TERRORYZM

studia
analizy
prewencja

CENTRALNY OŚRODEK
SZKOLENIA I EDUKACJI ABW
im. gen. dyw. Stefana Roweckiego „Grota”

ISSN 2720-4383
e-ISSN 2720-6351

Recenzji są poddawane materiały zamieszczone w dziale Artykuły
oraz artykuły recenzyjne zamieszczone w dziale
Artykuły recenzyjne/recenzje

Artykuły wyrażają poglądy autorów

Deklaracja o wersji pierwotnej:
Wersja drukowana czasopisma jest jego wersją pierwotną
Wersja online czasopisma jest dostępna na stronie www.abw.gov.pl/wyd/

Czasopismo jest dostępne w Portalu Czasopism Naukowych Uniwersytetu
Jagiellońskiego pod adresem: https://www.ejournals.eu/Terroryzm/

Materiały do czasopisma należy składać przez panel redakcyjny dostępny
pod adresem: https://ojs.ejournals.eu/Terroryzm/about/submissions

Wydawnictwo Agencji Bezpieczeństwa Wewnętrznego
Centralny Ośrodek Szkolenia i Edukacji
im. gen. dyw. Stefana Roweckiego „Grota”
ul. Nadwiślańczyków 2, 05-462 Wiązowna

Kontakt
tel. (+48) 22 58 58 695
e-mail: wydawnictwo@abw.gov.pl
www.abw.gov.pl/wyd/

Numer zamknięto i oddano do druku w lipcu 2025 r.

Druk
Biuro Logistyki Agencji Bezpieczeństwa Wewnętrznego
ul. Rakowiecka 2A, 00-993 Warszawa
tel. (+48) 22 58 57 657

SPIS TREŚCI

Szanowni Państwo!

Przez te wszystkie lata, kiedy miałem zaszczyt brać udział w rozwoju polskiego systemu antyterrorystycznego na poziomach: strategicznym, taktycznym czy operacyjnym, z przyjemnością współpracowałem z dowódcami i operatorami krajowych jednostek kontrterrorystycznych, zarówno cywilnych, jak i wojskowych. W ramach współpracy zagranicznej obserwowałem, jakim uznaniem polscy kontrterroryści cieszą się w państwach NATO. Ta aprobata nie wynikała z kurtuazji. Została zyskana dzięki wspólnym działaniom na lądzie, morzu i w powietrzu. Warto wiedzieć, że rozwiązania powstające w Polsce były i są implementowane w wielu krajach partnerskich. Tworzyli je ludzie, którzy budowali w naszym kraju podwaliny kontrterroryzmu i nieustannie pracują nad jego doskonaleniem. Daleki jestem od nadmiernego zachwytu nad tym filarem polskiego systemu antyterrorystycznego, ale widzę i doceniam progres, który się dokonał w tym obszarze po 11 września 2001 r.

W siódmym numerze czasopisma „Terroryzm – studia, analizy, prewencja" (T-SAP) publikujemy materiały na temat elitarnej Jednostki Wojskowej 2305 GROM. Chcemy w ten sposób uhonorować 35. rocznicę jej powstania oraz złożyć zasłużone gratulacje od służby partnerskiej. Polecam artykuł, w którym można przeczytać o potencjalnych kierunkach rozwoju współpracy JW GROM ze służbami specjalnymi. Mam nadzieję, że w ten sposób wywołamy dyskusje na temat tego, jak doskonalić system antyterrorystyczny RP, aby był bardziej skuteczny, elastyczny i lepiej odpowiadał na aktualne wyzwania i zagrożenia.

O tym, jak kształtuje się obecnie poziom tych zagrożeń na terenie Unii Europejskiej, dowiedzą się Państwo z artykułu

omawiającego dane zawarte w dorocznym raporcie Europolu (*European Union Terrorism Situation and Trend Report 2024*), czyli w najbardziej miarodajnym źródle wiedzy o terroryzmie w krajach członkowskich. Jest on przedmiotem oceny wszystkich europejskich organów ścigania. O jego krytyczną analizę poprosiliśmy polskich ekspertów ds. terroryzmu.

Duży wpływ na skalę zagrożenia terrorystycznego w Europie ma to, co się dzieje w Afryce. Zjawisko migracji na wschodniej flance NATO i granicy UE, sztucznie wywołane przez Rosję i Białoruś, nie osiągnęłoby takiej skali, gdyby m.in. nie trudna sytuacja w regionie Sahelu. Niestabilność polityczna w krajach tej części Afryki, kryzysy humanitarne, rosnące wpływy grup terrorystycznych i działania najemników wojskowych zwiększają ryzyko destabilizacji południowej flanki Sojuszu. O tym, jak duży wpływ ma ten region na aktywność terrorystyczną w UE, dowiedzą się Państwo z kolejnej analizy eksperckiej zamieszczonej w tym numerze. Pytanie, czy po tegorocznym szczycie NATO w Hadze dojdzie do rewizji strategii działania dotyczących tego regionu i kierunku, pozostaje otwarte.

Jednym z filarów walki z terrorystami jest blokowanie propagandy rozpowszechnianej przez nich w internecie. Stwarzanie iluzji przynależności do społeczności bojowników o wspólną sprawę to skuteczny sposób pozyskiwania kolejnych pokoleń młodych ludzi. W Polsce weszła w życie znowelizowana ustawa o działaniach antyterrorystycznych wdrażająca zapisy *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym*. Zgodnie z nią służbą wiodącą w tym obszarze jest Agencja Bezpieczeństwa Wewnętrznego. Publikujemy komentarz prawny na temat zapisów tej ustawy, dotyczących nakazów usunięcia treści o charakterze terrorystycznym oraz środków szczególnych, tj. trybu wydawania decyzji w sprawie dostawców usług hostingowych narażonych na tego rodzaju treści. To najbardziej kompleksowe opracowanie w Polsce poświęcone tej tematyce.

Wydarzenia ostatnich lat pozwalają zaryzykować stwierdzenie, że nie wolno bagatelizować scenariuszy zagrożeń, które dotychczas były klasyfikowane przez służby jako mało

prawdopodobne. Jednym z nich jest wykorzystanie czynników biologicznych do działań hybrydowych. Zachęcam do zapoznania się z artykułem stanowiącym wprowadzenie do problematyki ochrony biologicznej. Obejmuje on przegląd i analizę środków służących zabezpieczeniu i ochronie czynników biologicznych oraz związanych z nimi technologii, które mogą zostać wykorzystane w charakterze broni czy środka terroru.

Na zakończenie chciałbym zwrócić uwagę na pierwszą od lat pogłębioną analizę dotyczącą stanu sektora ochrony mienia i osób w Polsce. Podmioty, które działają w ramach prywatnego sektora ochrony, są kluczowym partnerem służb i instytucji tworzących krajową wspólnotę antyterrorystyczną. Od siły tych sojuszy zależy nie tylko porządek publiczny, lecz także bezpieczeństwo obiektów o charakterze strategicznym, w tym infrastruktury krytycznej. Problemy i wyzwania stojące przed sektorem ochrony w Polsce nie po raz pierwszy pojawiają się na łamach T-SAP. Autorzy raportu, którego wyniki prezentujemy, wskazują nasz periodyk jako cenne źródło wiedzy dla tej branży. Dziękujemy za docenienie naszej pracy.

Czasopismo wydawane przez ABW staje się ważnym głosem nie tylko w budowaniu bezpieczeństwa wewnętrznego RP. W instytucjach i agendach UE coraz skuteczniej promujemy polski punkt widzenia na unijną politykę antyterrorystyczną. Przy tej okazji polecam Państwa uwadze numer specjalny T-SAP pt. *Zagrożenia terrorystyczne i sabotażowe infrastruktury krytycznej*, przygotowany przy współpracy ABW i Rządowego Centrum Bezpieczeństwa. Numer ten, wpisujący się w priorytety polskiej prezydencji w Radzie UE, jest dostępny w dwóch językach: polskim i angielskim na naszej stronie internetowej. Przygotowaliśmy go z myślą o wsparciu krajowych i unijnych inicjatyw na rzecz zwiększania odporności infrastruktury krytycznej na zagrożenia hybrydowe.

https://abw.gov.pl/wyd/terroryzm-studia-analizy-prewe/1974,Wstep.html

Redaktor naczelny
dr Damian Szlachter

ARTYKUŁY

Terroryzm – studia, analizy, prewencja, 2025, nr 7: 13–33

https://doi.org/10.4467/27204383TER.25.025.21802

Artykuł

Nowe oblicze zagrożenia terrorystycznego w Unii Europejskiej. Analiza „TE-SAT. European Union Terrorism Situation and Trend Report 2024" i innych źródeł

The new face of terrorist threat in the European Union. Analysis of the EU Terrorism Situation and Trend Report 2024 (TE-SAT) and other sources

SEBASTIAN WOJCIECHOWSKI https://orcid.org/0000-0002-7972-6618

Uniwersytet im. Adama Mickiewicza w Poznaniu
Instytut Zachodni w Poznaniu

ARTUR WEJKSZNER https://orcid.org/0000-0002-7638-9708

Uniwersytet im. Adama Mickiewicza w Poznaniu

Abstrakt

W artykule dokonano analizy zagrożenia terrorystycznego w Unii Europejskiej w 2023 r. na podstawie *TE-SAT. European Union Terrorism Situation and Trend Report 2024* opublikowanego w grudniu 2024 r. i innych źródeł. Autorzy opisują zarówno aspekt przedmiotowy zagrożenia (ze strony grup etnonacjonalistycznych i separatystycznych, skrajnie lewicowych i anarchistycznych, dżihadystycznych oraz skrajnie prawicowych), jak i ilościowy (liczba zdarzeń o charakterze terrorystycznym oraz liczba osób zaangażowanych w poszczególne typy aktywności terrorystycznej). W 2023 r. odnotowano w UE aż 120 ataków terrorystycznych, w tym 98 przeprowadzonych, 9 nieudanych i 13 udaremnionych. Dla porównania w 2021 r. zarejestrowano 18 ataków, a w 2022 r. – 28.

W 2023 r. nastąpił zatem ponadczterokrotny wzrost w stosunku do poprzedniego roku. Do ataków doszło w 7 państwach UE: Francja – 80, Włochy – 30, Niemcy i Hiszpania – po 3, Belgia – 2, Grecja oraz Luksemburg – po 1. W 2023 r. aresztowano 426 osób oskarżonych o przestępstwa powiązane z terroryzmem. Dla porównania w 2022 r. było ich 380. Do największej liczby takich przypadków w 2023 r. doszło w Hiszpanii, Francji, Belgii i Niemczech – ponad 50 w każdym z tych państw. Oznacza to, że terroryzm stanowi poważne zagrożenie dla bezpieczeństwa UE zarówno w wymiarze wertykalnym (dotyczącym liczby ataków oraz liczby osób oskarżonych o terroryzm), horyzontalnym (odnoszącym się do zróżnicowanej taktyki i strategii działania sprawców), jak i behawioralnym (analizującym zróżnicowaną motywację oraz profil działania terrorystów).

Słowa kluczowe

terroryzm, Unia Europejska, bezpieczeństwo, Europol

Abstract

This article focuses on the issue of the terrorist threat in the European Union in 2023. The starting point for the analysis is Europol's latest report entitled 'TE-SAT. European Union Terrorism Situation and Trend Report 2024', and other sources. The analysis covers both the substantive aspect (in the form of articulating the threat from jihadists, far-right, far-left, anarchist, ethno-national and separatist groups) and the quantitative aspect (indicating the number of terrorist incidents and the number of people involved in particular types of terrorist activity). In 2023, as many as 120 terrorist attacks were reported in the EU, including 98 completed, 9 failed and 13 foiled. This compares with 18 attacks in 2021 and 28 in 2022. – 28. In 2023 there was over a fourfold increase in the number of attacks compared to the previous year. The attacks occurred in 7 EU countries: France – 80, Italy – 30, Germany and Spain – 3, Belgium – 2, Greece and Luxembourg – 1. In 2023, 426 people were arrested for terrorism – in 2022 – 380. The highest number of arrests in 2023 was in Spain, France, Belgium, and Germany – over 50 in each of them. It means that terrorism poses a serious threat to the security of the EU in a vertical dimension (concerning the number of attacks and accused of terrorism), a horizontal dimension (relating to the diverse tactics and strategies of the perpetrators), and a behavioral dimension (analyzing the motivations and profiles of terrorists).

Keywords

terrorism, European Union, security, Europol

Wprowadzenie

Ponowna eskalacja zagrożenia terrorystycznego, która następuje w latach 20. XXI w. w różnych częściach świata, oraz towarzyszące temu zjawiska niestety nie zawsze są dostrzegane, a środki przeciwdziałania – odpowiednio implementowane. Ilustrują to wyniki raportu na temat zagrożeń dla współczesnego świata, który ukazał się przed obradami Światowego Forum Ekonomicznego (World Economic Forum) w Davos (20–24 stycznia 2025 r.). Z tego publikowanego cyklicznie badania wynika, że w ocenie zdecydowanej większości spośród ponad 900 respondentów (liderów biznesu, polityki i nauki) terroryzm[1] nie jest istotnym zagrożeniem w perspektywie najbliższych 12 miesięcy, kolejnych 2 lat czy dekady[2]. Na pierwszym miejscu wśród odpowiedzi dotyczących zagrożeń w 2025 r. uplasował się konflikt zbrojny na tle państwowym (ang. *state-based armed conflict*) – 23%. Taki wybór respondenci tłumaczyli m.in. największym od czasu zakończenia zimnej wojny poziomem światowej polaryzacji[3]. Podkreślili ponadto, że w ciągu ostatniej dekady wzrosła liczba wojen. Zwraca na to uwagę również Stockholm International Peace Research Institute (SIPRI), według ustaleń którego w 2023 r. aż 52 państwa doświadczyły konfliktów zbrojnych[4]. Na kolejnych miejscach w rankingu odpowiedzi znalazły się ekstremalne zjawiska pogodowe (ang. *extreme weather events*) – 14% odpowiedzi i konfrontacja geoekonomiczna (ang. *geoeconomic confrontation*) – 8%. Ponadto w pierwszej piątce wymieniono wprowadzanie w błąd i dezinformację (ang. *misinformation and disinformation*) – 7% oraz polaryzację społeczną (ang. *societal polarization*) – 6%. Za największe niebezpieczeństwa w następnych dwóch latach uznano: dezinformację, ekstremalne zjawiska pogodowe, eskalację działań zbrojnych, polaryzację społeczeństw oraz cyberwojny.

[1] Na temat definiowania pojęcia terroryzmu zob. np. S. Wojciechowski, *The Hybridity of Terrorism: Understanding Contemporary Terrorism*, Berlin 2013; *The Routledge Companion to Terrorism Studies. New Perspectives and Topics*, M. Abrahms (red.), London 2024; K. Maniszewska, *Towards a New Definition of Terrorism: Challenges and Perspectives in a Shifting Paradigm*, series: Contributions to Security and Defence Studies, Cham 2024. https://doi.org/10.1007/978-3-031-58719-1.

[2] *The Global Risks Report 2025. 20th Edition. Insight Report*, World Economic Forum, https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf [dostęp: 6 II 2025].

[3] Tamże, s. 7–8.

[4] R. Gowan, *Overview, 2. Trends in armed conflicts*, w: *SIPRI Yearbook 2024*, Stockholm International Peace Research Institute, https://www.sipri.org/yearbook/2024/02 [dostęp: 5 II 2025].

Nieco inaczej prezentowały się odpowiedzi dotyczące postrzegania niebezpieczeństw w perspektywie dekady. W tym przypadku pierwsze 4 z 5 dominujących kategorii dotyczyły różnych zagadnień środowiskowych, ostatnia natomiast – wprowadzania w błąd i dezinformacji. W przeciwieństwie do niektórych wcześniejszych raportów[5] nigdzie nie wskazano terroryzmu. Jest to tym bardziej zaskakujące, że do jego eskalacji w zróżnicowanym stopniu dochodzi od kilku lat w różnych częściach świata[6], w tym w Afryce, na Bliskim Wschodzie czy w Unii Europejskiej, o czym będzie mowa w dalszej części artykułu.

Co więcej, jak wynika z badania Fundacji Bertelsmanna przeprowadzonego w 2024 r. w 27 państwach członkowskich UE oraz w Wielkiej Brytanii z udziałem ponad 26 000 respondentów, ataki terrorystyczne są drugim (21% wskazań) największym zagrożeniem pokoju w Europie, po braku skutecznej ochrony granic (25%). Na kolejnych miejscach wymieniono duże cyberataki (19%), atak obcego mocarstwa (18%) oraz przestępczość zorganizowaną (17%)[7].

Za punkt wyjścia analizy przeprowadzonej w ramach tego artykułu przyjęto hipotezę, że terroryzm stanowi poważne zagrożenie bezpieczeństwa państw członkowskich UE i ich mieszkańców zarówno w wymiarze wertykalnym (dotyczącym liczby ataków oraz osób oskarżonych o terroryzm), horyzontalnym (odnoszącym się do zróżnicowanej taktyki i strategii działania sprawców), jak i behawioralnym (analizującym motywację oraz profil działania terrorystów)[8].

---

[5] Zob. np. *The Global Risks Report 2021. 16th Edition. Insight Report*, World Economic Forum, https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf [dostęp: 7 II 2025]; *The Global Risks Report 2022. 17th Edition. Insight Report*, World Economic Forum, https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf [dostęp: 12 V 2025].

[6] Zob. np. R. Gunaratna, *Global Terrorism Threat Forecast 2025*, „RSIS Commentary" 2025, nr 002; *Security Council debates growing terrorism threat in Africa*, United Nations, 21 I 2025 r., https://news.un.org/en/story/2025/01/1159246 [dostęp: 8 II 2025].

[7] I. Hoffmann, C.E. De Vries, *Old Habits Die Hard – Member States Report. Part II: Remaking the Transatlantic Partnership: Public Opinion in the EU and seven Member States*, Eupinions, 20 XI 2024 r., https://eupinions.eu/de/text/old-habits-die-hard-member-states-report [dostęp: 15 III 2025].

[8] Na temat przyczyn terroryzmu zob. szerzej: S. Wojciechowski, *Reasons of Contemporary Terrorism. An Analysis of Main Determinants*, w: *Radicalism and Terrorism in the 21st Century. Implications for Security*, A. Sroka, F. Castro-Rial Garrone, R.D. Torres Kumbrián (red.), Frankfurt am Main 2017.

Zagrożenie terrorystyczne w kontekście sytuacji w Afryce, na Bliskim Wschodzie i wojny w Ukrainie

W raporcie Europolu *TE-SAT. European Union Terrorism Situation and Trend Report 2024*[9] zaprezentowano nie tylko zakres i charakter zagrożenia w UE, lecz także związany z nimi szerszy kontekst, dotyczący m.in. wojny w Ukrainie, sytuacji na Bliskim Wschodzie czy eskalacji terroryzmu w Afryce. Na ten ostatni aspekt zwrócono uwagę również w raporcie United States Africa Command (AFRICOM)[10]. Wskazano w nim, że w pierwszej połowie 2024 r. tylko Państwo Islamskie (Islamic State of Iraq and Syria, ISIS) i powiązane z nim grupy przeprowadziły na świecie 788 ataków, z których aż do 536 doszło w Afryce. Nawiązują do tego informacje przekazane Radzie Bezpieczeństwa Organizacji Narodów Zjednoczonych przez komisarza Unii Afrykańskiej ds. Politycznych, Pokoju i Bezpieczeństwa (Political Affairs, Peace and Security, PAPS) Bankole Adeoye. Wynika z nich, że obecnie Afryka jest obszarem najbardziej zagrożonym terroryzmem. W 2024 r. doszło tam do ponad 3400 ataków terrorystycznych, w których śmierć poniosło prawie 14 000 osób. Dotyczy to przede wszystkim Afryki Subsaharyjskiej, gdzie zginęło 59% spośród wszystkich ofiar terroryzmu na świecie. Rozprzestrzenianie się Al-Kaidy i ISIS z Mali, Nigru i Burkiny Faso na państwa nadmorskie Afryki Zachodniej, takie jak Nigeria, Benin, Togo, Ghana, Wybrzeże Kości Słoniowej, spowodowało wzrost liczby ataków o 250% względem lat 2022–2024. Zastępczyni Sekretarza Generalnego Rady Bezpieczeństwa ONZ Amina Mohammed skomentowała to następująco: *Tragiczne jest to, że Afryka pozostaje epicentrum globalnego terroryzmu*[11]. Pogarszające się tam warunki ekonomiczne, społeczne i polityczne, skutkujące m.in. masową migracją czy konfliktami zbrojnymi, to czynniki, które mają wpływ na wzrost zagrożenia terrorystycznego w Afryce. To wszystko destabilizuje sytuację nie tylko w regionie, lecz także poza nim, w tym w UE[12].

[9] Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2024*, https://www.europol.europa.eu/cms/sites/default/files/documents/TE-SAT%202024.pdf [dostęp: 9 II 2025].

[10] *U.S. Africa Command Civilian Casualty Assessment Report; 2nd Quarter, FY2024*, https://www.africom.mil/what-we-do/airstrikes/civilian-harm-report/us-africa-command-civilian-casualty-assessment-report-2nd-quarter-fy2024 [dostęp: 14 IV 2025].

[11] *Security Council debates growing terrorism...* Tłumaczenie pochodzi od autorów (dop. red.).

[12] Zob. np. S. Wojciechowski, P. Osiewicz, *Zrozumieć współczesny terroryzm*, Warszawa 2017.

Wyraźne odradzanie się ISIS i towarzyszącą temu operacyjno-propagandową ofensywę skomentował szef Biura ONZ ds. Zwalczania Terroryzmu (United Nations Office of Counter-Terrorism, UNOCT) Władimir Woronkow. Podkreślił on, że ISIS i jego filie zaczęły prowadzić działalność również poza Afryką – w Syrii, Iraku czy Afganistanie[13], co spowodowało znaczny wzrost liczby ataków i ich ofiar, głównie wśród ludności cywilnej[14]. Jest to wywołane m.in. spektakularnym sukcesem opozycji w Syrii, w tym jej islamistycznych nurtów reprezentowanych także przez ISIS. Zarówno to, jak i wcześniejsze sukcesy ISIS w Syrii czy Iraku oraz Talibów w Afganistanie są propagandowo wykorzystywane przez fundamentalistów.

Z kolei w Europie od października 2023 r. do początku 2025 r. aktywność dżihadystów wzrosła czterokrotnie, na co wskazuje Peter Neumann, ekspert ds. terroryzmu z King's College London[15]. Na przykład w Hiszpanii w 2024 r. zatrzymano 81 osób podejrzanych o dżihadyzm, w tym 25 w Katalonii. Liczba osób aresztowanych w związku z podejrzeniami o działalność dżihadystyczną zwiększyła się w tym państwie drugi rok z rzędu i osiągnęła poziom niespotykany od czasu ataków terrorystycznych w Madrycie w marcu 2004 r.

Wśród państw UE o podwyższonym poziomie ryzyka terrorystycznego należy wymienić zarówno te już dotychczas często atakowane, np. Francję, Włochy, Hiszpanię czy Niemcy, jak i inne, np. Polskę. Chociaż we wskazanym raporcie Europolu nie odnotowano żadnej próby ataku w Polsce i tylko 1 przypadek aresztowania z powodu działalności terrorystycznej, to ten kazus jest ważny m.in. ze względu na zaangażowanie Polski na rzecz Ukrainy. Na podwyższenie poziomu tego ryzyka w dużym stopniu wpływa także kumulacja zagrożenia zarówno ze strony terroryzmu państwowego inspirowanego np. przez Rosję, Białoruś czy Iran, jak i pozapaństwowego, który przybiera różne formy: etnonacjonalistyczny i separatystyczny, skrajnie lewicowy i anarchistyczny, islamistyczny, skrajnie prawicowy. Na wzrost zagrożenia terrorystycznego w wybranych państwach UE wskazuje również

[13] S. Wojciechowski, *History Repeats Itself. The Issue of Terrorism and Afghanistan on the Twentieth Anniversary of the 9/11 Attacks*, „Przegląd Strategiczny" 2021, nr 14, s. 9–22. https://doi.org/10.14746/ps.2021.1.1.

[14] *Nineteenth report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat*, United Nations Security Council, 31 VII 2024 r., https://docs.un.org/en/S/2024/583 [dostęp: 6 II 2025].

[15] M. Auermann, F. Piatov, *Der IS-Terror ist zurück!*, Bild, 3 I 2025 r., https://www.bild.de/politik/ausland-und-internationales/top-experte-warnt-in-bild-der-is-terror-ist-zurueck-677687610195b908c1898f69 [dostęp: 13 IV 2025].

Global Terrorism Index 2025 opublikowany przez Institute for Economics & Peace. Wynika z niego, że w 2024 r. liczba incydentów terrorystycznych w Europie podwoiła się w stosunku do danych z poprzedniego raportu – było ich 67. Dotyczyły one przede wszystkim 6 państw: Szwecji, Finlandii, Holandii, Danii, Szwajcarii oraz Niemiec. W przypadku niektórych państw członkowskich UE zwiększyła się także ocena poziomu zagrożenia terrorystycznego (Global Terrorism Index). Najwyżej – tj. na 27 miejscu – sklasyfikowano pod tym względem Niemcy, co stanowi przesunięcie w górę o 13 pozycji względem danych z poprzedniego raportu. Kolejne miejsca zajęły: Grecja – 36 (spadek o 1 lokatę), Czechy – 39 (spadek o 6), Francja – 40 (spadek o 2), Polska – 47 (wzrost aż o 33), Szwecja – 50 (wzrost o 22)[16].

Zagrożenie terrorystyczne w Unii Europejskiej w 2023 r. – analiza raportu TE-SAT

W przypadku UE jednym z ważniejszych źródeł informacji na temat zagrożenia terrorystycznego są coroczne raporty Europolu pt. *TE-SAT European Union Situation and Trend Report*. Jego analizowana wersja opublikowana w grudniu 2024 r. dotyczy danych za 2023 r. i została przygotowana we współpracy z państwami członkowskimi UE oraz innymi partnerami zaangażowanymi w zwalczanie terroryzmu. Raport ze wstępem dyrektor wykonawczej Europolu Catherine De Bolle zawiera analizę najważniejszych trendów, które obecnie mają wpływ na zjawisko terroryzmu. Są w nim informacje dotyczące m.in. przeprowadzonych, nieudanych oraz udaremnionych ataków, liczby osób aresztowanych z powodu działalności terrorystycznej, a także prowadzonych postępowań sądowych. Uwzględniono w nim różne rodzaje terroryzmu, takie jak: etnonacjonalistyczny i separatystyczny (ang. *ethno-nationalist and separatist*), skrajnie lewicowy i anarchistyczny (ang. *left-wing and anarchist*), dżihadystyczny (ang. *jihadist*) oraz skrajnie prawicowy (ang. *right-wing*).

W 2023 r. odnotowano w UE aż 120 ataków terrorystycznych, w tym 98 przeprowadzonych, 9 nieudanych i 13 udaremnionych. Dla porównania, w 2021 r. odnotowano 18 ataków, a w 2022 r. – 28. W 2023 r. nastąpił zatem ponadczterokrotny wzrost w stosunku do poprzedniego roku. Te dane

[16] *Global Terrorism Index 2025*, Institute for Economics & Peace, https://www.economicsandpeace.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf [dostęp: 4 V 2025].

pokazują, że terroryzm stanowi coraz poważniejsze zagrożenie bezpieczeństwa państw członkowskich UE.

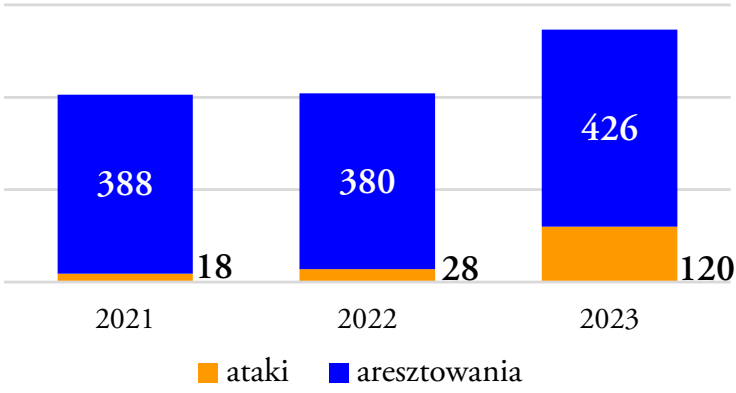
Na uwagę zasługuje duża dysproporcja między liczbą ataków przeprowadzonych a udaremnionych w 2023 r. W tym roku ataki dotyczyły 7 państw UE: Francji – 80, Włoch – 30, Niemiec i Hiszpanii – po 3, Belgii – 2, Grecji i Luksemburga – po 1. Ponad 90% przypadków dotyczyło zatem 2 państw – Francji i Włoch. W nich też zarejestrowano najwięcej przeprowadzonych zamachów, odpowiednio 72 i 23. Pozostałe nastąpiły w Belgii, Niemczech i Hiszpanii – po 1. Do nieudanych ataków doszło we Włoszech – 7 oraz w Grecji i Hiszpanii – po 1. Udaremniono natomiast: we Francji – 8 ataków, w Niemczech – 2, w Belgii, Luksemburgu i Hiszpanii – po 1. Najwięcej aktów terrorystycznych było skierowanych przeciwko infrastrukturze krytycznej – 15 zdarzeń, pozostałe wymierzono m.in. w firmy prywatne – 7, ludność cywilną – 4 i funkcjonariuszy policji – 3. Najczęstszą formą ataku było podpalenie – 20, pozostałe wskazane to: zamachy bombowe – 8, niszczenie mienia – 6, ataki z użyciem noża – 6 i broni palnej – 5.

Zjawisko terroryzmu w raportach Europolu jest rozpatrywane także pod względem wskaźnika osób aresztowanych z powodu działalności terrorystycznej czy postępowań sądowych prowadzonych w tym zakresie. Przykładowo w 2023 r. organy ścigania w państwach członkowskich UE zatrzymały 426 osób oskarżonych o przestępstwa powiązane z terroryzmem. Dla porównania w 2022 r. było ich 380 (wykres 1). Najwięcej takich przypadków było w 2023 r. w Hiszpanii, we Francji, w Belgii i Niemczech – ponad 50 w każdym z tych państw. Spadła natomiast, jak informuje Eurojust, liczba wyroków sądowych, których w 2023 r. było 358, podczas gdy w 2022 r. – 427. Postępowania sądowe zakończone w 2023 r. doprowadziły do 290 wyroków skazujących i 68 uniewinnień w 14 państwach UE[17].

Ataki terrorystyczne są realizowane już od dawna z wykorzystaniem wielu środków, od użycia noża czy samochodu przez zastosowanie broni palnej, materiałów wybuchowych, a nawet tzw. brudnej bomby, po atak dronów czy w cyberprzestrzeni. Zaobserwowano również znaczny wzrost pozyskiwania online materiałów szkoleniowych, instrukcji co do taktyki i strategii przeprowadzania ataków, informacji na temat wytworzenia broni w technologii 3D, militarnego wykorzystania dronów, zdobycia broni palnej czy materiałów wybuchowych, a nawet możliwości posiadania broni chemicznej. Dotyczy to osób o różnych poglądach i powiązaniach

[17] Europol, *TE-SAT. European Union Terrorism Situation...*, s. 15.

ideologicznych, które trudno przypisać do jednego nurtu, np. islamistycznego czy skrajnie prawicowego. Dochodzi do tego kwestia wykorzystywania sztucznej inteligencji przez terrorystów lub ich sympatyków. Internet i technologie cybernetyczne, z których chętnie korzystają młodzi ludzie, pozostają ważnym narzędziem stosowanym np. w celach propagandowych, werbunkowo-rekrutacyjnych czy do pozyskiwania środków finansowych. Służą one też do wpływania na radykalizację postaw i propagowania mowy nienawiści. Generuje to poważne następstwa, m.in. przeprowadzanie ataków przez coraz młodszych zamachowców. Na przykład podczas świąt Bożego Narodzenia w 2024 r. niemiecka policja zatrzymała 15-letniego terrorystę, który planował zamach na kościół w Berlinie. Podkreślenia wymagają również coraz silniejsze związki w ramach triady: terrorysta/terroryści – grupy przestępcze – służby specjalne państw wrogich wobec UE.



Wykres 1. Liczba przeprowadzonych, nieudanych lub udaremnionych ataków terrorystycznych oraz osób aresztowanych z powodu działalności terrorystycznej w Unii Europejskiej w latach 2021–2023.

Źródło: Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2024*, https://www.europol.europa.eu/cms/sites/default/files/documents/TE-SAT%202024.pdf, s. 11 [dostęp: 9 II 2025].

Dane statystyczne potwierdzają, że terroryzm pozostaje zagrożeniem o złożonym charakterze, obejmującym różne ideologie, formy czy metody działania. W raporcie Europolu podkreślono, że zjawisko terroryzmu w UE wynika z różnych przesłanek i nie ma, jak nadal dość często błędnie się uważa, tylko podłoża islamistycznego (tabela 1).

Tabela 1. Liczba przeprowadzonych, nieudanych lub udaremnionych ataków terrorystycznych w Unii Europejskiej w 2023 r. z podziałem na motywację zamachowców.

PAŃSTWO/ rodzaj terroryzmu	DŻIHADYSTYCZNY	PRAWICOWY	LEWICOWY I ANARCHISTYCZNY	ETNONACJONALISTYCZNY I SEPARATYSTYCZNY	INNE	RAZEM
Belgia	2					2
Francja	8	1		70	1	80
Niemcy	3					3
Grecja			1			1
Włochy			30			30
Luksemburg		1				1
Hiszpania	1		1		1	3
RAZEM	14	2	32	70	2	120

Źródło: Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2024*, https://www.europol.europa.eu/cms/sites/default/files/documents/TE-SAT%20 2024.pdf, s. 62 [dostęp: 9 II 2025]. Dokonano zmian w postaci tłumaczenia i oprawy graficznej (dop. red.).

W raporcie są wymienione także 2 incydenty, w przypadku których nie wskazano motywacji zamachowców. Jednym z nich było zastrzelenie 9 listopada 2023 r. w Madrycie hiszpańskiego polityka przez niezidentyfikowanego sprawcę. Nie są też znane powody jego postępku[18]. Czyn ten należy uznać za wyłącznie kryminalny, ponieważ uznanie czegoś za akt terroryzmu wymaga poznania rzeczywistych motywów sprawcy.

