siebie uzależnia od aklamacji publiczności);
- przejawia cechy merkantylnych relacji ze światem, tj. nastawienie na własny sukces i silną potrzebę władzy, zogniskowanie na materialnej stronie życia (kulturze konsumpcji), utrzymywanie kontaktów z wpływowymi i znaczącymi ludźmi;
- pielęgnuje przekonanie, że własne ideały są bardziej wyszukane od wartości innych ludzi, postrzega świat niemal wyłącznie przez pryzmat własnych potrzeb, przecenia własne możliwości, nie potrafi przyjąć perspektywy innej osoby;
- nawiązuje instrumentalne relacje z innymi ludźmi, sprowadzonedo procesu konsumowania, relacje wyłącznie dla korzyści własnej, „inni są niezbędni do odczuwania pełni satysfakcji i szczęścia z podejmowanych działań";
- idealizuje własne *ja*, jest zakochany we własnym wizerunku (nadmiernie zainteresowany sobą, własną fizycznością), ma zawyżoną samoocenę, traktuje siebie jak markę (ang. *personal brand, self-branding*), którą należy kreować, aby móc efektywnie się sprzedawać;
- odczuwa kompulsywną potrzebę pozostawiania po sobie wielu informacji w internecie oraz wyszukiwania informacji na swój własny temat (tzw. *narcissutfing* czyli narcystyczne surfowanie);

- żyje pod presją haseł reklamowych i trendów lansowanych przez kolorowe czasopisma, akceptuje jedynie ciało młode;
- kształtuje się w warunkach relatywizmu moralnego i moralnej deprywacji.

Jak zauważa M. Szpunar, narcystyczne schorzenie nie tylko dotyka pojedynczych jednostek czy struktur społecznych (organizacje, instytucje), lecz także infekuje kulturę, w której funkcjonuje jednostka. Jawi nam się zatem kultura narcyzmu, do której ukształtowania – według Christophera Lascha, amerykańskiego historyka, twórcy tego pojęcia – przyczyniły się przemiany zachodzące w społeczeństwie: biurokracja, rozprzestrzenianie się obrazów, terapeutyczne → i d e o l o g i e, kult konsumpcji oraz degradacja rodziny. Nadrzędnymi wartościami w takiej kulturze staje się realizacja siebie, zogniskowanie wyłącznie na sobie i własnych potrzebach. Innymi słowy: „Kultura staje się narcystyczna, kiedy bogactwo osiąga rangę wyższąniż mądrość, a rozgłos zyskuje większy podziw niż godność".

W ten sposób problematyka narcyzmu w kulturze, podjęta przez Lascha, toczy się wokół jednego z trzech głównych nurtów podejmowanych w dyskursie naukowych – wokół ujęcia kulturowo-społecznego. Ta perspektywa pozwala zrozumieć, że narcystyczna może być nie tylko pojedyncza jednostka (narcyzm rozumiany jako naturalny i prawidłowy etapu rozwoju człowieka lub zaburzenie stanowiące jednostkę chorobową), lecz także cała zainfekowana nim kultura, w której przychodzi nam żyć. To szersze pojmowanie narcyzmu transmituje to pojęcie z rozumienia indywidualistycznego, które odnajdujemy zarówno w nurcie genetycznym, jak i w klinicznym, w obszar zbiorowości i kultury przez nią generowanej. Warto także dodać, że na wagę analiz i interpretacji narcyzmu jako zjawiska społeczno-kulturowego o szerokim zasięgu zwracają uwagę Vincenzo Cesareo i Italo Vaccarini – współcześni włoscy socjolodzy, którzy wykorzystują samo pojęcie narcyzmu jako metaforę służącą do opisu współczesnej kultury lub do wskazania jej najbardziej charakterystycznych cech. A zatem – jak zauważają w swoich pracach Robert McCrae i Alexander Lowen – „nie tylko kultura może kształtować/modelować osobowość, ale i jednostka może modelować kulturę według obrazu samej siebie", co w konsekwencji – o czym piszą Jean Twenge i Keith Campbell – może prowadzić wręcz do epidemii czy plagi narcyzmu. Z jednej strony – narcystyczna kultura sprzyja wszakże wzrostowi narcyzmu wśród jednostek, a z drugiej – narcystyczne jednostki infekują swym zaburzeniem kulturę.

Według M. Szpunar: „Laschowska kultura narcyzmu ewoluowała w kulturę cyfrowego narcyzmu, gdzie przestrzeń internetowa, zamiast wzmacniać interakcje międzyludzkie, prowadzi do egocentrycznego skupienia na samym sobie i własnych internetowych kreacjach, a kontakty z innymi stają się niczym więcej niż naskórkową i powierzchowną formą okazywania aprobaty". Zatem w takiej kulturze mamy do czynienia m.in. z:

- imperatywem szczęścia utożsamianym z sukcesem, który ma je warunkować (wymuszony i nienaturalny uśmiech, sztuczne zadowolenie, udawana sympatia, „miła osobowość", „kontrolowany uśmiech", wszystko musi być *cool*);

- imperatywem sukcesu stanowiącym komponent tożsamości współczesnego człowieka (wyprzedzenie innych, zwycięstwo nad innymi, cel sam w sobie – nie chodzi o sukces osiągnięty własną pracą, pomysłowością, samodyscypliną);
- deficytem autentyczności lub zainscenizowaną autentycznością (fastfoodyzacja kontaktów interpersonalnych, kultura podglądactwa, maskowanie się, połowiczne związki, samorealizacja bez względu na więzi między ludźmi, autopromocja, a nie – autentyczna ekspresja siebie);
- imperatywem fałszu (kreowanie osobowości fasadowej zgodnej z oczekiwaniami innych, np. fałszywe piękno osiągnięte dzięki operacjom plastycznym, mądrość oparta na pustych frazesach);
- konsumpcjonizmem (umacnianie poglądu, że o wartości człowieka stanowi to, co człowiek posiada: że bogactwo, sława i atrakcyjny wygląd to sposób na szczęście i sukces w życiu, że w relacjach społecznych najważniejsza jest korzyść zewnętrzna – realizacja celów przy minimum wysiłku, związki bez zobowiązań).

Oto destrukcyjne oblicze kultury cyfrowego narcyzmu. Skazuje ona jednostki na funkcjonowanie w patologicznym kontekście, prowadzącym do patologicznych konsekwencji, wśród których – za M. Szpunar – możemy wymienić m.in.: pozostawanie jednostki w stanie konfliktu samej ze sobą (dysonans między tym, co realne, a tym, co wyidealizowane, nieustanna walka o doskonały wizerunek), permanentny stan udręczenia przez niespełnienie, trwanie w stanie ciągłej niepewności, napięcia, w niewiedzy, co może przynieść jutro, kult samouwielbienia (selfizm – samoafirmacja i zapatrzenie w siebie, zaabsorbowanie własną fizycznością), niepohamowane odsłanianie się, zewnątrzsterowanie (życie w taki sposób, aby zyskać akceptację i aprobatę innych), obsesyjne pragnienie zostania gwiazdą (potrzeba życia w blasku sławy, życia, które zachwyca i wzbudza zainteresowanie, głód atencji ze strony innych, imperatyw absorbowania sobą uwagi innych), bezwzględność w działaniu, celebrowanie przedmiotów, kierowanie się wartościami umacniania *ja*, powierzchowność, upatrywanie sensu i istoty własnej egzystencji w konsumpcji i w nieustannym zaspakajaniu własnych zachcianek, zaburzenie umiejętności kształtowania zdrowych i efektywnych relacji z innymi (głęboki introwertyzm i nieumiejętność kontaktu z innymi staje się przejawem – według Alfreda Ledera – autyzmu w sensie kulturowym), przymus bycia nieustannie online (tzw. FOMO).

Istnieje też inny sposób rozumienia narcyzmu – nie jako patologii, ale jako stałej cechy (lub zbioru określonych cech), która w różnym nasileniu występuje bez wyjątku u każdego człowieka. To prowadzi niektórych badaczy do wniosku, że ma on też swój pozytywny (dojrzały) wymiar. A zatem narcyzm to nie tylko choroba – rozpatrywany jako całe spektrum (przy odpowiednim nasileniu cech), okazuje się także wyrazem zdrowia. Kultura narcyzmu staje się wtedy nie tyle destrukcyjna, ile ryzykowna. Daria Jezierska-Geburczyk zauważa, że to nowe określenie pozwala „mieć na uwadze → z a g r o ż e n i a [t. 4], jakie niesie ze sobą współczesna kultura w wyjaskrawianiu

cech narcystycznych, i jednocześnie dostrzegać jej nieradykalność – a nawet dopuszczać tkwiący w niej potencjał do umacniania zdrowego *ja*".

Sposobu odejścia od kultury cyfrowego narcyzmu można szukać – jak twierdzą Cesareo i Vaccarini – wśród ludzi zdefiniowanych jako *homo civicus*, czyli angażujących się w relacje społeczne i podejmujących zobowiązania, świadomych, że ich samorealizacja jest nieodzownie związana z umiejętnością tworzenia więzi międzyludzkich i przynależnością do grupy, a także z poczuciem solidarności i lojalności. Ograniczać przyrost zachowań narcystycznych może też wszechstronne kształcenie humanistyczne. Martha Nussbaum uważa, że „edukacja humanistyczna jest szansą na zbudowanie głębokich relacji międzyludzkich, a nie takich, które oparte są na manipulacji i instrumentalnym wykorzystaniu". Konieczne staje się więc rozumienie perspektywy drugiego człowieka, czyli wyobraźnia współczująca.