Terroryzm etnonacjonalistyczny i separatystyczny

Zdecydowanie największą aktywność terrorystyczną podejmowali w 2023 r. terroryści motywowani ideologią etnonacjonalistyczną i separatystyczną[19]. W tym okresie odnotowano 70 ataków terrorystycznych o takim podłożu, wszystkie przeprowadzono na Korsyce we Francji. Do 34, czyli prawie połowy, doszło w nocy z 8 na 9 października. Afiliacja osób aresztowanych w związku z terroryzmem motywowanym ideologią etnonacjonalistyczną i separatystyczną obejmowała następujące organizacje terrorystyczne: korsykańskie Fronte di Liberazione Naziunale Corsu (FLNC) i Ghjuventù clandestina Corsa (GcC), irlandzką Dissident Republican, kurdyjską Partiya Karkerên Kurdistanê (PKK) oraz baskijską Euskadi ta Askatasuna (ETA). Do zatrzymań i aresztowań osób podejrzewanych o aktywność terrorystyczną doszło także we Włoszech, Szwecji, Niemczech i Grecji. Wśród oskarżeń, jakie wniesiono przeciwko aresztowanym, znalazły się: uczestnictwo w spiskach terrorystycznych, posiadanie broni, finansowanie terroryzmu oraz rekrutacja i propagowanie aktywności terrorystycznej[20].

Terroryzm skrajnie lewicowy i anarchistyczny

Grupy skrajnie lewicowe[21] i anarchistyczne wykazywały w UE w 2023 r. znacznie większą aktywność w porównaniu z grupami dżihadystycznymi

[18] Tamże, s. 55.

[19] W raporcie Europolu w opisie grup terrorystycznych o charakterze etnonacjonalistycznym i separatystycznym wskazano, że te grupy odwołują się w ramach agendy politycznej do nacjonalizmu czy też przynależności etnicznej lub religijnej. Celem tych grup jest stworzenie własnego terytorium przez oddzielenie od już istniejącego państwa lub przyłączenie oddzielonego terytorium do innego państwa. Zob. tamże, s. 51.

[20] Tamże, s. 51–52.

[21] W raporcie Europolu terroryzm grup skrajnie lewicowych (ang. *left-wing terrorism*) jest rozumiany jako użycie przemocy, aby wywołać gwałtowną rewolucję marksistowsko-leninowską skierowaną przeciwko demokratycznemu państwu, której celem jest ustanowienie socjalizmu, komunizmu czy też bezklasowego społeczeństwa. Celem terroryzmu anarchistycznego jest zaś zniszczenie aktualnego modelu władzy politycznej

i skrajnie prawicowymi. Ich członkowie byli odpowiedzialni za 32 incydenty terrorystyczne, z których 23 zakończyły się przeprowadzeniem zamachów terrorystycznych. Wszystkich dokonano we Włoszech. Również głównie w tym państwie udaremniono ataki – 7, a w Grecji i Hiszpanii – po 1. Według danych publikowanych przez samych anarchistów większość ataków przeprowadzono w geście solidarności z więzionymi przez włoskie władze członkami Informal Anarchist Federation/International Revolutionary Front (IAF/FAI). Atak anarchistów w Hiszpanii również był wyrazem poparcia dla uwięzionych we Włoszech. Modus operandi zamachowców nie różnił się od tego z poprzednich lat i obejmował m.in. wykorzystanie improwizowanych ładunków wybuchowych (ang. *improvised explosive devices,* IED), które detonowano w pobliżu masztów telefonii mobilnej czy innej infrastruktury firm telekomunikacyjnych i energetycznych, a także podpalenia czy fizyczne niszczenie, głównie nieruchomości. Zamachy były usprawiedliwiane hasłami antykapitalistycznymi (krytyka coraz silniejszej roli korporacji we włoskiej gospodarce), antypaństwowymi i antywojennymi (w tym sprzeciw wobec NATO)[22], krytykowano rosnącą techniczno-przemysłową dominację współczesnych potęg (państwowych i niepaństwowych), pogarszanie się sytuacji gospodarczej (w tym zwiększającą się inflację), wzrost popularności grup neofaszystowskich, brak poszanowania praw robotników i migrantów oraz kryzys klimatyczny i wzmagające się represje ze strony struktur państwowych. W związku z tym nie dziwi to, że celami ataków byli także funkcjonariusze państwowi, w tym policjanci i pracownicy wymiaru sprawiedliwości. Włoskim władzom udało się aresztować jedynie 10 osób z tej bardzo aktywnej grupy terrorystycznej. Pozostałe osoby zatrzymano w Hiszpanii – 1, Niemczech – 1 i Grecji – 2. W większości byli to mężczyźni w przedziale wiekowym od 27 do 75 lat. Aresztowano także jedną kobietę[23]. Część zatrzymanych była związana z turecką DHKP-C (The Revolutionary People's Liberation Party/Front, tur. Devrimci Halk Kurtulus Partisi-Cephesi)[24]. Terroryści powiązani z ideologią lewicową i anarchistyczną zdobywali środki na swoją aktywność w sposób podobny do wcześniej omawianych grup, tj. z wykorzystaniem źródeł zarówno legalnych, jak i nielegalnych.

i zastąpienia go modelem antydyskryminacyjnym i antykapitalistycznym, promującym równość, wolność i sprawiedliwość społeczną. Zob. tamże, s. 43.

22 Tamże, s. 46.

23 Tamże, s. 45–48.

24 Tamże, s. 47–48.

Terroryzm dżihadystyczny

W UE w 2023 r. w porównaniu z poprzednim rokiem wzrosła aktywność terrorystyczna podejmowana przez dżihadystów[25]. Na terytorium Francji, Belgii, Niemiec i Hiszpanii terroryści o takich powiązaniach przeprowadzili lub próbowali przeprowadzić 14 zamachów. Zginęło w nich 6 osób, a 12 zostało rannych. Modus operandi sprawców obejmował aktywność tzw. samotnych wilków luźno powiązanych z istniejącymi grupami terrorystycznymi[26]. Sprawcami ataków byli wyłącznie mężczyźni, którzy zabijali swoje ofiary najczęściej przez pchnięcie nożem. Tylko raz, w przypadku zamachu w Brukseli, użyto broni palnej. Do ataków doszło wyłącznie na obszarach zurbanizowanych. Wskazana liczba obejmuje także 9 spisków terrorystycznych, które udało się zawczasu wykryć: najwięcej we Francji – 6, a także w Niemczech – 2 i w Belgii – 1[27]. Interesującym zjawiskiem jest brak jednoznacznych powiązań sprawców z istniejącymi grupami terrorystycznymi. Służbom policyjnym udało się potwierdzić powiązanie zamachowców z ISIS jedynie w 4 przypadkach, a tylko za 1 przypadek ISIS wzięło na siebie pełną odpowiedzialność[28]. O istnieniu rozbudowanej dżihadystycznej sieci terrorystycznej na obszarze UE[29] może świadczyć aresztowanie przez organy ścigania 334 osób. Ta liczba wzrosła o 68 z 266

[25] W raporcie Europolu dżihadyzm jest definiowany jako radykalny nurt salafizmu (ruchu odrodzenia sunnickich muzułmanów), którego zwolennicy odrzucają współczesną demokrację, argumentując, że ustawodawstwo tworzone przez ludzi jest sprzeczne ze statusem Boga jako jedynego prawodawcy. Dżihadyści dążą do stworzenia państwa islamskiego rządzonego wyłącznie prawem islamskim (szariatem). W przeciwieństwie do innych nurtów salafickich dżihadyści legitymizują stosowanie przemocy, odwołując się do islamskich doktryn dżihadu (ten termin oznacza dosłownie 'dążenie' lub 'wysiłek', ale dżihadyści interpretują go jako wojnę sankcjonowaną religijnie). Wszyscy, którzy sprzeciwiają się dżihadystycznym interpretacjom prawa islamskiego, są uważani za wrogów islamu, a zatem stają się uzasadnionymi celami ataków. Niektórzy dżihadyści do grupy wrogów zaliczają szyitów i innych muzułmanów. Zob. Europol, *TE-SAT. European Union Terrorism Situation...*, s. 20. Zagadnienie terroryzmu dżihadystycznego zostało w tym artykule opisane bardziej szczegółowo niż inne rodzaje terroryzmu w UE z uwagi na szczególny w ostatnich latach wpływ tego typu incydentów o charakterze terrorystycznym na zadania realizowane przez organy ścigania.

[26] Na temat samotnych wilków zob. szerzej: A. Wejkszner, *Samotne wilki kalifatu? Państwo Islamskie i indywidualny terroryzm dżihadystyczny w Europie Zachodniej*, Warszawa 2018, s. 27–47.

[27] Europol, *TE-SAT. European Union Terrorism Situation...*, s. 20.

[28] Tamże.

[29] Na ten temat zob. szerzej: A. Wejkszner, *Europejska armia kalifatu. Tom 1. Centrum supersieci*, Warszawa 2020, s. 30–48.

w poprzednim roku. Spośród aresztowanych 133 osoby nie miały obywatelstwa państwa należącego do UE. Zdecydowaną większość aresztowanych (276 osób) stanowili mężczyźni. Zatrzymanych oskarżono o przynależność do organizacji terrorystycznej – 30%, planowanie lub przeprowadzenie ataku – 14%, finansowanie działalności terrorystycznej – 12%[30]. Postępowania sądowe w 208 przypadkach zakończyły się wyrokami skazującymi. Najwięcej skazanych pochodziło z Belgii, Francji, Niemiec i Austrii. Ich przynależność do grupy terrorystycznej, jeśli została potwierdzona, obejmowała sieci 2 największych i konkurencyjnych wobec siebie dżihadystycznych organizacji terrorystycznych działających na terytorium UE, tj. ISIS i Al-Kaidy. Mimo utraty wpływów przez oba ugrupowania na Bliskim Wschodzie były one w stanie zwiększać swoją obecność w Europie. W tym przypadku nie chodzi o rozbudowę struktur organizacyjnych, lecz o popularyzację ideologii dżihadystycznej, której skutkiem jest radykalizacja terrorystyczna wielu młodych ludzi. Co więcej, ten proces się skrócił i zintensyfikował, a jego uczestnicy są gotowi na użycie przemocy przeciwko cywilom[31]. Oznacza to utrzymywanie się zagrożenia ze strony indywidualnego terroryzmu dżihadystycznego[32]. Nie udało się uniknąć także dodatkowych zagrożeń w postaci radykalizacji dżihadystycznej w więzieniach, niskiej efektywności procesu deradykalizacji oraz powrotów na terytorium UE (często z wykorzystaniem fałszywych dokumentów tożsamości) tzw. zagranicznych bojowników (czy też zagranicznych bojowników terrorystycznych)[33]. Procesy te były wzmacniane przez propagandę dżihadystów podejmowaną przede wszystkim w dark webie[34]. Wśród najczęściej pojawiających się tam wątków narracyjnych znalazły się: rosnąca opresja wobec muzułmanów w Europie, brak reakcji na znieważenie Koranu w Szwecji, Danii czy Holandii, gloryfikacja aktywności terrorystycznej Hamasu, zwłaszcza po ataku na Izrael z 7 października 2023 r., oraz wsparcie rosnącej polaryzacji na Bliskim Wschodzie i antycypowanej wojny religijnej muzułmanów z żydami czy

[30] Europol, *TE-SAT. European Union Terrorism Situation…*, s. 23.

[31] Tamże, s. 25.

[32] Zob. I.J. Sandboe, M. Obaidi, *Imagined Extremist Communities: The Paradox of the Community-Driven Lone-Actor Terrorist*, „Perspectives on Terrorism" 2023, t. 17, nr 4, s. 19–41. https://doi.org/10.19165/CAQH8148.

[33] Zob. A. Wejkszner, *Państwo Islamskie. Narodziny nowego kalifatu?*, Warszawa 2016, s. 164–169.

[34] Europol, *TE-SAT. European Union Terrorism Situation…*, s. 27–28.

reprezentantami innych grup religijnych. Otwarcie nawoływano do atakowania celów symbolicznych, np. miejsc kultu.

Terroryzm skrajnie prawicowy

Terroryzm grup skrajnie prawicowych[35] w UE stanowił w 2023 r. najmniejsze zagrożenie, zdecydowanie mniejsze niż terroryzm dżihadystyczny. W tym okresie doszło do próby użycia przemocy motywowanej ideologią skrajnie prawicową raz we Francji i raz w Luksemburgu. Taka motywacja charakteryzowała przede wszystkim terrorystów indywidualnych, nienależących do żadnej znanej organizacji terrorystycznej. Aresztowano 26 osób oskarżonych o udział w działaniach terrorystycznych motywowanych ideologią skrajnie prawicową, w tym 5 w Holandii oraz po 4 we Francji i w Belgii. Byli to wyłącznie mężczyźni, prawie zawsze obywatele państwa, na terenie którego zostali zatrzymani. Celem ich ataków były różnego rodzaju mniejszości, np. religijne czy seksualne. Posługiwali się głównie bronią palną, zdobytą najczęściej legalnie – co jest ewenementem w odniesieniu do terrorystów motywowanych innymi ideologiami – a także bronią białą oraz IED. W raportach policyjnych wskazywano, że sposobem na pozyskanie broni palnej, np. karabinka półautomatycznego FGC-9[36], było wykorzystanie nowoczesnych technologii, takich jak drukarki 3D[37]. Popularność terroryzmu motywowanego ideologią skrajnie prawicową widać także w liczbie osób skazanych – 35, która wzrosła w stosunku do poprzedniego roku.

[35] Twórcy raportu Europolu termin „terroryzm grup skrajnie prawicowych" (ang. *right-wing terrorism*) rozumieją jako użycie przemocy w celu przekształcenia współczesnego systemu politycznego, społecznego i ekonomicznego w model autorytarny, w którym wartości i instytucje demokratyczne zostałyby odrzucone. Prawicowe ideologie odwołujące się do tego modelu wykorzystują agresywną narrację skupioną na nacjonalizmie, rasizmie, ksenofobii czy innych przejawach nietolerancji. Podstawową koncepcją prawicowego ekstremizmu jest supremacja narodu czy rasy. W praktyce oznacza to, że jakiś element charakteryzujący daną grupę powoduje, że te osoby uważają się za lepsze od innych i mają przez to naturalne prawo do dominacji nad resztą populacji. Prawicowe ideologie ekstremistyczne popularyzują też idee, takie jak mizoginia, wrogość wobec społeczności LGBTQ+ oraz postawy antyimigracyjne, które sprzeciwiają się różnorodności społeczeństwa i równym prawom mniejszości. Zob. Europol, *TE-SAT. European Union Terrorism Situation...*, s. 34.

[36] Broń zaprojektowana przez Niemca kurdyjskiego pochodzenia o pseudonimie JStark. Skrót FGC-9 pochodzi od słów „Fuck Gun Control 9 milimeter". Karabinek jest zasilany amunicją 9x19 mm. Zob. szerzej: P. Juraszek, *Broń z drukarki 3D w Birmie. Zaprojektował ją Niemiec*, WP Tech, 18 XII 2021 r., https://tech.wp.pl/bron-z-drukarki-3d-w-birmie-zaprojektowal-ja-niemiec,6716336908528512a [dostęp: 25 III 2025].

[37] Europol, *TE-SAT. European Union Terrorism Situation...*, s. 37.

Na radykalizację poglądów osób o skrajnie prawicowym nastawieniu miały wpływ hasła neofaszystowskie, ekofaszystowskie, rasistowskie, antysemickie czy akceleracjonistyczne, promowane zarówno online, jak i poza internetem. Nieco rzadziej pojawiały się hasła o podłożu mizoginistycznym czy incelskim. Charakterystyczne było też wzmocnienie narracji przez wykorzystanie wielu teorii spiskowych, szczególnie wątku spisku żydowskiego[38]. Udział w akcji terrorystycznej miał być dla prawicowych ekstremistów drogą do zdobycia sławy. Celami ataków była zarówno własność prywatna, jak i publiczna, atakowano konkretne osoby, komisje wyborcze, siedziby opozycyjnych partii, podpalano też centra dla uchodźców. Skrajnie prawicowi terroryści zdobywali środki na swą działalność przez organizowanie szkoleń z obsługi broni, a także przyjmując wpłaty, m.in. w kryptowalutach. Wielu z nich miało kryminalną przeszłość, co ułatwiało im gromadzenie funduszy pochodzących z nielegalnych źródeł, takich jak przemyt narkotyków czy broni palnej[39].

Podsumowanie

1. Jak wynika z raportów Europolu, w latach 2021–2023 liczba ataków terrorystycznych wzrosła z 18 do 120.
2. W raporcie Europolu z 2024 r. zwrócono uwagę, że zjawisko terroryzmu w UE wynika z różnych przesłanek i nie ma jedynie podłoża islamistycznego. Różne typy zagrożeń terrorystycznych obejmują tylko część państw członkowskich UE. Państwem, w którym ataki terrorystyczne okazały się najbardziej różnorodne pod względem motywacji zamachowców, była Francja.
3. Zagrożenie terrorystyczne na terytorium UE w 2023 r. miało negatywny wpływ na bezpieczeństwo zarówno indywidualne, jak i narodowe przynajmniej w 7 państwach członkowskich. We Francji i Włoszech to zagrożenie było szczególnie wysokie.
4. Towarzysząca odradzaniu się ISIS ofensywa operacyjno-propagandowa będzie się sukcesywnie nasilać w różnych częściach świata.

[38] Tamże, s. 38–39.

[39] Tamże, s. 41. Na temat ewolucji różnych form współczesnego terroryzmu zob. M. Ingelevič-Citak, Z. Przyszlak, *Jihadist, Far Right and Far Left Terrorism in Cyberspace. Same Threat and Same Countermeasures?*, „International Comparative Jurisprudence" 2020, t. 6, nr 2, s. 154–177. https://doi.org/10.13165/j.icj.2020.12.005.

Jest to spowodowane wieloma determinantami, m.in. sukcesem opozycji w Syrii, w tym jej islamistycznych nurtów. Jednym z regionów bardziej zagrożonych terroryzmem islamistycznym jest UE. Wśród państw o podwyższonym poziomie ryzyka należy wskazać zarówno te dotychczas często atakowane, jak i inne, np. Polskę.

5. Chociaż w omawianym raporcie Europolu nie wskazano żadnej próby ataku i tylko 1 przypadek aresztowania z powodu działalności terrorystycznej w Polsce, to kazus Polski jest ważny ze względu na kumulację zagrożenia ze strony terroryzmu zarówno państwowego (inspirowanego np. przez Rosję, Białoruś czy Iran), jak i pozapaństwowego, przybierającego różne formy.
6. Analiza politycznej motywacji sprawców ataków terrorystycznych w UE wskazuje, że większość z nich ma związek z postulatami organizacji ekstremistycznych. Dominują w tym zakresie poglądy separatystyczne, np. w ramach długotrwałych konfliktów społeczno-politycznych na Korsyce czy w Kraju Basków.
7. Interesującą kwestią jest modus operandi sprawców podobny dla większości zamachów terrorystycznych. Obejmuje on wykorzystanie najbardziej popularnych narzędzi i technik, w tym broni palnej, noża, ładunków wybuchowych czy podpalenia.
8. Unia Europejska potrzebuje nowego podejścia do postrzegania terroryzmu i jego efektywnego zwalczania. Jest to istotne ze względu na eskalację oraz ewolucję tego zagrożenia. Ewolucja ta obejmuje możliwość wykorzystania przez sprawców m.in. broni palnej masowo przemycanej z Bałkanów czy Ukrainy, a także nowoczesnych rozwiązań, takich jak drony, broń palna wytworzona w technologii 3D, sztuczna inteligencja itd. Niepokój budzą również coraz silniejsze powiązania w ramach triady: terrorysta/terroryści – grupy przestępcze – służby specjalne państw wrogich wobec UE.
9. Skuteczne przeciwdziałanie zagrożeniu terrorystycznemu musi być realizowane nie tylko przez pogłębioną współpracę (wywiadowczą, logistyczną, prawną, polityczną itd.) wszystkich państw członkowskich UE, lecz także przez rozszerzone współdziałanie z NATO oraz innymi sojusznikami w różnych częściach świata. Celem jest budowanie wieloaspektowej odporności w wymiarach zewnętrznym i wewnętrznym. Wymaga to efektywnego zapobiegania również

innym wyzwaniom, wskazanym np. w raportach Mario Draghiego[40] czy Sauliego Niinistö[41].

10. Zagrożeniem dla skutecznej realizacji planów przeciwdziałania terroryzmowi mogą być partykularne interesy poszczególnych państw członkowskich UE, trwający w niektórych z nich kryzys polityczny, rozdźwięk w relacjach transatlantyckich, brak środków finansowych czy coraz częściej zapowiadany krach ekonomiczny.

Bibliografia

Gunaratna R., *Global Terrorism Threat Forecast 2025*, „RSIS Commentary" 2025, nr 002.

Ingelevič-Citak M., Przyszlak Z., *Jihadist, Far Right and Far Left Terrorism in Cyberspace. Same Threat and Same Countermeasures?*, „International Comparative Jurisprudence" 2020, t. 6, nr 2, s. 154–177. https://doi.org/10.13165/j.icj.2020.12.005.

Maniszewska K., *Towards a New Definition of Terrorism: Challenges and Perspectives in a Shifting Paradigm*, series: Contributions to Security and Defence Studies, Cham 2024. https://doi.org/10.1007/978-3-031-58719-1.

Sandboe I.J., Obaidi M., *Imagined Extremist Communities: The Paradox of the Community-Driven Lone-Actor Terrorist*, „Perspectives on Terrorism" 2023, t. 17, nr 4, s. 19–41. https://doi.org/10.19165/CAQH8148.

The Routledge Companion to Terrorism Studies. New Perspectives and Topics, M. Abrahms (red.), London 2024.

Wejkszner A., *Europejska armia kalifatu. Tom 1. Centrum supersieci*, Warszawa 2020.

Wejkszner A., *Państwo Islamskie. Narodziny nowego kalifatu?*, Warszawa 2016.

Wejkszner A., *Samotne wilki kalifatu? Państwo Islamskie i indywidualny terroryzm dżihadystyczny w Europie Zachodniej*, Warszawa 2018.

[40] M. Draghi, *The future of European competitiveness*, European Commission, https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf [dostęp: 4 II 2025].

[41] S. Niinistö, *Safer Together Strengthening Europe's Civilian and Military Preparedness and Readiness*, European Union, 26 XI 2024 r., https://civil-protection-knowledge-network.europa.eu/media/safer-together-strengthening-europes-civilian-and-military-preparedness-and-readiness [dostęp: 8 II 2025].

Wojciechowski S., *History Repeats Itself. The Issue of Terrorism and Afghanistan on the Twentieth Anniversary of the 9/11 Attacks*, „Przegląd Strategiczny" 2021, nr 14, s. 7–21. https://doi.org/10.14746/ps.2021.1.1.

Wojciechowski S., *Reasons of Contemporary Terrorism. An Analysis of Main Determinants*, w: *Radicalism and Terrorism in the 21st Century. Implications for Security*, A. Sroka, F. Castro-Rial Garrone, R.D. Torres Kumbrián (red.), Frankfurt am Main 2017.

Wojciechowski S., *The Hybridity of Terrorism: Understanding Contemporary Terrorism*, Berlin 2013.

Wojciechowski S., Osiewicz P., *Zrozumieć współczesny terroryzm*, Warszawa 2017.

Źródła internetowe

Auermann M., Piatov F., *Der IS-Terror ist zurück!*, Bild, 3 I 2025 r., https://www.bild.de/politik/ausland-und-internationales/top-experte-warnt-in-bild-der-is-terror-ist-zurueck-677687610195b908c1898f69 [dostęp: 13 IV 2025].

Global Terrorism Index 2025, Institute for Economics & Peace, https://www.economicsandpeace.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf [dostęp: 4 V 2025].

Gowan R., *Overview, 2. Trends in armed conflicts*, w: *SIPRI Yearbook 2024*, Stockholm International Peace Research Institute, https://www.sipri.org/yearbook/2024/02 [dostęp: 5 II 2025].

Hoffmann I., De Vries C.E., *Old Habits Die Hard – Member States Report. Part II: Remaking the Transatlantic Partnership: Public Opinion in the EU and seven Member States*, Eupinions, 20 XI 2024 r., https://eupinions.eu/de/text/old-habits-die-hard-member-states-report [dostęp: 15 III 2025].

Juraszek P., *Broń z drukarki 3D w Birmie. Zaprojektował ją Niemiec*, WP Tech, 18 XII 2021 r., https://tech.wp.pl/bron-z-drukarki-3d-w-birmie-zaprojektowal-ja-niemiec,6716336908528512a [dostęp: 25 III 2025].

Security Council debates growing terrorism threat in Africa, United Nations, 21 I 2025 r., https://news.un.org/en/story/2025/01/1159246 [dostęp: 8 II 2025].

U.S. Africa Command Civilian Casuality Assessment Report; 2nd Quarter, FY2024, https://www.africom.mil/what-we-do/airstrikes/civilian-harm-report/us-africa-command-civilian-casualty-assessment-report-2nd-quarter-fy2024 [dostęp: 14 IV 2025].

Inne dokumenty

Draghi M., *The future of European competitiveness*, European Commission, https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf [dostęp: 4 II 2025].

Europol, *TE-SAT. European Union Terrorism Situation and Trend. Report 2024*, https://www.europol.europa.eu/cms/sites/default/files/documents/TE-SAT%202024.pdf [dostęp: 9 II 2025].

Niinistö S., *Safer Together Strengthening Europe's Civilian and Military Preparedness and Readiness*, European Union, 26 XI 2024 r., https://civil-protection-knowledge-network.europa.eu/media/safer-together-strengthening-europes-civilian-and-military-preparedness-and-readiness [dostęp: 8 II 2025].

Nineteenth report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat, United Nations Security Council, 31 VII 2024 r., https://docs.un.org/en/S/2024/583 [dostęp: 6 II 2025].

The Global Risks Report 2021. 16th Edition. Insight Report, World Economic Forum, https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf [dostęp: 7 II 2025].

The Global Risks Report 2022. 17th Edition. Insight Report, World Economic Forum, https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf [dostęp: 12 V 2025].

The Global Risks Report 2025. 20th Edition. Insight Report, World Economic Forum, https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf [dostęp: 6 II 2025].

Prof. dr hab. Sebastian Wojciechowski

Kierownik Zakładu Studiów Strategicznych i Bezpieczeństwa Międzynarodowego na Wydziale Nauk Politycznych i Dziennikarstwa Uniwersytetu im. Adama Mickiewicza w Poznaniu. Główny analityk Instytutu Zachodniego w Poznaniu. Ekspert ds. bezpieczeństwa, w tym terroryzmu, Organizacji Bezpieczeństwa i Współpracy w Europie.

Redaktor naczelny „Przeglądu Strategicznego". Dwukrotny stypendysta Fundacji na rzecz Nauki Polskiej i Departamentu Stanu USA. Laureat nagrody naukowej Prezesa Rady Ministrów RP oraz nagrody naukowej ufundowanej przez Unię Europejską. Członek m.in.: Komisji Bałkanistyki PAN, Rady Naukowej Centrum Badań nad Terroryzmem Collegium Civitas. Autor wielu ekspertyz i analiz przygotowanych dla polskich i zagranicznych instytucji, a także publikacji z zakresu stosunków międzynarodowych oraz bezpieczeństwa wewnętrznego i międzynarodowego. Ekspert ds. bezpieczeństwa NATO DEEP eAcademy.

Kontakt: sebastian.wojciechowski@amu.edu.pl

Dr hab. Artur Wejkszner, prof. UAM

Politolog, profesor w Zakładzie Studiów Strategicznych i Bezpieczeństwa Międzynarodowego na Wydziale Nauk Politycznych i Dziennikarstwa Uniwersytetu im. Adama Mickiewicza w Poznaniu. Autor kilkudziesięciu publikacji na temat współczesnych stosunków międzynarodowych oraz problematyki terroryzmu międzynarodowego i radykalizmu islamskiego, m.in. dwutomowej monografii pt. *Europejska armia kalifatu*.

Kontakt: artur.wejkszner@amu.edu.pl

Terroryzm – studia, analizy, prewencja, 2025, nr 7: 35–92

https://doi.org/10.4467/27204383TER.25.026.21803

Artykuł

Komentarz do zmiany ustawy o działaniach antyterrorystycznych w związku z przeciwdziałaniem rozpowszechnianiu w internecie treści o charakterze terrorystycznym

Commentary on the amendment of the Act on anti-terrorist activities in relation to countering the dissemination of terrorist content on the internet

MARIUSZ CICHOMSKI

https://orcid.org/0000-0003-3707-7856

Ministerstwo Spraw Wewnętrznych i Administracji

Abstrakt

Artykuł stanowi komentarz do *Ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych* w zakresie przepisów wprowadzonych do tej regulacji *Ustawą z dnia 18 października 2024 r. o zmianie ustawy o działaniach antyterrorystycznych i ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*. Celem wprowadzonych przepisów jest zapewnienie stosowania w polskim porządku prawnym *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym*. Autor przywołał poprzednie nowelizacje ustawy o działaniach antyterrorystycznych oraz omówił podstawowe rozwiązania zawarte w rozporządzeniu 2021/784 dotyczące dostawców usług hostingowych – nakazy usunięcia treści o charakterze terrorystycznym oraz środki szczególne, czyli wydawanie decyzji w sprawie dostawców usług hostingowych narażonych na treści o charakterze terrorystycznym.

Słowa kluczowe

terroryzm, blokowanie treści w internecie, ustawa o działaniach antyterrorystycznych, treści o charakterze terrorystycznym, dostawca usług hostingowych, dostawca treści

Abstract

The article is a commentary on the *Act of 10 June 2016 on anti-terrorist activities* in terms of the provisions introduced to this regulation by the *Act of 18 October 2024 amending the Act on anti-terrorist activities and the Act on the Internal Security Agency and the Foreign Intelligence Agency*. The purpose of the introduced provisions is to ensure the application in the Polish legal order of the *Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online*. The author recalled previous amendments to the Act on anti-terrorist activities and discussed the basic solutions contained in Regulation 2021/784 concerning hosting providers – orders to remove terrorist content and special measures, i.e. issuing decisions on hosting providers exposed to terrorist content.

Keywords

terrorism, internet content blocking, the act on anti-terrorist activities, terrorist content, hosting provider, content provider

Wprowadzenie. Dotychczasowe nowelizacje ustawy o działaniach antyterrorystycznych

Ustawą z dnia 18 października 2024 r. o zmianie ustawy o działaniach antyterrorystycznych i ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu zapewniono stosowanie w polskim porządku prawnym *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym* (dalej: rozporządzenie 2021/784), co zostało zrealizowane przez nowelizację *Ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych* (dalej: ustawa o działaniach AT). Regulacją z 18 października 2024 r. dokonano również, przez nowelizację *Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (dalej: ustawa

o ABW oraz AW), uzupełniającej implementacji *Dyrektywy Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępującej decyzję ramową Rady 2002/475/WSiSW oraz zmieniającej decyzję Rady 2005/671/WSiSW* (dalej: dyrektywa 2017/541).

Była to pierwsza tak istotna zmiana ustawy o działaniach AT od momentu jej uchwalenia w 2016 r., czyli po blisko dziewięciu latach obowiązywania. Zmiana ta polegała zarówno na rozszerzeniu zakresu przedmiotowego normowania regulacji, jak i objęciu nią nowych kategorii adresatów. Poprzednie nowelizacje, choć ich liczba (12) może wydawać się stosunkowo wysoka, miały charakter dostosowujący, korygujący czy usprawniający w odniesieniu do wdrożonych wcześniej mechanizmów i nie wprowadzały nowych instytucji prawnych w istotny sposób zmieniających zakres stosowania tej ustawy.

W pięciu przypadkach zmiany dotyczyły uwzględnienia podmiotu, który powstał wskutek przekształcenia innego podmiotu po wejściu w życie pierwotnej wersji ustawy o działaniach AT. Były to: powstanie Krajowej Administracji Skarbowej w miejsce rozproszonych struktur resortu finansów, zwłaszcza Służby Celnej, kontroli skarbowej, wywiadu skarbowego i administracji podatkowej[1], przekształcenie Biura Ochrony Rządu w Służbę Ochrony Państwa[2], zmiana statusu Straży Marszałkowskiej na państwową służbę mundurową oraz korekta jej zadań[3], uwzględnienie, pominiętego wcześniej wskutek zmieniającego się statusu, Generalnego Inspektora Informacji Finansowej[4] czy ustawowe przypisanie Prokuratorowi Krajowemu zadań przynależnych dotychczas Prokuratorowi Generalnemu[5].

Kolejna grupa nowelizacji to trzy przypadki zmian związane z uspójnieniem z innymi powstającymi lub zmieniającymi się ustawami w celu zachowania legislacyjnej zgodności odesłań bądź poprawności terminologicznej. W ten sposób należy odczytywać zmiany wprowadzone *Ustawą z dnia 6 marca 2018 r. – Prawo przedsiębiorców*, *Ustawą z dnia 21 stycznia*

[1] *Ustawa z dnia 16 listopada 2016 r. – Przepisy wprowadzające ustawę o Krajowej Administracji Skarbowej*. W artykule przedstawiono stan prawny na 23 II 2025 r.

[2] *Ustawa o Służbie Ochrony Państwa z dnia 8 grudnia 2017 r.*

[3] *Ustawa z dnia 26 stycznia 2018 r. – Przepisy wprowadzające ustawę o Straży Marszałkowskiej*.

[4] *Ustawa z dnia 30 marca 2021 r. o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw*.

[5] *Ustawa z dnia 7 lipca 2023 r. o zmianie ustawy – Kodeks postępowania cywilnego, ustawy – Prawo o ustroju sądów powszechnych, ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw*.

2021 r. o służbie zagranicznej oraz *Ustawą z dnia 11 marca 2022 r. o obronie Ojczyzny*.

Ostatnia grupa zmian to cztery nowelizacje mające wprawdzie znaczenie merytoryczne, lecz ich charakter był wycinkowy i miały one stanowić usprawnienie lub skorygowanie dotychczasowych przepisów z perspektywy praktyki stosowania prawa. *Ustawą z dnia 12 marca 2022 r. o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa* doprecyzowano art. 13 ustawy o działaniach AT, normujący zagadnienia związane z zakładaniem tymczasowych instalacji radiokomunikacyjnych oraz budową, przebudową lub instalowaniem infrastruktury przewodowej i innych urządzeń lub infrastruktury w zakresie niezbędnym do uruchomienia i prawidłowego użytkowania tych instalacji. Ponadto do ustawy o działaniach AT dodano art. 13a, zgodnie z którym Prezes Rady Ministrów, z uwagi na możliwość wystąpienia zdarzenia o charakterze terrorystycznym albo zagrożenia bezpieczeństwa i porządku publicznego, może, w drodze zarządzenia, ograniczyć publiczny dostęp do wykazów, rejestrów, baz danych i systemów teleinformatycznych zawierających dane lokalizacyjne infrastruktury technicznej.

Ustawą z dnia 7 lipca 2023 r. o zmianie ustawy o ochronie żeglugi i portów morskich oraz niektórych innych ustaw dokonano korekty dotyczącej zakresu art. 24 ustawy o działaniach AT przez uwzględnienie polskiej wyłącznej strefy ekonomicznej jako obszaru, w którym mogą być prowadzone działania antyterrorystyczne. Zgodnie z nowym brzmieniem przepisu działania antyterrorystyczne na zasadach określonych w tej ustawie mogą być prowadzone poza granicami RP, na akwenach w polskiej strefie odpowiedzialności SAR (ang. *search and rescue*), zgodnie z *Międzynarodową Konwencją o poszukiwaniu i ratownictwie morskim, sporządzoną w Hamburgu dnia 27 kwietnia 1979 r.,* i w polskiej wyłącznej strefie ekonomicznej. Analogicznie służby ratownicze mogą prowadzić działania zmierzające do usunięcia skutków zdarzenia o charakterze terrorystycznym i w tym zakresie współdziałają ze sobą oraz ze służbami prowadzącymi działania antyterrorystyczne na ww. obszarach. W pierwotnej wersji przepis ten ograniczał obszar działania do strefy odpowiedzialności SAR.

Kolejna zmiana została wprowadzona *Ustawą z dnia 17 sierpnia 2023 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw* i dotyczyła dwóch najbardziej kontrowersyjnych z perspektywy konstytucyjnej, w opinii autora, przepisów ustawy o działaniach AT. Pierwsza zmiana modyfikowała art. 9 ustawy, stanowiący podstawę do prowadzenia przez Szefa ABW

kontroli operacyjnej w odniesieniu do cudzoziemców w celu rozpoznawania, zwalczania i wykrywania przestępstw o charakterze terrorystycznym i zapobiegania im oraz ścigania ich sprawców. Przepis ten został rozszerzony o dodatkową przesłankę, tj. przestępstwo szpiegostwa[6]. Druga zmiana dotyczyła art. 26 ust. 2 – wydłużono do 30 dni maksymalny termin tymczasowego aresztowania zastosowanego na podstawie tej ustawy. Wprowadzone zmiany zakładały zwiększenie możliwości praktycznego zastosowania ww. przepisów. Ich celem nie było jednak dokonanie zmian mogących minimalizować wątpliwości natury konstytucyjnej[7].

Nieco większy zakres zmian został wprowadzony do ustawy o działaniach AT *Ustawą z dnia 26 lipca 2024 r. o zmianie niektórych ustaw w celu usprawnienia działań Sił Zbrojnych Rzeczypospolitej Polskiej, Policji oraz Straży Granicznej na wypadek zagrożenia bezpieczeństwa państwa*. Zmiany te nie tworzyły jednak nowych instytucji prawnych. Ich celem było natomiast podniesienie funkcjonalności wcześniejszych rozwiązań przez wprowadzenie możliwości przekazania opinii co do zasadności wprowadzenia, zniesienia lub zmiany stopnia alarmowego także ustnie, telefonicznie, za pomocą środków komunikacji elektronicznej (art. 16 ustawy o działaniach AT)[8]. Analogiczne rozwiązanie przyjęto także do przekazywania wniosku o uruchomienie pomocy dla Policji ze strony Sił Zbrojnych RP (art. 22 ustawy o działaniach AT). Ujednolicono także zapisy z *Ustawą z dnia 6 kwietnia 1990 r. o Policji* przez wskazanie, że żołnierzom oddziałów i pododdziałów Wojsk Specjalnych użytych do pomocy oddziałom i pododdziałom Policji

[6] W tym kontekście warto przywołać przede wszystkim wyrok Europejskiego Trybunału Praw Człowieka (ETPCz) w sprawie Pietrzak i Bychawska-Siniarska i inni przeciwko Polsce, w którym ETPCz uznał, że doszło do naruszenia art. 8 *Konwencji o ochronie praw człowieka i podstawowych wolności* w związku ze sposobem ukształtowania systemu kontroli operacyjnej w Polsce. ETPCz zwrócił uwagę, że w odniesieniu do kontroli operacyjnej prowadzonej na podstawie ustawy o działaniach AT ani wprowadzenie niejawnego nadzoru, ani jego stosowanie w początkowym trzymiesięcznym okresie nie podlega żadnej kontroli ze strony niezależnego organu zewnętrznego w stosunku do funkcjonariuszy ABW prowadzących ten nadzór. Zob. Wyrok Europejskiego Trybunału Praw Człowieka w sprawie Pietrzak i Bychawska-Siniarska i inni przeciwko Polsce, https://arch-bip.ms.gov.pl/pl/prawa-czlowieka/europejski-trybunal-praw-czlowieka/orzecznictwo-europejskiego-trybunalu--praw-czlowieka/listByYear,2.html?ComplainantYear=2024 [dostęp: 18 V 2025].

[7] Zob. szerzej: M. Gabriel-Węglowski, *Działania antyterrorystyczne. Komentarz*, Warszawa 2018, s. 36, 76–116, 213–214, 224–229.

[8] Kwestia ta jako postulat de lege ferenda została wskazana w: M. Cichomski, I. Idzikowska-Ślęzak, *Stopnie alarmowe – praktyczny i prawny wymiar ich stosowania*, „Terroryzm – studia, analizy, prewencja" 2022, nr 2, s. 65. https://doi.org/10.4467/27204383TER.22.018.16338.

przysługują, w zakresie niezbędnym do wykonywania ich zadań, uprawnienia funkcjonariuszy Policji, a korzystanie z tych uprawnień następuje na zasadach i w trybie określonych dla funkcjonariuszy Policji (również art. 22 ustawy o działaniach AT).

Konieczność zapewnienia polskich ram stosowania rozporządzenia 2021/784

Na początek warto zadać pytanie, czy zapewnienie stosowania rozporządzenia 2021/784 wymagało wprowadzenia zmian na poziomie ustawowym, a jeśli tak, to czy mogło się ono odbyć na podstawie innych regulacji niż ustawa o działaniach AT. Ograniczone ramy opracowania nie pozwalają na całościowy komentarz do poszczególnych przepisów rozporządzenia 2021/784, dlatego też, na potrzeby tego artykułu, dokonano jedynie syntetycznego omówienia głównych instrumentów prawnych wprowadzonych przez to rozporządzenie w celu zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym. W części będącej komentarzem do poszczególnych przepisów zostały omówione podstawowe regulacje rozporządzenia 2021/784 w odniesieniu do polskich rozwiązań, a także kwestia wyboru na gruncie krajowym organu właściwego do wykonania zobowiązań wynikających z rozporządzenia 2021/784, z uwzględnieniem rozwiązań instytucjonalnych przyjętych w innych państwach UE. Ponadto opisano procedury wydawania i zaskarżania nakazów wynikających ze wskazanego rozporządzenia.

Jak wspomniano we wprowadzeniu, ustawą o zmianie ustawy o działaniach AT i ustawy o ABW oraz AW uzupełniono również wcześniejszą implementację dyrektywy 2017/541. Należy podkreślić, że o ile zapewnieniu stosowania rozporządzenia 2021/784 służyła zmiana ustawy o działaniach AT, o tyle transpozycję dyrektywy 2017/541 zapewniła zmiana ustawy o ABW oraz AW. Połączenie w ramach jednej ingerencji ustawodawczej wykonania obu tych aktów prawa UE należy ocenić jako optymalne rozwiązanie, chociaż obie regulacje, mimo zbieżności obszarów, których dotyczą, związanej z usuwaniem i blokowaniem treści w internecie, mają inny zakres stosowania i nie nakładają się na siebie.

Rozporządzenie 2021/784 weszło w życie 7 czerwca 2021 r., a państwa członkowskie musiały w ciągu jednego roku dostosować do niego swoje regulacje. Jest ono pierwszym kompleksowym aktem prawnym bezpośredniego

stosowania na poziomie UE normującym zagadnienia związane z przeciwdziałaniem rozpowszechnianiu w internecie treści o charakterze terrorystycznym. Poprzedziły go jednak inne inicjatywy. Na przykład w 2015 r. wprowadzono ramy dobrowolnej współpracy między państwami członkowskimi a dostawcami usług hostingowych. Na posiedzeniu w dniach 22–23 czerwca 2017 r. Rada Europejska w odpowiedzi na ataki o charakterze terrorystycznym, do których doszło w krajach UE, oraz związaną z nimi propagandę rozpowszechnianą w internecie stwierdziła, że:

> „oczekuje, że branża [...] opracuje nowe technologie i narzędzia usprawniające automatyczne wykrywanie treści podżegających do aktów terrorystycznych i usuwanie tych treści". W rezolucji z dnia 15 czerwca 2017 r. Parlament Europejski wezwał te platformy internetowe „do wzmocnienia środków zwalczania nielegalnych i szkodliwych treści". Wezwanie przedsiębiorstw do przyjęcia bardziej proaktywnego podejścia, jeśli chodzi o ochronę ich użytkowników przed treściami o charakterze terrorystycznym, zostało powtórzone przez ministrów państw członkowskich w ramach Forum UE ds. Internetu[9].

Dnia 28 września 2017 r. Komisja Europejska (KE) przyjęła komunikat zawierający wytyczne dotyczące obowiązków dostawców usług online w odniesieniu do nielegalnych treści w internecie[10]. Następnie wydała *Zalecenie Komisji (UE) 2018/334 z dnia 1 marca 2018 r. w sprawie działań na rzecz skutecznego zwalczania nielegalnych treści w internecie*, które w rozdziale 3 określiło szczegółowe zalecenia dotyczące treści o charakterze terrorystycznym. Zalecenie to było następstwem wezwania Parlamentu Europejskiego do wzmocnienia środków przeciwdziałania nielegalnym i szkodliwym treściom w internecie, zgodnie z ramami horyzontalnymi ustanowionymi w *Dyrektywie 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego*, a także zgodnie z odpowiedzią na wezwania

[9] Motyw 5 *Zalecenia Komisji (UE) 2018/334 z dnia 1 marca 2018 r. w sprawie działań na rzecz skutecznego zwalczania nielegalnych treści w internecie*.

[10] *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Zwalczanie nielegalnych treści w internecie. W kierunku większej odpowiedzialności platform internetowych*, Bruksela, 28 IX 2017 r., COM (2017) 555 final.

Rady Europejskiej do usprawnienia wykrywania i usuwania treści w internecie, które podżegają do aktów terrorystycznych.

Kolejnym krokiem stało się przyjęcie rozporządzenia 2021/784. Za KE warto zauważyć, że: *Ramy regulacyjne dotyczące zwalczania nielegalnych treści w internecie zostały dodatkowo wzmocnione wraz z wejściem w życie 16 listopada 2022 r. aktu o usługach cyfrowych. Akt o usługach cyfrowych reguluje obowiązki dostawców usług cyfrowych, którzy pełnią rolę pośredników w łączeniu konsumentów z treściami, usługami i towarami, tym samym zapewniając lepszą ochronę użytkowników w internecie i przyczyniając się do bezpieczniejszego środowiska internetowego*[11]. Na podstawie tego aktu KE zyskała uprawnienia nadzorcze i wykonawcze do podejmowania działań wobec dużych platform internetowych i wyszukiwarek internetowych. Może ona m.in. kierować wnioski o udzielenie informacji i prowadzić postępowania w sprawie działań przedsiębiorstw w zakresie moderowania treści, wraz z możliwością nakładania grzywien.

Podstawowym motywem wydania rozporządzenia 2021/784 było zapewnienie sprawnego funkcjonowania jednolitego rynku cyfrowego w otwartym i demokratycznym społeczeństwie przez przeciwdziałanie wykorzystywaniu usług hostingowych do celów terrorystycznych oraz przyczynienie się do poprawy bezpieczeństwa publicznego w całej Unii[12]. Założeniem UE była również poprawa funkcjonowania jednolitego rynku cyfrowego przez zwiększenie pewności prawa dla dostawców usług hostingowych i zaufania użytkowników do środowiska internetowego, a także wzmocnienie gwarancji dotyczących wolności wypowiedzi, w tym wolności otrzymywania i przekazywania informacji i idei w otwartym i demokratycznym społeczeństwie oraz wolności i pluralizmu mediów. Unijny prawodawca dostrzegł, że dostawcy usług hostingowych działający w internecie odgrywają kluczową rolę w gospodarce cyfrowej przez łączenie przedsiębiorstw i obywateli, a także ułatwianie publicznej debaty oraz dystrybucji i otrzymywania informacji, opinii i idei, co wyraźnie przyczynia się do wprowadzania innowacji, wzrostu gospodarczego i tworzenia miejsc

[11] *Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady z wykonania rozporządzenia (UE) 2021/784 w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym*, Bruksela, 14 II 2024 r., COM(2024) 64 final, s. 1.

[12] Motyw 1 rozporządzenia 2021/784. Kwestia ta została również poruszona w: *Rządowy projekt ustawy o zmianie ustawy o działaniach antyterrorystycznych i ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* – uzasadnienie, druk nr 661, s. 1, https://www.sejm.gov.pl/Sejm10.nsf/druk.xsp?nr=661 [dostęp: 24 XII 2024].

pracy w Unii[13]. W tym kontekście zaznacza się, że to nie dostawcy usług hostingowych mogą stanowić zagrożenie w zakresie szerzenia treści o charakterze terrorystycznym, lecz ich usługi mogą być w tym celu wykorzystywane przez osoby trzecie. Zauważono jednak, że to na dostawcach usług hostingowych, ze względu na ich potencjał techniczny, spoczywają szczególne obowiązki wobec społeczeństwa w zakresie ochrony swoich usług przed wykorzystaniem przez terrorystów i udzielania pomocy w przeciwdziałaniu rozpowszechnianiu w internecie tego rodzaju treści[14]. Tym bardziej że: *Szczególnie niepokojące jest wykorzystywanie tych usług przez grupy terrorystyczne i ich zwolenników do rozpowszechniania w internecie treści o charakterze terrorystycznym w celu szerzenia ich przesłania, w celu radykalizacji i rekrutacji zwolenników oraz w celu ułatwiania działalności terrorystycznej i kierowania nią*[15].

Jeśli jednak zasady zapobiegania publikacji treści o charakterze terrorystycznym i reagowania na nią zostały uregulowane na poziomie rozporządzenia unijnego, a zatem aktu prawa mającego bezpośrednie zastosowanie we wszystkich państwach członkowskich, to w związku z § 1 ust. 1 pkt 3 *Rozporządzenia Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej"* (dalej: Zasady techniki prawodawczej) należy zadać pytanie, czy istniała możliwość podjęcia środków interwencji organów władzy publicznej alternatywnych w stosunku do uchwalenia ustawy. W tym przypadku odpowiedź jest prosta. Zgodnie z art. 291 ust. 1 *Traktatu o funkcjonowaniu Unii Europejskiej* państwa członkowskie są zobowiązane do podjęcia wszelkich środków prawa krajowego niezbędnych do wprowadzenia w życie prawnie wiążących aktów Unii. W art. 4 ust. 3 zdanie drugie *Traktatu o Unii Europejskiej* wskazano z kolei, że państwa członkowskie podejmują wszelkie środki ogólne lub szczególne właściwe dla zapewnienia wykonania zobowiązań wynikających z traktatów lub aktów instytucji UE. Ponadto już w samym rozporządzeniu 2021/784 zobowiązano państwa do podjęcia konkretnych działań wymagających interwencji ustawodawczej. Na przykład w art. 12 zobligowano państwa członkowskie do wyznaczenia właściwych organów w zakresie wydawania nakazów usuwania treści czy stosowania szczególnych środków zapobiegawczych. Z perspektywy krajowej natomiast, w związku z art. 7 *Konstytucji Rzeczpospolitej Polskiej z dnia*

[13] Motyw 4 rozporządzenia 2021/784.

[14] Motyw 5 rozporządzenia 2021/784.

[15] Motyw 4 zdanie 3 rozporządzenia 2021/784.

2 kwietnia 1997 r., określenie właściwości organów stanowi normę ustawową, a organy władzy publicznej działają na podstawie i w granicach prawa (zasada legalizmu). Nie budzi zatem wątpliwości potrzeba przyjęcia ustawowych rozwiązań w omawianym zakresie.

Drugim zagadnieniem ogólnym dotyczącym zapewnienia stosowania rozporządzenia 2021/784 na gruncie polskiego prawa pozostaje to, czy to zapewnienie słusznie zostało dokonane przez dodanie przepisów do ustawy o działaniach AT i czy istniały inne możliwe rozwiązania. W kontekście tych rozważań będzie pomocna krótka analiza aktualnego stanu prawnego w dziedzinie objętej regulacją, a zatem wykonanie obowiązku, o którym mowa w § 1 ust. 1 pkt 2 wspomnianych Zasad techniki prawodawczej, poprzedzającego przystąpienie do opracowania aktu prawnego.

W uzasadnieniu do ustawy o zmianie ustawy o działaniach AT i ustawy o ABW oraz AW wskazano, że tematyka rozporządzenia 2021/784 obecnie jest częściowo objęta regulacją krajową, która nie wdraża w pełni obowiązującej w tym zakresie dyrektywy 2017/541[16]. Zgodnie bowiem z jej art. 21 państwa członkowskie są zobowiązane do wprowadzenia środków, które w pierwszej kolejności zapewnią natychmiastowe usunięcie treści internetowych nawołujących do popełnienia przestępstwa terrorystycznego znajdujących się na serwerach na ich terytorium. Zgodnie z art. 21 ust. 1 dyrektywy państwa mają też podjąć działania mające doprowadzić do usunięcia takich treści znajdujących się na serwerach poza ich terytorium. Dopiero jeżeli usunięcie takich treści nie jest możliwe, państwa członkowskie mogą podjąć środki w celu zablokowania dostępu do nich (art. 21 ust. 2 dyrektywy). Polskie ustawodawstwo przewiduje zaś jedynie blokowanie treści, co w ocenie KE nie jest wystarczające do uznania implementacji za prawidłową. Brakuje podstawowego mechanizmu, który pozwalałby w pierwszej kolejności na usuwanie tych treści ze stron internetowych. W ustawie o ABW oraz AW funkcjonują bowiem przepisy, zgodnie z którymi Szef ABW, za zgodą sądu, może spowodować tzw. blokadę dostępności w internecie określonych danych powiązanych ze zdarzeniem o charakterze terrorystycznym. Zgodnie z art. 32c tej ustawy sąd może zarządzić zablokowanie dostępności w systemie teleinformatycznym określonych danych informatycznych lub usług teleinformatycznych mających związek ze zdarzeniem o charakterze terrorystycznym lub uprawdopodabniającym popełnienie przestępstwa szpiegostwa. Może to zrobić

[16] *Rządowy projekt ustawy o zmianie ustawy*... – uzasadnienie..., s. 4.

na pisemny wniosek Szefa ABW złożony po uzyskaniu pisemnej zgody Prokuratora Krajowego. Blokada dostępności danych teleinformatycznych jest zarządzana na okres nie dłuższy niż 30 dni z możliwością jej sądowego przedłużenia na okres nie dłuższy niż trzy miesiące. Ustawa przewiduje również uproszczony tryb działania w przypadkach niecierpiących zwłoki[17]. W swoim stanowisku KE stwierdza, że:

> Polskie prawo nie przewiduje środków zapewniających natychmiastowe usuwanie takich treści internetowych, w szczególności gdy takie treści znajdują się na serwerach na terytorium Polski. Chociaż może się to różnić w niektórych indywidualnych przypadkach, nie ma powodu, aby sądzić, że usunięcie treści u źródła byłoby zasadniczo niewykonalne. Art. 21 ust. 2 nie może być rozumiany jako powód, dla którego państwo członkowskie nie dokonało transpozycji art. 21 ust. 1. Zgodnie z dyrektywą państwa członkowskie są bowiem zobowiązane do transpozycji obu przepisów, tak aby możliwe było usunięcie treści zgodnie z art. 21 ust. 1 jako zasada ogólna oraz zablokowanie dostępu zgodnie z art. 21 ust. 2, jeżeli w indywidualnych przypadkach usunięcie nie jest wykonalne[18].

Należy także zaznaczyć, że przepisy dyrektywy 2017/541 nie zostały uchylone rozporządzeniem 2021/784, co oznacza, że oba akty są względem siebie komplementarne i powinny być stosowane równolegle. *Rozporządzenie 2021/784 nakłada zobowiązania do usuwania treści o charakterze terrorystycznym wyłącznie na dostawców usług hostingowych, nie nakładając takich obowiązków na inne podmioty świadczące usługi drogą elektroniczną, w tym np. usługi tzw. cachingu, które należy rozumieć jako usługi polegające na automatycznym i krótkotrwałym przechowywaniu na serwerze pośredniczącym cudzych danych przez stworzenie ich kopii w celu ich szybszego udostępnienia użytkownikowi końcowemu*[19].

Ponadto dyrektywa 2017/541 w przeciwieństwie do rozporządzenia 2021/784 nie wiąże treści o charakterze terrorystycznym z publicznym charakterem ich rozpowszechniania jako przesłanki warunkującej możliwość wydania nakazu usunięcia treści lub zablokowania dostępu do niej.

[17] Tamże

[18] *Stanowisko Komisji Europejskiej z 9 czerwca 2021 r.* (sygn. INFR(2021)2046, C(2021)3630 final), s. 7; *Rządowy projekt ustawy o zmianie ustawy...* – uzasadnienie..., s. 15.

[19] *Rządowy projekt ustawy o zmianie ustawy...* – uzasadnienie..., s. 14.

Na bazie dyrektywy można więc dążyć do usuwania treści np. w ramach forów internetowych o ograniczonej dostępności.

W rezultacie, chociaż wskazany przepis ustawy o ABW oraz AW dotyczy kwestii blokowania treści w internecie, to nie może być utożsamiany z obowiązkami regulacyjnymi związanymi z zapewnieniem stosowania rozporządzenia 2021/784. W związku z tym utrzymano w mocy art. 32c ustawy o ABW oraz AW, ale przeprowadzono jego modyfikację, zgodnie z którą ten przepis ma zastosowanie w przypadkach publikowania lub prób publikowania w internecie treści o charakterze terrorystycznym przez podmioty niebędące dostawcami usług hostingowych w rozumieniu rozporządzenia 2021/784.

Skoro jednak dotychczasowe regulacje znajdowały się w ustawie o ABW oraz AW, to warto się zastanowić, czy nowe regulacje, zbieżne tematycznie, również nie powinny znaleźć się w tej ustawie. W opinii autora pozytywna odpowiedź na to pytanie budzi istotne wątpliwości. Owszem, zapewnienie stosowania rozporządzenia 2021/784 wymaga wyznaczenia właściwego organu po stronie państwa członkowskiego. Jeśli w przypadku Polski zdecydowano, że będzie nim Szef ABW, to wskazanie to mogłoby nastąpić w ustawie pragmatycznej określającej zadania i uprawnienia tej służby oraz jej organy, czyli w ustawie o ABW oraz AW. Zakres spraw przekazanych przez unijnego prawodawcę do uregulowania na poziomie krajowym jest jednak znacznie szerszy. Rozporządzenie 2021/784 określa bowiem nie tylko sferę działania organów właściwych, lecz także prawa, w tym do zaskarżenia decyzji organów państwowych, i obowiązki dostawców usług hostingowych i dostawców treści oraz system i wymiar kar możliwych do nałożenia na nich. Jest to zatem zakres znacznie wykraczający poza sferę, która może być normowana w ustawie pragmatycznej dotyczącej danej formacji. Ustawy pragmatyczne nie powinny, choć obecnie się to zdarza, regulować praw i obowiązków innych podmiotów. Co więcej, w opinii autora należy uznać za wątpliwe pod względem legislacyjnym dotychczasowe umiejscowienie przepisów art. 32c ustawy o ABW oraz AW. Przepisy te zostały wprowadzone przepisami zmieniającymi w ramach pierwotnego tekstu ustawy o działaniach AT w 2016 r., zatem już wtedy ustawodawca mógł je umieścić w tej ustawie. Inna decyzja prawdopodobnie była podyktowana tym, że konstrukcja przepisów w wymiarze proceduralnym jest zbliżona do instytucji prawnej kontroli operacyjnej unormowanej w art. 27 ustawy o ABW oraz AW (analogicznie jak w przypadku ustaw pragmatycznych innych służb uprawnionych do

jej prowadzenia, np. w art. 19 ustawy o Policji). Zatem to nie przepisy zapewniające stosowanie rozporządzenia 2021/784 powinny znaleźć się w ustawie o ABW oraz AW, lecz odwrotnie – to dotychczasowe przepisy związane z blokowaniem treści ujętej w tej ustawie mogłyby docelowo znaleźć się w ustawie o działaniach AT. Na marginesie warto zauważyć, że uwaga ta odnosi się również do art. 32a–32b ustawy o ABW oraz AW dotyczących prowadzenia przez ABW oceny bezpieczeństwa systemów teleinformatycznych organów administracji publicznej i operatorów infrastruktury krytycznej, a także systemów ostrzegania.

Kolejnego argumentu potwierdzającego słuszność ujęcia przepisów związanych z rozporządzeniem 2021/784 dostarcza § 2 Zasad techniki prawodawczej, zgodnie z którym ustawa powinna wyczerpująco regulować daną dziedzinę spraw i nie pozostawiać poza zakresem swego unormowania istotnych fragmentów tej dziedziny. W kontekście związanym z problematyką zagrożeń o charakterze terrorystycznym podstawową regulacją jest ustawa o działaniach AT i to w niej co do zasady powinny zawierać się zagadnienia związane z tą problematyką. Ten argument jest adekwatny również w odniesieniu do drugiej potencjalnej alternatywnej lokalizacji przepisów służących stosowaniu rozporządzenia 2021/784, tj. do unormowania tej kwestii w nowej odrębnej regulacji.

Na marginesie warto zauważyć, że z analogicznych powodów do ustawy o działaniach AT mogłyby zostać włączone przepisy obecnej *Ustawy z dnia 13 kwietnia 2016 r. o bezpieczeństwie obrotu prekursorami materiałów wybuchowych,* która służy stosowaniu *Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 98/2013 z dnia 15 stycznia 2013 r. w sprawie wprowadzania do obrotu i używania prekursorów materiałów wybuchowych*. Zostało ono wydane w następstwie zamachów przeprowadzonych przez norweskiego ekstremistę Andersa Breivika na siedzibę premiera Norwegii oraz na uczestników obozu młodzieżówki norweskiej Partii Pracy[20].

[20] Zob. szerzej: M. Cichomski, P. Marchliński, *Krajowe rozwiązania w zakresie bezpieczeństwa obrotu prekursorami materiałów wybuchowych – po zamachu terrorystycznym w Norwegii 22 lipca 2011 r. w kontekście nowych zadań Policji*, w: *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, W. Zubrzycki, K. Jałoszyński, A. Babiński (red.), Szczytno 2016, s. 591–600.

Podstawowe rozwiązania zawarte w rozporządzeniu 2021/784 w związku z przeciwdziałaniem rozpowszechnianiu w internecie treści o charakterze terrorystycznym – nakazy usunięcia i środki szczególne

W kontekście komentarza do poszczególnych przepisów ustawy o działaniach AT są konieczne liczne odwołania do przepisów i motywów rozporządzenia 2021/784, ale służą one wykładni poszczególnych przepisów polskiego prawa. Niezbędne jest jednak syntetyczne przedstawienie podstawowych instrumentów zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym, wprowadzanych rozporządzeniem 2021/784. Umożliwienie ich stosowania w Polsce to cel działań na poziomie krajowego ustawodawcy.

Na potrzeby tego opracowania można wyróżnić dwa podstawowe mechanizmy przeciwdziałania rozpowszechnianiu w internecie wspomnianych treści:

- wydawanie nakazów zobowiązujących dostawców usług hostingowych do usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do treści terrorystycznych we wszystkich państwach członkowskich, zgodnie z art. 3 rozporządzenia 2021/784 (dalej: nakazy usunięcia);
- wydawanie decyzji w sprawie dostawców usług hostingowych narażonych na treści o charakterze terrorystycznym, na podstawie art. 5 rozporządzenia 2021/784 (dalej: środki szczególne).

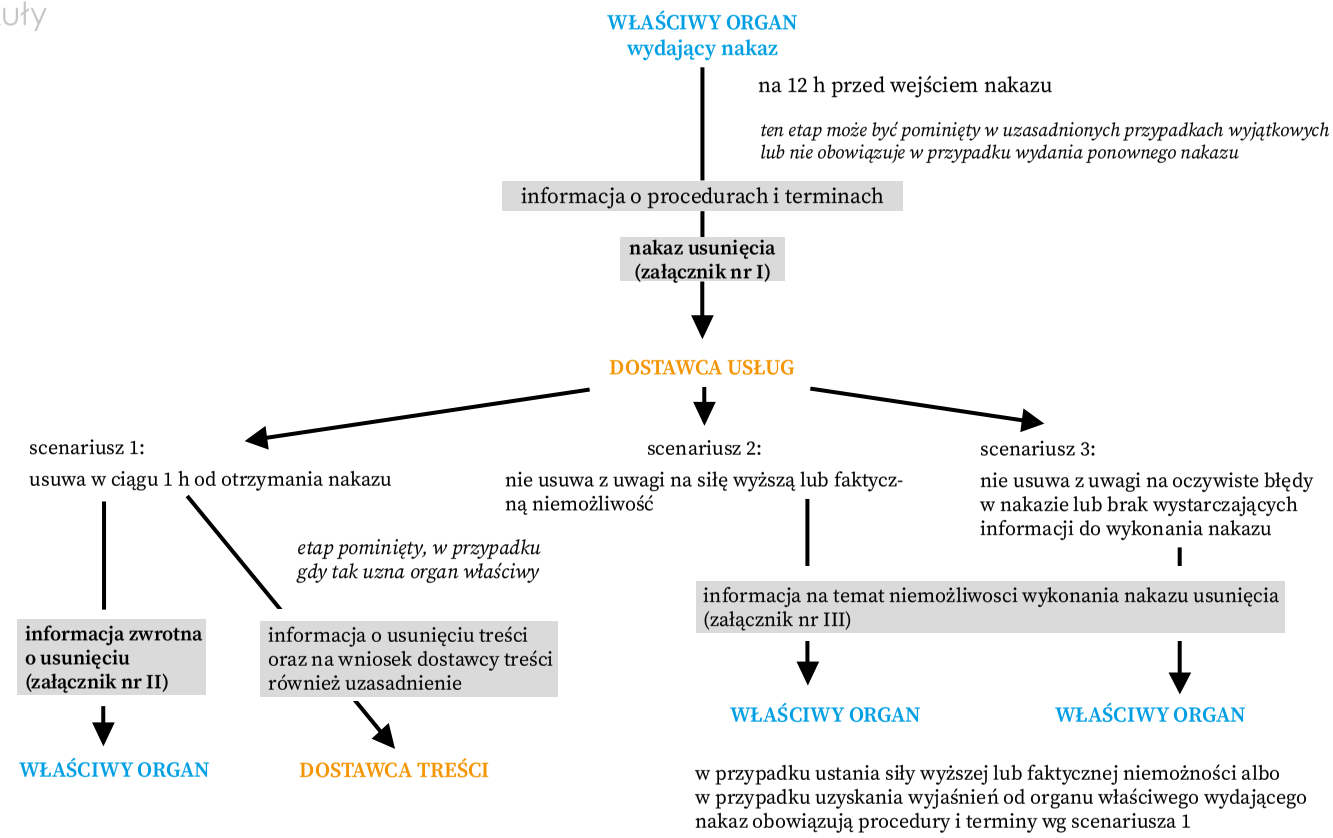
Tym dwóm wskazanym instrumentom odpowiada szereg dodatkowych uprawnień i przepisów proceduralnych, a także mechanizmów i narzędzi współpracy między państwami UE, KE i Agencją Unii Europejskiej ds. Współpracy Organów Ścigania, czyli Europolem, a także dostawcami usług hostingowych (schematy 1 i 2).

Pierwszy z wymienionych instrumentów – nakaz usunięcia – zakłada, że właściwy organ każdego państwa członkowskiego jest uprawniony do wydania nakazu usunięcia zobowiązującego dostawców usług hostingowych do usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do treści terrorystycznych we wszystkich państwach członkowskich. W następstwie wydanego nakazu dostawcy usług hostingowych jak najszybciej, nie później niż w ciągu jednej godziny od otrzymania nakazu usunięcia, usuwają treści lub uniemożliwiają do nich dostęp we wszystkich państwach członkowskich.

Nakazy są wydawane na ujednoliconym formularzu i zawierają takie informacje, jak: dane identyfikacyjne właściwego organu wydającego nakaz, uzasadnienie, dokładny ujednolicony format adresowania zasobów (adres URL) oraz, w razie potrzeby, dodatkowe informacje służące identyfikacji treści o charakterze terrorystycznym czy informację na temat środków zaskarżenia przysługujących dostawcy usług hostingowych i dostawcy treści. Następnie dostawcy usług hostingowych informują właściwy organ o wykonaniu nakazu – wskazują zwłaszcza czas usunięcia lub uniemożliwienia dostępu do treści (wzór nakazu usunięcia został określony w załączniku I do rozporządzenia 2021/784).

Jeżeli w odniesieniu do danego dostawcy usług hostingowych taki nakaz jest wydawany po raz pierwszy, to poprzedza go udzielenie temu dostawcy informacji o mających zastosowanie procedurach i terminach co najmniej 12 godzin przed wydaniem nakazu usunięcia. Obowiązek ten może zostać pominięty w szczególnie uzasadnionych przypadkach.