Emilia Musiał

E. Aboujaoude, *Wirtualna osobowość naszych czasów. Mroczna strona e-osobowości*, tłum. R. Andruszko, Wydawnictwo UJ, Kraków 2012; V. Cesareo, I. Vaccarini, *L'era del narcisismo*, Franco Angeli, Milano 2012; P. Ciołkiewicz, *„Brawo ja", czyli wszyscy jesteśmy narcyzami*, „Interdyscyplinarne Studia Społeczne" 2016, nr 1(1); M. Drabek, *Dominacja wzroku. Kryzys pisma po zwrocie wizualnym*, „Kultura –Historia – Globalizacja" 2010, nr 8; D. Jezierska-Geburczyk, *Zawodowy obraz siebie a obraz współczesnego narcyzm*u, „Kultura Współczesna" 2020, nr 1(108); T. Korulczyk, M. Korulczyk, *Narcystyczne cechy osobowości a inteligencja płynna*, „Studia z Psychologii w KUL" 2012, nr 18; Ch. Lasch, *Kultura narcyzmu. Amerykańskie życie w czasach malejących oczekiwań*, tłum. G. Ptaszek, A. Skrzypek, Wydawnictwo Akademickie „Sedno", Warszawa 2019; A. Lowen, *Narcyzm. Zaprzeczenie prawdziwemu Ja*, Agencja Wydawnicza Jacek Santorski & Co, Warszawa 1995; R. McCrae, *Trait Psychology and Culture: Exploring Intercultural Comparisons*, „Journal of Personality" 2001, iss. 69; M. Nussbaum, *Not For Profit: Why Democracy Needs the Humanities*, Princeton University Press, Princeton 2010; M. Rygielska, *Narcyzm po włosku albo digitambulicy i selfiści*, „Kultura Współczesna" 2020, nr 1(108); G. Sartori, *Homo videns. Telewizja i postmyślenie*, Wydawnictwo UW, Warszawa 2007; M. Szpunar, *Kultura cyfrowego narcyzmu*, Wydawnictwa AGH, Kraków 2016; taż, *Kultura narcystycznie skierowana*, „Kultura Sspółczesna" 2020, nr 1(108); taż, *Od narcyzmu jednostki do kultury narcyzmu*, „Kultura – Media – Teologia" 2014, nr 18; taż, *Od pierwotnej oralności do wtórnej piśmienności w epoce dominacji internetowego biasu*, „Zeszyty Prasoznawcze" 2014, t. 57, nr 4; B. Świątek, *Narcyzm jako źródło zaburzeń orientacji życiowych człowieka*, [w:] *Narcyzm. Jednostka, społeczeństwo, kultura*, J. Sieradzan (red.), Wydawnictwo Uniwersytetu w Białymstoku, Białystok 2011; Ł. Tomczyk, K. Potyrała, *Zjawisko selfie wśród nastolatków. Kontekst narcyzmu w dyskursie psychospołecznym, pedagogicznym i kulturowym*, „Kultura Współczesna" 2020, nr 1(108).

CYFROWY ŻOŁNIERZ – programy związane z opracowaniem tzw. systemów → ż o ł n i e r z a [t. 4] przyszłości (ang. *future soldier systems*) skupiające się głównie, chociaż nie wyłącznie, na zwiększeniu świadomości sytuacyjnej pododdziałów, a nawet pojedynczych żołnierzy przez zastosowanie systemów cyfrowych, przede wszystkim przez wprzęgnięcie żołnierzy w sieciocentryczne systemy zarządzania polem walki C4ISR, zgodnie z → k o n c e p c j ą d z i a ł a ń s i e c i o c e n t r y c z n y c h [t. 2].

Programy w tym zakresie prowadzone są od lat 90. XX w. i pewne rozwiązania, a nawet całościowe systemy zostały już przyjęte do wyposażenia niektórych sił zbrojnych. W większości przypadków założono jednak schemat rozwoju etapowego, więc wdraża się nie docelowe rozwiązania, ale pewne elementy, które wraz z modyfikacją bazy technicznej, zmieniającymi się wymaganiami i wnioskami z wykorzystania wdrożonych rozwiązań (także w warunkach bojowych) ulegają udoskonaleniu lub uzupełnieniu o inne części składowe.

U podstaw tworzenia rozwiązań cyfrowego żołnierza, oprócz potrzeby dogłębnej implementacji koncepcji → w o j n y s i e c i o c e n t r y c z n e j [t. 4] aż do poziomu pojedynczego żołnierza, legły uwarunkowania prowadzenia działań zbrojnych przede wszystkim przez zaawansowane technologicznie armie krajów zachodnich. W zdecydowanej większości przypadków są one złożone z żołnierzy zawodowych, którym należy zapewnić warunki skutecznego i możliwie bezpiecznego prowadzenia działań (chociażby ze względu na wysoki koszt wyszkolenia współczesnego żołnierza zawodowego oraz z uwagi na koszty polityczne, które ponoszą systemy militarne w przypadku wysokich strat własnych w ludziach, zwłaszcza w państwach demokratycznych). Ważnym czynnikiem jest dążenie do zapewnienia przewagi taktycznej nawet na najniższych poziomach prowadzenia walki, szczególnie w przypadku działań w ramach tzw. konfliktów asymetrycznych. W takich konfliktach rośnie znaczenie bezpośrednich działań realizowanych przez żołnierzy piechoty w bliskim kontakcie z nieprzyjacielem, odmiennie niż w przypadku konfliktów o dużej intensywności, gdzie decydujący wpływ na przebieg działań ma zastosowanie uzbrojenia pozwalającego razić przeciwnika z dystansu (lotnictwo, → a r t y l e r i a). Doszło też do zniwelowania różnic w zakresie wykorzystywanej → b r o n i s t r z e l e c k i e j, która zazwyczaj jest podobna w przypadku nowoczesnych armii oraz oddziałów militarnych o charakterze nieregularnym. Należy więc poszukiwać innych metod osiągnięcia taktycznej przewagi.

Co więcej, 2 kolejne czynniki wpływają na rosnącą rolę świadomości sytuacyjnej niewielkich pododdziałów i pojedynczych żołnierzy na współczesnym polu walki, chociaż są one równocześnie czynnikami znacznie utrudniającymi wdrożenie skutecznych systemów w tym zakresie. Pierwszym z nich jest rosnąca rola prowadzenia działań w warunkach miejskich. Szacuje się, że tereny zurbanizowane, charakteryzujące się dużym zagęszczeniem ludności (w tym → l u d n o ś c i c y w i l n e j [t. 3]) i istnieniem skomplikowanej infrastruktury, warunkującej charakter działań, będą areną ok. 80% obecnych i przyszłych konfliktów zbrojnych. Infrastruktura miejska jest tymczasem wyjątkowo nieprzejrzysta dla technicznych środków obserwacji. W sytuacji przebywania na tych terenach ludności cywilnej, w przypadku armii zachodnich, prowadzących działania zgodnie z wymogami → p o p r a w n o ś c i p o l i t y c z n e j [t. 3] i pod rosnącym wpływem przekazów medialnych, dochodzi czynnik dążenia do minimalizacji strat wśród owej ludności. Wyklucza to wykorzystanie np. zmasowanego ostrzału artyleryjskiego i zmusza do prowadzenia bezpośrednich starć

z wykorzystaniem spieszonej piechoty. Drugim czynnikiem jest trudność w ustaleniu statusu osób pojawiających się w przestrzeni bitewnej, szczególnie w rozróżnieniu między wrogimi bojownikami a ludnością cywilną (począwszy od tego, że często są to grupy wzajemnie przenikające się, a granica między nimi jest nieostra).

W skład większości systemów cyfrowego żołnierza wchodzą następujące podsystemy:

- Podsystem świadomości sytuacyjnej i transmisji danych. Na wdrożenie rozwiązań w tym zakresie jest obecnie ukierunkowana większość rozwiązań żołnierza przyszłości. Odpowiada on za przekazywanie → i n f o r m a c j i [t. 2] o lokalizacji własnej, własnych oddziałów oraz oddziałów przeciwnika oraz o zadaniach własnych i innych własnych jednostek. Kluczowym problemem do rozwiązania jest odpowiednia selekcja i dystrybucja informacji, tak by nie doszło do → p r z e c i ą ż e n i a i n f o r m a c y j n e g o [t. 3] oraz by odpowiedni zakres informacji znalazł się na poszczególnych szczeblach dowodzenia. Wyzwaniem jest również zaprojektowanie intuicyjnego, łatwego w obsłudze interfejsu takiego systemu, by nie absorbował on zanadto żołnierza. Chodzi przy tym zarówno o odczytywanie, jak i wprowadzanie danych. Coraz częściej wykorzystuje się w tym celu rozwiązania komercyjne, w postaci smartfonów lub niewielkich tabletów, umieszczonych na nadgarstku lub klatce piersiowej (np. smartfon Samsung Galaxy Note II w amerykańskim systemie Nett Warrior). Postęp w zakresie komercyjnych rozwiązań w tej dziedzinie jest bowiem niezwykle szybki, a żołnierze są oswojeni z obsługą urządzeń, z którymi spotykają się w życiu codziennym. Kluczowe znaczenie z wojskowego punktu widzenia ma z kolei nie *hardware*, który z łatwością można zastąpić nowocześniejszym rozwiązaniem w miarę postępu technicznego, ale oprogramowanie i integracja całego systemu. Interfejs jest zazwyczaj uzupełniony zestawem słuchawkowym, często integrującym również aktywne ochronniki słuchu, oraz – w niektórych rozwiązaniach – wyświetlaczem nahełmowym, pozwalającym np. na wyświetlanie map i pełniącym równocześnie funkcję noktowizora. Coraz częściej przybiera on formę specjalnych okularów pracujących w trybie tzw. rzeczywistości rozszerzonej, integrującej obraz rzeczywisty z obrazami elektronicznymi. Tego typu działania mają rozwiązać problemy z adaptacją wzroku żołnierzy w sytuacji przejścia z obserwacji rzeczywistego obrazu na obserwację danych wirtualnych.
  Do transmisji danych wykorzystuje się z kolei specjalistyczne radiostacje wojskowe (w tym lekkie radiostacje osobiste będące na wyposażeniu każdego żołnierza), najczęściej nowoczesne radiostacje programowalne. Odpowiadają one nie tylko za transmisję fonii, ale również – co jest kluczowe w systemach cyfrowego żołnierza – za przekazywanie różnorodnych danych, np. danych syntetycznych (informacji taktycznych w formie wykresów czy znaków, danych o położeniu pozyskiwanych z podsystemu pozycjonowania w formie np. mapy cyfrowej), obrazów i plików wideo, komunikatów w formie pisemnej.

Elementem systemu zwiększenia świadomości sytuacyjnej stają się coraz częściej doręczne systemy identyfikacji swój–obcy (IFF, Identification Fried or Foe), przede wszystkim w postaci lekkich transponderów, odpowiadających zakodowanym sygnałem na zapytanie wysyłane przez interrogator. Planuje się także zastąpienie systemów łączności opartych na propagacji fal radiowych systemami działającymi na zasadzie przesyłania wiązki światła.