Jeżeli dostawca usług hostingowych nie jest w stanie wykonać nakazu ze względu na siłę wyższą lub faktyczną niemożliwość, których nie można przypisać temu dostawcy, w tym z przyczyn technicznych lub operacyjnych, dających się obiektywnie uzasadnić, informuje o tym właściwy organ, który wydał nakaz, a godzinny termin na usunięcie treści lub zablokowanie dostępu do niej zaczyna biec od momentu, gdy ustaną ww. powody. Jeżeli natomiast dostawca usług hostingowych nie jest w stanie wykonać nakazu, ponieważ zawiera on błędy lub nie zawiera informacji wystarczających do jego wykonania, informuje o tym właściwy organ, który wydał nakaz usunięcia. W tym wypadku termin zaczyna biec od momentu, gdy dostawca usług hostingowych otrzymał niezbędne wyjaśnienia. Nakaz staje się ostateczny po upływie terminu do wniesienia środka zaskarżenia, w przypadku gdy nie został on wniesiony zgodnie z prawem krajowym albo na skutek utrzymania nakazu usunięcia w wyniku wniesienia środka zaskarżenia.



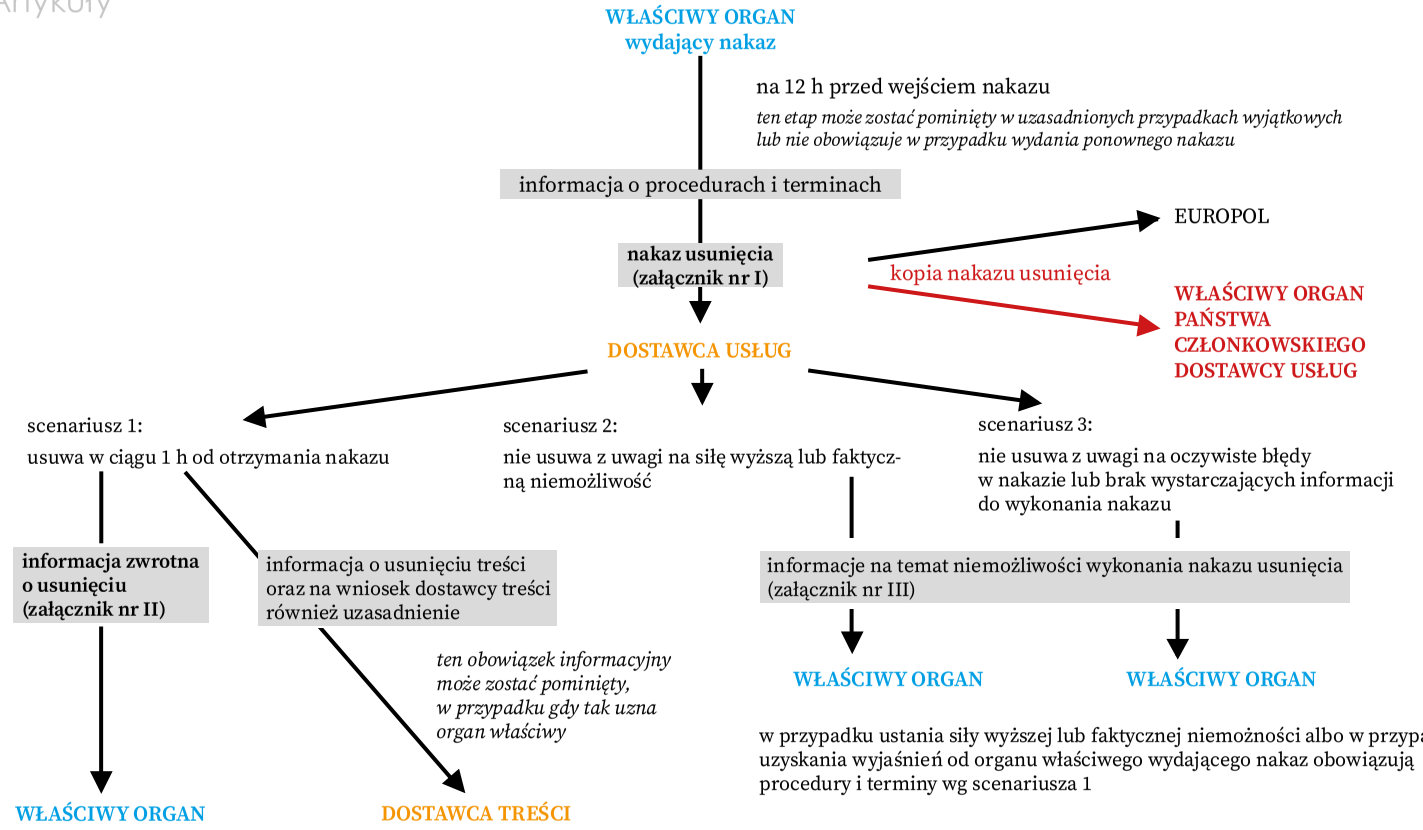
Schemat 1. Procedura nałożenia nakazu usunięcia treści o charakterze terrorystycznym, w przypadku gdy główna jednostka organizacyjna lub przedstawiciel prawny dostawcy usług hostingowych znajduje się na terenie tego samego państwa członkowskiego co właściwy organ wydający nakaz.

Źródło: opracowanie Anety Sudy, *Mechanizmy blokowania w internecie treści o charakterze terrorystycznym w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym*, prezentacja Ministerstwa Spraw Wewnętrznych i Administracji przygotowana na potrzeby Międzyresortowego Zespołu ds. Zagrożeń Terrorystycznych.

Należy wspomnieć o mechanizmie weryfikowania nakazów usunięcia wydanych przez właściwe organy innych państw członkowskich oraz stwierdzania ewentualnych naruszeń w tym zakresie (art. 4 rozporządzenia 2021/784). Jest to tzw. procedura dotycząca transgranicznych nakazów usunięcia (schemat 3). Zgodnie z tym rozwiązaniem w przypadku, gdy dostawca usług hostingowych nie ma głównej jednostki organizacyjnej ani przedstawiciela prawnego w państwie członkowskim właściwego organu, który wydał nakaz, organ ten przekazuje kopię nakazu usunięcia właściwemu organowi państwa członkowskiego, w którym dostawca usług hostingowych ma główną jednostkę organizacyjną lub w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę.

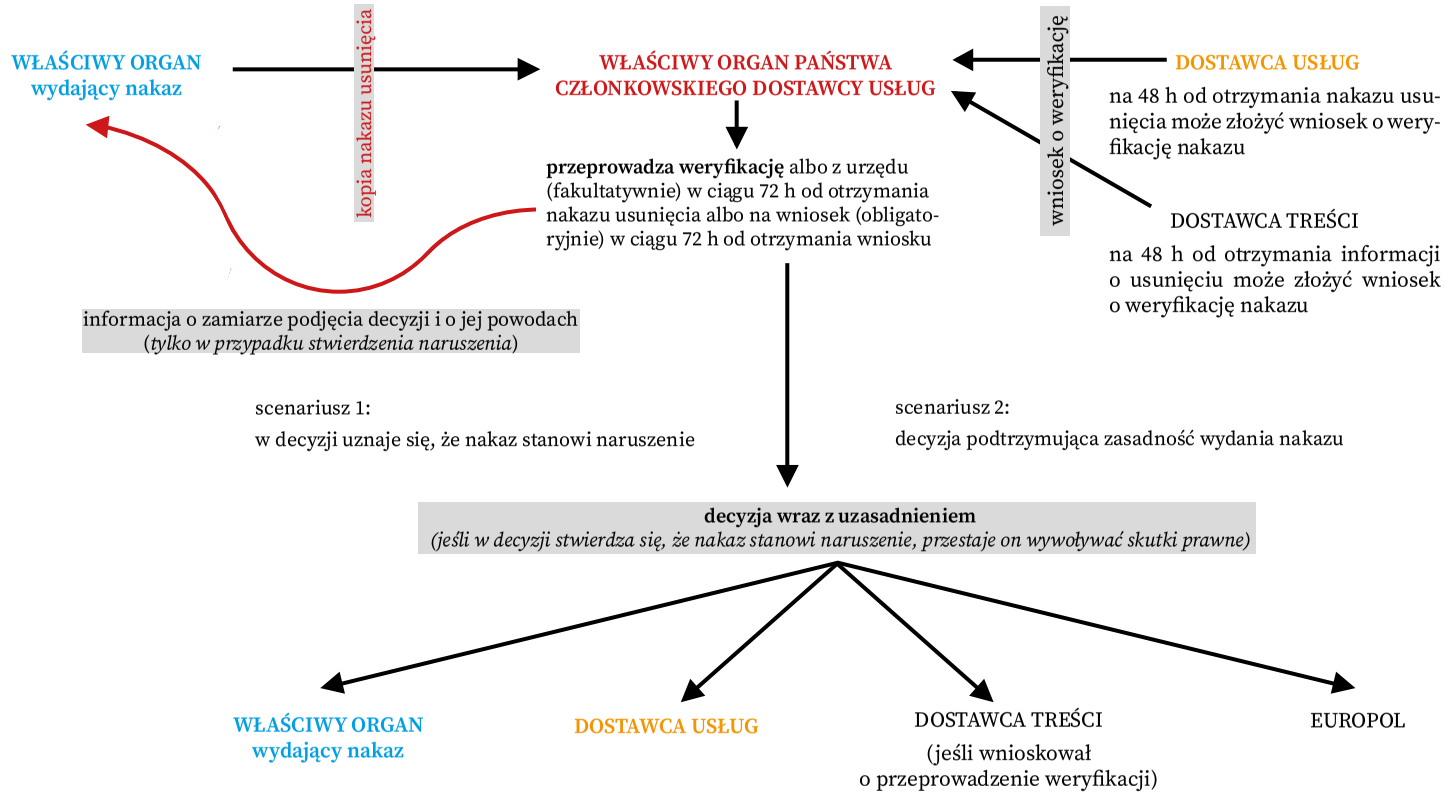
Właściwy organ państwa członkowskiego, w którym dostawca usług hostingowych ma główną jednostkę organizacyjną lub w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę, może z własnej inicjatywy, w ciągu 72 godzin od otrzymania kopii tego nakazu dokonać jego weryfikacji, aby ustalić, czy nie narusza on w sposób poważny lub oczywisty podstaw prawnych jego wydania lub praw podstawowych i wolności. W przypadku stwierdzenia takiego naruszenia podejmuje w tej sprawie decyzję wraz z uzasadnieniem, w tym samym terminie.

Również dostawcy usług hostingowych i dostawcy treści mają możliwość zainicjowania działań weryfikacyjnych – w ciągu 48 godzin od otrzymania nakazu mogą wystąpić z wnioskiem o przeprowadzenie weryfikacji do właściwego organu państwa członkowskiego, w którym dostawca usług hostingowych ma główną jednostkę organizacyjną lub w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę. Weryfikacja ta jest przeprowadzana w ciągu 72 godzin od otrzymania wniosku. W jej wyniku właściwy organ podejmuje decyzję, której wydanie jest poprzedzone przekazaniem informacji do organu wydającego nakaz o zamiarze jej podjęcia. W przypadku podjęcia decyzji organ ten niezwłocznie powiadamia o niej właściwy organ, który wydał nakaz usunięcia, dostawcę usług hostingowych, dostawcę treści, który wystąpił o przeprowadzenie weryfikacji, oraz Europol. W przypadku gdy stwierdza się, że nakaz usunięcia stanowi naruszenie, przestaje on wywoływać skutki prawne, a dostawca usług hostingowych natychmiast przywraca dane treści lub dostęp do nich.



Schemat 2. Procedura nałożenia nakazu usunięcia treści o charakterze terrorystycznym, w przypadku gdy główna jednostka organizacyjna lub przedstawiciel prawny dostawcy usług hostingowych nie znajduje się na terenie tego samego państwa członkowskiego co właściwy organ wydający nakaz.

Źródło: opracowanie Anety Sudy, *Mechanizmy blokowania w internecie treści o charakterze terrorystycznym w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym*, prezentacja Ministerstwa Spraw Wewnętrznych i Administracji przygotowana na potrzeby Międzyresortowego Zespołu ds. Zagrożeń Terrorystycznych.



Schemat 3. Procedura nałożenia transgranicznego nakazu usunięcia.

Źródło: opracowanie Anety Sudy, *Mechanizmy blokowania w internecie treści o charakterze terrorystycznym w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym*, prezentacja Ministerstwa Spraw Wewnętrznych i Administracji przygotowana na potrzeby Międzyresortowego Zespołu ds. Zagrożeń Terrorystycznych.

Drugi z wyróżnionych podstawowych mechanizmów zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym i reagowaniem na te incydenty (środki szczególne) to wydawanie decyzji w sprawie dostawców usług hostingowych narażonych na treści o charakterze terrorystycznym oraz nadzoru nad wdrażaniem przez nich środków szczególnych.

Tłumacząc *ratio legis* tego rozwiązania, unijny ustawodawca wskazał, że:

> W celu zmniejszenia dostępności treści o charakterze terrorystycznym w ramach świadczonych przez siebie usług dostawcy usług hostingowych narażeni na takie treści powinni wdrożyć środki szczególne, uwzględniając ryzyko i poziom narażenia na treści o charakterze terrorystycznym, a także wpływ na prawa osób trzecich oraz interes publiczny w zakresie informacji. Dostawcy usług hostingowych powinni ustalić, jakie odpowiednie, skuteczne i proporcjonalne środki szczególne powinny zostać wdrożone, by identyfikować i usuwać treści o charakterze terrorystycznym. Środki szczególne mogą obejmować odpowiednie techniczne lub operacyjne środki lub zdolności, takie jak personel lub środki techniczne, do celów identyfikowania i niezwłocznego usuwania treści o charakterze terrorystycznym lub uniemożliwiania dostępu do nich, mechanizmy umożliwiające użytkownikom zgłaszanie lub sygnalizowanie domniemanych treści o charakterze terrorystycznym lub inne środki, które dostawca usług hostingowych uzna za odpowiednie i skuteczne w celu przeciwdziałania dostępności, w ramach jego usług, treści o charakterze terrorystycznym[21].

Dostawca usług hostingowych uznany za dostawcę narażonego na treści o charakterze terrorystycznym zamieszcza w swoich warunkach umownych oraz stosuje postanowienia mające przeciwdziałać wykorzystywaniu jego usług do publicznego rozpowszechniania treści o charakterze terrorystycznym i podejmuje w tym celu środki szczególne. Mogą to być np.:

- techniczne i operacyjne środki lub zdolności, takie jak odpowiedni personel lub środki techniczne do celów identyfikowania i niezwłocznego usuwania treści o charakterze terrorystycznym lub uniemożliwiania dostępu do nich;
- łatwo dostępne i przyjazne dla użytkownika mechanizmy umożliwiające użytkownikom zgłaszanie lub sygnalizowanie dostawcy

[21] Motyw 22 rozporządzenia 2021/784.

usług hostingowych domniemanych treści o charakterze terrorystycznym;
- inne mechanizmy zwiększające świadomość na temat dostępności treści o charakterze terrorystycznym w ramach świadczonych przez niego usług, takie jak mechanizmy służące moderowaniu użytkowników;
- inne środki, które dostawca usług hostingowych uzna za stosowne, by przeciwdziałać dostępności treści o charakterze terrorystycznym w ramach świadczonych przez niego usług.

Zgodnie z założeniem środki szczególne mają skutecznie zmniejszać poziom narażenia usług dostawcy usług hostingowych na treści o charakterze terrorystycznym, być ukierunkowane i proporcjonalne, a także stosowane w sposób staranny i niedyskryminacyjny, uwzględniający pełne poszanowanie praw i uzasadnionego interesu użytkowników.

Dostawcę usług hostingowych należy uznać za narażonego na treści o charakterze terrorystycznym w przypadku, gdy właściwy organ państwa członkowskiego, w którym dostawca usług hostingowych ma główną jednostkę organizacyjną lub w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę, podjął decyzję, że ten dostawca jest narażony na treści o charakterze terrorystycznym. Ta decyzja powinna zostać podjęta na podstawie obiektywnych czynników, takich jak otrzymanie przez dostawcę w ciągu ostatnich 12 miesięcy co najmniej dwóch ostatecznych nakazów usunięcia tego rodzaju treści.

Po otrzymaniu decyzji dostawca usług hostingowych w terminie trzech miesięcy powiadamia właściwy organ o środkach szczególnych, które podjął lub które zamierza podjąć w celu zapewnienia wykonania ciążących na nim obowiązków. Następnie raz do roku dostawca usług hostingowych sporządza sprawozdanie z ich realizacji.

Jeżeli właściwy organ uzna, że podjęte środki szczególne nie są zgodne z wymogami, kieruje do dostawcy usług hostingowych decyzję zobowiązującą go do podjęcia niezbędnych środków. Dostawca usług hostingowych może wybrać, jaki rodzaj środków szczególnych podejmie. Może również w dowolnym momencie zwrócić się do właściwego organu o dokonanie przeglądu oraz, w stosownych przypadkach, o zmianę lub uchylenie decyzji o uznaniu go za dostawcę usług hostingowych narażonego na treści o charakterze terrorystycznym.

Na koniec tej części artykułu warto przywołać kilka danych statystycznych dotyczących stosowania rozporządzenia 2021/784 do 31 grudnia

2023 r.[22] Zgodnie z ustaleniami KE państwa członkowskie wydały 349 nakazów usunięcia treści o charakterze terrorystycznym. Z tej możliwości skorzystały organy właściwe sześciu państw członkowskich, tj. Hiszpanii – 62 nakazy, Rumunii – 2 nakazy, Francji – 26 nakazów, Niemiec – 249 nakazów (wszystkie wydane po ataku przeprowadzonym przez Hamas 7 października 2023 r.), Czech – 2 nakazy, Austrii – 8 nakazów. Nakazy były kierowane m.in. do następujących podmiotów: Telegram, Meta, JustPaste.it, TikTok, DATA ROOM S.R.L., FlokiNET S.R.L., Archive.org, SoundCloud, X, Jumpshare, KrakenFiles.com, Top4toP oraz Catbox.

Na 349 wydanych nakazów usunięcia tylko w 10 przypadkach dostawca usług hostingowych nie usunął treści o charakterze terrorystycznym lub nie zablokował ich w maksymalnym terminie, tj. do jednej godziny od otrzymania nakazu. Tylko w jednym przypadku dostawca usług hostingowych stwierdził, że wykonanie nakazu jest niemożliwe.

Żaden nakaz nie podlegał weryfikacji w procedurze dotyczącej transgranicznych nakazów usunięcia. W związku z tym nie odnotowano przypadku stwierdzającego, że wydany nakaz dokonał takiego naruszenia.

Dotychczas żaden z dostawców usług hostingowych nie został określony jako narażony na treści o charakterze terrorystycznym, a zatem żaden z dostawców nie był zobowiązany do wdrożenia środków szczególnych.

Co warte odnotowania, żaden wydany nakaz nie został dotychczas zaskarżony do sądu.

Komentarz do poszczególnych przepisów ustawy o działaniach AT w związku z zapobieganiem rozpowszechnianiu w internecie treści o charakterze terrorystycznym

Ustawą o zmianie ustawy o działaniach AT i ustawy o ABW oraz AW wprowadzono do ustawy o działaniach AT dwie grupy przepisów. Pierwsza z nich to poszerzenie słownika ustawowego, zawartego w art. 2 znowelizowanej ustawy, o trzy definicje, z których każda zawiera odwołanie do rozporządzenia 2021/784. Druga grupa przepisów została objęta nową jednostką systematyki ustawowej oznaczoną jako rozdział 5a – przeciwdziałanie rozpowszechnianiu w internecie treści o charakterze terrorystycznym. Zawarto w nim sześć przepisów związanych z wyznaczeniem właściwego organu po

[22] Na podstawie *Sprawozdania Komisji z wykonania rozporządzenia (UE) 2021/784...*

stronie krajowej, przepisy proceduralne i przepisy określające kary administracyjne, czyli normy prawne bezpośrednio zapewniające stosowanie rozporządzenia 2021/784. Ponadto uzupełniono tytuł ustawy o odesłanie do tego rozporządzenia.

Kolejna część artykułu to komentarz do poszczególnych przepisów.

> Art. 1. W ustawie z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2024 r. poz. 92 i 1248) wprowadza się następujące zmiany:
>
> 1) do tytułu ustawy dodaje się odnośnik w brzmieniu:
>
> „1) Niniejsza ustawa służy stosowaniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym (Dz. Urz. UE L 172 z 17.05.2021, str. 79)".

Przez uzupełnienie tytułu ustawy o działaniach antyterrorystycznych o odnośnik do stosowania rozporządzenia 2021/784 zrealizowano obowiązek wynikający z § 19a ust. 2 Zasad techniki prawodawczej. Zgodnie z nim w przypadku ustawy, której uchwalenie jest związane z wydaniem lub obowiązywaniem aktu normatywnego ustanowionego przez instytucję UE dającego się bezpośrednio stosować, po określeniu przedmiotu ustawy zamieszcza się odnośnik do tytułu ustawy informujący o akcie normatywnym, z którym ustawa jest związana, co wyraża się w szczególności zwrotem „niniejsza ustawa służy stosowaniu... [tytuł aktu]".

> 2) w art. 2 w pkt 7 kropkę zastępuje się średnikiem i dodaje się pkt 8–10 w brzmieniu:
>
> [ilekroć w ustawie jest mowa o:]
>
> „8) dostawcy usług hostingowych – należy przez to rozumieć dostawcę usług polegających na przechowywaniu informacji dostarczonych przez dostawcę treści i na jego wniosek, o którym mowa w art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym (Dz. Urz. UE L 172 z 17.05.2021, str. 79), zwanego dalej „rozporządzeniem 2021/784"; (...)

Zgodnie z art. 2 pkt 1 rozporządzenia 2021/784 „dostawca usług hostingowych" oznacza dostawcę usług (zdefiniowanych w art. 1 lit. b *Dyrektywy (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiającej procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego*), polegających na przechowywaniu informacji dostarczonych przez dostawcę treści i na jego wniosek. Zgodnie ze wskazaną dyrektywą „usługa" oznacza każdą usługę społeczeństwa informacyjnego, to znaczy każdą usługę normalnie świadczoną za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług. Z tym że „na odległość" oznacza, że usługa jest świadczona bez równoczesnej obecności stron. „Drogą elektroniczną" oznacza, że usługa jest wysyłana i odbierana w miejscu przeznaczenia za pomocą sprzętu elektronicznego do przetwarzania (włącznie z kompresją cyfrową) oraz przechowywania danych, i która jest całkowicie przesyłana, kierowana i otrzymywana za pomocą kabla, fal radiowych, środków optycznych lub innych środków elektromagnetycznych. „Na indywidualne żądanie odbiorcy usług" oznacza, że usługa jest świadczona przez przesyłanie danych na indywidualne żądanie.

Warto zwrócić uwagę na motyw 13 przywoływanego rozporządzenia, zgodnie z którym:

> Aby w skuteczny sposób przeciwdziałać rozpowszechnianiu w internecie treści o charakterze terrorystycznym, a jednocześnie zapewniać poszanowanie życia prywatnego osób, niniejsze rozporządzenie powinno mieć zastosowanie do dostawców usług społeczeństwa informacyjnego, którzy przechowują i publicznie rozpowszechniają informacje i materiały dostarczone przez użytkownika usługi na jego wniosek, nawet jeżeli przechowywanie i publiczne rozpowszechnianie takich informacji i materiałów ma charakter czysto techniczny, automatyczny i bierny. Pojęcie „przechowywania" należy rozumieć jako przechowywanie danych w pamięci fizycznego lub wirtualnego serwera. Dostawcy usług „zwykłego przekazu" lub „cachingu" oraz innych usług świadczonych w innych warstwach infrastruktury internetowej, które nie obejmują przechowywania, takie jak rejestry i rejestratorzy, a także dostawcy usług DNS (system nazw domen), usług płatniczych lub usług ochrony przed atakami typu DDoS (rozproszony atak typu „odmowa usługi") nie powinni zatem być objęci zakresem stosowania niniejszego rozporządzenia.

Rozporządzenie 2021/784 zakresem swej regulacji objęło dostawców usług hostingowych oferujących usługi w UE, tj. umożliwiających osobom fizycznym lub prawnym w co najmniej jednym państwie członkowskim korzystanie z usług dostawcy usług hostingowych, którego łączy z danym państwem członkowskim istotny związek wynikający z posiadania przez niego jednostki organizacyjnej w Unii, albo ze szczególnych kryteriów faktycznych, takich jak posiadanie przez dostawcę znacznej liczby użytkowników jego usług w co najmniej jednym państwie członkowskim lub kierowanie jego działalności do co najmniej jednego państwa członkowskiego (art. 2 pkt 4 i 5 rozporządzenia). Oferowanie usług musi być prowadzone w zakresie, w jakim dostawcy usług hostingowych publicznie rozpowszechniają informacje (art. 1 ust. 2 tego rozporządzenia), bez względu na umiejscowienie ich głównej jednostki organizacyjnej, tj. siedziby głównej lub siedziby statutowej, w której są wykonywane główne funkcje finansowe i jest sprawowana kontrola operacyjna (art. 2 pkt 9 rozporządzenia). Należy jednak pamiętać, że w przypadku gdy dostęp do informacji wymaga rejestracji lub dopuszczenia do udziału w grupie użytkowników – zgodnie z art. 2 pkt 3 i motywem 14 rozporządzenia – informacje te należy uznawać za publicznie rozpowszechniane jedynie wtedy, gdy użytkownicy poszukujący dostępu do informacji są automatycznie rejestrowani lub dopuszczani do udziału w grupie użytkowników, bez konieczności podejmowania przez człowieka decyzji, komu przyznać taki dostęp.

W celu zapewnienia realnego stosowania rozporządzenia w odniesieniu do dostawców usług hostingowych na podstawie art. 17 rozporządzenia 2021/784 wprowadzono obowiązek, zgodnie z którym, jeżeli dostawca nie ma głównej jednostki organizacyjnej w UE, to wyznacza na piśmie osobę fizyczną lub prawną jako swojego przedstawiciela prawnego w Unii do celów odbioru, stosowania się do i wykonywania nakazów usunięcia i decyzji wydanych przez właściwe organy. Co więcej, przekazuje on swojemu przedstawicielowi prawnemu uprawnienia i zasoby niezbędne do stosowania się do tych nakazów usunięcia i decyzji oraz do współpracy z właściwymi organami. Dostawca usług hostingowych powiadamia o wyznaczeniu przedstawiciela prawnego właściwy organ państwa członkowskiego, w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę, a także udostępnia publicznie informacje na temat przedstawiciela prawnego. Przedstawiciel prawny może zostać pociągnięty do odpowiedzialności z tytułu naruszeń niniejszego rozporządzenia, bez uszczerbku dla odpowiedzialności dostawcy usług hostingowych i działań prawnych przeciwko dostawcy usług hostingowych.

Wspomniana kwestia, w opinii autora, ma kluczowe znaczenie dla efektywności stosowania samego rozporządzenia 2021/784 z perspektywy skuteczności usuwania lub blokowania treści o charakterze terrorystycznym. W przeciwieństwie bowiem do rozwiązań przyjmowanych na poziomie poszczególnych państw, w tym obowiązujących w Polsce mechanizmów określonych w ustawie o ABW oraz AW, daje się ono skutecznie zastosować względem treści zamieszczanych u dostawcy usług hostingowych znajdującego się poza danym państwem. Analogiczną opinię wyraziła KE:

> Chociaż dobrowolne środki i niewiążące zalecenia przyczyniły się do ograniczenia dostępności w internecie treści o charakterze terrorystycznym, ze względu na pewne wyzwania – w tym ze względu na fakt, że niewielu dostawców usług hostingowych wprowadziło mechanizmy dobrowolne[23], a także ze względu na rozdrobnienie przepisów proceduralnych w poszczególnych państwach członkowskich – skuteczność i efektywność współpracy między państwami członkowskimi a dostawcami usług hostingowych była ograniczona, w związku z czym zaistniała konieczność ustanowienia środków regulacyjnych[24]. W związku z tym skuteczne stosowanie rozporządzenia ma kluczowe znaczenie dla przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym. Komisja aktywnie wspierała właściwe organy krajowe w tym procesie[25].

---

2) w art. 2 w pkt 7 kropkę zastępuje się średnikiem i dodaje się pkt 8–10 w brzmieniu: […]
[ilekroć w ustawie jest mowa o:]
„9) dostawcy treści – należy przez to rozumieć użytkownika, o którym mowa w art. 2 pkt 2 rozporządzenia 2021/784;"

Zgodnie z art. 2 pkt 2 rozporządzenia 2021/784 „dostawca treści" oznacza użytkownika, który dostarczył informacje, które są lub były przechowywane i publicznie rozpowszechniane przez dostawcę usług hostingowych.

[23] *Commission Staff Working Document Impact Assessment. Accompanying the document. Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online*, Brussels, 12 IX 2018 r., SWD(2018) 408 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2018:408:FIN [dostęp: 4 V 2023].

[24] Tamże.

[25] *Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady z wykonania rozporządzenia (UE) 2021/784…*, s. 4.

„Publiczne rozpowszechnianie" oznacza natomiast udostępnianie informacji, na wniosek dostawcy treści, potencjalnie nieograniczonej liczbie osób (art. 2 pkt 3 rozporządzenia 2021/784).

O ile unijny prawodawca wyraźnie podkreśla kluczową w wymiarze społecznym i gospodarczym rolę dostawców usług hostingowych jako łączników pomiędzy przedsiębiorstwami i obywatelami ustanawiających przestrzeń do publicznej debaty czy wymiany informacji, a których działalność może być wykorzystana przez osoby trzecie do przekazywania treści o charakterze terrorystycznym, o tyle w odniesieniu do dostawcy treści wskazuje się wprost, że ponosi on odpowiedzialność redakcyjną za swoją działalność.

2) w art. 2 w pkt 7 kropkę zastępuje się średnikiem i dodaje się pkt 8–10 w brzmieniu: […]
[ilekroć w ustawie jest mowa o:]
10) treściach o charakterze terrorystycznym – należy przez to rozumieć materiały, o których mowa w art. 2 pkt 7 rozporządzenia 2021/784.

Zgodnie z art. 2 pkt 7 rozporządzenia 2021/784 treści o charakterze terrorystycznym oznaczają materiały, które:

- podżegają do popełnienia jednego z przestępstw, o których mowa w art. 3 ust. 1 lit. a–i dyrektywy 2017/541 (wskazane poniżej), w przypadku gdy takie materiały, bezpośrednio lub pośrednio, np. przez pochwalanie aktów terrorystycznych, popierają popełnianie przestępstw terrorystycznych i tym samym stwarzają niebezpieczeństwo popełnienia jednego lub większej liczby takich przestępstw;
- nakłaniają osobę lub grupę osób do popełnienia lub przyczynienia się do popełnienia jednego z niżej wskazanych przestępstw w rozumieniu dyrektywy 2017/541;
- nakłaniają osobę lub grupę osób do uczestniczenia w działaniach grupy terrorystycznej;
- udzielają instruktażu w zakresie wytwarzania lub stosowania materiałów wybuchowych, broni palnej lub innych rodzajów broni lub trujących lub niebezpiecznych substancji, lub w zakresie innych szczególnych metod lub technik w celu popełnienia lub przyczynienia się do popełnienia jednego z niżej wymienionych przestępstw w rozumieniu dyrektywy 2017/541;

– stwarzają zagrożenie popełnienia jednego z niżej wskazanych przestępstw w rozumieniu dyrektywy 2017/541.

Zgodnie z art. 3 ust. 1 lit. a-j dyrektywy 2017/541 przestępstwa o charakterze terrorystycznym to czyny umyślne, określone zgodnie z polskim prawem jako przestępstwa, które ze względu na swój charakter lub kontekst mogą wyrządzić poważne szkody państwu lub organizacji międzynarodowej i zostały popełnione w określonym celu. Są to:

a) ataki na życie ludzkie, które mogą powodować śmierć;
b) ataki na integralność fizyczną osoby;
c) porwania lub branie zakładników;
d) spowodowanie rozległych zniszczeń obiektów rządowych lub obiektów użyteczności publicznej, systemu transportowego, infrastruktury, w tym systemu informacyjnego, stałych platform umieszczonych na szelfie kontynentalnym, miejsca publicznego lub mienia prywatnego – jeżeli zniszczenia te mogą zagrozić życiu ludzkiemu lub spowodować poważne straty gospodarcze;
e) zajęcie statku powietrznego, statku wodnego lub innego środka transportu publicznego lub towarowego;
f) wytwarzanie, posiadanie, nabywanie, przewożenie, dostarczanie lub używanie materiałów wybuchowych lub broni, w tym broni chemicznej, biologicznej, radiologicznej lub jądrowej, jak również badania nad taką bronią i jej rozwój;
g) uwalnianie substancji niebezpiecznych lub powodowanie pożarów, powodzi lub wybuchów, czego rezultatem jest zagrożenie życia ludzkiego;
h) zakłócanie lub przerywanie dostaw wody, energii elektrycznej lub wszelkich innych podstawowych zasobów naturalnych, czego rezultatem jest zagrożenie życia ludzkiego;
i) niezgodna z prawem ingerencja w systemy, o której mowa w art. 4 dyrektywy Parlamentu Europejskiego i Rady 2013/40/UE (1), w przypadkach gdy zastosowanie ma art. 9 ust. 3 lub art. 9 ust. 4 lit. b) lub c) tej dyrektywy, oraz niezgodna z prawem ingerencja w dane, o której mowa w art. 5 tej dyrektywy, w przypadkach gdy zastosowanie ma art. 9 ust. 4 lit. c) tej dyrektywy[26];

[26] Zgodnie z art. 4 i 5 *Dyrektywy Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne i zastępującej decyzję ramową Rady 2005/222/WSiSW*, niezgodna z prawem ingerencja w systemy informatyczne polega na wprowadzeniu, przekazywaniu, uszkadzaniu, usuwaniu, pogarszaniu, zmienianiu lub

j) grożenie popełnieniem jednego z wymienionych czynów.

Zgodnie z art. 3 ust. 2 dyrektywy 2017/541 wskazane kategorie przestępstw są przestępstwami terrorystycznymi, jeżeli zostały popełnione w celu:

- poważnego zastraszenia ludności;
- bezprawnego zmuszenia rządu lub organizacji międzynarodowej do podjęcia lub zaniechania jakiegoś działania;
- poważnej destabilizacji lub zniszczenie podstawowych struktur politycznych, konstytucyjnych, gospodarczych lub społecznych danego państwa lub danej organizacji międzynarodowej.

Przytoczona definicja, co do zasady, odpowiada definicji przestępstwa o charakterze terrorystycznym zawartej w art. 115 § 20 *Ustawy z dnia 6 czerwca 1997 r. Kodeks karny*, zgodnie z którą przestępstwem o charakterze terrorystycznym jest czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat, popełniony w celu:

1) poważnego zastraszenia wielu osób,
2) zmuszenia organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności,
3) wywołania poważnych zakłóceń w ustroju lub gospodarce RP, innego państwa lub organizacji międzynarodowej,

– a także groźba popełnienia takiego czynu.

Jednak polska definicja, wbrew definicji zawartej w dyrektywie 2017/541, nie określa rodzajów przestępstw bazowych, a jedynie określa je przez wskazanie, że ich górna granica wynosi co najmniej 5 lat. Na marginesie warto zauważyć, że ta odmienność była wskazywana jako brak właściwego wdrożenia dyrektywy[27], z drugiej strony zapewnia jednak elastyczność stosowania krajowej regulacji.

W kontekście stosowania rozporządzenia 2021/784 oraz zabezpieczenia przed ewentualnymi nadużyciami najważniejsza jest właściwa ocena

eliminowaniu danych komputerowych lub czynieniu ich niedostępnymi. Niezgodna z prawem ingerencja w dane to natomiast umyślne i bezprawne usuwanie, uszkadzanie, pogarszanie, zmienianie lub eliminowanie danych komputerowych w systemie informatycznym lub czynienie ich niedostępnymi.

[27] Kwestia ta była podnoszona m.in. podczas wizyty w Polsce Dyrekcji Wykonawczej Komitetu Organizacji Narodów Zjednoczonych ds. Zwalczania Terroryzmu (United Nations Counter-Terrorism Committee Executive Directorate, UN CTED), której celem było dokonanie ewaluacji wdrożonych przez Polskę rezolucji Rady Bezpieczeństwa ONZ w zakresie walki z terroryzmem.

faktu ujawnienia treści o charakterze terrorystycznym. Wskazówkę w tym zakresie zawiera motyw 11 tego rozporządzenia. Zgodnie z nim, z uwagi na potrzebę przeciwdziałania najbardziej szkodliwej propagandzie terrorystycznej w internecie, definicja treści o charakterze terrorystycznym powinna obejmować:

> (...) materiały, które podżegają lub nakłaniają kogoś do popełniania przestępstw terrorystycznych lub do przyczynienia się do ich popełniania, materiały, które nakłaniają kogoś do uczestniczenia w działaniach grupy terrorystycznej lub które pochwalają działalność terrorystyczną, w tym poprzez rozpowszechnianie materiałów przedstawiających atak terrorystyczny. Definicja ta powinna także obejmować materiały, które udzielają instruktażu w zakresie wytwarzania lub stosowania materiałów wybuchowych, broni palnej lub innych rodzajów broni lub trujących lub niebezpiecznych substancji, jak również substancji chemicznych, biologicznych, radiologicznych i jądrowych (CBRJ), lub instruktażu w zakresie innych szczególnych metod lub technik, w tym w zakresie wyboru celów, w celu popełniania przestępstw terrorystycznych lub przyczynienia się do ich popełniania. Materiały takie obejmują tekst, obrazy, nagrania dźwiękowe i nagrania wideo, a także transmisje na żywo przestępstw terrorystycznych, które stwarzają niebezpieczeństwo popełnienia kolejnych takich przestępstw.

Dalsza część tego motywu rozporządzenia 2021/784 wskazuje, że przy ocenie, czy materiały stanowią treści o charakterze terrorystycznym, właściwe organy oraz dostawcy usług hostingowych powinni uwzględniać takie czynniki, jak charakter i treść komunikatów, kontekst, w jakim komunikaty te zostały przedstawione, oraz to, w jakim stopniu mogą one spowodować skutki szkodliwe dla bezpieczeństwa i ochrony osób. W motywie tym sformułowano jednak istotne ograniczenie. Zgodnie z nim ważny czynnik w tej ocenie stanowi fakt, że dany materiał został wyprodukowany przez osobę, grupę lub podmiot umieszczone w unijnym wykazie osób, grup i podmiotów uczestniczących w aktach terrorystycznych i podlegających środkom ograniczającym, że można go przypisać takiej osobie, grupie lub podmiotowi lub że jest on rozpowszechniany w imieniu takiej osoby, grupy lub podmiotu. Z jednej strony ma to służyć zapewnieniu wolności słowa i opinii, z drugiej strony, przy wykładni literalnej, a nie celowościowej, stanowi zawężanie danej treści do powiązania z osobami, grupami lub podmiotami umieszczonymi w unijnym wykazie osób, grup i podmiotów

uczestniczących w aktach terrorystycznych. Nie każdy bowiem dostawca tego rodzaju treści może wprost wykazywać tego rodzaju powiązanie.

W art. 1 ust. 3 rozporządzenia 2021/784 wskazano natomiast wprost, że nie uznaje się za treści o charakterze terrorystycznym materiałów publicznie rozpowszechnianych w celach edukacyjnych, dziennikarskich, artystycznych lub badawczych bądź w celach zapobiegania terroryzmowi lub zwalczania terroryzmu, w tym materiałów służących wyrażaniu polemicznych lub kontrowersyjnych poglądów w ramach debaty publicznej. Co więcej, to w drodze oceny ma być ustalane, jaki jest rzeczywisty cel rozpowszechniania danych treści. Warto w tym kontekście wspomnieć o motywie 12 rozporządzenia 2021/784. Zgodnie z nim przy ustalaniu, czy dany materiał dostarczony przez dostawcę treści stanowi „treści o charakterze terrorystycznym", należy uwzględnić zwłaszcza prawo do wolności wypowiedzi i informacji, w tym wolność i pluralizm mediów, oraz wolność sztuki i nauki.

Z perspektywy legislacyjnej warto zwrócić uwagę na spójność konstrukcyjną terminologii stosowanej w Kodeksie karnym, ustawie o działaniach AT i rozporządzeniu 2021/784. Wskazane akty prawne posługują się odpowiednio terminami „przestępstwo o charakterze terrorystycznym", „zdarzenie o charakterze terrorystycznym" i „treści o charakterze terrorystycznym". Jednak nie wszystkie polskie akty prawne je uwzględniają. Na przykład w ustawie o ABW oraz AW jest mowa o „przestępstwie terroryzmu".

Art. 26a. Szef ABW jest organem właściwym w rozumieniu rozporządzenia 2021/784.

Przy analizie zakresu wskazanej właściwości na początku należy zwrócić uwagę na wspomniany wcześniej art. 12 rozporządzenia 2021/784, zgodnie z którym każde państwo członkowskie wyznacza organ lub organy właściwe w zakresie:

- wydawania nakazów zobowiązujących dostawców usług hostingowych do usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do treści terrorystycznych we wszystkich państwach członkowskich (nakaz usunięcia),
- weryfikowania nakazów usunięcia wydanych przez właściwe organy innych państw członkowskich oraz stwierdzania ewentualnych

naruszeń w tym zakresie (procedura dotycząca transgranicznych nakazów usunięcia),
- nadzoru nad wdrażaniem środków szczególnych przez dostawcę usług hostingowych,
- nakładania kar za złamanie przepisów przedmiotowego rozporządzenia.

Powyższe wskazanie nie wyczerpuje wszystkich obowiązków i uprawnień nakładanych na organy właściwe w innych przepisach rozporządzenia 2021/784. W tym zakresie można wskazać m.in. na:
- przedłużanie okresu zachowania treści o charakterze terrorystycznym, które zostały usunięte lub do których dostęp został uniemożliwiony, na skutek wydanego nakazu usunięcia (art. 6 ust. 2 rozporządzenia 2021/784),
- wydawanie decyzji w sprawie dostawców usług hostingowych narażonych na treści o charakterze terrorystycznym oraz nadzoru nad wdrażaniem przez nich środków szczególnych, na podstawie art. 5 rozporządzenia 2021/784,
- prowadzenie współpracy, w tym wymiany informacji, z innymi właściwymi organami ustanowionymi przez pozostałe państwa członkowskie, Europolem oraz dostawcami usług hostingowych, zgodnie z art. 14 rozporządzenia 2021/784,
- publikację sprawozdania, na podstawie art. 8 rozporządzenia 2021/784,
- przekazywanie do KE rocznej informacji na podstawie art. 21 rozporządzenia 2021/784.

We wskazanym art. 12 rozporządzenia 2021/784 unijny prawodawca przewidział możliwość wyznaczenia różnych organów jako organów właściwych do realizacji wskazanych uprawnień i obowiązków. Polski ustawodawca nie skorzystał z tej możliwości i wskazał Szefa ABW jako jedyny organ właściwy na gruncie krajowym. Rozwiązanie to wydaje się optymalne i wpisuje się w całokształt krajowych unormowań w tym zakresie, w związku z czym należy zwrócić uwagę na przynajmniej cztery aspekty. Po pierwsze, Szef ABW zgodnie z art. 3 ust. 1 ustawy o działaniach AT odpowiada za zapobieganie zdarzeniom o charakterze terrorystycznym[28]. Po drugie, na podstawie art. 5 ust. 1 pkt 1 ustawy o ABW oraz AW do zadań tej formacji

[28] Zob. szerzej: P. Burczaniuk, *Zadania i uprawnienia organów ścigania karnego w zakresie zwalczania terroryzmu w Polsce – perspektywa prawna*, „Terroryzm – studia, analizy, prewencja" 2022, nr 2, s. 9–30. https://doi.org/10.4467/27204383TER.22.017.16337.

należy m.in. rozpoznawanie i wykrywanie przestępstw terroryzmu oraz zapobieganie im, a treści o charakterze terrorystycznym w dużej mierze służą przeprowadzeniu zamachów o charakterze terrorystycznym. Po trzecie, już wcześniej Szef ABW uzyskał kompetencję do blokowania treści o charakterze terrorystycznym na podstawie przepisów ustawy o ABW oraz AW. Po czwarte, ABW ma również strukturę organizacyjną w postaci Centrum Antyterrorystycznego ABW, w pełni przygotowaną do realizacji tego celu, działającą w trybie całodobowym.

Zgodnie z motywem 35 rozporządzenia 2021/784 państwa członkowskie powinny mieć możliwość decydowania o liczbie właściwych organów, które mają zostać wyznaczone, a także o tym, czy mają to być organy administracyjne, organy ścigania czy organy sądowe. Organy te muszą wypełniać swoje zadania w sposób obiektywny i niedyskryminacyjny oraz nie powinny zwracać się o instrukcje do żadnego innego organu w związku z wykonywaniem zadań powierzonych im na podstawie tego rozporządzenia. Co jednak istotne, nie powinno to wykluczać sprawowania nadzoru zgodnie z krajowym prawem konstytucyjnym.

Na podstawie art. 12 ust. 4 rozporządzenia 2021/784 KE utworzyła i na bieżąco aktualizuje internetowy rejestr zawierający wykaz właściwych organów w poszczególnych państwach oraz ich punktów kontaktowych wyznaczonych lub ustanowionych na podstawie art. 12 ust. 2 rozporządzenia, o którym mowa w dalszej części artykułu, w komentarzu do art. 26b ustawy o działaniach AT[29]. Zgodnie z rejestrem opublikowanym na stronie internetowej KE w dniu, gdy polski parlament przyjmował rozwiązania w zakresie blokowania treści, z 27 państw członkowskich UE, takie informacje przekazało 25 (zgłoszeń nie dokonały Słowenia i Portugalia)[30]. Z tej grupy 13 państw wyznaczyło organ właściwy – analogicznie jak Polska – spośród służb o charakterze policyjnym lub specjalnym, cztery państwa wskazały na właściwość komórki organizacyjnej funkcjonującej w ramach ministerstwa spraw wewnętrznych i tyle samo państw w innych urzędach centralnych, np. w przypadku Węgier to Narodowy Urząd ds. Mediów i Komunikacji (Nemzeti Média- és Hírközlési Hatóság), w Austrii – Urząd do

[29] *List of national competent authority (authorities) and contact points*, European Commission, 27 I 2025 r., https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/prevention-radicalisation/terrorist-content-online/list-national-competent-authority-authorities-and-contact-points_en?prefLang=pl [dostęp: 15 II 2025].

[30] Na 23 II 2025 r. jedynym państwem, które nie dokonało zgłoszenia, była Portugalia.

Spraw Łączności (Kommunikationsbehörde Austria). W dwóch państwach jest to organ prokuratorski, a w jednym właściwy jest sąd[31].

Decyzja polskiego ustawodawcy, tj. wskazanie Szefa ABW jako organu właściwego, jest zgodna z wytycznymi UE i nie odbiega od rozwiązań przyjętych w innych państwach, jednak praktyka w tym zakresie jest różna.

> Art. 26b. 1. Szef ABW wyznacza w ABW punkt kontaktowy, o którym mowa w art. 12 ust. 2 rozporządzenia 2021/784, działający w systemie całodobowym przez 7 dni w tygodniu.
> 2. Informacje o siedzibie i danych kontaktowych punktu, o którym mowa w ust. 1, oraz sposobie składania wniosków o wyjaśnienie i informacje zwrotne w sprawie nakazów usunięcia zobowiązujących dostawców usług hostingowych do usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do treści o charakterze terrorystycznym, zwanych dalej „nakazami usunięcia", udostępnia się w Biuletynie Informacji Publicznej na stronie podmiotowej ABW.

Artykułem 12 ust. 2 rozporządzenia 2021/784 państwa członkowskie zostały zobowiązane do zapewnienia, że w ramach organu właściwego do wydawania nakazów usunięcia zostanie wyznaczony lub ustanowiony punkt kontaktowy zajmujący się wnioskami o wyjaśnienie i informacjami zwrotnymi, które dotyczą tych nakazów. W Polsce konsekwencją wyboru Szefa ABW jako organu właściwego było wyznaczenie przez niego punktu kontaktowego w kierowanej przez siebie Agencji. Państwa członkowskie zostały również zobowiązane do zapewnienia, że informacje na temat punktu kontaktowego będą publicznie dostępne.

Warto zauważyć, że polski ustawodawca rozszerzył minimalny zakres informacji zamieszczonych na stronie podmiotowej stosownie do wymogów wynikających z rozporządzenia 2021/784. Oprócz informacji o punkcie kontaktowym na stronie podmiotowej musi się znajdować również informacja o sposobie składania wniosków o wyjaśnienie i informacje zwrotne w sprawie nakazów usunięcia. Zgodnie z komunikatem zawartym na stronie ABW:

> Wnioski o wyjaśnienie w sprawie nakazów usunięcia zobowiązujących dostawców usług hostingowych do usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do treści o charakterze

[31] Zob. szerzej: *Rządowy projekt ustawy o zmianie ustawy*...

terrorystycznym, złożone przy użyciu wzoru określonego w załączniku nr III do rozporządzenia 2021/784, można kierować w postaci papierowej na adres pocztowy punktu kontaktowego bądź w postaci elektronicznej na adres e-mail punktu kontaktowego. Informacje zwrotne po usunięciu treści o charakterze terrorystycznym lub uniemożliwieniu dostępu do nich, złożone przy użyciu wzoru określonego w załączniku nr II do rozporządzenia 2021/784, będą przekazywane w tej samej postaci[32].

Należy odnotować, że punkt kontaktowy jest przeznaczony wyłącznie dla dostawców usług hostingowych, których dotyczy nakaz usunięcia. Agencja Bezpieczeństwa Wewnętrznego nie prowadzi ogólnego portalu zgłaszania nielegalnych treści w internecie.

Art. 26c. 1. Szef ABW sprawuje nadzór nad wdrażaniem środków szczególnych, o których mowa w art. 5 ust. 1–3 rozporządzenia 2021/784, przez:
1) dokonywanie kontroli środków szczególnych, które podjął dostawca usług hostingowych, w tym pod kątem ich zgodności z art. 5 ust. 2 i 3 rozporządzenia 2021/784;
2) wydawanie dostawcy usług hostingowych pisemnych zaleceń, mających na celu usunięcie stwierdzonych nieprawidłowości i dostosowanie jego działalności do przepisów rozporządzenia 2021/784.

2. Upoważniony funkcjonariusz ABW, przeprowadzając czynności, o których mowa w ust. 1, ma prawo:
1) wstępu na teren kontrolowanych obiektów wykorzystywanych do świadczenia usług hostingowych;
2) żądania od dostawcy usług hostingowych wyjaśnień i udostępnienia dokumentacji technicznej i operacyjnej wynikającej ze stosowania środków szczególnych bądź wglądu w tę dokumentację.

3. Dostawca usług hostingowych narażony na treści o charakterze terrorystycznym usuwa naruszenia przepisów prawa i nieprawidłowości stwierdzone w ramach nadzoru sprawowanego przez Szefa ABW w terminie określonym w pisemnym zaleceniu.

Umożliwienie objęcia dostawcy usług hostingowych środkami szczególnymi przez uznanie go za dostawcę narażonego na treści o charakterze terrorystycznym jest powiązane z zobowiązaniem państw do zapewnienia przez właściwe organy skutecznych funkcji nadzorczych. Jak wskazano

[32] *Punkt kontaktowy TCO*, BIP ABW, https://bip.abw.gov.pl/bip/punkt-kontatowy-tco/525, Punkt-kontaktowy-TCO.html [dostęp: 13 XII 2024].

wcześniej, wdrażane przez dostawcę usług hostingowych środki zabezpieczające mogą dotyczyć odpowiednich środków technicznych i operacyjnych umożliwiających użytkownikom zgłaszanie treści o charakterze terrorystycznym, a także innych mechanizmów zwiększających świadomość odbiorców treści. Jeżeli natomiast właściwy organ uzna, że podjęte środki szczególne nie są zgodne z wymogami, kieruje on do dostawcy usług hostingowych decyzję zobowiązującą go do podjęcia niezbędnych środków uzupełniających lub naprawczych.

Zapewnienie stosowania tych przepisów wymagało wskazania, że Szef ABW sprawuje nadzór nad wdrażaniem środków szczególnych, który będzie polegał ma dokonywaniu kontroli środków szczególnych stosowanych przez dostawcę usług hostingowych, a także na wydawaniu mu pisemnych zaleceń w przypadku stwierdzenia nieprawidłowości w tym zakresie.

W celu zapewnienia wykonania tych czynności upoważniony funkcjonariusz ABW ma prawo wstępu na teren kontrolowanych obiektów wykorzystywanych do świadczenia usług hostingowych oraz żądania od dostawcy usług hostingowych wyjaśnień i udostępnienia dokumentacji technicznej i operacyjnej wynikającej ze stosowania środków szczególnych bądź wglądu w nią.

W myśl przepisów dostawca usług hostingowych jest zobowiązany do terminowego usunięcia stwierdzonych nieprawidłowości.

Wprowadzone przepisy z jednej strony w niektórych elementach nawiązują do *Ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia*, z drugiej zaś, co niezwykle istotne z perspektywy zasad realizacji czynności, nie wyłączają stosowania ustawy – Prawo przedsiębiorców.

W kontekście ustawy o ochronie osób i mienia warto zwrócić uwagę na brzmienie jej art. 43 ust. 2 pkt 3–5, który określa zasady nadzoru Komendanta Głównego Policji nad działalnością specjalistycznych uzbrojonych formacji ochronnych. Wskazany tam nadzór polega m.in. na wstępie na teren siedziby przedsiębiorcy prowadzącego działalność i wydawaniu pisemnych zaleceń mających na celu usunięcie stwierdzonych nieprawidłowości i dostosowanie działalności tych formacji do przepisów prawa.

W uzasadnieniu do rządowego projektu ustawy o zmianie ustawy o działaniach AT i ustawy o ABW oraz AW stwierdzono natomiast: *Podkreślenia wymaga, że do kontroli, w zakresie nieuregulowanym niniejszą*

ustawą, będą miały zastosowanie przepisy ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców, w tym art. 48, art. 49 ust. 1–3 i 6–9, a także art. 51–57[33].

W kontekście art. 48 ustawy – Prawo przedsiębiorców należy zwrócić uwagę m.in. na obowiązek zawiadamiania przedsiębiorcy przez organ kontroli o zamiarze wszczęcia kontroli. Wszczyna się ją nie wcześniej niż po upływie 7 dni i nie później niż przed upływem 30 dni od dnia doręczenia zawiadomienia o zamiarze wszczęcia kontroli. Na wniosek przedsiębiorcy może być ona wszczęta przed upływem 7 dni od dnia doręczenia zawiadomienia. Z czynności kontrolnych wykonywanych w trybie związanych z oględzinami sporządza się protokół.

Zgodnie z art. 49 tej regulacji czynności kontrolne mogą być wykonywane przez pracowników organu kontroli po okazaniu przedsiębiorcy albo osobie przez niego upoważnionej legitymacji służbowej upoważniającej do wykonywania takich czynności oraz po doręczeniu upoważnienia do przeprowadzenia kontroli. Jej zakres nie może wykraczać poza ten wskazany w upoważnieniu.

Na podstawie art. 51–57 tej ustawy kontrolę przeprowadza się, co do zasady, w siedzibie przedsiębiorcy lub w miejscu wykonywania działalności gospodarczej oraz w godzinach pracy lub w czasie faktycznego wykonywania działalności gospodarczej przez przedsiębiorcę. Czynności kontrolne wykonuje się jak najsprawniej i tak, by w miarę możliwości nie zakłócić funkcjonowania przedsiębiorcy. Ustalenia kontroli zamieszcza się w protokole. W przypadku gdy przedsiębiorca wskaże na piśmie, że wykonywane czynności zakłócają w sposób istotny działalność gospodarczą przedsiębiorcy, konieczność podjęcia takich czynności uzasadnia się w protokole kontroli. Ponadto ma zastosowanie zakaz podejmowania i prowadzenia więcej niż jednej kontroli działalności przedsiębiorcy. Czas trwania wszystkich kontroli u przedsiębiorcy w jednym roku kalendarzowym zależy od wielkości przedsiębiorstwa. Przedłużenie czasu trwania kontroli jest możliwe jedynie z przyczyn niezależnych od organu kontroli i wymaga uzasadnienia na piśmie.

Wskazane normy wynikające z ustawy – Prawo przedsiębiorców nie wyczerpują całości uregulowań w zakresie kontroli, jednak na podstawie przywołanych rozwiązań należy podkreślić, że kontrola stosowania środków szczególnych jest prowadzona na standardowych zasadach przewidzianych dla kontroli przedsiębiorców i nie zawiera wyróżniających się rozwiązań.

[33] *Rządowy projekt ustawy o zmianie ustawy...* – uzasadnienie..., s. 9.

Art. 26d. 1. Nakaz usunięcia lub stwierdzenie naruszenia, o którym mowa w art. 4 ust. 3 i 4 rozporządzenia 2021/784, następuje w drodze decyzji administracyjnej. Do postępowań w tych sprawach w zakresie nieuregulowanym w rozporządzeniu 2021/784 i niniejszej ustawie stosuje się przepisy art. 6, art. 7, art. 7b, art. 8, art. 12, art. 14, art. 16, art. 24, art. 26 § 1 i 2, art. 28–30, art. 32, art. 33, art. 35 § 1, art. 50, art. 54–56, art. 63–65, art. 72, art. 75 § 1, art. 77, art. 97 § 1 pkt 4 i § 2, art. 104, art. 105 § 1, art. 112, art. 113 § 1, art. 156–158, art. 217 oraz art. 268a ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz.U. z 2024 r. poz. 572).

2. Wskazywanie dostawców usług hostingowych narażonych na treści o charakterze terrorystycznym, o których mowa w art. 5 rozporządzenia 2021/784, następuje w drodze decyzji administracyjnej. Do postępowań w tych sprawach stosuje się przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, o których mowa w ust. 1, oraz art. 107 tej ustawy.
3. Decyzje, o których mowa w ust. 1 i 2, są ostateczne i podlegają natychmiastowemu wykonaniu.
4. Dostawcy usług hostingowych, w stosunku do którego Szef ABW wydał nakaz usunięcia, lub dostawcy treści, którego treści obejmuje nakaz usunięcia, przysługuje prawo do wniesienia na ten nakaz skargi do sądu administracyjnego w terminie 30 dni od dnia:
   1) jego dostarczenia w trybie, o którym mowa w art. 3 ust. 5 rozporządzenia 2021/784 – w przypadku dostawcy usług hostingowych;
   2) otrzymania informacji, o której mowa w art. 11 ust. 1 rozporządzenia 2021/784 – w przypadku dostawcy treści.
5. Dostawcy usług hostingowych lub dostawcy treści, w stosunku do którego Szef ABW wydał decyzję, o której mowa w art. 4 ust. 4 rozporządzenia 2021/784, przysługuje prawo do wniesienia na tę decyzję skargi do sądu administracyjnego w terminie 30 dni od dnia otrzymania powiadomienia o tej decyzji.
6. Dostawcy usług hostingowych, w stosunku do którego Szef ABW wydał decyzję, o której mowa w art. 5 ust. 4, 6 lub 7 rozporządzenia 2021/784, przysługuje prawo do wniesienia na tę decyzję skargi do sądu administracyjnego.
7. Skargi, o których mowa w ust. 4–6, mogą być rozpoznawane w trybie uproszczonym, o którym mowa w art. 120 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz.U. z 2024 r. poz. 935), o ile strona nie zawnioskuje o przeprowadzenie rozprawy, a sąd uzna, że wszystkie okoliczności sprawy zostały dostatecznie wyjaśnione i przeprowadzenie rozprawy jest zbędne. Przepis art. 122 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi stosuje się.

W świetle brzmienia art. 26d ust. 1 i 2 nakaz usunięcia lub stwierdzenie naruszenia w procedurze dotyczącej transgranicznych nakazów usunięcia, a także wskazywanie dostawców usług hostingowych narażonych na treści o charakterze terrorystycznym następują w drodze decyzji administracyjnej. Norm proceduralnych do wydawania decyzji dostarcza zatem nie tylko rozporządzenie 2021/784 czy znowelizowana ustawa o działaniach AT, lecz także *Ustawa z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego* (dalej: k.p.a.). Zakres stosowania k.p.a. jest jednak znacznie ograniczony przez enumeratywne wskazanie konkretnych przepisów.

To, czy rzeczywiście tak głębokie wyłączenie k.p.a. pozwala realnie traktować nakaz usunięcia jako decyzję administracyjną, może być dyskusyjne, szczególnie w kontekście braku zastosowania w tych sprawach art. 107 k.p.a. określającego niezbędne elementy decyzji. Jednak jak wskazano w uzasadnieniu do ustawy:

> Częściowe zastosowanie uregulowań Kodeksu postępowania administracyjnego w tym przypadku jest niezbędne. Stanowi o tym fakt, że tryb postępowania opisany w rozporządzeniu 2021/784 odnośnie do wydawania nakazów usunięcia ma zapewnić na poziomie unijnym (a zatem w wymiarze transgranicznym) spójny i efektywny mechanizm usuwania lub blokowania w sieci wszelkich treści o charakterze terrorystycznym. Skuteczność tego mechanizmu jest natomiast mierzona szybkością reakcji i wykonania stosownych czynności. W rezultacie przyjęty w unijnym akcie sposób postępowania zarówno w odniesieniu do wydawania nakazów usunięcia, jak i stwierdzenia naruszeń, o których mowa w art. 4 ust. 3 i 4 rozporządzenia 2021/784, znacząco odbiega od niektórych rozwiązań przyjętych na gruncie krajowych przepisów prawa administracyjnego. Ponadto większość elementów w rozumieniu postępowania administracyjnego zostało wprost określonych w samym rozporządzeniu, np. elementy decyzji, moment i skutek jej doręczenia, a zatem w takim przypadku jest niezbędne wyłączenie uregulowań krajowych[34].

W uzasadnieniu do ustawy wskazano również, że przyjęty w art. 26d ust. 1 katalog przepisów k.p.a. jest wzorowany na art. 4 ust. 1 *Ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa*

[34] *Rządowy projekt ustawy o zmianie ustawy...* – uzasadnienie..., s. 9–10.

narodowego[35]. Dokonano jednak niezbędnych uzupełnień i dostosowania do mechanizmu postępowania wynikającego wprost z przepisów rozporządzenia 2021/784.

Należy zatem zauważyć, że do postępowań prowadzonych w sprawach nakazów oraz wskazania dostawców usług hostingowych narażonych na treści o charakterze terrorystycznym (środki szczególne) mają zastosowanie podstawowe zasady k.p.a., w tym:

- zasada praworządności (art. 6),
- zasada prawdy obiektywnej (art. 7),
- zasada uwzględniania interesu społecznego i słusznego interesu obywateli (art. 7),
- zasada zaufania do władzy publicznej (art. 8),
- zasada szybkości i prostoty postępowania (art. 12),
- zasada pisemności postępowania (art. 14),
- zasada trwałości decyzji administracyjnych (art. 16).

Powyższe przepisy mają charakter ściśle gwarancyjny z perspektywy ochrony interesów strony. Obiektywność postępowań jest zabezpieczona również przez możliwość wyłączenia pracownika danego organu od udziału w postępowaniu, zgodnie z art. 24 k.p.a.

Z perspektywy stron warto także wspomnieć o stosowaniu art. 28 i 29 k.p.a., zgodnie z którymi stroną jest każdy, czyjego interesu prawnego lub obowiązku dotyczy postępowanie, albo kto żąda czynności organu ze względu na swój interes prawny lub obowiązek. Stronami mogą być osoby fizyczne i osoby prawne, a gdy chodzi o państwowe i samorządowe jednostki organizacyjne i organizacje społeczne – również jednostki nieposiadające osobowości prawnej.

W przeciwieństwie do wspomnianego wzorca z ustawy o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, w sprawach objętych analizowaną regulacją ma zastosowanie cały art. 77 k.p.a. Zgodnie z nim organ jest zobowiązany w sposób wyczerpujący zebrać i rozpatrzyć cały materiał dowodowy, może też w każdym stadium postępowania zmienić, uzupełnić lub uchylić swoje postanowienie dotyczące przeprowadzenia dowodu. Organ przeprowadzający postępowanie na wezwanie organu

[35] Zob. szerzej: M. Cichomski, *Między konfliktem zbrojnym a terroryzmem państwowym – szczególne indywidualne środki ograniczające przyjęte w Polsce w kontekście wojny w Ukrainie i sytuacji w Białorusi. Perspektywa prawna*, „Terroryzm – studia, analizy, prewencja" 2024, nr 5, s. 118–121. https://doi.org/10.4467/27204383TER.24.003.19391.

właściwego do załatwienia sprawy (art. 52 k.p.a.) może też z urzędu lub na wniosek strony przesłuchać nowych świadków i biegłych na okoliczności będące przedmiotem tego postępowania.

Analogicznie do nakazów usunięcia oraz stwierdzania naruszeń w formie decyzji administracyjnej następuje także wskazanie dostawców usług hostingowych narażonych na treści o charakterze terrorystycznym, zgodnie z art. 5 rozporządzenia 2021/784. Do tych decyzji k.p.a. również ma zastosowanie, lecz w ograniczonym zakresie. W tym wypadku jednak, w przeciwieństwie do postępowań związanych z wydaniem nakazu usunięcia lub stwierdzenia naruszenia, o którym mowa w art. 4 ust. 3 i 4 rozporządzenia 2021/748, ma zastosowanie art. 107 k.p.a., czyli przepis określający elementy decyzji. Wynika to z faktu, że ww. rozporządzenie w tym wypadku nie określa formy ani elementów składowych tego rozstrzygnięcia.

Jednocześnie we wszystkich tych przypadkach postępowania są jednoinstancyjne, a wydane decyzje podlegają natychmiastowej wykonalności, co wiąże się z potrzebą zapewnienia sprawności i efektywności prowadzenia takich postępowań. W kontekście jednoinstancyjności postępowań administracyjnych należy przywołać art. 78 Konstytucji RP, zgodnie z którym każda ze stron ma prawo do zaskarżenia orzeczeń i decyzji wydanych w pierwszej instancji, a wyjątki od tej zasady oraz tryb zaskarżania określa ustawa. Konstytucja RP dopuszcza zatem takie rozwiązanie, ale stanowi ono odstępstwo od zasady, co musi mieć swoje uzasadnienie. W tej sytuacji należy go szukać w konstytucyjnej przesłance zapewnienia bezpieczeństwa i porządku publicznego. Zgodnie bowiem z art. 31 ust. 3 Konstytucji RP ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw, w tym wypadku prawa zaskarżenia decyzji wydanej w pierwszej instancji, mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w państwie demokratycznym dla jego bezpieczeństwa lub porządku publicznego bądź dla ochrony środowiska, zdrowia i moralności publicznej albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw. W tym wypadku brak możliwości zaskarżenia decyzji pierwszej instancji nie wydaje się, w opinii autora, naruszać istoty praw, o których mowa powyżej, pozostaje bowiem droga sądowa. Osobna kwestia to natomiast ocena, czy to rozwiązanie jest konieczne w państwie demokratycznym dla jego bezpieczeństwa lub porządku publicznego. Ono również wydaje się spełniać ten wymóg konstytucyjny. Wprawdzie można sobie wyobrazić, że wskutek zaskarżenia decyzji Szef ABW będzie rozpatrywał wniosek o ponowne rozpatrzenie sprawy, jednak istota

rozstrzyganych spraw wymaga natychmiastowej wykonalności. Nakaz usunięcia nie może oczekiwać na uprawomocnienie, bo jego istotą jest natychmiastowe uniemożliwienie rozpowszechniania treści o charakterze terrorystycznym. Okres oczekiwania na uprawomocnienie decyzji pozbawiłby to narzędzie prawne znaczenia zapobiegawczego, ponieważ nakaz usunięcia to nie kara, lecz instrument prewencyjny. Dopiero na podstawie innych przepisów prawnych w oddzielnym postępowaniu, już nie administracyjnym, lecz karnym, jest możliwe ukaranie dostawcy takiej treści. Analogicznie należałoby postrzegać rozwiązanie, zgodnie z którym zaskarżenie decyzji następowałoby do organu drugiej instancji, czyli organu nadzorującego formację, w tym wypadku Prezesa Rady Ministrów.