- Podsystem pozycjonowania. Dwoma zasadniczymi funkcjami systemu pozycjonowania są ustalenie własnej pozycji oraz jej transmisja do sieciocentrycznego systemu zarządzania polem walki. Do ustalenia własnej pozycji stosuje się systemy nawigacji, przede wszystkim satelitarnej (amerykański GPS, europejski Galileo, rosyjski Glonass oraz chiński Beidou). Ze względu na możliwość względnie łatwego zakłócenia nawigacji satelitarnej oraz zaburzony dostęp do sygnału w niektórych obszarach coraz częściej są one uzupełniane komplementarnymi systemami nawigacyjnymi, np. bezwładnościowymi.
- Podsystem współpracy z systemami bezzałogowymi. Systemy bezzałogowe są elementem sprzyjającym budowie świadomości sytuacyjnej w systemach cyfrowego żołnierza. Przede wszystkim chodzi o bezpilotowe aparaty latające najniższego szczebla (np. brytyjsko-norweski Black Hornet o masie zaledwie 18 gramów i promieniu działania 1,6 km lub nieco większy 600-gramowy amerykański SQ-4 Recon). Funkcje rozpoznawcze mogą też wypełniać niewielkie roboty lądowe, np. Recon Scout – może on być wrzucany do pomieszczeń, które ma spenetrować. W dalszej perspektywie planowane jest zastosowanie na większą skalę systemów bezzałogowych do realizacji innych zadań. Chodzi w pierwszej kolejności o zadania logistyczne. Przykładami rozwiązań są m.in. rozwijany w ramach programu Future Combat Systems, lecz anulowany w 2009 r. kołowy pojazd bezzałogowy XM1217, pojazd SMSS Ox 1, służący zarówno jako środek transportu sprzętu dla spieszonej drużyny piechoty, jak i stacja ładowania używanych przez żołnierzy baterii, czy też czworonożny Big Dog rozwijany przez firmę Boston Dynamics pod auspicjami DARPA (Defense Advanced Research Projects Agency). Rozwijane są również systemy do zadań bojowych. Niektóre, jak amerykański TALON SWORDS, są już stosowane operacyjnie, ale ze względu na ograniczoną autonomię ich użyteczność sprowadza się do realizacji stosunkowo prostych zadań, np. dozorowania.
- Podsystem energetyczny. Wszystkie systemy elektroniczne wymagają źródeł energii do pracy. Obecnie są to głównie akumulatory. Co prawda prowadzi się prace nad zwiększeniem ich efektywności (np. zastąpienie akumulatorów litowo-jonowych litowo-siarkowymi, co ma zwiększyć tzw. gęstość energetyczną, czyli ilość energii zmagazynowaną w określonej objętości lub masie), ale pewne cechy ograniczają ich użyteczność. Chodzi przede wszystkim o konieczność ich regularnego ładowania. Z tego względu rozwijane są inne źródła energii, niemające jednak

zastąpić akumulatorów, lecz je uzupełnić. Przykładami takich rozwiązań są niewielkie rozkładane panele słoneczne oraz wykorzystanie efektu pizoelektrycznego (specjalny układ umieszczony w butach żołnierza wytwarza prąd pod wpływem naprężeń wywołanych chodzeniem).

- Podsystem uzbrojenia. Pierwsze rozwiązania cyfrowego żołnierza koncentrowały się wokół wprowadzenia nowatorskich rozwiązań w zakresie indywidualnej broni żołnierza. Przykładem może być amerykański program Future Combat Systems, w ramach którego rozwijano broń XM29 Objective Individual Combat Weapon, integrującą karabinek kalibru 5,56 mm oraz granatnik kalibru 20 mm wystrzeliwujący amunicję programowalną za pomocą zaawansowanego systemu kierowania ogniem. Obecnie rezygnuje się z rozwoju tego typu futurystycznych rozwiązań. Okazały się one nieporęczne na polu walki ze względu na znaczną masę i rozmiary, często również pękate kształty, utrudniające precyzyjne operowanie bronią. Tego typu systemy są również kosztowne, zarówno w zakupie, jak i w eksploatacji (droga amunicja precyzyjna). W zamian postępuje rozwój klasycznej broni strzeleckiej, jednak zazwyczaj w ramach osobnych programów, niezwiązanych ściśle z programami cyfrowego żołnierza. Elementem łączącym te programy z rozwojem broni strzeleckiej jest rozwój akcesoriów mocowanych na broni, w tym celowników dzienno-nocnych, które dzięki wyposażeniu w dalmierze laserowe oraz komputery balistyczne zaczynają odgrywać rolę indywidualnych systemów kierowania ogniem. Co więcej, niektóre rozwiązania łączą się z urządzeniami rozwijanymi w ramach programów cyfrowego żołnierza, pozwalając na transmisję obrazu do innych elementów wyposażenia żołnierza (np. transmisja obrazu z celownika wychylonego razem z bronią zza przeszkody do wyświetlacza nahełmowego żołnierza) oraz za pośrednictwem systemu transmisji danych do → sieciocentrycznego systemu zarządzania walką [t. 4].
- Ważnym elementem pozostaje za to rozwój lekkiej broni wsparcia, możliwej do przenoszenia przez pojedynczego żołnierza i zwiększającej siłę ognia pododdziału. Do tego rodzaju broni należą lekkie modułowe wyrzutnie pocisków, przeznaczone do neutralizacji siły żywej oraz celów nieopancerzonych i lekko opancerzonych. Do konstrukcji tego typu należą francuski Enforcer o masie całkowitej 9 kg, kalibrze 86 mm i zasięgu 2 km, a także amerykański NAVAIR Spike o masie 4,5 kg, kalibrze 57 mm i zasięgu 3,2 km. Stosunkowo niewielka siła rażenia tego typu broni, wynikająca z ograniczonej masy głowicy bojowej, niwelowana jest przez system precyzyjnego naprowadzania. Innym rozwiązaniem jest amunicja krążąca, która służy zarówno za lekki i możliwy do przenoszenia przez pojedynczego żołnierza substytut amunicji artyleryjskiej, jak i za system rozpoznawczy, ze względu na możliwość przebywania przez dłuższy czas w powietrzu nad pozycjami nieprzyjaciela.
- Podsystem osłony. Obejmuje on zarówno klasyczną pasywną ochronę balistyczną (w tym przypadku wyzwaniem jest redukcja jej masy przy zachowaniu poziomu

ochrony), środki ochrony przed skażeniami, jak i systemy redukujące możliwość otrzymania trafienia – przede wszystkim chodzi o akustyczne detektory strzału.

- Podsystem umundurowania i oporządzenia. Rozwój umundurowania, przede wszystkim w zakresie zastosowania odpowiednich materiałów (zapewniających odpowiedni mikroklimat w trudnych warunkach pogodowych i coraz częściej cechujących się niepalnością), ergonomicznego kroju oraz nowych wzorów kamuflażu postępuje nieustannie pod wpływem doświadczeń z najnowszych konfliktów zbrojnych. Nowe rozwiązania w tej dziedzinie mogą być zarówno elementem programów cyfrowego żołnierza, jak i być rozwijane niezależnie od nich. Elementem silnie powiązanym z tymi programami jest oporządzenie, gdyż poza dotychczasowymi funkcjami (przenoszenie wyposażenia oraz ochrona balistyczna) powinno być ono zaprojektowane pod kątem wygodnego przenoszenia elementów systemu (np. radiostacji, źródeł energii, urządzeń wchodzących w skład interfejsu). Projekt oporządzenia musi uwzględniać też takie niuanse jak przebieg okablowania systemu cyfrowego żołnierza – przewody nie mogą blokować systemu zrzutu kamizelki w sytuacji awaryjnej.
- Podsystem monitorowania stanu żołnierza. Przeznaczony do ciągłej diagnozy stanu zdrowia żołnierza i gotowości do wykonywania przez niego zadań. Służą do tego biosensory, np. zakładane do uszu i mierzące istotne parametry, jak temperatura ciała czy tętno. W Module Monitorowania Życia, rozwijanym w ramach polskiego programu Tytan, stelażem dla sensorów są szelki lub koszulka. Informacja na temat kondycji żołnierza transmitowana jest do sieciocentrycznego systemu zarządzania polem walki, dzięki czemu pomoc będzie docierała w pierwszej kolejności do najciężej rannych. W przypadku śmierci żołnierza system będzie generował sygnał dezaktywacji, co doprowadzi do skasowania informacji przechowywanych przez urządzenia elektroniczne przenoszone przez żołnierza (np. map, kodów komunikacyjnych, śladu GPS). W bardziej futurystycznych rozwiązaniach planuje się zastosowanie mundurów, które nie tylko będą monitorować funkcje życiowe żołnierza, ale również będą w stanie automatycznie założyć mu opaskę uciskową lub podać lek.
- Podsystem wsparcia mobilności. Ze względu na rosnącą masę wyposażenia przenoszonego przez żołnierza, która zmniejsza jego efektywność oraz może prowadzić do kontuzji i urazów, dąży się do wyposażenia żołnierzy w egzoszkielety, które pozwalają przenosić większy ciężar. Do rozwiązań tego typu należy amerykański HULC (Human Universal Load Carrier) o masie 23 kg, pozwalający przenosić obciążenie nawet do 90 kg, czy francuski Hercules. Egzoszkielety nie wymagają sterowania, lecz samoczynnie dostosowują się do ruchów ludzkiego ciała. Rozwiązania tego typu są rozlicznie testowane, jednak nie doszło do ich wdrożenia na większą skalę. Co prawda nowoczesne egzoszkielety w coraz mniejszym stopniu krępują ruchy, ale nierozwiązaną kwestią jest zaopatrzenie ich w zapas energii pozwalający działać przez

dłuższy czas (np. wspomniany Hercules pozwala na pokonanie zaledwie 20 km) oraz w sytuacji utraty zasilania lub uszkodzenia elementów systemu.

- Inne. Wśród ciekawych i bardzo przydatnych rozwiązań znajdują się np. doręczne translatory, pozwalające na komunikację z ludnością cywilną w regionie operacji.

W rozwoju systemów cyfrowego żołnierza przodują Amerykanie. Od lat 90. XX w. do 2007 r. realizowany był program Land Warrior, od 2010 r. prowadzony jest zaś jego następca – Nett Warrior (nazwa pochodzi od płk R.B. Netta, odznaczonego podczas II wojny światowej Medalem Honoru). Nowy system jest lżejszy od poprzedniego, sprawniejszy pod względem informatycznym (m.in. szybszy procesor, więcej pamięci operacyjnej), działa dłużej na bateriach, w większym stopniu wykorzystuje rozwiązania komercyjne oraz charakteryzuje się większą modułowością, rozumianą jako możliwość rozmaitej konfiguracji z uwzględnieniem wymagań danej misji. Głównym założeniem przy jego opracowaniu, wynikającym z wniosków z użytkowania poprzedniego systemu, była konieczność ograniczenia oddziaływania na użytkownika, czyli spieszonego żołnierza. Ograniczenie to dotyczy nie tylko konieczności zredukowania masy i wymiarów systemu, ale także unikania rozpraszania uwagi obsługą systemu, tak by przyspieszał on, a nie spowalniał podejmowanie decyzji.

Sercem systemu jest oprogramowanie, a sprzęt jest częściowo oparty na rozwiązaniach dostępnych „z półki". Przykładem jest tzw. EUD (End User Device), którym jest komercyjny smartfon. Wykorzystuje on specjalne oprogramowanie Android Tactical Assault Kit, pozwalające na odbieranie i wysyłanie informacji za pomocą zabezpieczonych, kodowanych kanałów transmisji danych (w tym obrazów i materiałów audiowideo), wyświetlanie podręcznej mapy z zamieszczonymi informacjami taktycznymi, wyświetlanie informacji na temat otoczenia i warunków walki. Smartfon jest mocowany z przodu kamizelki ochronnej w wodo- i pyłoochronnym etui, co pozwala na szybki dostęp do urządzenia i korzystanie z niego bez potrzeby odkładania broni. EUD połączony jest z baterią noszoną na bocznym panelu kamizelki ochronnej oraz z radiostacją osobistą służącą do transmisji danych, przenoszoną na plecach.

Wśród innych rozwiązań w tym zakresie można wymienić programy takie jak rosyjski Ratnik, francuski Felin (Fantassin à Équipement et Liaisons Intégrés), brytyjski FIST (Future Integrated Soldier Technology), niemiecki IdZ-ES (Infanterist der Zukunft Erweitertes System), szwajcarski IMES, izraelski Dominator. W Polsce realizowany jest program Zintegrowany Indywidualny System Walki Tytan, lecz notuje on duże opóźnienie.

Rafał Kopeć

M. Dąbrowski, *Jest czy może dopiero będzie? Program żołnierza przyszłości*, „Nowa Technika Wojskowa" 2018, nr 3; *Designing Soldier Systems: Current Issues in Human Factors*, P. Savage-Knepshield (ed.), Ashgate Publishing Group, Farnham–Burlington 2012; Ł. Kamieński, *Nowy wspaniały żołnierz. Rewolucja biotechnologiczna i wojna w XXI wieku*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2014; R. Kopeć, *Cyfrowy żołnierz*, [w:] *Vademecum*

bezpieczeństwa informacyjnego, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; Nett Warrior: Initial Operational Test and Evaluation (IOT&E) Report, 2015; I.R. Porche III, C. Paul, C.S. Serena i in., *Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below*, Rand Corporation, Santa Monica 2017.

CYRKON – rosyjski hipersoniczny → p o c i s k m a n e w r u j ą c y [t. 5] przeznaczony do niszczenia okrętów nawodnych i celów znajdujących się na lądzie. Pod pewnymi względami przypomina amerykański pocisk manewrujący Tomahawk, jednak jest znacznie szybszy. Może osiągać prędkość do 9 Ma i zniszczyć cele w promieniu 1 tys. km. Może być wystrzeliwany z okrętów zarówno nawodnych, jak i podwodnych. W 2018 r. podczas prezentacji nowej generacji broni strategicznej prezydent Władimir Putin określił Cyrkon i inne pociski hipersoniczne jako systemy, za pomocą których Rosja może uderzyć w niemal każdy punkt na świecie i omijać amerykańską tarczę antyrakietową. Lot Cyrkonu składa się z 2 części. W pierwszym etapie wykorzystywane jest paliwo stałe, które umożliwia podniesienie się rakiety na wyższy pułap (30–40 km) oraz jej przyśpieszenie. W drugim uruchamiany jest silnik scramjet (strumieniowy) umożliwiający poruszanie się z prędkością naddźwiękową.

Do 2022 r. Cyrkon nie został przedstawiony (przetestowany) jako pocisk zdolny do przenoszenia głowic atomowych, podobnie jak to było w wypadku UGM-109A TLAM-N Tomahawk. Zdaniem części obserwatorów nie jest wykluczone, że w przyszłości może to się wydarzyć. Przypuszcza się również, że prowadzone są prace mające na celu dostosowanie samolotu Tupolew Tu-160/M/M2 oraz mobilnych wyrzutni rakiet przybrzeżnych Bastion do przenoszenia pocisku. Cyrkon kierowany jest przez połączenie nawigacji bezwładnościowej oraz GPS. Powszechnie dostępne →i n f o r m a c j e [t. 2] wskazują jednak, że próby przeprowadzane w latach 2020–2021 odbywały się wyłącznie z okrętów nawodnych i podwodnych. W 2021 r. 2 rakiety Cyrkon odpalone zostały z okrętu podwodnego Siewierodwińsk (okręt klasy Jasień). Pierwsza z nich została wystrzelona, kiedy okręt pozostawał na powierzchni, druga w czasie zanurzenia 40 m pod wodą. Według źródeł rosyjskich próba zakończona została sukcesem. Kolejna podejście przeprowadzono z wykorzystaniem nowej fregaty Admirał Gorszkow, wchodzącej w skład Floty Północnej. Pocisk trafił wówczas w cel na Morzu Barentsa oddalony o 45 km, osiągnął prędkość 5,7 tys. km/h. Maksymalna wysokość lotu wyniosła 28 km, a czas – 4,5 min.Pociski Cyrkon w czasie → k o n f l i k t u z b r o j n e g o [t. 5] mają być wykorzystane przede wszystkich do niszczenia okrętów wojskowych. Biorąc pod uwagę ich prędkość, brytyjskie lub amerykańskie okręty miałby prawdopodobnie mniej niż 5 min na namierzenie i przechwycenie zagrożenia. Systemy, jakimi dysponowały kraje anglosaskie do 2022 r., nie były przygotowane do zwalczania celów poruszających się na takiej wysokości z tak dużą prędkością. W z związku z powyższym konieczne jest opracowanie broni defensywnej umożliwiającej skuteczną obronę.

Do wybuchu → w o j n y [t. 4] z Ukrainą Rosji nie udało się wprowadzić do służby Cyrkonów. Dostawy pocisków do baz → m a r y n a r k i w o j e n n e j [t. 3] rozpoczęły się w grudniu 2022 r. Siergiej Szojgu na posiedzeniu kolegium resortu obrony narodowej 21 grudnia 2022 r. podkreślił, że fregata Admirał Gorszkow jest gotowa do wyjścia w swój pierwszy rejs na wody oceanu światowego z pociskami Cyrkon na pokładzie. Obok wielu opinii ostrzegających przed nową rosyjską → b r o n i ą h i p e r s o n i c z n ą [t. 1] pojawiły się również analizy podważające jej skuteczność. Sidharth Kaushal – ekspert ds. walki morskiej w brytyjskim ośrodku badawczym Royal United Services Institute (RUSI) – podkreślił, że nie należy wyolbrzymiać znaczenia Cyrkonu. Jego zdaniem obiekty poruszające się z prędkością hipersoniczną, czyli 5 Ma i więcej, jonizują powietrze wokół siebie, co blokuje docierające sygnały radarowe. Utrudnia to w fazie końcowej lotu skanowanie terenu i namierzanie celu. Aby namierzyć cele ruchome, jakimi są okręty nawodne, pocisk będzie musiał zwolnić do prędkości znacznie mniejszej niż hipersoniczna (2,5 Ma), co z kolei zwiększa szanse na jego zniszczenie. Ponadto w przeciwieństwie do innych przeciwokrętowych pocisków manewrujących, które poruszają się z prędkością naddźwiękową nisko nad powierzchnią wody, Cyrkon wznoszony jest na wysokość ok. 20 km. Jest to konieczne, aby jego silnik mógł zacząć działań i osiągać prędkość hipersoniczną. Lot na takie wysokości sprawia jednak, że będzie on lepiej widoczny dla radarów.

Tomasz Wójtowicz

J. Hruby, *Hypersonic Delivery Systems*, Nuclear Threat Initiative 2019, https:// www.jstor.org/stable/pdf/resrep19984.8.pdf (dostęp 16.03.2022); M. Kucharczyk, *„Mrożący krew w żyłach" rosyjski Cyrkon. Kolejna hiperbroń przesady*, 12.10.2021, https://wiadomosci.gazeta.pl/wiadomosci/7,114881,27677847,mrozacy-krew-wzylach-rosyjski-cyrkon-kolejna-hiperbron-przesady.html (dostęp 16.03.2022); *Analysis: Russia Hypersonic Missile Tsirkon New Threat for Ukraine?*, 24.01.2023, https://www.navyrecognition.com/index.php/focus-analysis/naval-technology/ 12737-analysis-russia-hypersonic-missile-tsirkon-a-new-threat-for-ukraine.html? utm_content=cmp-true (dostęp 1.05.2023); *Hipersoniczne Cyrkony wystrzelone z okrętów podwodnych*, 31.12.2021, https://defence24.pl/sily-zbrojne/hipersoniczne-cyrkony-wystrzelone-z-okretow-podwodnych (dostęp 1.05.2023); *Rosja testuje hipersonicznego Cyrkona*, 7.10.2022, https://defence24.pl/technologie/ rosja-testuje-hipersonicznego-cyrkona (dostęp 1.05.2023); A.M. Maciejewski, *Seryjne hipersoniczne pociski przeciwokrętowe Cyrkon w linii*, 3.01.2023, https://zbiam.pl/seryjne-hipersoniczne-pociski-przeciwokretowe-cyrkon-w-linii/ (dostęp 1.05.2023); M. Peck, *Retoryka Kremla nie zmieni praw fizyki. Niezwyciężony pocisk Putina ma pospolity problem*, 22.02.2023, tłum. M. Albin, https://businessinsider. com.pl/wiadomosci/putin-niezmieni-praw-fizyki-jego-superpocisk-ma-typowyproblem/zemyed2 (dostęp 1.05.2023).

CZYNNOŚCI DOCHODZENIOWO-ŚLEDCZE – różnokierunkowe czynności procesowe wykonywane głównie przez policję w celu uzyskania wszelkich → i n f o r m a c j i [t. 2] o przestępstwach i przestępcach. Ukierunkowane na zatrzymanie sprawców, są prowadzone w pierwszym stadium procesu karnego w postępowaniu przygotowawczym.

Proces karny reguluje przewidziane prawem zachowanie organów państwowych i pozostałych uczestników zmierzające do wykrycia i ustalenia → c z y n u z a b r o n i o n e g o [t. 1], jego sprawcy, a także do wymierzenia kary, uniewinnienia oskarżonego bądź zastosowania innych środków. Cele postępowania karnego zostały określone w Kodeksie postępowania karnego. Proces karny ma rozstrzygnąć o przedmiocie procesu, którym jest ustalenie, czy rzeczywiście został naruszony przepis prawa karnego materialnego, a także zastosowanie środków przewidzianych w prawie karnym lub ich niezastosowanie w wypadku osoby niewinnej. Ponadto w postępowaniu karnym należy chronić interesy pokrzywdzonego z jednoczesnym poszanowaniem jego godności, a sprawa powinna być rozstrzygnięta w terminie bez zbędnej zwłoki.