Dostawcy usług hostingowych, w stosunku do którego Szef ABW wydał nakaz usunięcia, lub dostawcy treści, którego treści obejmuje nakaz usunięcia, przysługuje prawo do wniesienia skargi do sądu administracyjnego w terminie 30 dni. W pierwszym przypadku termin ten jest liczony od dostarczenia decyzji, a w drugim przypadku – od dnia otrzymania informacji. W tym zakresie art. 26d ustawy jest wykonaniem art. 9 rozporządzenia 2021/784, który przyznaje prawo do zaskarżania wydanych nakazów usunięcia oraz pozostałych decyzji wydanych przez organ właściwy.

W przypadku dostawcy usług hostingowych właściwy organ kieruje nakaz usunięcia do jego głównej jednostki organizacyjnej lub do jego przedstawiciela prawnego. Nakaz usunięcia jest przekazywany punktowi kontaktowemu dostawcy usług hostingowych za pomocą środków elektronicznych dających możliwość sporządzenia pisemnego potwierdzenia na warunkach umożliwiających ustalenie autentyczności nadawcy, w tym podanie dokładnej daty oraz godziny wysłania i otrzymania nakazu.

Dostawcy usług hostingowych lub dostawcy treści, w stosunku do którego Szef ABW wydał decyzję we wspomnianej procedurze dotyczącej transgranicznych nakazów usunięcia, przysługuje prawo do wniesienia na tę decyzję skargi do sądu administracyjnego w terminie 30 dni od dnia otrzymania powiadomienia o tej decyzji.

Również dostawcy usług hostingowych, który został uznany za dostawcę szczególnie narażonego na treści o charakterze terrorystycznym (środki szczególne), przysługuje prawo do wniesienia na tę decyzję skargi do sądu administracyjnego.

Skargi wniesione we wszystkich z ww. przypadków mogą być rozpoznawane w trybie uproszczonym, o którym mowa w art. 120 *Ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi*,

tj. na posiedzeniu niejawnym w składzie trzech sędziów, o ile strona nie zawnioskuje o przeprowadzenie rozprawy, a sąd uzna, że wszystkie okoliczności sprawy zostały dostatecznie wyjaśnione i przeprowadzenie rozprawy jest zbędne. Jak wskazano w uzasadnieniu do ustawy, to rozwiązanie ma zapewnić, że rozpatrywanie środków sądowego zaskarżenia decyzji będzie realizowane sprawnie i efektywnie, z zachowaniem wszelkich gwarancji prawa do sądu[36].

Przyjęta w ustawie procedura jest procedurą administracyjną. Zgodnie z uzasadnieniem do projektu:

> W postępowaniach, o których mowa powyżej, właściwy pozostaje sąd administracyjny, co wynika z faktu, że postępowania te będą dotyczyły wyłącznie kwestii prawno-administracyjnych. Należy zauważyć, że określone rozporządzeniem 2021/784 sankcje odnoszą się do sytuacji niespełnienia określonych obowiązków o charakterze administracyjnym przez dostawcę usług hostingowych, nie zaś dopuszczenia się przez nich [niego] czynów karalnych na gruncie przepisów prawa karnego materialnego. Samo usuwanie treści nie jest środkiem sankcyjnym, lecz środkiem ograniczającym. W związku z tym projektodawca przewiduje, że w tym zakresie jedynie sądy administracyjne będą kompetentnymi jednostkami sądownictwa do rozpatrywania skarg na decyzje Szefa ABW[37].

W toku prac parlamentarnych nad ustawą było rozpatrywane jeszcze jedno rozwiązanie, które miało usprawnić etap prowadzonego postępowania sądowego. Zgodnie z nim przekazanie akt i odpowiedzi na skargę do sądu administracyjnego następowałaby w terminie 15 dni od dnia otrzymania skargi, skarga zaś byłaby rozpatrywana przez Wojewódzki Sąd Administracyjny (WSA) w terminie 30 dni od dnia otrzymania akt i odpowiedzi na skargę[38]. To rozwiązanie było wzorowane na art. 21 *Ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej*. Strona rządowa, czyli projektodawca, negatywnie odniosła się do propozycji. Wskazała, że nie zagwarantuje ona rzeczywistego przyspieszenia rozpatrywania

[36] *Rządowy projekt ustawy o zmianie ustawy*... – uzasadnienie..., s. 11.

[37] Tamże.

[38] *Sprawozdanie Komisji Administracji i Spraw Wewnętrznych oraz Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii o rządowym projekcie ustawy o zmianie ustawy o działaniach antyterrorystycznych i ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (druk nr 661)*, druk nr 706, https://orka.sejm.gov.pl/Druki10ka.nsf/0/C75A45601BC82E4EC1258BB3003DFB3A/%24File/706.pdf [dostęp: 21 XII 2024].

ewentualnych skarg na etapie sądowym, ponieważ zawarte w niej terminy w odniesieniu do sądu mają charakter instrukcyjny.

Strona rządowa zaproponowała inne rozwiązanie – rozważenie przez Prezydenta RP zastosowania art. 13 § 3 ustawy – Prawo o postępowaniu przed sądami administracyjnymi przez wydanie rozporządzenia, na którego podstawie nie tylko WSA w Warszawie, lecz także inne wojewódzkie sądy administracyjne, np. właściwe według miejsca zamieszkania lub siedziby skarżącego albo miejsca pobytu lub siedziby jego przedstawiciela prawnego, mogłyby rozpoznawać sprawy z zakresu skarg na decyzje wydane przez Szefa ABW. Alternatywnym rozwiązaniem mogłoby być również wskazanie na stałe właściwości WSA innego niż ten w Warszawie.

> Art. 26e. Dostawca usług hostingowych, w stosunku do którego został wydany nakaz usunięcia, w terminie do dnia 1 marca każdego roku przekazuje Szefowi ABW dane, o których mowa w art. 21 ust. 1 lit. b i d rozporządzenia 2021/784, za rok poprzedni.

Przywołany art. 21 ust. 1 rozporządzenia 2021/784 zobowiązuje państwa członkowskie do gromadzenia i przekazywania do KE, do 31 marca każdego roku, informacji, które uzyskały od swoich właściwych organów i dostawców usług hostingowych podlegających ich jurysdykcji za poprzedni rok kalendarzowy. Informacje te, zgodnie z rozporządzeniem 2021/784, obejmują:

- liczbę wydanych nakazów usunięcia oraz liczbę przypadków usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do nich, a także szybkość, z jaką dokonano usunięcia lub uniemożliwiono dostęp;
- środki szczególne podjęte na podstawie rozporządzenia, w tym liczbę przypadków usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do nich, a także szybkość, z jaką dokonano usunięcia lub uniemożliwiono dostępu;
- liczbę wniosków o dostęp, z którymi wystąpiły właściwe organy, w odniesieniu do treści zachowywanych przez dostawcę usług hostingowych na podstawie art. 6 rozporządzenia (dostawcy usług hostingowych zachowują treści o charakterze terrorystycznym, które zostały usunięte lub do których dostęp został uniemożliwiony w wyniku nakazu usunięcia lub środków szczególnych, które zostały usunięte w wyniku usunięcia takich treści o charakterze

terrorystycznym, które to treści i dane są konieczne do: kontroli w postępowaniach administracyjnych lub sądowych lub rozpatrywania skarg na w przypadku decyzji o usunięciu treści o charakterze terrorystycznym i związanych z nimi danych lub o uniemożliwieniu do nich dostępu; lub zapobiegania przestępstwom terrorystycznym, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania);
– liczbę wszczętych procedur rozpatrywania skarg oraz działań podjętych przez dostawców usług hostingowych;
– liczbę wszczętych kontroli w postępowaniach administracyjnych lub sądowych oraz decyzji podjętych przez właściwy organ zgodnie z prawem krajowym.

Art. 26f. 1. Dostawca usług hostingowych, który nie dopełnia obowiązku, o którym mowa w art. 3 ust. 3 lub 6, art. 4 ust. 2 lub 7, art. 5 ust. 1–3, 5 lub 6, art. 6, art. 7, art. 10, art. 11, art. 14 ust. 5, art. 15 ust. 1 lub art. 17 rozporządzenia 2021/784, podlega karze pieniężnej.
2. Karę pieniężną, o której mowa w ust. 1, nakłada Szef ABW, w drodze decyzji administracyjnej, biorąc pod uwagę warunki i okoliczności określone w art. 18 rozporządzenia 2021/784 w wysokości do 4% całkowitych obrotów uzyskanych przez dostawcę usług hostingowych w poprzednim roku obrotowym.
3. Decyzja, o której mowa w ust. 2, jest ostateczna.
4. Środki z kar pieniężnych, o których mowa w ust. 1, stanowią dochód budżetu państwa.

Art. 26f zawiera normy penalizujące w postaci administracyjnych kar pieniężnych za konkretne zachowania stanowiące naruszenie obowiązków określonych w rozporządzeniu 2021/784. Zgodnie z art. 18 rozporządzenia państwa członkowskie ustanawiają przepisy dotyczące kar mających zastosowanie w przypadku naruszeń tego aktu prawnego przez dostawców usług hostingowych i podejmują wszelkie środki niezbędne do zapewnienia ich wykonania. Wyliczenie artykułów rozporządzenia 2021/784, w których mowa o obowiązkach dostawcy usług hostingowych, zostało powielone za unijnym prawodawcą w opisywanym art. 26f ustawy. Sankcja może być zastosowana względem dostawcy usług hostingowych w przypadkach, gdy:
– dostawca usług hostingowych nie usunął treści o charakterze terrorystycznym lub nie uniemożliwił dostępu do tych treści we wszystkich państwach członkowskich jak najszybciej, a w każdym razie

zrobił to później niż w ciągu jednej godziny od otrzymania nakazu usunięcia (art. 3 ust. 3);
- dostawca usług hostingowych nie poinformował właściwego organu, przy użyciu wzoru określonego w załączniku II rozporządzenia, o usunięciu treści o charakterze terrorystycznym lub o uniemożliwieniu dostępu do treści terrorystycznych we wszystkich państwach członkowskich, ze wskazaniem w szczególności czasu tego usunięcia lub uniemożliwienia dostępu (art. 3 ust. 6);
- dostawca usług hostingowych, który otrzymał nakaz usunięcia treści o charakterze terrorystycznym w procedurze transgranicznych nakazów usunięcia, nie podjął środków przewidzianych dla nakazów usunięcia lub nie podjął środków niezbędnych, by móc przywrócić usunięte treści lub dostęp do nich (art. 4 ust. 2);
- gdy właściwy organ państwa członkowskiego, w którym dostawca usług hostingowych ma główną jednostkę organizacyjną lub w którym jego przedstawiciel prawny ma miejsce pobytu lub siedzibę, wydał decyzję o stwierdzeniu naruszenia przepisów rozporządzenia przez organ innego państwa, który wydał nakaz usunięcia, dostawca usług hostingowych natychmiast nie przywrócił danych treści lub dostępu do nich (art. 4 ust. 7);
- dostawca usług hostingowych narażony na treści o charakterze terrorystycznym nie zamieścił w swoich warunkach umownych oraz nie stosuje postanowień mających przeciwdziałać wykorzystywaniu jego usług do publicznego rozpowszechniania treści o charakterze terrorystycznym. Nie działa on przy tym z zachowaniem należytej staranności, w sposób proporcjonalny i niedyskryminacyjny, z uwzględnieniem odpowiednio we wszystkich okolicznościach praw podstawowych użytkowników, zwłaszcza wolności wypowiedzi i informacji w otwartym i demokratycznym społeczeństwie, tak aby uniknąć usuwania materiałów, które nie stanowią treści o charakterze terrorystycznym (art. 5 ust. 1);
- dostawca usług hostingowych narażony na treści o charakterze terrorystycznym nie podejmuje środków szczególnych w celu ochrony swoich usług przed publicznym rozpowszechnianiem treści o charakterze terrorystycznym (art. 5 ust. 2);
- środki szczególne stosowane przez dostawcę usług hostingowych narażonego na treści o charakterze terrorystycznym nie spełniają wszystkich następujących wymogów:

  - skutecznie zmniejszają poziom narażenia usług dostawcy usług hostingowych na treści o charakterze terrorystycznym;
  - są ukierunkowane i proporcjonalne, przy uwzględnieniu poziomu narażenia usług na treści o charakterze terrorystycznym;
  - są stosowane w sposób, który uwzględnia pełne poszanowanie praw i uzasadnionego interesu użytkowników, zwłaszcza podstawowych praw użytkowników dotyczących wolności wypowiedzi i informacji, poszanowania życia prywatnego i ochrony danych osobowych;
  - są stosowane w staranny i niedyskryminacyjny sposób;
- dostawca usług hostingowych narażony na treści o charakterze terrorystycznym nie powiadamia właściwego organu o środkach szczególnych, które podjął i które zamierza podjąć w celu wykonania ciążących na nim obowiązków (art. 5 ust. 5);
- dostawca usług hostingowych narażony na treści o charakterze terrorystycznym nie wykonał decyzji organu właściwego zobowiązującego go do podjęcia dodatkowych niezbędnych środków zabezpieczających (art. 5 ust. 6);
- dostawca usług hostingowych nie zachował treści o charakterze terrorystycznym, które zostały usunięte lub do których dostęp został uniemożliwiony w wyniku nakazu usunięcia lub środków szczególnych na podstawie art. 3 lub 5 rozporządzenia, jak również związanych z nimi danych, które to treści i dane są konieczne do kontroli w postępowaniach administracyjnych lub sądowych lub rozpatrywania skarg lub też do zapobiegania przestępstwom terrorystycznym, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania (art. 6 rozporządzenia);
- dostawca usług hostingowych nie określił w swoich warunkach umownych w sposób jasny swoich zasad dotyczących przeciwdziałania rozpowszechnianiu treści o charakterze terrorystycznym (art. 7);
- dostawca usług hostingowych, który w danym roku kalendarzowym podjął działania mające na celu przeciwdziałanie rozpowszechnianiu treści o charakterze terrorystycznym lub został zobowiązany do podjęcia działań na podstawie niniejszego rozporządzenia, nie udostępnia publicznie ogólnie dostępnego sprawozdania z przejrzystości na temat tych działań za dany rok. Nie publikuje on sprawozdania przed 1 marca kolejnego roku lub sprawozdanie nie zawiera elementów przewidzianych rozporządzeniem (art. 7);

- dostawca usług hostingowych nie ustanowił skutecznego i dostępnego mechanizmu umożliwiającego dostawcom treści, w przypadku gdy ich treści zostały usunięte lub dostęp do nich został uniemożliwiony w wyniku środków szczególnych, złożenia skargi dotyczącej danego usunięcia lub uniemożliwienia dostępu z żądaniem przywrócenia treści lub dostępu do nich (art. 10);
- dostawca usług hostingowych nie rozpatruje skarg i nie przywraca w terminie treści lub dostępu do nich, w przypadku gdy ich usunięcie lub uniemożliwienie dostępu do nich było nieuzasadnione (art. 10);
- dostawca usług hostingowych, który usunął treści o charakterze terrorystycznym lub uniemożliwił dostęp do nich, nie udostępnił dostawcy treści informacji na temat takiego usunięcia lub uniemożliwienia dostępu lub też, mimo wniosku dostawcy treści, nie poinformował go o powodach usunięcia lub uniemożliwienia dostępu oraz o jego prawach do zaskarżenia nakazu usunięcia albo nie udostępniał dostawcy treści kopię nakazu usunięcia (art. 11);
- dostawca usług hostingowych, który dowiedział się o treściach o charakterze terrorystycznym wiążących się z bezpośrednim zagrożeniem życia, nie poinformował natychmiast organu właściwego w zakresie prowadzenia postępowań przygotowawczych i ścigania przestępstw w zainteresowanym państwie członkowskim lub zainteresowanych państwach członkowskich (art. 14 ust. 5);
- dostawca usług hostingowych nie wskazał lub nie ustanowił punktu kontaktowego do celów odbioru nakazów usunięcia za pomocą środków elektronicznych lub nie zapewnił, aby informacje o punkcie kontaktowym były publicznie dostępne (art. 15 ust. 1);
- dostawca usług hostingowych, który nie ma głównej jednostki organizacyjnej w UE, nie wyznaczył osoby fizycznej lub prawnej jako swojego przedstawiciela prawnego w UE do celów odbioru, stosowania się do i wykonywania nakazów usunięcia i decyzji wydanych przez właściwe organy (art. 17).

Wskazane działania lub zaniechania mimo swej dużej liczby nie wyczerpują całości zachowań, które mogą być sankcjonowane na podstawie przepisów katalogowych określonych w art. 26f ust. 1 ustawy. Należy jednak podkreślić ich wielowymiarowość i to, że nie odnoszą się one wyłącznie do kwestii stosowania samych nakazów usunięcia lub środków

szczególnych, lecz dotyczą m.in. realizacji obowiązków związanych z zapewnieniem przejrzystości działań ze strony tych dostawców.

Procedurę nakładania kary i jej formę (przez Szefa ABW w drodze decyzji administracyjnej), a także dyrektywy wymiaru kary i jej maksymalną wysokość ustawodawca określił w art. 26f ust. 2. Zgodnie z przywołanym w tym przepisie art. 18 rozporządzenia 2021/784 Szef ABW przy podejmowaniu decyzji w sprawie nałożenia kary i ustalaniu jej rodzaju i wysokości jest zobowiązany do uwzględnienia wszystkich istotnych okoliczności sprawy, w tym:

- charakteru, wagi i czasu trwania naruszenia;
- umyślności lub charakteru naruszenia wynikającego z zaniedbania;
- wcześniejszego naruszenia popełnionego przez dostawcę usług hostingowych;
- kondycji finansowej dostawcy usług hostingowych;
- poziomu współpracy dostawcy usług hostingowych z właściwymi organami;
- charakteru i rozmiaru dostawców usług hostingowych, zwłaszcza tego, czy jest on mikro-, małym lub średnim przedsiębiorstwem;
- stopnia winy dostawcy usług hostingowych, z uwzględnieniem podjętych przez niego środków technicznych i organizacyjnych w celu spełnienia wymogów rozporządzenia.

Przyjęta w przepisie maksymalna kara administracyjna, która może być orzeczona na podstawie przepisów ustawy, również wynika wprost z rozporządzenia 2021/784. W jego art. 18 ust. 3 jest wskazane, że państwa członkowskie zapewniają, że systematyczne lub uporczywe niedopełnianie obowiązków będzie podlegało karom pieniężnym w wysokości do 4% całkowitych obrotów dostawcy usług hostingowych w poprzednim roku obrotowym.

Należy ponadto zauważyć, że ustawa, w zakresie prowadzonych postępowań, nie wyłącza ani nie ogranicza stosowania k.p.a. W efekcie Szef ABW będzie miał możliwość skorzystania z narzędzi łagodzących karę, np. z instytucji jej odroczenia albo rozłożenia na raty. Zasada proporcjonalności jest zachowana również dzięki możliwości zastosowania przez organ przepisów pozwalających na odstąpienie od kary pieniężnej na rzecz lżejszej formy ukarania, np. pouczenia, przy założeniu zaistnienia ku temu określonych prawem przesłanek (art. 189f k.p.a.)[39].

[39] *Rządowy projekt ustawy o zmianie ustawy...* – uzasadnienie..., s. 13.

Decyzje Szefa ABW mają charakter ostateczny, dlatego również w tym przypadku zostały wyłączone pozasądowe mechanizmy zaskarżenia.

Środki z kar pieniężnych stanowią dochód budżetu państwa. W tym kontekście warto przywołać ocenę skutków regulacji, załączoną do projektu ustawy, zgodnie z którą (...) *projektowana ustawa przewiduje nakładanie przez Szefa ABW na dostawców usług hostingowych administracyjnych kar pieniężnych za naruszenia wynikające z rozporządzenia, które będą stanowiły dochód budżetu państwa, należy z tego tytułu prognozować przychód do budżetu państwa. Niemniej trzeba przyjąć, że będzie on znikomy, a ponadto niemożliwy na tym etapie do zwymiarowania*[40]. Zapis ten wskazuje, że w opinii projektodawcy rzeczywiste zastosowanie rozporządzenia 2021/784 i samej ustawy będzie incydentalne, a poziom zagrożenia w Polsce rozpowszechnianiem treści o charakterze terrorystycznym jest niski. Ta opinia wynika z częstotliwości stosowania obecnie funkcjonujących w polskim porządku prawnym rozwiązań z art. 32c ustawy o ABW oraz AW.

> Art. 26g. 1. W związku z toczącym się postępowaniem w sprawie nałożenia kary pieniężnej dostawca usług hostingowych jest obowiązany do dostarczenia Szefowi ABW, na każde jego żądanie, w terminie 30 dni od dnia otrzymania żądania danych niezbędnych do określenia podstawy wymiaru kary pieniężnej.
> 2. W przypadku niedostarczenia przez dostawcę usług hostingowych danych lub gdy dostarczone przez tego dostawcę dane uniemożliwiają ustalenie podstawy wymiaru kary pieniężnej Szef ABW ustala podstawę wymiaru tej kary w sposób szacunkowy, uwzględniając ogólnie dostępne dane finansowe dotyczące tego dostawcy, w tym kryteria, o których mowa w art. 7 ust. 1 pkt 1–3 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców.

Art. 26g ustawy obliguje dostawcę usług hostingowych do współpracy z Szefem ABW w związku z toczącym się postępowaniem w sprawie nałożenia kary pieniężnej. Niewykonanie obowiązku zawartego w ust. 1 lub dostarczenie danych, które uniemożliwiają ustalenie podstawy wymiaru kary, skutkuje tym, że Szef ABW ustala podstawę wymiaru tej kary w sposób szacunkowy, z uwzględnieniem ogólnie dostępnych danych finansowych dotyczących tego dostawcy, w tym kryteria, o których mowa

[40] *Rządowy projekt ustawy o zmianie ustawy...* – ocena skutków regulacji, https://orka.sejm.gov.pl/Druki10ka.nsf/0/5083CA680B1B465AC1258B97003B446F/%24File/661.pdf, s. 8 [dostęp: 14 XII 2024].

w ustawie – Prawo przedsiębiorców. Wspomniane kryteria to wielkość przedsiębiorstwa – czy jest on mikroprzedsiębiorcą, małym przedsiębiorcą czy średnim przedsiębiorcą.

Przepis ten jest analogiczny względem funkcjonującego w porządku prawnym art. 101a *Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych*.

> Art. 26h. Karę pieniężną uiszcza się w terminie 14 dni od dnia, w którym decyzja Szefa ABW, o której mowa w art. 26f ust. 2, stała się prawomocna.

Termin na uiszczenie kary pieniężnej to 14 dni liczone od dnia, w którym decyzja administracyjna Szefa ABW o nałożeniu kary pieniężnej stała się prawomocna, i jak wskazano, jest ona ostateczna.

Podsumowanie

Ustawą o zmianie ustawy o działaniach antyterrorystycznych i ustawy o ABW i AW przez nowelizację ustawy o działaniach antyterrorystycznych, w opinii autora, zostało zapewnione właściwe stosowanie rozporządzenia 2021/784. Wyznaczenie Szefa ABW jako polskiego właściwego organu w rozumieniu wyżej wskazanego rozporządzenia, a także ustanowienie punktu kontaktowego w kierowanej przez niego formacji jest optymalne z perspektywy usprawnienia funkcjonowania polskiego systemu antyterrorystycznego oraz jego podziału kompetencyjnego. Jako w pełni uzasadnione należy uznać również oparcie polskich przepisów proceduralnych, subsydiarnych względem przepisów rozporządzenia 2021/784, na rozwiązaniach przyjętych w k.p.a., przy jednoczesnym uznaniu, że w niektórych przypadkach mogą mieć zastosowanie tylko jego wybrane przepisy.

Mimo to w opinii autora do ustawy o działaniach antyterrorystycznych powinny zostać przeniesione wszystkie przepisy mające znaczenie z perspektywy przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym, a zatem art. 32c ustawy o ABW oraz AW. Zabieg ten miałby jednak wymiar jedynie legislacyjny, ponieważ te regulacje zawierają normy kolizyjne gwarantujące spójność ich stosowania.

Zapewnienie stosowania rozporządzenia 2021/784 przez nowelizację ustawy o działaniach AT, w kontekście legislacyjnym, powinno zostać uzupełnione o modyfikację art. 1 tej ustawy, zgodnie z którym określa ona

zasady prowadzenia działań antyterrorystycznych (zatem działań administracji publicznej) oraz współpracy między organami właściwymi w zakresie prowadzenia tych działań. Rozwiązania przyjęte w nowym rozdziale 5a tej ustawy służące przeciwdziałaniu rozpowszechnianiu w internecie treści o charakterze terrorystycznym, zwłaszcza w kontekście będących ich skutkiem praw i obowiązków dostawców usług hostingowych i dostawców treści, powinny znaleźć odzwierciedlenie w przepisie określającym zakres regulacji.

Z perspektywy praktycznej zapewnienie stosowania rozporządzenia 2021/784 można ocenić jako wzmocnienie polskiego systemu antyterrorystycznego. W tym kontekście warto odnotować, że od 3 lipca 2023 r. funkcjonuje opracowana przez Europol platforma PERCI. Jest to rozwiązanie oparte na chmurze, zapewniające bezpieczeństwo i ochronę zamieszczanych w niej danych. Platforma ta ułatwia przekazywanie nakazów usunięcia, sprawozdawczość państw członkowskich i koordynację, a także usuwanie konfliktów, w sytuacji gdy toczy się postępowanie przygotowawcze w sprawie treści, wobec których ma zostać wysłany nakaz usunięcia[41].

W powyższym kontekście należy zauważyć, że choć zgodnie z rozporządzeniem 2021/784 państwa powinny zapewnić jego stosowanie od 7 czerwca 2022 r., to w Polsce nastąpiło to dopiero 3 grudnia 2024 r. Do tego czasu Polska była pozbawiona zarówno formalnych podstaw stosowania rozporządzenia, jak i możliwości korzystania z narzędzi jego wsparcia technicznego. Kwestia ta pozostaje tym istotniejsza, że w tym okresie na terytorium Polski obowiązywały stopnie alarmowe związane z podwyższonym zagrożeniem o charakterze terrorystycznym[42].

Warto też przywołać na koniec motyw 2 rozporządzenia 2021/784, który wskazuje, że:

> środki regulacyjne mające przeciwdziałać rozpowszechnianiu w internecie treści o charakterze terrorystycznym powinny zostać uzupełnione strategiami państw członkowskich dotyczącymi walki z terroryzmem, obejmującymi między innymi wzmacnianie umiejętności korzystania z mediów i umiejętności krytycznego myślenia,

[41] *Rządowy projekt ustawy o zmianie ustawy*... – uzasadnienie..., s. 5.

[42] *Dotychczas wprowadzane stopnie alarmowe i stopnie alarmowe CRP na terytorium RP*, Ministerstwo Spraw Wewnętrznych i Administracji, https://www.gov.pl/web/mswia/dotychczas-wprowadzane-stopnie-alarmowe-i-stopnie-alarmowe-crp-na-terytorium-rp [dostęp: 23 XII 2024].

> przedstawianie alternatywnych narracji lub kontrnarracji i inne inicjatywy służące zmniejszeniu wpływu umieszczanych w internecie treści o charakterze terrorystycznym i podatności na te treści, a także inwestycje w pracę społeczną, inicjatywy na rzecz deradykalizacji i kontakty z zainteresowanymi społecznościami, w celu wypracowania trwałego zapobiegania radykalizacji w społeczeństwie[43].

Tę wytyczną, choć niemającą charakteru obligatoryjnego, należy mieć na uwadze w kontekście przyszłej oceny stosowania przyjętych przepisów. Jeśli okaże się, że nakazy lub środki szczególne znajdą częste zastosowanie na poziomie krajowym, stanie się zasadne podjęcie dodatkowych działań o charakterze profilaktycznym.

Bibliografia

Burczaniuk P., *Zadania i uprawnienia organów ścigania karnego w zakresie zwalczania terroryzmu w Polsce – perspektywa prawna*, „Terroryzm – studia, analizy, prewencja" 2022, nr 2, s. 9–30. https://doi.org/10.4467/27204383TER.22.017.16337.

Cichomski M., *Między konfliktem zbrojnym a terroryzmem państwowym – szczególne indywidualne środki ograniczające przyjęte w Polsce w kontekście wojny w Ukrainie i sytuacji w Białorusi. Perspektywa prawna*, „Terroryzm – studia, analizy, prewencja" 2024, nr 5, s. 91–131. https://doi.org/10.4467/27204383TER.24.003.19391.

Cichomski M., Idzikowska-Ślęzak I., *Stopnie alarmowe – praktyczny i prawny wymiar ich stosowania*, „Terroryzm – studia, analizy, prewencja" 2022, nr 2, s. 31–70. https://doi.org/10.4467/27204383TER.22.018.16338.

Cichomski M., Marchliński P., *Krajowe rozwiązania w zakresie bezpieczeństwa obrotu prekursorami materiałów wybuchowych – po zamachu terrorystycznym w Norwegii 22 lipca 2011 r. w kontekście nowych zadań Policji*, w: *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, W. Zubrzycki, K. Jałoszyński, A. Babiński (red.), Szczytno 2016, s. 591–600.

Gabriel-Węglowski M., *Działania antyterrorystyczne. Komentarz*, Warszawa 2018.

[43] Motyw 2 rozporządzenia 2021/784.

Źródła internetowe

Dotychczas wprowadzane stopnie alarmowe i stopnie alarmowe CRP na terytorium RP, Ministerstwo Spraw Wewnętrznych i Administracji, https://www.gov.pl/web/mswia/dotychczas-wprowadzane-stopnie-alarmowe-i-stopnie-alarmowe-crp-na-terytorium-rp [dostęp: 23 XII 2024].

List of national competent authority (authorities) and contact points, European Commission, 27 I 2025 r., https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/prevention-radicalisation/terrorist-content-online/list-national-competent-authority-authorities-and-contact-points_en?prefLang=pl [dostęp: 15 II 2025].

Punkt kontaktowy TCO, BIP ABW, https://bip.abw.gov.pl/bip/punkt-kontatowy-tco/525,Punkt-kontaktowy-TCO.html [dostęp: 13 XII 2024].

Akty prawne

Międzynarodowa Konwencja o poszukiwaniu i ratownictwie morskim, sporządzona w Hamburgu dnia 27 kwietnia 1979 r. (DzU z 1988 r. nr 27 poz. 184 i 185).

Traktat o funkcjonowaniu Unii Europejskiej (wersja skonsolidowana) – (Dz. Urz. UE C 202/47 z 7 VI 2016 r.).

Traktat o Unii Europejskiej (wersja skonsolidowana) – (Dz. Urz. UE C 202/13 z 7 VI 2016 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym (Dz. Urz. UE L 172/79 z 17 V 2021 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 98/2013 z dnia 15 stycznia 2013 r. w sprawie wprowadzania do obrotu i używania prekursorów materiałów wybuchowych (Dz. Urz. UE L 39/1 z 9 II 2013 r.).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępująca decyzję ramową Rady 2002/475/WSiSW oraz zmieniająca decyzję Rady 2005/671/WSiSW (Dz. Urz. UE L 88/6 z 31 III 2017 r.).

Dyrektywa (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz. Urz. UE L 241/1 z 17 IX 2015 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 VIII 2013 r.).

Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) – (Dz. Urz. L 178/1 z 17 VII 2000 r.).

Konstytucja Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r. (t.j. DzU z 1997 r. nr 78 poz. 483, ze zm.).

Ustawa z dnia 18 października 2024 r. o zmianie ustawy o działaniach antyterrorystycznych i ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (DzU z 2024 r. poz. 1684).

Ustawa z dnia 26 lipca 2024 r. o zmianie niektórych ustaw w celu usprawnienia działań Sił Zbrojnych Rzeczypospolitej Polskiej, Policji oraz Straży Granicznej na wypadek zagrożenia bezpieczeństwa państwa (DzU z 2024 r. poz. 1248).

Ustawa z dnia 17 sierpnia 2023 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (DzU z 2023 r. poz. 1834).

Ustawa z dnia 7 lipca 2023 r. o zmianie ustawy – Kodeks postępowania cywilnego, ustawy – Prawo o ustroju sądów powszechnych, ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw (DzU z 2023 r. poz. 1860).

Ustawa z dnia 7 lipca 2023 r. o zmianie ustawy o ochronie żeglugi i portów morskich oraz niektórych innych ustaw (DzU z 2023 r. poz. 1489).

Ustawa z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (t.j. DzU z 2024 r. poz. 507).

Ustawa z dnia 12 marca 2022 r. o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa (DzU z 2022 r. poz. 583).

Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny (t.j. DzU z 2024 r. poz. 248, ze zm.).

Ustawa z dnia 30 marca 2021 r. o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw (t.j. DzU z 2021 r. poz. 815, ze zm.).

Ustawa z dnia 21 stycznia 2021 r. o służbie zagranicznej (t.j. DzU z 2024 r. poz. 1691, ze zm.).

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. DzU z 2019 r. poz. 1781).

Ustawa z dnia 6 marca 2018 r. – Prawo przedsiębiorców (t.j. DzU z 2024 r. poz. 236, ze zm.).

Ustawa z dnia 6 marca 2018 r. – Przepisy wprowadzające ustawę – Prawo przedsiębiorców oraz inne ustawy dotyczące działalności gospodarczej (DzU z 2018 r. poz. 650).

Ustawa z dnia 26 stycznia 2018 r. – Przepisy wprowadzające ustawę o Straży Marszałkowskiej (DzU z 2018 r. poz. 730).

Ustawa z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (DzU z 2018 r. poz. 138).

Ustawa z dnia 16 listopada 2016 r. – Przepisy wprowadzające ustawę o Krajowej Administracji Skarbowej (t.j. DzU z 2016 r. poz. 1948, ze zm.).

Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (DzU z 2024 r. poz. 92, 1248, 1684).

Ustawa z dnia 13 kwietnia 2016 r. o bezpieczeństwie obrotu prekursorami materiałów wybuchowych (t.j. DzU z 2019 r. poz. 994).

Ustawa z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (t.j. DzU z 2024 r. poz. 935, ze zm.).

Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t.j. DzU z 2024 r. poz. 812, ze zm.).

Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. DzU z 2022 r. poz. 902).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. DzU z 2024 r. poz. 17).

Ustawa z dnia 6 kwietnia 1990 r. o Policji (t.j. DzU z 2024 r. poz. 145, ze zm.).

Ustawa z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (t.j. DzU z 2024 r. poz. 572).

Rozporządzenie Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej" (t.j. DzU z 2016 r. poz. 283).