Przedmiotem postępowania karnego jest kwestia odpowiedzialności karnej osoby za zarzucany jej czyn, który stanowi przestępstwo będące zbrodnią albo występkiem. Na podstawie przepisów zawartych w Kodeksie karnym można sformułować definicję przestępstwa. Jest to czyn zabroniony pod groźbą kary przez ustawę obowiązującą w czasie jego popełnienia, zawiniony i szkodliwy społecznie w stopniu wyższym niż znikomy. Czyn zabroniony zostaje uznany za przestępstwo tylko w sytuacji, gdy wszystkie wymienione elementy występują łącznie. Podstawowym źródłem prawa jest Kodeks postępowania karnego, dodatkowo przepisy procesowe zawarte są w innych ustawach i ustawach szczególnych, rozporządzeniach wykonawczych, przepisach ustrojowych, zarządzeniach, decyzjach i wytycznych. Szczegółowy podział i zakres ich wykonywania został uregulowany w wytycznych Komendanta Głównego Policji w sprawie wykonywania niektórych czynności dochodzeniowo-śledczych przez policjantów. Wytyczne uwzględniają:

- przyjęcie zawiadomienia o przestępstwie,
- prowadzenie postępowania sprawdzającego,
- postępowanie w niezbędnym zakresie w celu zabezpieczenia śladów i dowodów przestępstwa przed ich utratą, zniekształceniem lub zniszczeniem,
- wydanie postanowienia o wszczęciu dochodzenia,
- czynności dowodowe,
- przesłuchanie świadka,
- przedstawienie zarzutów i przesłuchanie podejrzanego,
- zebranie danych o podejrzanym,
- oględziny miejsca, osoby i rzeczy,
- eksperyment procesowy,
- zatrzymanie rzeczy i danych informatycznych,
- przeszukanie osoby, miejsca, urządzenia zawierającego dane informatyczne i systemu informatycznego,
- powołanie biegłych, specjalistów i tłumaczy,
- konfrontację,
- okazanie,

- środki przymusu w postępowaniu przygotowawczym,
- przedłużenie okresu prowadzenia i zawieszenie postępowania,
- wyłączanie materiałów i łączenie postępowań,
- zamknięcie postępowania, zakończenie postępowania przeciwko osobie,
- umorzenie postępowania,
- postępowanie zażaleniowe,
- podjęcie na nowo i wznowienie postępowania.

Zawiadomienia o przestępstwie przyjmuje się od każdej osoby, która dowiedziała się o popełnieniu przestępstwa ściganego z urzędu. Obowiązek ten ma charakter społeczny, jednakże powinien wynikać z poczucia odpowiedzialności, uczciwości i odpowiedniej reakcji na wyrządzaną krzywdę. Przyjmując zawiadomienie w sprawach o przestępstwa o charakterze seksualnym, należy ograniczyć się do uzyskania najistotniejszych faktów i dowodów. Policjant może odstąpić od sporządzenia protokołu przyjęcia ustnego zawiadomienia o przestępstwie, jeżeli z wypowiedzi ustnej wynika, że nie dokonano czynu zabronionego. W trakcie wykonywania czynności procesowej może być obecna osoba wskazana przez pokrzywdzonego, jeżeli jej udział nie uniemożliwia i nie utrudnia przyjęcia zawiadomienia. Wymienionej czynności może również dokonać sam sprawca, a także małoletni. Osoba składająca zawiadomienie o przestępstwie jest informowana m.in. o odpowiedzialności karnej za powiadomienie organów ścigania o niepopełnionym przestępstwie, za fałszywe oskarżenie oraz za składanie fałszywych zeznań. W wypadku małoletnich procedura obejmuje: poinformowanie o mówieniu prawdy dzieci, jeżeli osoba nie ukończyła 17 lat, uprzedzenie o treści artykułów Kodeksu karnego. W sytuacji zgłoszenia się osoby niewładającej językiem polskim protokół sporządza się z udziałem tłumacza.

Postępowanie sprawdzające stanowi formę oficjalnych czynności przedprocesowych podejmowanych przez organy dochodzeniowo-śledcze przed wszczęciem postępowania przygotowawczego. W wypadku niewystarczających informacji umożliwiających wszczęcie postępowania można wykonać czynności o charakterze weryfikacyjnym. Polegają one na zarejestrowaniu rozmów, wywiadów i sporządzeniu innych dokumentów w formie notatek. Jedyną czynnością procesową jest przyjęcie ustnego zawiadomienia o przestępstwie lub wniosku o ściganie oraz przesłuchanie w charakterze świadka osoby zawiadamiającej. Postępowanie musi zakończyć się przed upływem 30 dni od otrzymania zawiadomienia. Czynności kończą się wszczęciem lub odmową wszczęcia postępowania przygotowawczego. Postępowanie w niezbędnym zakresie wykonuje się sytuacji niecierpiącej zwłoki, szczególnie gdy zachodzi potrzeba zabezpieczenia śladów i dowodów przestępstwa przed ich utratą, zniekształceniem lub zniszczeniem. W takiej sytuacji czynności procesowe można wykonać jeszcze przed wydaniem postanowienia o wszczęciu dochodzenia lub śledztwa. Prowadzący może dokonać oględzin, w razie potrzeby z udziałem biegłego, przeszukania oraz czynności wobec osoby podejrzanej. Prowadzący może również przesłuchać osobę podejrzaną

o popełnienie przestępstwa przed wydaniem postanowienia o przedstawieniu zarzutów, jeżeli zachodzą warunki umożliwiające sporządzenie takiego postanowienia. W sprawach wymagających prowadzenia śledztwa konieczne jest w ciągu 5 dni wydanie postanowienia o przedstawieniu zarzutów albo, w razie braku warunków pozwalających na jego sporządzenie, o umorzeniu postępowania w stosunku do osoby przesłuchanej.

Wszczęcie postępowania przygotowawczego następuje obligatoryjnie, gdy chodzi o czyn zabroniony ścigany z urzędu. Jeżeli okoliczności zdarzenia wskazują, że zostało popełnione przestępstwo, fakt ten przesądza o podstawie faktycznej wszczęcia postępowania. Jeśli istnieje uzasadnione podejrzenie popełnienia czynu zabronionego, powstaje podstawa prawna tej czynności. Postanowienie o wszczęciu postępowania zawiera: oznaczenie organu wydającego postanowienie, datę wydania, okoliczności faktyczne należące do znamion przestępstwa, wartość przedmiotu przestępstwa albo szkody wyrządzonej lub grożącej, czas i miejsce popełnienia przestępstwa oraz osobę pokrzywdzoną, rozstrzygnięcie z podaniem podstawy prawnej, ewentualnie uzasadnienie. Postanowienie o wszczęciu dochodzenia wydaje się również w wypadku podjęcia na nowo dochodzenia wcześniej umorzonego. W szczególnych sytuacjach, gdy liczba nieustalonych pokrzywdzonych jest duża, a ustalenie ich wiąże się z trudnościami, można przekazać ogłoszenie w prasie, radiu, telewizji lub internecie. Organ prowadzący postępowanie dowodowe przeprowadza czynności z urzędu albo na wniosek stron. W postępowaniu przygotowawczym należy ustalić, czy na miejscu zdarzenia były obecne osoby, czy odnaleziono przedmioty związane z przestępstwem, czy ujawniono inne ślady przestępstwa. Określone czynności wymagają sporządzenia protokołu, w wypadku innych można ograniczyć się do sporządzenia notatki urzędowej. Środki dowodowe utrwala się przez wykonanie szkiców, zdjęć, nagrań, odlewów gipsowych, przeniesienie odcisków linii papilarnych, przesłuchanie świadków lub podejrzanego. Każdy środek dowodowy musi zostać poddany ocenie, aby mógł stanowić dla organów ścigania podstawę wnioskowania. W związku z powyższym wyodrębnia się etapy dowodzenia: ujawnienie dowodów, zabezpieczenie procesowe lub techniczne, sprawdzenie i ocenę przydatności dowodu w postępowaniu przygotowawczym.

Jeśli można wskazać świadków zdarzenia, następuje ich przesłuchanie. Świadek stanowi osobowe źródło dowodowe. Podczas przesłuchania przekazuje niezbędne informacje, dostarczając tym samym środka dowodowego w postaci zeznań. Na podstawie przekazanych faktów organy niejednokrotnie podejmują określone czynności procesowe. W wyniku zeznania świadka organ procesowy może podejmować stosowne decyzje o innych osobach. Świadkiem może być każda osoba bez względu na wiek i stan psychiczny czy fizyczny. Świadka obejmują obowiązki procesowe, przede wszystkim mówienie prawny i niezatajanie jej, obowiązek stawiennictwa i poddania się badaniom lub oględzinom lekarskim. Świadek ma również uprawnienia, szczególnie odmowy składania zeznań, nieodpowiadania na niektóre pytania, prawo do

przesłuchania z wyłączeniem jawności, wnioskowania o zwolnienie od zeznawania i wzmożoną ochronę prawną. Przed pierwszym przesłuchaniem przesłuchujący poucza świadka o jego uprawnieniach i obowiązkach. Podczas wykonywania czynności z udziałem świadka należy przestrzegać procedur zapewniających zachowanie w tajemnicy miejsca jego zamieszkania lub miejsca pracy – anonimizacja danych.

Przedstawienie zarzutów wobec podejrzanego jest momentem, od którego postępowanie przygotowawcze kierowane jest przeciwko tej osobie.

Wydanie i ogłoszenie postanowienia o przedstawieniu zarzutów umożliwia przesłuchanie konkretnej osoby w charakterze podejrzanego. Postanowienie powinno zawierać: dane podejrzanego, dokładne określenie zarzucanego czynu, kwalifikację prawną. Po jego sporządzeniu należy ogłosić treść postanowienia podejrzanemu, następnie należy pouczyć podejrzanego o prawie żądania uzasadnienia przedstawionych zarzutów. Po przesłuchaniu podejrzanego w toku dalszych czynności mogą wystąpić okoliczności, na podstawie których należy dokonać zmiany lub uzupełnienia przedstawionych zarzutów. Podejrzany ma prawo do obrony, składania wyjaśnień i ich odmowy, wniosków dowodowych oraz uczestnictwa w czynnościach procesowych. Podejrzany jest również zobowiązany do stawiennictwa, poddania się oględzinom zewnętrznym ciała, pobrania odcisków, sfotografowania, pobrania wymazu ze śluzówki policzków, a jeżeli jego zachowanie podczas przesłuchania nasuwa uzasadnioną wątpliwość co do jego poczytalności – poddania badaniom psychologicznym i psychiatrycznym. Zebranie danych o podejrzanym należy rozpocząć niezwłocznie po wydaniu w stosunku do niego postanowienia o przedstawieniu zarzutów. W ramach gromadzenia danych o podejrzanym prowadzący postępowanie ustala rodzaj majątku ruchomego i nieruchomego podejrzanego, rodzaj i wielkość zobowiązań na rzecz innych osób, instytucji lub przedsiębiorców, szczególnie z tytułu alimentów, rent, pożyczek, kredytów, należności podatkowych lub ubezpieczeniowych.