Zalecenie Komisji (UE) 2018/334 z dnia 1 marca 2018 r. w sprawie działań na rzecz skutecznego zwalczania nielegalnych treści w internecie (Dz. Urz. L 63/50 z 6 III 2018 r.).

Orzecznictwo

Wyrok Europejskiego Trybunału Praw Człowieka w sprawie Pietrzak i Bychawska-Siniarska i inni przeciwko Polsce, https://arch-bip.ms.gov.pl/pl/prawa-czlowieka/europejski-trybunal-praw-czlowieka/orzecznictwo-europejskiego-trybunalu-praw-czlowieka/listByYear,2.html?ComplainantYear=2024 [dostęp: 18 V 2025].

Inne dokumenty

Commission Staff Working Document Impact Assessment. Accompanying the document. Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, Brussels, 12 IX 2018 r., SWD(2018) 408 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2018:408:FIN [dostęp: 4 V 2023].

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetów Regionów. Zwalczanie nielegalnych treści w internecie. W kierunku większej odpowiedzialności platform internetowych, Bruksela, 28 IX 2017 r., COM (2017) 555 final.

Mechanizmy blokowania w internecie treści o charakterze terrorystycznym w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym, prezentacja Ministerstwa Spraw Wewnętrznych i Administracji, przygotowana na potrzeby Międzyresortowego Zespołu ds. Zagrożeń Terrorystycznych.

Rządowy projekt ustawy o zmianie ustawy o działaniach antyterrorystycznych i ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, druk nr 661, https://www.sejm.gov.pl/Sejm10.nsf/druk.xsp?nr=661 [dostęp: 24 XII 2024].

Sprawozdanie Komisji Administracji i Spraw Wewnętrznych oraz Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii o rządowym projekcie ustawy o zmianie ustawy o działaniach antyterrorystycznych i ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (druk nr 661), druk nr 706, https://orka.sejm.gov.pl/Druki10ka.nsf/0/C75A45601BC82E4EC1258BB3003DFB3A/%24File/706.pdf [dostęp: 21 XII 2024].

Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady z wykonania rozporządzenia (UE) 2021/784 w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym, Bruksela, 14 II 2024 r., COM(2024) 64 final.

Stanowisko Komisji Europejskiej z 9 czerwca 2021 r. (sygn. INFR(2021)2046, C(2021)3630 final).

Mariusz Cichomski

Prawnik, socjolog. Zawodowo zajmuje się zagadnieniami związanymi z terroryzmem, przestępczością zorganizowaną, nadzorem nad działalnością służb, legislacją w zakresie bezpieczeństwa oraz sprawami dotyczącymi stosowania krajowych środków ograniczających. Autor ponad 30 publikacji z zakresu bezpieczeństwa, zwłaszcza w wymiarze prawnym, i socjologii.

Terroryzm – studia, analizy, prewencja, 2025, nr 7: 93–137

https://doi.org/10.4467/27204383TER.25.027.21804

Artykuł

Wyzwania terrorystyczne w Sahelu a południowa flanka NATO

Terrorist challenges in the Sahel and NATO's southern flank

ALEKSANDER OLECH
https://orcid.org/0000-0002-3793-5913
Defence24

PAWEŁ WÓJCIK
https://orcid.org/0009-0002-8476-0746
Opportunity Institute for Foreign Affairs

Abstrakt

Celem artykułu jest analiza rosnących zagrożeń bezpieczeństwa w regionie Sahelu oraz ich wpływu na stabilność południowej flanki Sojuszu Północnoatlantyckiego (NATO). Autorzy przyjmują tezę, że nasilająca się obecność grup zbrojnych i aktywność organizacji terrorystycznych, przede wszystkim Państwa Islamskiego i Al-Kaidy, prowadzą do eskalacji przemocy, kryzysu politycznego i społecznego, co w konsekwencji zagraża bezpieczeństwu międzynarodowemu, zwłaszcza w Europie i w państwach NATO. Artykuł opiera się na analizie raportu opracowanego przez autorów, przeglądzie dostępnej literatury oraz źródeł uzupełniających, w tym relacji dziennikarzy i ekspertów specjalizujących się w regionie Sahelu. Przeprowadzono kwerendę badawczą, w której sformułowano cztery kluczowe pytania dotyczące przyczyn eskalacji konfliktów, wpływu interwencji i wycofań sił międzynarodowych, roli zewnętrznych aktorów, m.in. Rosji i Chin, oraz skuteczności działań NATO i Unii Europejskiej. W wyniku analizy wykazano, że wyzwania te wymagają kompleksowej, długofalowej strategii międzynarodowej, łączącej działania wojskowe z reformami politycznymi i wsparciem rozwoju regionu, przy

jednoczesnym uwzględnieniu zagrożeń nie tylko na południowej, lecz także na wschodniej flance NATO.

Słowa kluczowe

Sahel, terroryzm, NATO, Afryka, Grupa Wagnera, ISIS, Al-Kaida, migracja

Abstract

The aim of the article is to analyse the growing security threats in the Sahel region and their impact on the stability of the North Atlantic Alliance's (NATO) southern flank. The authors adopt the thesis that the increasing presence of armed groups and the activity of terrorist organisations, primarily the Islamic State and Al-Qaeda, are leading to escalation of violence, political and social crisis, which consequently threatens international security, particularly in Europe and NATO countries. The article is based on the author's analysis of the report, a review of the available literature and complementary sources, including reports from journalists and experts specialising in the Sahel region. A research query was conducted, which formulated four key questions concerning the causes of conflict escalation, the impact of interventions and withdrawals of international forces, the role of external actors (Russia and China among others) and the effectiveness of NATO and European Union actions. The analysis showed that these challenges require a comprehensive, long-term international strategy, combining military actions with political reforms and the region development support, while at the same time taking into account threats not only in the southern, but also in the eastern NATO's flank.

Keywords

Sahel, terrorism, NATO, Africa, Wagner Group, ISIS, Al-Qaeda, migration

Wprowadzenie

Sahel jest regionem o znaczeniu strategicznym i obszarem rywalizacji międzynarodowej[1]. Ze względu na intensyfikację dżihadystycznych powstań[2], niestabilność polityczną nasilaną zamachami stanu[3], nielegalną migrację[4], jak również rosnącą degradację środowiska[5] potrzeba kompleksowego międzynarodowego zaangażowania w tym regionie nigdy nie była tak pilna. Źródłem kryzysu są m.in. niezdolne do rządzenia i utrzymania pokoju oraz bezpieczeństwa junty wojskowe, których władza znacznie utrudnia rozwój państw. Trudną sytuację potwierdza obecność w Sahelu sił pokojowych Organizacji Narodów Zjednoczonych (ONZ), zagranicznych wojsk, prywatnych firm wojskowych (ang. *private military company*, PMC) i najemników. Wydaje się, że wiodące organizacje, przede wszystkim Unia Europejska[6] i Sojusz Północnoatlantycki (NATO)[7], powinny przewartościować swoje strategie w celu stabilizacji regionu i zapobieżenia jego dalszemu rozpadowi.

Kraje Sahelu, w których powstanie jest wpisana złożona historia kolonializmu, zmagają się z długofalowymi skutkami braku rozwoju, fragmentacji społecznej i politycznego wykluczenia. Wyzwania, jakimi są rozwój regionu i jego stabilność, łączą się tam z zagrożeniami, takimi jak terroryzm,

---

1 S. As-Sazid, *Emerging Security Challenges in the Sahel and the Need for an Adaptative Approach towards Peacebuilding*, „International Day of United Nations Peacekeepers Journal" 2023, t. 9, nr 9, s. 17–34.

2 D. Lounnas, *Le djihadisme au Sahel après la chute de Daech*, „Politique étrangère" 2019, nr 2, s. 105–114.

3 *Military juntas in Africa's 'coup belt' fail to contain extremist violence*, Financial Times, 24 XI 2024 r., https://www.ft.com/content/d0af5533-ecdd-4be0-bbb8-e5b3e4bb11b4 [dostęp: 30 XII 2024].

4 A. Fakhry, *More than borders: effects of EU interventions on migration in the Sahel*, Institute for Security Studies, 16 VIII 2023 r., https://issafrica.org/research/west-africa-report/more-than-borders-effects-of-eu-interventions-on-migration-in-the-sahel [dostęp: 30 XII 2024].

5 *Ecological Threat Report 2024. Analysing ecological threats, resilience & peace*, The Institute for Economics & Peace, https://www.economicsandpeace.org/wp-content/uploads/2024/10/ETR-2024-web.pdf [dostęp: 15 XII 2024].

6 R. Marangio, *Sahel reset: time to reshape the EU's engagement*, European Union Institute for Security Studies, 5 II 2024 r., https://www.iss.europa.eu/publications/briefs/sahel-reset-time-reshape-eus-engagement [dostęp: 15 XII 2024].

7 *Independent expert group supporting NATO's comprehensive and deep reflection process on the southern neighbourhood. Final Report. May 2024*, NATO, https://nato.int/nato_static_fl2014/assets/pdf/2024/5/pdf/240507-NATO-South-Report.pdf [dostęp: 16 XII 2024].

ekstremizm, napięcia etniczne i systemowa korupcja. Ten stan rzeczy ma negatywny wpływ zarówno na krajowe, jak i międzynarodowe wysiłki zmierzające do poprawy sytuacji w Sahelu. Niestabilność regionu jest potęgowana przez zmieniającą się dynamikę zewnętrznych wpływów. Federacja Rosyjska[8] i Chińska Republika Ludowa[9] coraz częściej stawiają się w roli partnerów dla państw Sahelu. Oferują pomoc finansową i wojskową, przy czym nie oczekują zmian w kwestii praw człowieka czy wprowadzania zasad demokracji, co zwykle jest jednym z warunków stawianych przez kraje Zachodu. To pozwala reżimom Sahelu zachować pozory autonomii bez poświęcania własnej niezależności politycznej. Państwa Afryki decydują się na krótkoterminowe korzyści kosztem długotrwałej stabilności[10]. Geopolitykę Sahelu kształtują więc zarówno lokalne problemy, jak i interesy globalnych mocarstw. Zagraniczna rywalizacja o wpływy polityczne, gospodarcze i militarne osłabia struktury państwowe, pogłębia podziały społeczne i zagraża bezpieczeństwu nie tylko w Afryce, lecz także poza kontynentem[11]. Należy podkreślić, że w Mali, Burkinie Faso i Nigrze sytuacja jest dynamiczna pod względem poziomu bezpieczeństwa oraz aktywności terrorystycznej. Zjawiska, które zachodzą na północy kontynentu afrykańskiego, bezpośrednio zagrażają UE i naruszają bezpieczeństwo NATO nie tylko na jego południowej flance, lecz także na wschodniej[12]. Nadszedł czas na skoordynowaną, zorientowaną na działanie strategię, która wyjdzie naprzeciw nie tylko obecnym od lat, lecz także nowym problemom Sahelu.

W artykule omówiono najważniejsze czynniki, które podsycają kryzysy w Sahelu. Autorzy przedstawiają argumenty na rzecz opracowania nowej strategii międzynarodowej, w której państwa członkowskie NATO

---

8 *Moscow's winning return to Africa*, Le Monde, 21 VIII 2024 r., https://www.lemonde.fr/en/international/article/2024/08/21/moscow-s-winning-return-to-africa_6719241_4.html [dostęp: 7 XII 2024].

9 S. Bhattacharya, *China's Great Game in the Sahel*, Vivekananda International Foundation, 12 X 2022 r., https://www.vifindia.org/article/2022/china-s-great-game-in-the-sahel [dostęp: 7 XII 2024].

10 F. Mintoiba, *Footsteps of change: Rising influence of China and Russia in Africa*, Daily Sabah, 3 X 2024 r., https://www.dailysabah.com/opinion/op-ed/footsteps-of-change-rising-influence-of-china-and-russia-in-africa [dostęp: 7 XII 2024].

11 A. Olech, B. Wójtowicz, *Rywalizacja o surowce w Sahelu – region konfliktu mocarstw*, Trimarium.pl, 18 XI 2022 r., https://trimarium.pl/projekt/rywalizacja-o-surowce-w-sahelu-region-konfliktu-mocarstw/ [dostęp: 7 XII 2024].

12 A. Olech, P. Wójcik, *Wojna o Sahel [Raport]*, Defence24, 17 XI 2024 r., https://defence24.pl/geopolityka/wojna-o-sahel-raport [dostęp: 15 XII 2024].

i UE odegrałyby kluczową rolę. Strategia ta powinna opierać się na trwałym i skoordynowanym zaangażowaniu, obejmującym wsparcie dla lokalnych struktur bezpieczeństwa, inwestycje w rozwój społeczno-gospodarczy regionu, działania na rzecz stabilizacji instytucji państwowych oraz przeciwdziałanie radykalizacji i przymusowej migracji. Takie podejście powinno mieć priorytet nad doraźnymi, reaktywnymi interwencjami wojskowymi. Autorzy przyjęli tezę badawczą: znaczna obecność grup zbrojnych oraz wzrost aktywności terrorystycznej w regionie Sahelu prowadzą do eskalacji przemocy i destabilizacji politycznej, co zwiększa zagrożenie bezpieczeństwa międzynarodowego, zwłaszcza dla Europy i państw NATO, oraz potęguje niekontrolowaną migrację. W kwerendzie naukowej wyszczególniono następujące pytania badawcze:

1. Jakie czynniki nasilają wzrost liczby grup zbrojnych i eskalację konfliktów w regionie Sahelu?
2. W jaki sposób międzynarodowe interwencje wojskowe i wycofania wojsk wpłynęły na bezpieczeństwo i stabilność Sahelu?
3. W jaki sposób rosnące wpływy zewnętrznych aktorów, tj. Rosji i Chin, zmieniają dynamikę polityczną i bezpieczeństwo w regionie Sahelu?
4. Czy działania NATO i UE mogą skutecznie powstrzymać rozprzestrzenianie się terroryzmu w Sahelu i nielegalną migrację?

Artykuł został przygotowany na podstawie raportu opracowanego przez autorów[13], analizy dostępnej literatury oraz nielicznych materiałów, w tym informacji przekazanych przez dziennikarzy i specjalistów zajmujących się regionem Sahelu.

Sahel – charakterystyka regionu

Sahel to półpustynny region Afryki rozciągający się od Atlantyku na zachodzie po Morze Czerwone na wschodzie, stanowiący strefę przejściową między pustynną Saharą a żyznymi sawannami Afryki Subsaharyjskiej[14]. Obejmuje części następujących państw: Senegalu, Mauretanii, Mali, Burkiny Faso, Nigru, Czadu, Sudanu, Erytrei, Nigerii i Kamerunu. Region ten

[13] Tamże.

[14] *Sahel*, Britannica, https://www.britannica.com/place/Sahel [dostęp: 14 XII 2024]; H.O. Ibrahim, *The Sahel – a Land of Opportunity*, United Nations, 10 VI 2019 r., https://unpartnerships.un.org/news/2019/sahel-land-opportunity [dostęp: 14 XII 2024].

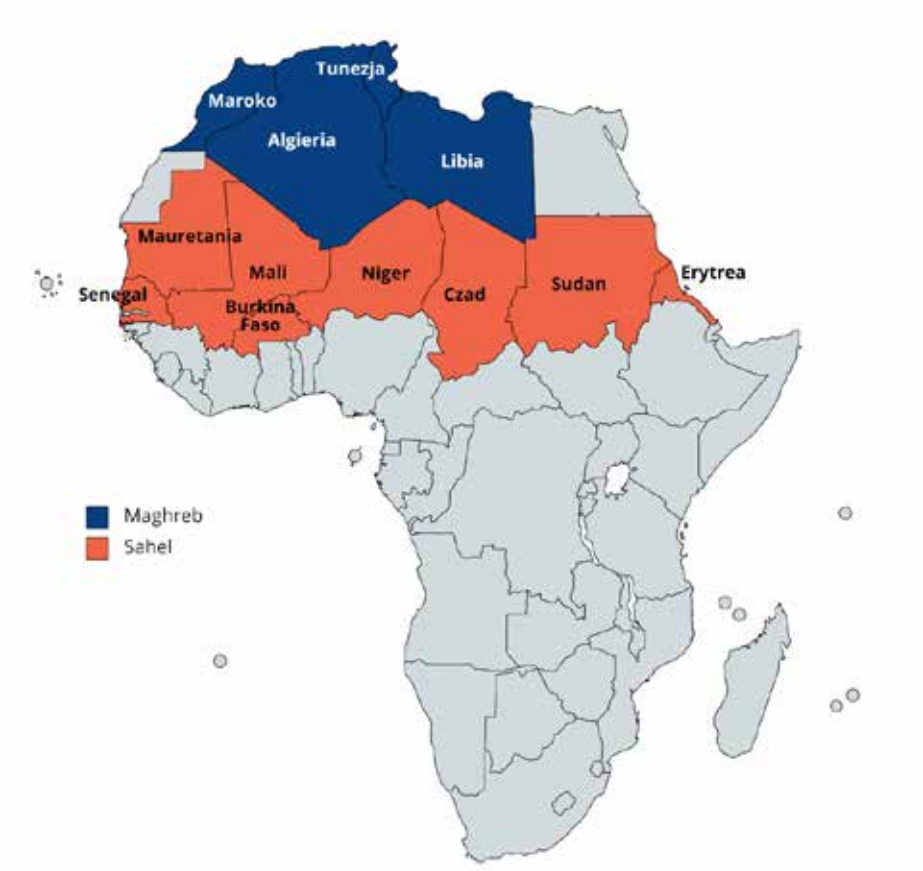
charakteryzuje się surowym klimatem – z wysokimi temperaturami oraz nieregularnymi i trudnymi do przewidzenia opadami – co znacznie utrudnia rolnictwo i utrzymanie się lokalnych społeczności, które są zależne od upraw i hodowli[15]. Niekorzystne warunki środowiskowe mają duży wpływ na codzienne życie mieszkańców Sahelu, jednak coraz większą rolę w destabilizacji regionu odgrywają czynniki polityczne, w tym słabość instytucji państwowych, konflikty zbrojne oraz rywalizacja o wpływy pomiędzy globalnymi mocarstwami.

Krajami najczęściej uznawanymi za centralną część Sahelu są Mali, Niger, Burkina Faso, Czad i Mauretania, tworzące ugrupowanie G5 Sahel. W innych ujęciach region ten obejmuje także części Senegalu, Sudanu oraz Erytrei, co pokazuje, jak złożoną kwestią są geograficzne i polityczne granice Sahelu (rysunek 1). Chociaż podstawowe rozumienie tego regionu jako półpustynnej strefy między Saharą a sawannami pozostaje niezmienne, to postrzeganie jego zasięgu może się różnić w zależności od przyjętej perspektywy – ekologicznej, klimatycznej, geopolitycznej, militarnej, religijnej czy kulturowej. Ujęcia Sahelu z perspektywy ekologicznej koncentrują się na charakterystyce środowiska naturalnego i roślinności typowej dla regionu. Te, których głównym wyznacznikiem są warunki klimatyczne, uwzględniają przede wszystkim czynniki, takie jak temperatura i rozkład opadów. W ujęciu geopolitycznym granice Sahelu są wyznaczane zgodnie z podziałami państwowymi i dynamiką zmian politycznych, podczas gdy definicje socjokulturowe opierają się na wspólnocie tradycji, języka i stylu życia lokalnych społeczności. W perspektywie militarnej uwzględnia się obecność baz wojskowych, poziom wyszkolenia sił zbrojnych i przepływ uzbrojenia, w rolniczej natomiast – specyfikę systemów uprawnych i zależność od warunków klimatycznych[16]. Różnorodność tych ujęć podkreśla, jak wielowymiarowy jest charakter regionu[17].

[15] T.A. Benjaminsen, H. Svarstad, *Climate Change, Scarcity and Conflicts in the Sahel*, w: T.A. Benjaminsen, H. Svarstad, *Political Ecology. A Critical Engagement with Global Environmental Issues*, bmw 2021, s. 183–205. https://doi.org/10.1007/978-3-030-56036-2_8.

[16] B. Tesfaye, *Climate Change and Conflict in the Sahel*, Council on Foreign Relations, November 2022, https://www.cfr.org/report/climate-change-and-conflict-sahel [dostęp: 27 V 2025].

[17] *G5 Sahel Region: Country Climate and Development Report – Annex*, World Bank Group, https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099150106302237600/p1773430dc79a10c09f600cf2ac1e0e9f3 [dostęp: 27 V 2025].



Rysunek 1. Maghreb i Sahel.

Źródło: A. Olech, *Grupa Wagnera w Afryce*, Defence24, s. 27. Raport jest dostępny na stronie: https://defence24.pl/geopolityka/rosyjscy-najemnicy-raport-z-dzialalnosci-w-afryce.

Około 64,5% populacji Sahelu stanowią osoby poniżej 25. roku życia, co czyni go jednym z najmłodszych pod względem demograficznym regionów na świecie. Taka struktura wiekowa stwarza potencjał dla rozwoju gospodarczego, pod warunkiem odpowiednich inwestycji w edukację, szkolenia zawodowe i tworzenie miejsc pracy[18]. Ponadto Sahel dysponuje znacznym potencjałem w zakresie energii odnawialnej, zwłaszcza

[18] A. Dieng, *The Sahel: Challenges and opportunities*, „International Review of the Red Cross" 2021, t. 103, nr 918, s. 775, https://international-review.icrc.org/articles/editorial-the-sahel-challenges-opportunities-adama-dieng-918 [dostęp: 15 XII 2024]. https://doi.org/10.1017/S1816383122000339.

słonecznej, co może przyczynić się do jego transformacji energetycznej. Inicjatywy takie jak Desert to Power mają na celu wykorzystanie tego potencjału przez rozwój infrastruktury energetycznej opartej na źródłach odnawialnych[19]. Realizacja tych możliwości wymaga jednak przezwyciężenia poważnych wyzwań, jakimi są niestabilność polityczna, zmiany klimatyczne i brak bezpieczeństwa żywnościowego[20].

Konflikty wewnętrzne w Sahelu zmusiły kilkadziesiąt milionów mieszkańców do opuszczenia swoich domów. Przemoc, ogromna korupcja, brak stabilizacji politycznej i ekstremalne zjawiska klimatyczne, szczególnie susze i nagłe powodzie, doprowadziły do licznych kryzysów humanitarnych. Brak odpowiedniej ilości pożywienia dotyka blisko 40 mln ludzi[21]. Sytuację pogarsza ograniczony dostęp do pomocy humanitarnej w ważnych krajach regionu – w Burkinie Faso, Mali, Nigrze i Czadzie, ponieważ sytuacja jest tam niestabilna i utrzymuje się przemoc. W 2025 r. amerykański rząd wycofał pomoc humanitarną, realizowaną głównie pod egidą United States Agency for International Development, która zapewniała niezbędne wsparcie w całej Afryce Subsaharyjskiej[22]. Organizacja Narodów Zjednoczonych alarmuje, że w sezonie letnim (między czerwcem a sierpniem) 2025 r. aż 52 mln ludzi będą zagrożone głodem, a największy kryzys żywnościowy na obszarze Afryki Zachodniej i Centralnej jest w Mali. Trzeba zgromadzić ponad 700 mln dolarów do października 2025 r., by ONZ mogła przeprowadzić niezbędne operacje humanitarne w Afryce Zachodniej i Sahelu[23].

Sahel stał się jednym z głównych ośrodków działalności grup zbrojnych, rebeliantów i organizacji dżihadystycznych[24], które bezkarnie operują

[19] *Desert to Power initiative*, African Development Bank Group, https://www.afdb.org/en/topics-and-sectors/initiatives-partnerships/desert-power-initiative [dostęp: 15 XII 2024].

[20] W. McMakin, *UN food agency says 40 million people are struggling to feed themselves in West and Central Africa*, AP, 20 XII 2024 r., https://apnews.com/article/africa-food-insecurity-hunger-304b66ef7b9b56262fe1114a4b28c7e6 [dostęp: 26 XII 2024].

[21] Tamże.

[22] R. Maclean, S. Jammeh, *Africa Received Billions in U.S. Aid. Here's What It Will Lose*, The New York Times, 8 III 2025 r., https://www.nytimes.com/2025/03/08/world/africa/africa-usaid-funds.html/ [dostęp: 20 IV 2025].

[23] *More than 50 million in West and Central Africa at risk of hunger*, United Nations, 9 V 2025 r., https://news.un.org/en/story/2025/05/1163086 [dostęp: 30 V 2025].

[24] L. Raineri, F. Strazzari, *Jihadism in Mali and the Sahel: evolving dynamics and patterns*, European Union Institute for Security Studies, 29 VI 2017 r., https://www.iss.europa.eu/publications/briefs/jihadism-mali-and-sahel-evolving-dynamics-and-patterns [dostęp: 16 XII 2024].

na rozległych, słabo nadzorowanych obszarach[25]. Brak skutecznej kontroli granicznej – zwłaszcza na długich i trudno dostępnych odcinkach między państwami – ułatwia przemieszczanie się terrorystów oraz przerzut ludzi i broni. Obecność ekstremistycznych frakcji pogłębia destabilizację polityczną, zagraża lokalnym gospodarkom i utrudnia działania humanitarne. W celu skutecznego przeciwdziałania tym zagrożeniom niezbędna jest skoordynowana reakcja zarówno regionalnych rządów, jak i organizacji międzynarodowych. Z punktu widzenia bezpieczeństwa największe znaczenie dla stabilizacji Sahelu mają Mali, Burkina Faso, Niger, Sudan i Czad – państwa szczególnie narażone na przemoc ze strony ugrupowań terrorystycznych i najemników oraz na wpływ reżimów wojskowych. Chociaż inne kraje regionu również stoją przed poważnymi wyzwaniami, to ich sytuacja wewnętrzna nie pogarsza się w tak dużym stopniu jak w wymienionych państwach[26]. Skuteczna odpowiedź na wyzwania związane z bezpieczeństwem jest warunkiem koniecznym do zapewnienia stabilnej i bardziej przewidywalnej przyszłości Sahelu[27]. Przyszłość ta nie pozostaje bez znaczenia także dla Europy, która już dziś odczuwa konsekwencje destabilizacji regionu – zarówno w wymiarze migracyjnym, jak i geopolitycznym[28].

Wielka rywalizacja w regionie

Sahel stanowi złożony obszar geopolityczny, w którym współistnieją grupy o różnych ideologiach, celach oraz strukturach – od wspólnot plemiennych, przedstawicielstw etnicznych i klanów, po organizacje religijne i lokalne instytucje. Wiele z nich jest tam obecnych od lat, jak choćby

[25] Center for Preventive Action, *Violent Extremism in the Sahel*, Council on Foreign Relations, 23 X 2024 r., https://www.cfr.org/global-conflict-tracker/conflict/violent-extremism-sahel [dostęp: 16 XII 2024].

[26] *Defining a New Approach to the Sahel's Military-led States*, International Crisis Group, 22 V 2025 r., https://www.crisisgroup.org/africa/sahel/burkina-faso-mali-niger/defining-new-approach-sahels-military-led-states [dostęp: 27 V 2025].

[27] L.V. del Portillo, *Challenges in the Sahel: Opportunities for Europe*, Eurodefense Network, 21 II 2021 r., https://eurodefense.eu/2021/02/21/challenges-in-the-sahel-opportunities-for-europe/ [dostęp: 18 XII 2024].

[28] J. Borrell, *Together for the security, stability and development of the Sahel*, European Union External Action, 8 V 2020 r., https://www.eeas.europa.eu/eeas/together-security-stability-and-development-sahel_en [dostęp: 27 V 2025].

Tuaregowie, którzy od wieków zamieszkują Azawad i roszczą sobie prawo do tych ziem. W ciągu ostatniej dekady struktura tego środowiska radykalnie się zmieniła. Wzrosło znaczenie ugrupowań dżihadystyczno-terrorystycznych, które nie tylko zdominowały istniejące wcześniej organizacje zbrojne, lecz także przejęły kontrolę nad częścią terytorium i znacznie zdestabilizowały sytuację w regionie. Po zamachu stanu w Nigrze, do którego doszło w 2023 r., Mali, Burkina Faso i Niger zawiązały Sojusz Państw Sahelu (Alliance des États du Sahel, AES), stanowiący pakt o wzajemnej obronie i alternatywę dla prozachodniego nurtu w regionie[29].

Mali

W Mali są trzy główne strony konfliktu. Obecnie reprezentuje je kilkadziesiąt odłamów i rebelii (ich liczba zmienia się z każdym miesiącem). Pierwszy obóz to nurt propaństwowy, którego narracja jest kształtowana i realizowana przez malijskie siły zbrojne (Forces Armées Maliennes, FAMa). Formacja ta korzysta ze wsparcia trzech głównych sojuszniczych struktur, które różnią się zasięgiem i charakterem działania:

1) milicje etniczne – przede wszystkim przedstawiciele ludu Dogonów, aktywnie wspierani przez władze w Bamako oraz juntę wojskową generała Assimiego Goïty. Milicje te biorą udział w trwającym konflikcie etnicznym z Fulanami, z których część – pozbawiona ochrony państwa – szuka bezpieczeństwa w strukturach organizacji takich jak Al-Kaida czy Państwo Islamskie (Islamic State, IS; Islamic State of Iraq and Syria, ISIS)[30];
2) Korpus Afrykański – rosyjska formacja paramilitarna, dawniej znana jako Grupa Wagnera, obecnie funkcjonująca jako oficjalna misja wsparcia dla władz Mali[31];
3) prorządowe grupy Tuaregów – w tym byli członkowie organizacji Groupe d'Autodéfense Tuareg Imghad et Alliés (GATIA), którzy

[29] J. Czerep, *Konsekwencje powołania Konfederacji Państw Sahelu*, Polski Instytut Spraw Międzynarodowych, 14 VIII 2024 r., https://www.pism.pl/publikacje/konsekwencje-powolania-konfederacji-panstw-sahelu [dostęp: 15 I 2025].

[30] A. Hauchard, *In Violence-shattered Central Mali, Victims Recount Their Lives*, Barron's, 9 II 2022 r., https://www.barrons.com/news/in-violence-shattered-central-mali-victims-recount-their-lives-01644458408 [dostęp: 5 I 2025].

[31] D. Ehl, *How the Russian Wagner Group is entrenching itself in Africa*, Deutsche Welle, 27 X 2024 r., https://www.dw.com/en/russia-kremlin-wagner-group-influence-in-central-african-republic-sudan-mali/a-70599853 [dostęp: 5 I 2025].

aktualnie operują m.in. w rejonie trójstyku granicznego Mali, Nigru i Burkiny Faso, gdzie wykonują zadania patrolowe i zabezpieczające[32].

Drugi obóz tworzą ugrupowania antyrządowe, z których najważniejsze to powiązana z Al-Kaidą Grupa Wsparcia Islamu i Muzułmanów (Jama'at Nusrat al-Islam wal-Muslimin, JNIM), koalicja Cadre stratégique pour la défense du peuple de l'Azawad (CSP-DPA) oraz nowo utworzony Front Wyzwolenia Azawadu, skupiający Tuaregów i inne mniejszości etniczne. Chociaż formalnie są to odrębne struktury, łączy je wrogie nastawienie do władz w Bamako, a także więzy rodzinne i relacje osobiste pomiędzy liderami, co umożliwia im utrzymywanie kruchego porozumienia[33]. Przywódcy JNIM i CSP-DPA byli aktywnymi uczestnikami konfliktu w latach 2012–2013, który zakończył się francuską interwencją wojskową. Wspomnienia dotyczące zdrady, jakiej w tym okresie Al-Kaida dopuściła się wobec Tuaregów, pozostają żywe i wpływają na obecne relacje wewnątrz tego obozu[34].

Trzecim obozem jest najbardziej brutalny uczestnik obecnego konfliktu – Państwo Islamskie Prowincji Sahel (Islamic State Sahel Province, IS Sahel, ISSP). Grupa ta przejęła kontrolę nad znaczną częścią pogranicza Mali i Nigru[35]. W odróżnieniu od innych aktorów ISSP nie utrzymuje sojuszy ani z władzami w Bamako, ani z innymi ugrupowaniami zbrojnymi w Mali, co czyni ją izolowaną, ale groźną siłą w regionie. Szybka ekspansja ISSP budzi niepokój w kontekście rosnącej liczby ugrupowań terrorystycznych aktywnych w Sahelu.

[32] H. Nsaibia, C. Weiss, *The End of the Sahelian Anomaly: How the Global Conflict between the Islamic State and al-Qa`ida Finally Came to West Africa*, „CTC Sentinel" 2020, t. 13, nr 7, https://ctc.westpoint.edu/wp-content/uploads/2020/07/CTC-SENTINEL-072020.pdf [dostęp: 5 I 2025].

[33] C. Weiss, *Tuareg rebels, JNIM each claim victory over Russia's Wagner Group in Mali*, Foundation for Defense of Democracies, 29 VII 2024 r., https://www.fdd.org/analysis/op_eds/2024/07/29/tuareg-rebels-jnim-each-claim-victory-over-russias-wagner-group-in-mali/ [dostęp: 5 I 2025].

[34] *Tuareg rebels driven out of Timbuktu*, Al Jazeera, 29 VI 2012 r., https://www.aljazeera.com/news/2012/6/29/tuareg-rebels-driven-out-of-timbuktu [dostęp: 5 I 2025].

[35] A.Y. Zelin, S. Cahn, *Exploiting a „Vast jihad Arena": The Islamic State Takes Territory in Mali*, The Washington Institute for Near East Policy, 26 IX 2023 r., https://www.washingtoninstitute.org/policy-analysis/exploiting-vast-jihad-arena-islamic-state-takes-territory-mali [dostęp: 5 I 2025].

Burkina Faso

W 2014 r. sytuację sił bezpieczeństwa w państwie znacznie pogorszyło odsunięcie od władzy prezydenta Blaise'a Compaoré oraz konflikt armii ze służbami specjalnymi i żandarmerią. W 2020 r. prezydent Roch Marc Christian Kaboré powołał milicję znaną jako Ochotnicy na rzecz Obrony Ojczyzny (Les Volontaires pour la défense de la Patrie, VDP), której celem było zaangażowanie ludności cywilnej w walkę z rosnącym zagrożeniem dżihadystycznym i zorganizowanie społecznej linii obrony przed brutalnymi atakami ze strony ugrupowań terrorystycznych[36]. Z biegiem czasu formacja okazała się jednak niewydolna operacyjnie i niezdolna do skutecznego przeciwdziałania przemocy. Pogarszająca się sytuacja bezpieczeństwa oraz ekspansja struktur JNIM spowodowały, że władze państwowe straciły kontrolę nad znaczną częścią terytorium. Obecnie, według dostępnych danych, junta wojskowa dowodzona przez kpt. Ibrahima Traorégo sprawuje faktyczną władzę nad mniej niż 60% terytorium Burkiny Faso[37].