Przeprowadzenie oględzin miejsca, osoby lub rzeczy ma na celu ujawnienie i zabezpieczenie śladów przestępstwa bądź ich nośników znajdujących się na miejscu zdarzenia, osobie lub rzeczy, które mogą mieć związek z zaistniałym przestępstwem. Zabezpieczone ślady mają służyć jako źródła dowodowe w toku prowadzonego postępowania przygotowawczego. W kwestii oględzin miejsca zdarzenia procedura polega na dokonaniu czynności taktycznych i techniczno-kryminalistycznych zmierzających do rozpoznania przebiegu zdarzenia. Z przeprowadzonych oględzin miejsca zdarzenia sporządza się protokół i stosowną dokumentację techniczną i dodatkową. W protokole oględzin dokumentuje się zastany stan miejsca, osoby lub rzeczy, opisując umiejscowienie ujawnionych śladów przestępstwa, ich nośników oraz rzeczy mogących mieć związek z danym zdarzeniem. Sporządzający oględziny musi przestrzegać następujących zasad: protokół sporządzać podczas oględzin w sposób czytelny, używać ujednoliconego nazewnictwa oraz nie odnotowywać wniosków lub przypuszczeń. Dokumentację techniczną stanowią: szkice, fotografie i nośniki z nagraniami obrazu

lub dźwięku. Ujawnione w trakcie oględzin ślady stanowią materiał dowodowy wykorzystywany w prowadzonym postępowaniu. Jeżeli podczas prowadzonych czynności był użyty pies służbowy, to przewodnik sporządza notatkę służbową. W sytuacji kiedy funkcjonariusz uzna, że na miejscu zdarzenia nie ma możliwości ujawnienia i zabezpieczenia śladów przestępstwa lub ich nośników, może odstąpić od wykonania oględzin, a jeżeli zachodzi podejrzenie przestępnego spowodowania śmierci, policjant dokonuje oględzin zwłok na polecenie prokuratora. Przeprowadzenie oględzin osoby dotyczy ciała osoby żyjącej, celem tych czynności jest identyfikacja lub ujawnienie śladów na ciele. Celem oględzin rzeczy jest zaś identyfikacja, wykrycie na niej śladów przestępstwa lub ustalenie właściwości danej rzeczy.

Eksperyment procesowy można przeprowadzić w każdym stadium postępowania przygotowawczego. Celem czynności fakultatywnej jest wyjaśnienie wątpliwości, które mogły powstać podczas zbierania materiału dowodowego. Przeprowadzenie eksperymentu nie może zagrażać dobru prawnie chronionemu. Eksperyment procesowy można wykonać w formie doświadczenia na miejscu zdarzenia lub w innym miejscu (stworzenie sztucznej sytuacji) albo odtworzenia, które powinno być ściśle powiązane z przebiegiem zdarzenia lub z jego częścią (zrekonstruowanie sytuacji). Przeprowadzenie eksperymentu wymaga sporządzenia protokołu wraz z dokumentacją techniczną. Jeżeli stanowi część oględzin, jego przebieg i wyniki dokumentuje się w protokole oględzin.

Prowadzący postępowanie może wystąpić do prokuratora z wnioskiem o wydanie postanowienia o zatrzymaniu rzeczy, danych informatycznych albo przeszukaniu, wskazując w nim cel tej czynności ze wskazaniem osoby podejrzanej, która ma być wykryta, zatrzymana lub przymusowo doprowadzona, bądź rzeczy lub danych informatycznych, które mają być znalezione lub zatrzymane. Wniosek musi być odpowiednio uzasadniony, należy w nim przedstawić dowody lub przytoczyć okoliczności dające podstawę przypuszczenia, że osoba podejrzana, rzeczy albo dane informatyczne znajdują się we wskazanym miejscu lub urządzeniu albo systemie informatycznym. Jeżeli w trakcie przeszukania znalezione zostają rzeczy mogące stanowić dowód w innej sprawie, należy wpisać je do protokołu. Przeprowadzający przeszukanie ma prawo zażądać od dysponenta lub użytkownika urządzenia zawierającego dane informatyczne lub systemu informatycznego ujawnienia hasła umożliwiającego dostęp do tych urządzeń.

Dokonując czynności procesowej zatrzymania lub przeszukania w pierwszej kolejności należy wezwać osobę, która ma dane rzeczy lub u której będzie przeprowadzone przeszukanie, do dobrowolnego ich wydania. W wypadku wydania wszystkich przedmiotów należy odstąpić od wykonania czynności. Z zatrzymania rzeczy, danych informatycznych lub nośników zawierających dane informatyczne sporządza się protokół zatrzymania rzeczy oraz pokwitowanie wydanych bądź odebranych przedmiotów zawierające dokładny ich opis. Jeśli w wypadku zatrzymania rzeczy lub nośników

zawierających dane informatyczne albo przeszukania osoby, miejsca lub systemu informatycznego zajdą okoliczności stanowiące lub zawierające → i n f o r m a c j ę n i e j a w n ą [t. 2], należy zastosować odpowiedni tryb uregulowany w stosownym rozporządzeniu ministra sprawiedliwości.

W niektórych postępowaniach konieczne jest powołanie biegłych, specjalistów lub tłumaczy. Biegłym jest osoba wezwana przez organ ścigania do wydania opinii o okolicznościach mających istotny wpływ na rozstrzygnięcie sprawy. Prowadzący postępowanie przed wydaniem postanowienia o dopuszczeniu dowodu z opinii biegłego określa przedmiot, zakres badań, zabezpiecza, kompletuje bądź uzyskuje materiał porównawczy, określa zakres badań, udostępnia akta sprawy, konsultuje powołanie biegłego z prokuratorem. Najczęściej powołuje się biegłych wydających opinie: medyczne, psychologiczne, psychiatryczne, kryminalistyczne. Biegły może być również przesłuchany w charakterze świadka. Funkcjonariusz może powołać w charakterze biegłego osobę, która wcześniej wykonywała w postępowaniu funkcję specjalisty, może również tę osobę przesłuchać jako świadka. Jeżeli w prowadzonym postępowaniu niezbędny jest udział tłumacza, prowadzący powinien wezwać taką osobę do uczestnictwa w danej czynności procesowej.

Niekiedy w postępowaniu przeprowadza się konfrontację – czynność procesową polegającą na równoczesnym przesłuchaniu 2 osób na tę samą okoliczność w celu wyjaśnienia zaistniałych sprzeczności wynikłych podczas wcześniejszych zeznań lub wyjaśnień. Konfrontować można świadka ze świadkiem lub z podejrzanym i podejrzanego z podejrzanym. Przygotowanie do konfrontacji polega na przeprowadzeniu analizy protokołów wcześniejszych czynności, określeniu zagadnień będących przedmiotem konfrontacji, ustaleniu miejsca i czasu czynności oraz wyznaczeniu kolejności wypowiedzi konfrontowanych. Pierwsza składa zeznania lub wyjaśnienia osoba, której wypowiedzi prowadzący ocenił jako bardziej wiarygodne. Przy konfrontacji świadka z podejrzanym pierwszy składa zeznanie świadek. Z przeprowadzonej czynności procesowej sporządza się protokół.

W postępowaniu przygotowawczym można również zastosować okazanie, którego celem jest rozpoznanie osoby lub rzeczy. Najczęściej okazywany jest podejrzany. Okazanie można przeprowadzić bezpośrednio lub pośrednio. Podczas okazania osoba okazywana powinna znajdować się w grupie obejmującej łącznie co najmniej 4 osoby. Osoba przybrana musi wyrazić zgodę na uczestnictwo w tej czynności. Okazanie pośrednie wizerunku osoby wykonuje się, gdy sprawca ukrywa się, przebywa poza granicami kraju albo jest nieznany. Wizerunek osoby okazywanej umieszcza się w zestawie zdjęć osób podobnych. Tablica poglądowa stanowi załącznik do protokołu okazania. Można także okazać rzeczy pochodzące z miejsca popełnienia przestępstwa lub służące do jego popełnienia oraz odzież i przedmioty osobiste podejrzanego. Przed okazaniem należy dokładnieprzesłuchać osobę rozpoznającą na okoliczność cech charakterystycznych określonych przedmiotów.

Środki przymusu w postępowaniu przygotowawczym to czynności zmierzające do wymuszenia spełnienia obowiązków procesowych lub zapewnienia prawidłowego toku procesu. Zatrzymanie to krótkotrwałe pozbawienie wolności danej osoby. Osobę podejrzaną można zatrzymać, gdy istnieje uzasadnione przypuszczenie, że dokonała przestępstwa i zachodzi obawa ucieczki, ukrycia się lub zatarcia śladów przestępstwa bądź nie można ustalić jej tożsamości albo istnieją przesłanki do przeprowadzenia przeciwko tej osobie postępowania w trybie przyspieszonym. Po zatrzymaniu osoby niezwłocznie informuje się ją o przyczynach zatrzymania i przysługujących jej prawach, przede wszystkim o prawie do skorzystania z pomocy adwokata lub radcy prawnego, do złożenia oświadczenia i odmowy złożenia oświadczenia. Z zatrzymania sporządza się protokół, w którym m.in. należy podać dane osoby zatrzymanej, dzień, godzinę, miejsce i przyczynę zatrzymania, rodzaj przestępstwa, o które się osobę podejrzewa. Niezwłocznie po zatrzymaniu osoby należy zawiadomić prokuratora. Zatrzymanemu przysługuje zażalenie do sądu, w którym może się domagać zbadania zasadności, legalności oraz prawidłowości jego zatrzymania. Stosowanymi środkami zapobiegawczymi są m.in.: tymczasowe aresztowanie, poręczenie majątkowe i dozór policji. → P o l i c j a [t. 3] może również nałożyć karę porządkową w postaci kary pieniężnej.

Okresy prowadzenia dochodzenia i śledztwa są ustalone ustawowo, są to odpowiednio 2 i 3 miesiące. Przepisy Kodeksu postępowania karnego umożliwiają ich wydłużenie. Wniosek o przedłużenie okresu prowadzenia postępowania musi zostać sporządzony w formie pisemnej i zawierać powody, które uniemożliwiły zakończenie postępowania w przewidzianym terminie. Jeżeli zachodzi długotrwała przeszkoda, która powstrzymuje prowadzenie postępowania, szczególnie gdy nie można ująć oskarżonego albo nie może on brać udziału w postępowaniu z powodu choroby psychicznej lub innej ciężkiej choroby, postępowanie można zawiesić na czas trwania przeszkody. Zawieszenie postępowania nie stanowi jego zakończenia, wstrzymuje jedynie jego bieg. W chwili ustania przeszkody postępowanie jest kontynuowane.

Prowadzący sprawę może wyłączyć materiały do odrębnego postępowania w stosunku do poszczególnych osób lub konkretnych czynów. Wyłączając materiały, funkcjonariusz wydaje postanowienie, które zawiera nazwy dokumentów, numery kart akt postępowania przygotowawczego, a także oznaczenia dowodów podlegających wyłączeniu. W wypadku wydania postanowienia o połączeniu postępowań przygotowawczych stosuje się następujące zasady: dochodzenie później wszczęte dołącza się do wszczętego wcześniej, do akt dochodzenia, w którym zastosowano tymczasowe aresztowanie, włącza się akta łączonego dochodzenia niezależnie od czasu wszczęcia tego dochodzenia. Czas trwania połączonych dochodzeń liczy się od daty najwcześniejszego wszczęcia.

Zamknięcie postępowania, zakończenie postępowania przeciwko osobie, wydanie postanowienia o zamknięciu dochodzenia lub śledztwa stanowi zakończenie postępowania dowodowego w stadium postępowania przygotowawczego. W wypadku

dochodzenia decyzję wydaje policjant, a w śledztwie – prokurator. Zamknięcie postępowania przygotowawczego następuje wtedy, gdy osiągnięte zostaną wszystkie cele procesowe. Podejrzany i jego obrońca mają prawo do przejrzenia akt sprawy. Prowadzący sprawę niezwłocznie po zakończeniu postępowania może sporządzić akt oskarżenia.

Umorzenie postępowania przygotowawczego następuje w chwili pojawienia się przewidzianej prawem przyczyny. Takim powodem może być ujemna przesłanka procesowa. Jeżeli postępowanie nie dostarczyło podstaw wniesienia aktu oskarżenia, śledztwo umarza się bez konieczności uprzedniego zaznajomienia z materiałami postępowania i jego zamknięcia. Postanowienie o umorzeniu śledztwa zawiera m.in. dokładne określenie czynu, jego kwalifikację prawną i wskazanie przyczyn umorzenia. Śledztwo umarza się wobec niewykrycia sprawcy przestępstwa, niepopełnienia przestępstwa przez podejrzanego bądź braku dowodów winy. Postanowienie o umorzeniu dochodzenia i wpisaniu sprawy do rejestru przestępstw wydaje się niezwłocznie po stwierdzeniu braku danych stwarzających dostateczne podstawy wykrycia sprawcy. Przesłanka taka powstaje szczególnie wtedy, gdy na miejscu zdarzenia nie ujawniono śladów działania sprawcy, pokrzywdzony nie miał kontaktu ze sprawcą, a na miejscu zdarzenia nie było żadnych świadków. Po wydaniu postanowienia o umorzeniu postępowania zawiadamia się odpowiednio: osobę lub instytucję państwową, samorządową lub społeczną, która złożyła zawiadomienie o przestępstwie, ujawnionego pokrzywdzonego oraz podejrzanego – z pouczeniem o przysługujących im uprawnieniach.

Zażalenie przysługuje na postanowienia sądu zamykające drogę do wydania wyroku, chyba że ustawa stanowi inaczej. Uprawnienie to dotyczy również sytuacji postanowienia co do środka zabezpieczającego, a także innych postanowień przewidzianych w ustawie. Zażalenie przysługuje stronom oraz osobie, których postanowienie bezpośrednio dotyczy. Zażalenie albo sprzeciw wnosi się w terminie 7 dni od daty ogłoszenia postanowienia, a jeżeli ustawa nakazuje doręczenie postanowienia – od daty doręczenia. Przed wydaniem zarządzenia o przyjęciu zażalenia niezbędne jest jego zbadanie w kwestiach: terminowości wniesienia, osoby uprawnionej oraz tego, czy jest dopuszczalne z mocy ustawy. Jeżeli zażalenie jest uwarunkowane formalnie, prowadzący postępowanie może wydać: niepodlegające zaskarżeniu postanowienie o uwzględnieniu zażalenia i uchyleniu zaskarżonego postanowienia albo podlegające zaskarżeniu postanowienie o uwzględnieniu zażalenia i zmianie zaskarżonego postanowienia.

Umorzone postępowanie przygotowawcze może być w każdym czasie podjęte na nowo na mocy postanowienia prokuratora. Wniosek musi zawierać: sygnaturę akt umorzonego postępowania, jego rodzaj, podstawę umorzenia oraz okoliczności i dowody uzasadniające podjęcie lub wznowienie postępowania. Umorzone dochodzenie może być podjęte na nowo w wypadku ujawnienia danych umożliwiających wykrycie sprawcy. Jeżeli ujawnienie takich danych nastąpiło w wyniku przeprowadzonych

→czynności operacyjno-rozpoznawczych [t. 1], dokumentuje się te działania w notatce urzędowej stanowiącej podstawę podjęcia na nowo dochodzenia.

Reasumując charakter, specyfikę i formę prowadzonych głównie przez policję czynności dochodzeniowo-śledczych, należy podkreślić, że powyższe uprawnienia przysługują także: organom Straży Granicznej, →Agencji Bezpieczeństwa Wewnętrznego [t. 1], Krajowej Administracji Skarbowej, → Centralnego Biura Antykorupcyjnego [t. 1], →Żandarmerii Wojskowej w zakresie ich właściwości oraz innym organom przewidzianym w przepisach szczególnych.

Dariusz Hybś

J. Jerzewska, *Elementy prawa Podręcznik z ćwiczeniami*, Wolters Kluwer Polska, Warszawa 2017; M.P. Krysiak, *Przesłuchanie podejrzanego*, Wydawnictwo Wyższej Szkoły Policji, Szczytno 2008; tenże, *Przesłuchanie świadka*, Wydawnictwo Wyższej Szkoły Policji, Szczytno 2008; J. Kudrelek, I. Wojciechowska, *Postępowanie przygotowawcze. Wybrane zagadnienia, orzecznictwo, przykłady*, Wydawnictwo Wyższej Szkoły Policji, Szczytno 2008; K. Marszał, *Proces karny*, Wydawnictwo „Volumen", Katowice 1997; Rozporządzenie Ministra Sprawiedliwości z dnia 20 lutego 2012 r. w sprawie sposobu postępowania z protokołami przesłuchań i innymi dokumentami lub przedmiotami, na które rozciąga się obowiązek zachowania w tajemnicy informacji niejawnych albo zachowania tajemnicy związanej z wykonywaniem zawodu lub funkcji, Dz.U. 2012, poz. 219; M. Śrubka, B. Waszkiewicz, *Postępowanie sprawdzające i postępowanie w niezbędnym zakresie (art. 307 i 308 kpk)*, Centrum Szkolenia Policji w Legionowie, Legionowo 2014; Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, Dz.U. 1997, nr 88, poz. 553 z późn. zm.; Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego, Dz.U. 1997, nr 89, poz. 555 z późn. zm.; Wytyczne Nr 3 Komendanta Głównego Policji z dnia 30 sierpnia 2017 r. w sprawie wykonywania niektórych czynności dochodzeniowo-śledczych przez policjantów, Dz.Urz. KGP 2017, poz. 59; Zarządzenie nr 4 Komendanta Głównego Policji z dnia 9 lutego 2017 r. w sprawie niektórych form organizacji i ewidencji czynności dochodzeniowo-śledczych Policji oraz przechowywania przez Policję dowodów rzeczowych uzyskanych w postępowaniu karnym, Dz.Urz. KGP 2017, poz. 9.

CZYN ZABRONIONY – jedna z niezbędnych i najważniejszych przesłanek składających się na definicję przestępstwa lub wykroczenia. Aby można było zakwalifikować dane zachowanie jako przestępstwo lub wykroczenie, obok czynu zabronionego muszą wystąpić jednocześnie: bezprawność czynu, społeczna szkodliwość czynu (wyższa niż znikoma), a także czyn ten musi być zawiniony. W przypadku wykroczenia nie jest wymagane, aby szkodliwość społeczna była wyższa niż znikoma.

Naruszenia prawa w polskim systemie prawnym można w zależności od stopnia społecznej szkodliwości zakwalifikować jako przestępstwo lub wykroczenie. Zakres odpowiedzialności jest związany m.in. z wypełnieniem określonych znamion, składających się na stwierdzenie czynu zabronionego.

Zasady odpowiedzialności karnej określono w art. 1 kk. Przepis precyzuje, że odpowiedzialności karnej podlega ten tylko, kto popełnia czyn zabroniony pod groźbą

kary przez ustawę obowiązującą w czasie jego popełnienia. Jednocześnie określa, że nie stanowi przestępstwa czyn zabroniony, którego społeczna szkodliwość jest znikoma. Nie popełnia przestępstwa sprawca czynu zabronionego, jeżeli nie można mu przypisać winy w czasie czynu. Ogólne zasady odpowiedzialności karnej jednoznacznie opierają swoją konstrukcję na aspekcie czynu zabronionego.

Definicję czynu zabronionego możemy znaleźć zarówno w art. 115 kk, jak też w art. 47 §1 kw. I w jednej, i w drugiej ustawie przybiera analogiczne brzmienie: czynem karalnym jest zachowanie o znamionach określonych w ustawie karnej. Obowiązujący kodeks karny w wielu miejscach posługuje się pojęciem czynu zabronionego, choć niekiedy wzbogaca je, mówiąc o czynie zabronionym pod groźbą kary (art. 1 § 1 i art. 4 § 4 kk). Oba te wyrażenia traktować należy jako synonimy. Pojęcie czynu zabronionego (art. 115 § 1 kk) nie jest równoznaczne z pojęciem przestępstwa. Nie każdy czyn zabroniony jest przestępstwem, ale każde przestępstwo jest czynem zabronionym. Nie stanowi przestępstwa czyn zabroniony popełniony w warunkach wyłączających bezprawność (np. obrona konieczna – art. 25

§ 1 kk) albo winę jego sprawcy (np. niepoczytalność – art. 31 § 1 kk, stan wyższej konieczności – art. 26 § 2 kk), jak również gdy społeczna szkodliwość tego czynu jest znikoma (art. 1 § 2 kk). Do zaistnienia przestępstwa konieczne jest wystąpienie wszystkich przesłanek określających odpowiedzialność karną. Jeżeli sprawca popełnił czyn zabroniony, który stanowi przestępstwo lub wykroczenie, podlega karze zapisanej we właściwej ustawie. Czyn zabroniony jest określonym zachowaniem się człowieka, które musi przybrać postać zarówno działania, jak i zaniechania. Owo działanie lub zaniechanie musi z kolei wypełniać opisane w ustawie karnej znamiona czynu zabronionego, zgodnie z kodeksem karnym, w przypadku zbrodni tylko w sposób umyślny, natomiast w przypadku występku także nieumyślnie, jeżeli ustawa tak stanowi. Wykroczenie można popełnić zarówno umyślnie, jak i nieumyślnie.

Możemy wyróżnić 3 typy czynu zabronionego:

- typ podstawowy – jest zazwyczaj określony w pierwszym paragrafie danego artykułu;
- typ kwalifikowany – skutkujący zaostrzoną sankcją, wynikający np. z określonego sposobu działania sprawcy lub skutku jego działania;
- typ uprzywilejowany – wskazujący przesłanki obniżające sankcje karne.

Do scharakteryzowania czynu zabronionego niezbędne jest opisanie jego ustawowych znamion, czyli opisanych w ustawie karnej cech, które są konieczne (niezbędne) i wystarczające do uznania (zakwalifikowania) konkretnego czynu za konkretne przestępstwo (lub wykroczenie). Należą do nich: przedmiot ochrony (zamachu), strona przedmiotowa, podmiot, strona podmiotowa.

Przedmiotem ochrony (zamachu) nazywamy określone dobro prawne lub określoną wartość społeczną, podlegające ochronie prawnej. Z punktu widzenia sprawcy czynu przedmiot ochrony to przedmiot zamachu. Nie ma przepisu karnego, który

nie został ustanowiony w celu ochrony dobra prawnego. Przedmiot ochrony (zamachu) można podzielić na ogólny (obejmujący ogół norm prawnych chronionych daną ustawą), rodzajowy (chroniony przez grupę przepisów prawnych zawartych w danym rozdziale części szczególnej ustawy) oraz indywidualny (dobro prawne chronione przez konkretny przepis ustawy). Strona przedmiotowa obejmuje uzewnętrznione elementy czynu sprawcy, takie jak: zachowanie się sprawcy (działanie, zaniechanie lub utrzymywanie pewnego stanu rzeczy), skutek (skutkowe, bezskutkowe), przedmiot czynności wykonawczej (przedmiot, na który sprawca bezpośrednio oddziałuje), związek przyczynowo-skutkowy (zależność między zachowaniem sprawcy a skutkiem tego zachowania) oraz okoliczności modalne (sposób działania sprawcy, sytuacja, w jakiej sprawca działa, środki/narzędzia, miejsce popełnienia przestępstwa, czas popełnienia).

Podmiot wskazuje cechy, które musi mieć osoba, aby można było ją pociągnąć do odpowiedzialności za popełnienie czynu zabronionego (podmiot powszechny lub indywidualny). Strona podmiotowa określa stosunek psychiczny sprawcy do realizacji znamion czynu zabronionego (umyślność lub nieumyślność). Strona podmiotowa jest jedną z przesłanek winy.

Czyn zabroniony jest jedną z niezbędnych i najważniejszych przesłanek składających się na definicję przestępstwa lub wykroczenia.

Pociągnięcie do odpowiedzialności prawnej sprawcy jest uwarunkowane wypełnieniem ustawowych znamion czynu zabronionego, które są konieczne i wystarczające do uznania konkretnego czynu za konkretne przestępstwo lub wykroczenie.

Krzysztof Dymura

L. Gardocki, *Prawo karne*, Wydawnictwo C.H.Beck, Warszawa 1999; T. Grzegorczyk, *Kodeks postępowania w sprawach o wykroczenia. Komentarz*, Dom Wydawniczy ABC, Warszawa 2003; *Kodeks karny. Komentarz*, R.A. Stefański (red.), Wydawnictwo C.H.Beck, Warszawa 2015; W. Świda, *Prawo karne*, Wydawnictwo PWN, Warszawa 1986; Ustawa z dnia 20 maja 1971 r. – Kodeks wykroczeń, Dz. U. 1971, nr 12, poz. 114 z późn. zm.; Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, Dz. U. 1997, nr 88, poz. 553 z późn. zm.; A. Wróblewska, *Część ogólna kodeksu karnego (wybrane zagadnienia*), Wydawnictwo Szkoły Policji w Pile, Piła 2013.

CZYNNOŚCI OPERACYJNO-ROZPOZNAWCZE – jeden z podstawowych rodzajów czynności wykonywanych przez uprawnione służby systemu → b e z p i e c z e ń s t w a państwa polegające na niejawnym (tajnym) pozyskiwaniu i przetwarzaniu → i n f o r m a c j i [t. 2] w celu rozpoznawania i wykrywania różnego rodzaju przestępstw i → z a g r o ż e ń [t. 4] oraz zapobiegania im. Uzyskane w ten sposób informacje nie są wykorzystywane jako dowody w postępowaniu procesowym.

B. Sprengel wskazuje na szerokie możliwości ich zastosowania w pracy wielu służb w ramach różnych obszarów bezpieczeństwa państwa, definiując je jako:

> pozaprocesowe, niejawne, ustawowo dopuszczalne i wynikające z zakresu obowiązków uprawnionych funkcjonariuszy działania, mające na celu zapobieganie, wykrywanie i ustalanie sprawców przestępstw oraz rozpoznawanie, zapobieganie i zwalczanie zagrożeń bezpieczeństwa wewnętrznego i zewnętrznego państwa, jego porządku konstytucyjnego, a także uzyskiwanie informacji istotnych dla jego międzynarodowej pozycji, potencjału ekonomicznego i obronnego.

S. Hoc podkreśla z kolei ich pozaprocesowe zastosowanie, uznając, że „czynności te nie mają charakteru procesowego, stanowią natomiast pozaprocesowe, techniczno-taktyczne czynności praktyki organów […], mające na celu zapobieganie i zwalczanie przestępczości". Natomiast w definicjach autorstwa A. Żebrowskiego można zauważyć odniesienia do bardziej praktycznych przykładów zastosowania tego rodzaju czynności, które:

> polegają na rozpoznawaniu środowisk znajdujących się w operacyjnym zainteresowaniu […], na wykrywaniu czynników sprzyjających przestępczości i zdarzeń mających cechy przestępstw, osób (organizacji), które mogą okazać się sprawcami, na wykrywaniu źródeł dowodowych oraz zapobieganiu przestępstwom i innym działaniom godzącym w bezpieczeństwo wewnętrzne i zewnętrzne państwa.

Najczęściej tego rodzaju czynności dotyczą korzystania z osobowych źródeł informacji (osób, które ze względu na przynależność do danej organizacji czy grupy, zajmowaną pozycję, posiadaną wiedzę itp. mogą mieć dostęp do istotnych informacji – informatorzy, tajni współpracownicy, agenci) oraz realizacji tzw. kontroli operacyjnej (m.in. kontrola treści korespondencji i zawartości przesyłek, → p o d s ł u c h [t. 3] rozmów telefonicznych i pozostałej korespondencji wymienianej z wykorzystaniem sieci teleinformatycznych, podgląd osób i zdarzeń itp.). W literaturze przedmiotu rozróżnia się formy proste i złożone czynności operacyjnej. Do pierwszej grupy można zaliczyć m.in.: obserwację, → w y w i a d [t. 4], prowadzenie osobowego źródła informacji, przesyłkę niejawnie kontrolowaną, zakup niejawnie kontrolowany, kontrolowane wręczenie lub przyjęcie korzyści majątkowej, niejawny i kontrolowany obrót przedmiotami przestępstw, korzystanie z niejawnych rejestrów, wykazów i ewidencji informacyjnych, niejawne pozyskiwanie i przetwarzanie danych osobowych, korzystanie z tzw. dokumentów legalizacyjnych (uniemożliwiających identyfikację osób oraz środków) czy poszczególne czynności prowadzone w ramach kontroli operacyjnej. Czynności złożone obejmują natomiast takie jej formy, jak m.in. gra operacyjna, kombinacja operacyjna, sprawdzenie operacyjne, rozpracowanie operacyjne, analiza operacyjna, inwigilacja, infiltracja, tajne przeszukanie, tajne zatrzymanie.

Charakter i zakres problemów rozwiązywanych z wykorzystaniem czynności operacyjno-rozpoznawczych jest bardzo szeroki, co widać chociażby w zestawieniu odnoszącym się głównie do służb wywiadu i → k o n t r w y w i a d u [t. 4] przedstawionym przez Żebrowskiego:

- rozpoznanie operacyjne dotyczące obywateli własnego państwa i cudzoziemców zamieszkałych na stałe lub przebywających czasowo na jego terytorium, w związku

z podejrzeniem o działalność terrorystyczną, uczestniczenie w grupach, organizacjach lub związkach, co do których istnieje podejrzenie o działalność terrorystyczną lub jej wspieranie;
- rozpoznanie operacyjne grup, organizacji i związków, co do których istnieje podejrzenie o działalność terrorystyczną oraz finansowanie takiej działalności w kraju lub poza jego granicami;
- zabezpieczanie potrzeb informacyjnych, tzn. wykorzystanie osobowych źródeł informacji tkwiących w wymienionych strukturach przestępczych lub pozwalających na dotarcie do środowisk posiadających wiedzę o nich albo których kontakt z ww. jest podyktowany wykonywaniem zawodu (np. obsługa hoteli, schronisk, restauracji, instruktorów tzw. szkół przetrwania, agencji towarzyskich);
- prowadzenie rozpoznania operacyjnego środowisk, które pochodzą z państw tzw. wysokiego ryzyka, w celu zdobycia informacji o osobach pochodzących z tych środowisk, a w szczególności: o ich ewentualnej przestępczej działalności; o istniejących grupach przestępczych;
- rozpoznanie osób posiadających zaburzenia psychiczne, które pod wpływem sytuacji na świecie mogą być zdolne do podjęcia czynów o charakterze terrorystycznym.

W funkcjonującym obecnie polskim systemie bezpieczeństwa uprawnienia takie ma 11 służb: → Agencja Bezpieczeństwa Wewnętrznego (ABW), →Agencja Wywiadu (AW), →Służba Kontrwywiadu Wojskowego (SKW) [t. 4] →Służba Wywiadu Wojskowego (SWW) [t. 4], → Centralne Biuro Antykorupcyjne (CBA), → Policja [t. 3], Straż Graniczna (SG), Żandarmeria Wojskowa (ŻW), → Służba Celno Skarbowa (SCS) [t. 4], → Służba Ochrony Państwa (SOP) [t. 4] i Biuro Nadzoru Wewnętrznego (BNW, w strukturach Ministerstwa Spraw Wewnętrznych i Administracji). Wcześniej uprawnione w tym zakresie były również już rozwiązane lub przekształcone służby: → Urząd Ochrony Państwa (UOP) [t. 4], → Wojskowe Służby Informacyjne (WSI) [t. 4], Służba Celna (SC), Inspekcja Kontroli Skarbowej (Wywiad Skarbowy) oraz Służba Ochrony Państwa (SOP).

Piotr Swoboda

S. Hoc, *Zagadnienia odpowiedzialności karnej za szpiegostwo*, Akademia Spraw Wewnętrznych, Warszawa 1985; B. Sprengel, *Służby mundurowe ochrony bezpieczeństwa wewnętrznego. Zarys problematyki*, Dom Organizatora, Toruń 2008; tenże, *Ustrój organów administracji bezpieczeństwa i porządku publicznego*, Wyższa Szkoła Humanistyczno-Ekonomiczna, Włocławek 2004; P. Swoboda, *Służby specjalne w Polsce po 1989 roku – problemy definicyjne*, [w:] *Niepodległa Polska. Bezpieczeństwo i polityka w latach 1918–2018*, P. Łubiński (red.), Katolicki Uniwersytet Lubelski Jana Pawła II w Lublinie, Stalowa Wola 2018; tenże, *Wywiad i kontrwywiad w Polsce w procesie przemian systemowych (1989–2007)*, Avalon, Kraków 2016; A. Żebrowski, *Ewolucja polskich służb specjalnych. Wybrane obszary walki informacyjnej. (Wywiad i kontrwywiad w latach 1989–2003)*, Oficyna Wydawnicza Abrys, Kraków 2005; tenże, *Wywiad i kontrwywiad w XXI wieku*, Innovatio Press, Lublin 2010.