Junta ta znacznie zwiększyła liczebność VDP i rozszerzyła jej udział w działaniach przeciwko ugrupowaniom dżihadystycznym. Wzrost liczby członków tej formacji zbiegł się jednak z oskarżeniami o poważne nadużycia. W latach 2023–2024 organizacje międzynarodowe i media ujawniły przypadki masowych przestępstw popełnianych przez VDP wobec ludności cywilnej, w tym zabójstw, porwań i grabieży[38]. Obecnie szacuje się, że VDP liczy ok. 100 000 ochotników wspierających regularną armię Burkiny Faso, ale pojawiają się poważne zastrzeżenia dotyczące jakości ich szkolenia, braku skutecznego nadzoru, a także wykluczania niektórych społeczności z procesu rekrutacji i nieuwzględniania części regionów w planowaniu operacyjnym. W związku z rosnącymi obawami o brutalizację konfliktu rząd w Wagadugu powinien pilnie wzmocnić mechanizmy kontroli i monitoringu działań VDP, aby zapobiec dalszej eskalacji przemocy i pogłębieniu kryzysu zaufania społecznego.

---

[36] H. Nsaibia, *Actor Profile: Volunteers for the Defense of the Homeland (VDP)*, Armed Conflict Location & Event Data, 26 III 2024 r., https://acleddata.com/2024/03/26/actor-profile-volunteers-for-the-defense-of-the-homeland-vdp/ [dostęp: 5 I 2025].

[37] *Crisis in Burkina Faso: What you need to know and how you can help*, International Rescue Committee, 14 II 2024 r., https://www.rescue.org/article/crisis-burkina-faso-what-you-need-know-and-how-you-can-help [dostęp: 5 I 2025].

[38] *Burkina Faso: Unlawful Killings, 'Disappearances' by the Army*, Human Rights Watch, 29 VI 2023 r., https://www.hrw.org/news/2023/06/29/burkina-faso-unlawful-killings-disappearances-army [dostęp: 5 I 2025].

Niger

Po obaleniu w 2023 r. przez juntę wojskową prezydenta Mohameda Bazouma zaczęły powstawać w Nigrze liczne prorządowe organizacje, popierające ideę jego przywrócenia do władzy. Część z nich wywodziła się ze środowisk zaangażowanych wcześniej w rebelie Tuaregów, na terytorium zarówno Nigru, jak i Mali. Jedną z najbardziej rozpoznawalnych postaci związanych z tym nurtem jest Rissa Ag Boula – były lider tuareskich ruchów zbrojnych, który powołał Radę Oporu dla Republiki (Conseil de la Résistance pour la République, CRR). Jej celem było zorganizowanie wsparcia polityczno-militarnego dla obalonego prezydenta Bazouma[39]. We wrześniu 2024 r. CRR została jednak rozwiązana z powodu wewnętrznych podziałów i nieporozumień dotyczących strategii oraz wizji przyszłości. W odpowiedzi na rozpad organizacji Rissa Ag Boula ogłosił utworzenie nowej formacji – Wolnych Sił Zbrojnych (Forces armées libres, FAL)[40].

Jednym z głównych ugrupowań wspierających obalonego prezydenta Bazouma jest Patriotic Liberation Front (PLF) – zyskująca na znaczeniu formacja zbrojna, coraz aktywniej zaznaczająca swoją obecność na nigeryjskiej scenie politycznej oraz w sferze militarnej. W czerwcu 2023 r. PLF przeprowadził atak na chiński rurociąg naftowy łączący Niger z Beninem. Uzasadnieniem był zarzut o zdradę interesów obalonego rządu przez wspieranie przez juntę obcych, głównie chińskich, wpływów[41]. W sierpniu 2024 r. lider organizacji spotkał się w miejscowości Tinzawaten, na północy Mali, z przedstawicielem tuareskiego przywództwa. Spotkanie odbyło się zaledwie miesiąc po bitwie między siłami wspieranego przez Rosję rządu Mali a koalicją Tuaregów i Al-Kaidy. To wydarzenie wskazuje na postępującą koordynację działań między PLF a tuareskimi ugrupowaniami rebelianckimi[42].

---

[39] P. Kum, *Niger: L'ancien rebelle nigérien, Rhissa Ag Boula, annonce son intention de reprendre les armes pour chasser les putschistes*, Alwihda Info, 21 VIII 2023 r., https://www.alwihdainfo.com/Niger-L-ancien-rebelle-nigerien-Rhissa-Ag-Boula-annonce-son-intention-de-reprendre-les-armes-pour-chasser-les_a125857.html [dostęp: 5 I 2025].

[40] J. le Bihan, *Former Niger minister launches movement to overthrow junta*, The Africa Report, 27 IX 2024 r., https://www.theafricareport.com/363047/former-niger-minister-launches-movement-to-overthrow-junta/ [dostęp: 5 I 2025].

[41] L. Fleming, T.I. Issoufou, *Niger confirms anti-junta rebels behind oil attack*, BBC, 22 VI 2024 r., https://www.bbc.com/news/articles/c511n4edl7lo [dostęp: 5 I 2025].

[42] *Mali and Niger rebels met to 'strengthen' ties amid political turmoil*, Al Arabiya News, 2 IX 2024 r., https://english.alarabiya.net/News/world/2024/09/02/mali-and-niger-rebels-met-to-strengthen-ties-amid-political-turmoil [dostęp: 5 I 2025].

Niger jest jedynym państwem w regionie Sahelu, na którego terytorium działają jednocześnie trzy ugrupowania powiązane z ISIS. Obecność tych frakcji, obejmujących zarówno struktury transgraniczne, jak i lokalne komórki, czyni ten kraj szczególnie podatnym na eskalację przemocy i stanowi poważne wyzwanie dla utrzymania stabilności wewnętrznej oraz bezpieczeństwa w regionie. Obecnie te frakcje to: Państwo Islamskie Wielkiej Sahary (Islamic State in the Greater Sahara, ISGS), które działa głównie w regionie przygranicznym Mali, Burkiny Faso i Nigru, gdzie przeprowadza ataki na siły rządowe i ludność cywilną; Państwo Islamskie – Prowincja Afryki Zachodniej (Islamic State West Africa Province, ISWAP) – aktywne w północno-wschodniej Nigerii, ale też w południowo-wschodnim Nigrze, w Czadzie i Kamerunie, gdzie atakuje wojsko i infrastrukturę, oraz Państwo Islamskie w Libii (Islamic State in Libya, IS Libya), które ma swoje główne struktury w Libii, ale jego bojownicy przenikali również na północ Nigru. Przywódcy ISIS pracują nad konsolidacją władzy, co ułatwia im brak zagrożenia ze strony amerykańskich i francuskich sił powietrznych, których bazy wojskowe zamknięto w maju 2024 r.[43] Zbrojne grupy terrorystów systematycznie wykorzystywały oblężenia, groźby i porwania oraz podkładały materiały wybuchowe i miny lądowe, aby kontrolować szlaki dostaw i rozszerzać swój wpływ w Mali, Burkinie Faso i Nigrze. Ugrupowania islamskie narzucają przymusowe podatki, niszczą i rabują cywilną infrastrukturę, taką jak miejsca kultu, ośrodki zdrowia, składy żywności, mosty[44], szkoły, a także grożą nauczycielom, porywają ich i zabijają.

Podział grup terrorystycznych w Sahelu

W Sahelu działa wiele organizacji terrorystycznych (rysunek 2). Najważniejsze z nich można podzielić na podstawie ich powiązań z globalnymi sieciami Al-Kaidy i ISIS:

1) Al-Kaida Islamskiego Maghrebu (Al-Qaeda in the Islamic Maghreb, AQIM) wywodzi się z dżihadystycznych grup walczących w wojnie

[43] *US military says withdrawal from Niger is complete*, France24, 16 IX 2024 r., https://www.france24.com/en/live-news/20240916-us-military-says-withdrawal-from-niger-is-complete [dostęp: 5 I 2025].

[44] E. Pertier, *After Military Took Power, Terrorist Attacks Only Got Worse*, The New York Times, 22 XII 2024 r., https://www.nytimes.com/2024/12/22/world/africa/niger-war-coup.html [dostęp: 5 I 2025].

domowej w Algierii, od 2007 r. pod egidą Al-Kaidy prowadzi walki w północnej i zachodniej Afryce. Jedno z kilku ugrupowań tworzących Radę Szury terrorystów wspomaga lokalne struktury w Sahelu w walkach przeciwko juntom wojskowym oraz rządom demokratycznym;

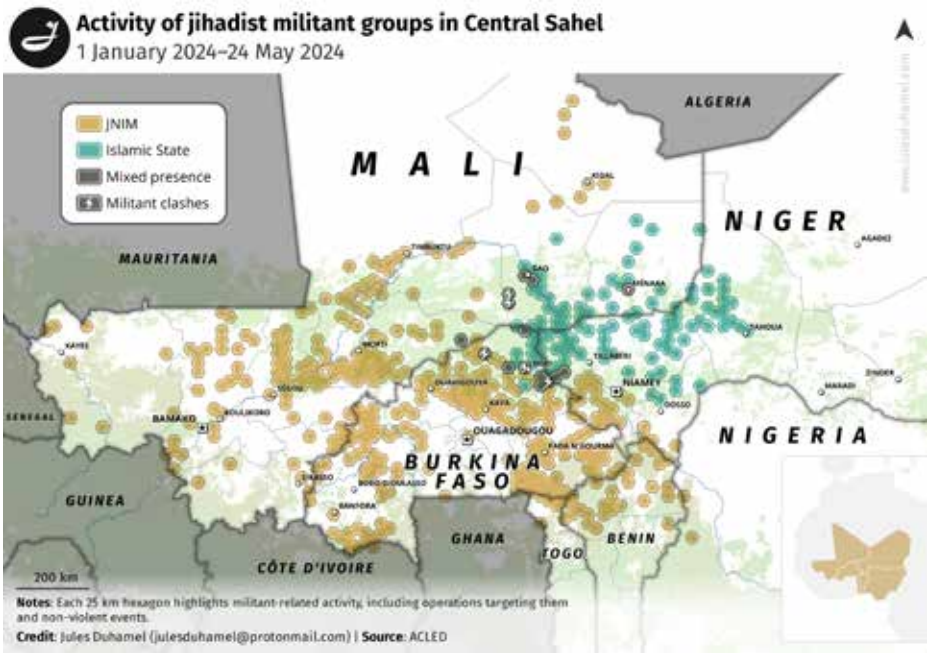
2) JNIM powstała w 2017 r. jako koalicja grup lojalnych, przyjaznych Al-Kaidzie, które zdecydowały się na reorganizację swoich działań w obliczu presji ze strony francuskich wojsk oraz ISIS. Po ośmiu latach z powodzeniem prowadzi działania militarne w Mali, Burkinie Faso i Nigrze oraz rozszerza wpływy na całą Afrykę Zachodnią. W 2025 r. JNIM prowadziła swoje operacje również na terenie północno-zachodniej Nigerii i w Beninie;
3) ISIS podzielone na trzy główne prowincje operacyjne:
   a) ISSP obejmujące Mali, Burkinę Faso i Niger,
   b) ISWAP w Nigerii i sąsiednich krajach,
   c) IS Libya na pograniczu libijsko-nigerskim.

Od 2024 r. te wszystkie jednostki mają jedną, nadrzędną strukturę, która koordynuje operacje zarówno z centralnym dowództwem w Syrii, jak i ze strukturami we wschodniej oraz południowej Afryce, co wzmacnia obecność ISIS na głównych szlakach przemytniczych i w strategicznych regionach Sahelu.

Liczba ugrupowań fundamentalistycznych, ekstremistycznych i terrorystycznych w regionie Sahelu systematycznie rośnie od początku XXI w. Od 2019 r. organizacje te rozszerzają swoją działalność na państwa nadbrzeżne Afryki Zachodniej – Benin, Wybrzeże Kości Słoniowej i Togo[45]. Od 2022 r. obserwuje się gwałtowny wzrost liczby ataków i są one wyjątkowo brutalne. W 2024 r. w Sahelu odnotowano ok. 11 200 ofiar śmiertelnych działań terrorystycznych – trzykrotnie więcej niż w 2021 r. Krajem najbardziej narażonym pozostaje Burkina Faso, na którą przypada 48% wszystkich ataków oraz 62% zabitych w regionie[46].

[45] M. Jeannin, *Ghana worries about rise of terrorist threat in Gulf of Guinea*, Le Monde, 7 VI 2022 r., https://www.lemonde.fr/en/le-monde-africa/article/2022/06/07/ghana-concerned-about-extension-of-terrorist-threat-to-coastal-states-of-gulf-of-guinea_5985936_124.html [dostęp: 5 I 2025].

[46] *Global Terrorism Index 2025*, Institute for Economics & Peace, https://www.visionofhumanity.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf [dostęp: 27 V 2025].



Rysunek 2. Działalność grup dżihadystycznych w centralnym Sahelu.

Źródło: ACLED. Za: J. Duhamel, *Central Sahel – Map of jihadist militant groups activity (Jan–May 2024)*, Jules Duhamel, 21 VI 2024 r., https://www.julesduhamel.com/central-sahel-map-of-jihadist-militant-groups-activity-jan-may-2024/ [dostęp: 15 I 2025].

Przed francuską interwencją w Sahelu istniało tam wiele grup powiązanych z Al-Kaidą. Ich osłabienie oraz ekspansja ISIS spowodowały dalszą fragmentaryzację dżihadyzmu w regionie. W odpowiedzi na to w 2017 r. Tuareg Iyad Ag Ghaly, wraz z przedstawicielami AQIM i innych ugrupowań, doprowadził do ich zjednoczenia w JNIM[47]. Celem było zarówno przeciwstawienie się francuskim i ONZ-owskim działaniom antyterrorystycznym, jak i ograniczenie rekrutacji bojowników przez ISIS, a przede wszystkim powstrzymanie rozdrobnienia grup dżihadystycznych i utrzymanie w Sahelu zjednoczonej organizacji.

Strategiczne plany operacyjne JNIM koncentrowały się początkowo na trzech państwach regionu: Mali, Burkinie Faso i Nigrze. Utworzenie koalicji miało na celu wzmocnienie skuteczności działań rekrutacyjnych oraz

[47] T. Joscelyn, *Analysis: Al Qaeda groups reorganize in West Africa*, FDD's Long War Journal, 13 III 2017 r., https://www.longwarjournal.org/archives/2017/03/analysis-al-qaeda-groups-reorganize-in-west-africa.php [dostęp: 5 I 2025].

budowę centrum władzy alternatywnego wobec lokalnych rządów postrzeganych jako sojusznicy „zachodnich krzyżowców”[48]. W dalszej perspektywie JNIM zakładała rozszerzenie działalności na kolejne kraje, w tym państwa nadbrzeżne Zatoki Gwinejskiej. Pomimo tych ambicji wysokie dowództwo tego ugrupowania – Madżlis al-Szura – zmaga się z wewnętrznymi problemami typowymi dla zdecentralizowanych organizacji terrorystycznych. Należą do nich konflikty lojalnościowe pomiędzy strukturą organizacyjną a więzami klanowymi, ambicje indywidualnych liderów oraz słabe zarządzanie na wszystkich szczeblach hierarchii.

Jednym z najważniejszych elementów *AQIM Playbook*[49] była zasada unikania powtarzania błędów popełnionych wcześniej przez inne ugrupowania dżihadystyczne. Abdelmalek Droukdel, długoletni emir AQIM, zabity w 2020 r. przez francuskie siły, przestrzegał przed działaniami mogącymi wywołać zagraniczną interwencję i tym samym zaszkodzić długofalowym interesom ruchu. Przewidywał potencjalne konsekwencje zbyt szybkiej ekspansji – szczególnie w kontekście wydarzeń z 2013 r., gdy rozprzestrzenienie się rebelii dżihadystycznej na południe Mali skłoniło Francję do uruchomienia operacji „Serval”[50]. Droukdel ostrzegał dowódców przed szybkim marszem na Bamako, gdyż uznał, że takie działania mogłyby sprowokować międzynarodową interwencję. Ta ostrożna strategia stała się jednak źródłem napięć wewnątrz AQIM oraz między AQIM a niektórymi sojuszniczymi ugrupowaniami, które preferowały bardziej agresywne podejście operacyjne.

Z perspektywy AQIM jednym z głównych błędów popełnionych przez wcześniejsze ruchy dżihadystyczne było zbyt szybkie narzucanie surowych kar wynikających z szariatu oraz przedwczesne wdrażanie struktur quasi-państwowych opartych na zasadach islamskiego emiratu. Takie podejście – zdaniem tej organizacji – doprowadziło do utraty poparcia społecznego i upadku projektu państwa dżihadystycznego. Po rozpoczęciu

[48] C. Weiss, *AQIM's Imperial Playbook. Understanding al-Qa'ida in the Islamic Maghreb's Expansion into West Africa*, bmw, April 2022, https://ctc.westpoint.edu/wp-content/uploads/2022/04/AQIMs-Imperial-Playbook.pdf [dostęp: 5 I 2025].

[49] *AQIM Playbook* – termin używany do opisu strategii, taktyk i metod działania stosowanych przez AQIM. Odnosi się do schematów operacyjnych, propagandowych i rekrutacyjnych tej grupy, opracowanych na podstawie jej doświadczeń w Afryce Północnej i Sahelu. Ważną rolę w stworzeniu i wdrożeniu *AQIM Playbook* odegrał Abdelmalek Droukdel. Jako emir Al-Kaidy Islamskiego Maghrebu od 2004 r. aż do swojej śmierci w 2020 r. był głównym strategiem i ideologiem tej organizacji.

[50] T. Joscelyn, *Analysis: Al Qaeda groups…*

francuskiej operacji „Barkhane" w 2014 r. AQIM przyjęła bardziej ostrożną strategię i skoncentrowała się na zdobywaniu poparcia lokalnych społeczności. Działania te przynosiły wymierne efekty, szczególnie w obszarach pozbawionych skutecznego zarządzania państwowego. Wycofanie się wojsk francuskich z Mali (2022 r.), Burkiny Faso i Nigru (2023 r.) umocniło wśród zwolenników AQIM przekonanie, że ich długoterminowa strategia przynosi rezultaty, a idea stworzenia islamskiego emiratu w regionie znów jest możliwa do urzeczywistnienia[51].

W ostatnich latach głównym obszarem działalności i ekspansji JNIM stało się Burkina Faso. Proces ten rozpoczął się w 2016 r., kiedy to Katiba Macina, jednostka AQIM szkolona przez Al-Kaidę, wspierana jej rekrutami, finansami i dowództwem, szybko zyskała wpływy w tym kraju. Sprzyjały temu brak spójnej wizji politycznej elit państwowych, niezdolność wojska do skutecznej walki z powstaniami oraz widoczna niechęć francuskich sił do bezpośredniego zaangażowania. Po serii zamachów stanu w Burkinie Faso i po przymusowym wycofaniu Francji dżihadyści na prośbę nowej junty znacznie poszerzyli swoje zdobycze terytorialne[52]. Terroryści otoczyli stolicę, Wagadugu, zajęli główne drogi w kraju i odcięli dostęp do miast. Sytuacja w Burkinie Faso ma wpływ na inne kraje regionu, które czują się zagrożone terroryzmem[53].

Al-Kaida jest w stanie przeprowadzać ataki na kierunku północnym i południowym, np. w Togo czy Beninie, i infiltrować kompleks parków narodowych W-Arly-Pendjari, obejmujący kraje Zatoki Gwinejskiej i Afryki Zachodniej. Liczba ataków terrorystycznych nieprzerwanie wzrasta od 2022 r., szczególnie w państwach położonych nad Zatoką Gwinejską[54]. Wzrost intensywności ataków oraz sukcesy w zabezpieczeniu w 2024 r. dróg

[51] H. Nsaibia, *Actor Profile: Jama'at Nusrat al-Islam wal-Muslimin (JNIM)*, Armed Conflict Location & Event Data, 13 XI 2023 r., https://acleddata.com/2023/11/13/actor-profile-jamaat-nusrat-al-islam-wal-muslimin-jnim/ [dostęp: 5 I 2025].

[52] *Deaths Linked to Militant Islamist Violence in Africa Continue to Spiral*, Africa Center for Strategic Studies, 29 I 2024 r., https://africacenter.org/spotlight/mig2024-deaths-militant-islamist-violence-africa-rise/ [dostęp: 5 I 2025].

[53] S. Douce, *Burkina Faso's Djibo city struggles under jihadist siege*, La Croix International, 7 XI 2024 r., https://international.la-croix.com/world/burkina-fasos-djibo-city-struggles-under-jihadist-siege [dostęp: 5 I 2025].

[54] J. Zenn, *Brief: JNIM Attacks in Benin Represented Group's Growing Operational Strength in Periphery*, The Jamestown Foundation, 11 XII 2024 r., https://jamestown.org/program/brief-jnim-attacks-in-benin-represented-groups-growing-operational-strength-in-periphery/ [dostęp: 5 I 2025].

i najważniejszych punktów komunikacyjnych w południowo-wschodniej części Burkiny Faso sprawiły, że w 2025 r. Al-Kaida pewnie wkracza do północnego Beninu i wzmacnia swoją pozycję w kraju. Według Critical Threats w pierwszych czterech miesiącach 2025 r. w atakach zginęło tam ponad 157 osób, o 50 więcej niż w 2024 r., a statystyki wskazują, że do końca 2025 r. liczba ofiar może wzrosnąć nawet pięciokrotnie[55]. Ze względu na dynamicznie zmieniającą się sytuację oraz kruchość struktur państwowych w Togo i Beninie dalsze umacnianie pozycji dżihadystów i zakładanie przez nich baz operacyjnych będzie miało bezpośrednie konsekwencje dla państw Sahelu. Region ten, już teraz zmagający się z problemem coraz gęstszej sieci szlaków zaopatrzeniowych wykorzystywanych przez ugrupowania terrorystyczne, może nie być w stanie skutecznie przeciwdziałać ich dalszej ekspansji.

Niger znajduje się pod silnym wpływem ugrupowań terrorystycznych operujących na pograniczu Mali, Libii oraz w dorzeczu jeziora Czad. Na terenie tego ubogiego, strategicznie położonego kraju przez lata przebywały francuskie i amerykańskie siły i pełnił on funkcję kluczowego partnera Zachodu w działaniach antyterrorystycznych w regionie Sahelu. Amerykańska baza dronów w Agadezie była największym tego rodzaju obiektem w regionie[56]. Została założona w celu monitorowania grup terrorystycznych i wspierania Nigru w walce z nimi. W ostatnich latach było to głównie ISIS.

Obecność ISIS w regionie Sahelu od początku budziła kontrowersje w środowisku dżihadystycznym. Konflikt o dominację pomiędzy Al-Kaidą a ISIS w Sahelu przyjął początkowo wyjątkową formę. Mimo rosnącego znaczenia ISIS, szczególnie w Mali, obie organizacje, tj. JNIM (powiązana z Al-Kaidą) oraz lokalne odłamy ISIS, przez długi czas unikały otwartego starcia. Ten stan rzeczy nazwano sahelskim wyjątkiem (ang. *Sahelian exceptionalism*)[57]. Termin ten, oznaczający nietypową dla globalnego dżihadyzmu

[55] L. Karr, *Africa File, April 24, 2025: JNIM's Growing Pressure on Benin; Turkey to Somalia; Salafi-Jihadi Cells Continue to Grow Across Nigeria*, Critical Threats, 24 IV 2025 r., https://www.understandingwar.org/backgrounder/africa-file-april-24-2025-jnim%E2%80%99s-growing-pressure-benin-turkey-somalia-salafi-jihadi/ [dostęp: 20 V 2025].

[56] M. Banchereau, *US hands over its last military base in Niger to the ruling junta*, The Associated Press, 7 VIII 2024 r., https://apnews.com/article/niger-united-states-troops-army-military-bases-junta-sahel-coup-1ae5334bc68eb6b45e1e2d612bfb2b6f [dostęp: 5 I 2025]; *US troops pull out of Niger's Air Base 101*, Reuters, 8 VII 2024 r., https://www.reuters.com/world/africa/us-troops-pull-out-nigers-air-base-101-2024-07-07/ [dostęp: 5 I 2025].

[57] W. Nasr, *ISIS in Africa: The End of the „Sahel Exception"*, New Lines Institute, 2 VI 2020 r., https://newlinesinstitute.org/nonstate-actors/isis-in-africa-the-end-of-the-sahel-exception [dostęp: 10 I 2025].

współegzystencję w jednym regionie dwóch konkurencyjnych organizacji, ukuł francuski dziennikarz Wassim Nasr.

Do końca 2019 r. JNIM i malijskie komórki ISIS (głównie ISGS) unikały bezpośredniej konfrontacji, a nawet można było dostrzec oznaki lokalnej współpracy w wybranych rejonach[58]. Jednak w 2020 r. JNIM, która dostrzegła rosnącą siłę ISGS oraz odpływ bojowników do tej frakcji, zdecydowała się na otwarte starcie i zacieśniła więzi z globalną strukturą Al-Kaidy. Od tego momentu konflikt między JNIM a ISGS przekształcił się w regularną wojnę, przerywaną jedynie sporadycznymi zawieszeniami broni i doraźnymi porozumieniami o charakterze taktycznym[59].

W latach 2022–2023 zarówno armia Mali przy wsparciu Francuzów, jak i Al-Kaida podejmowały próby pokonania ISGS[60]. Mimo że te siły są wobec siebie wrogie, łączył je cel ograniczenia wpływów ISGS w regionie. Państwo Islamskie znane jest z bardziej brutalnych i restrykcyjnych rządów niż Al-Kaida, co wynika m.in. z surowszego podejścia do doktryny *takfir*. Muzułmanie, którzy w interpretacji ISIS odstępują od prawdziwej wiary, są przez nie uznawani za niewiernych. Taka interpretacja pozwala na uzasadnianie przemocy nie tylko wobec przeciwników ideologicznych, lecz także wobec lokalnej ludności, która nie akceptuje władzy ISIS[61].

O nowym etapie w działalności ISIS może świadczyć atak uzbrojonych dronów przeprowadzony w Nigerii w grudniu 2024 r. Była to pierwsza tego typu akcja na tak dużą skalę[62]. W 2025 r. ISIS zapewne będzie próbowało rozszerzyć swoje wpływy w Sahelu i bezpośrednio w Nigerii, gdzie znajduje się największa w tym momencie filia organizacji ISWAP, która nie ukrywa swoich ambicji wobec terytorium Nigerii, Czadu, Nigru i Kamerunu i próbuje przywrócić władzę nad obszarami straconymi za czasów Abu Bakra Shekau, lidera organizacji Boko Haram.

---

58 H. Nsaibia, C. Weiss, *The End of the Sahelian Anomaly*...

59 Tamże.

60 *Islamic State group nearly doubled its Mali territory in under a year, UN says*, France 24, 26 VIII 2023 r., https://www.france24.com/en/africa/20230826-islamic-state-group-doubled-controlled-territory-in-mali-in-under-a-year-un-experts-say [dostęp: 5 I 2025].

61 J. Kadivar, *Exploring Takfir, Its Origins and Contemporary Use: The Case of Takfiri Approach in Daesh's Media*, „Sage Journals" 2020, t. 7, nr 3, https://journals.sagepub.com/doi/full/10.1177/2347798920921706 [dostęp: 5 I 2025]. https://doi.org/10.1177/2347798920921706.

62 T. David, *Troops Foil Boko Haram, ISWAP Drone Attack In Buni Gari*, Leadership, https://leadership.ng/troops-foil-boko-haram-iswap-drone-attack-in-buni-gari/ [dostęp: 5 I 2025].

W ciągu ostatnich dwóch lat odnotowano wyraźny wzrost aktywności ISGS w Maroku, Algierii i Hiszpanii. ISGS, podobnie jak inne odłamy ISIS, rozwija i testuje różne strategie operacyjne i dąży do przekształcenia się w samodzielnie działającą strukturę, zdolną do prowadzenia działań promocyjnych, rekrutacyjnych, a także koordynowania międzynarodowych bojowników. Celem tych działań jest stopniowe przesunięcie osi dżihadu w kierunku Europy.

Komórki stworzone w północnej Afryce mają skierować działania na Mali, gdzie ISGS posiada swoje terytorium[63]. W styczniu 2025 r. marokańskie służby udaremniły próbę operacji ISGS na swoim terenie. Aresztowano przygotowujących się do zamachów terrorystów, którzy byli w kontakcie z dżihadystami Państwa Islamskiego w Mali[64]. W lutym 2025 r. Marokańczycy ponownie rozbili siatkę ISGS, przeprowadzając operacje w dziewięciu miastach. Na jaw wyszły nowe plany ISGS, koordynowane z Mali przez zagranicznych bojowników pochodzenia arabskiego, którzy stworzyli specjalny komitet nawiązujący kontakty z zagranicą i werbujący rekrutów[65]. Za pomocą sieci powiązań transgranicznych ISGS przemyciło do Maroka broń ukrytą w specjalnych skrytkach. Mieli ją odebrać – przez podanie koordynatów GPS – dżihadyści planujący zamachy na dużą skalę[66]. To przykład jednej z wielu akcji terrorystycznych, które Hiszpanie oraz Marokańczycy wspólnie rozbili w latach 2023–2025[67].

W 2024 r. największą uwagę społeczności międzynarodowej przyciągało Państwo Islamskie – Prowincja Chorasan (Islamic State – Khorasan Province, ISKP), głównie ze względu na swoją rosnącą zdolność do oddziaływania

[63] A.Y. Zelin, *The Islamic State on the March in Africa*, The Washington Institute for Near East Policy, 1 III 2024 r., https://www.washingtoninstitute.org/policy-analysis/islamic-state-march-africa [dostęp: 5 I 2025].

[64] S. Kasroui, *Morocco's BCIJ Foils Terrorist Plot, Arrests 4 ISIS-Affiliated Suspects Near Casablanca*, Marocco World News, 26 I 2025 r., https://www.moroccoworldnews.com/2025/01/367913/morocco-s-bcij-foils-terrorist-plot-arrests-4-isis-affiliated-suspects-near-casablanca [dostęp: 20 V 2025].

[65] *Morocco: ISIS-instigated plot foiled, 12 suspects arrested*, The North Africa Post, 19 II 2025 r., https://northafricapost.com/84516-morocco-isis-instigated-terror-plot-foiled-12-suspects-arrested.html [dostęp: 20 V 2025].

[66] I. Toutate, *BCIJ Links 'Highly Dangerous' Foiled Terror Plot to Sahel Terrorist Groups*, Morocco World News, 24 II 2025 r., https://www.moroccoworldnews.com/2025/02/174948/bcij-links-highly-dangerous-foiled-terror-plot-to-sahel-terrorist-groups/ [dostęp: 20 V 2025].

[67] A. Zelin, *The Islamic State on the March*...

na różne grupy i diaspory, a także skuteczność w infiltracji Europy przez wysyłanie do niej agentów i zwolenników[68].

Nowa kampania dżihadystów w 2025 r. stwarza zagrożenie dla turystów w Maghrebie oraz Sahelu, a przez to dla lukratywnego biznesu turystycznego. Porwania Europejczyków w Algierii, Czadzie oraz Nigrze są znakiem ostrzegawczym[69]. Na podstawie dotychczasowych wydarzeń można przyjąć, że w 2026 r. istnieje prawdopodobieństwo zajęcia przez jedną z grup terrorystycznych dużego miasta w Mali lub Burkinie Faso. Wydaje się, że w pierwszym półroczu 2025 r. Al-Kaida przygotowuje grunt pod trwałe rządy. Przykładem tego jest miasto Djibo, oblężone od trzech lat i wyczerpane silnymi atakami[70]. Konsekwencjami tego będą niewidziana od dekady eskalacja konfliktu oraz utworzenie nowego „państwa" terrorystycznego, znacznie różniącego się od rządów Hayat Tahrir al-Sham w Syrii czy Talibanu w Afganistanie przez swój ekspansywny charakter.

Jeśli dżihadyści z Al-Kaidy lub ISIS zdołają doprowadzić do upadku władz w którymkolwiek z państw tworzących sojusz AES, istnieje poważne ryzyko, że efekt domina doprowadzi do destabilizacji pozostałych członków porozumienia. Najbardziej alarmująca sytuacja panuje obecnie w Burkinie Faso, gdzie rozprzestrzenienie się ugrupowań terrorystycznych stanowi bezpośrednie zagrożenie także dla sąsiednich państw w regionie[71].

Nawet nowo wybrany prezydent Senegalu, Bassirou Diomaye Faye, który początkowo był postrzegany jako przeciwnik Zachodu z powodu swojego stanowiska wobec międzynarodowych instytucji gospodarczych i politycznych, wezwał w 2024 r. do wsparcia ze strony Europy, co dobitnie pokazuje skalę zagrożenia. Aby zapobiec dalszej eskalacji, potrzebna jest skoordynowana i długofalowa inicjatywa stabilizacyjna, prowadzona z udziałem największych krajów Wspólnoty Gospodarczej Państw Afryki Zachodniej (Economic Community of West African States, ECOWAS), zwłaszcza Nigerii.

---

[68] A. Jadoon i in., *From Tajikistan to Moscow and Iran: Mapping the Local and Transnational Threat of Islamic State Khorasan*, „CTC Sentinel" 2024, t. 17, nr 5, https://ctc.westpoint.edu/from-tajikistan-to-moscow-and-iran-mapping-the-local-and-transnational-threat-of-islamic-state-khorasan/ [dostęp: 5 I 2025].

[69] P. Wójcik, wpis na portalu X, 19 I 2025 r., https://x.com/SaladinAlDronni/status/1881013944443363547 [dostęp: 24 I 2025].

[70] *Al Qaeda affiliate says 200 soldiers killed in Burkina Faso attack*, Reuters, 16 V 2025 r., https://www.reuters.com/world/africa/al-qaeda-affiliate-says-200-soldiers-killed-attack-burkina-military-site-reports-2025-05-15/ [dostęp: 16 V 2025].

[71] J. Wójcik, *Sahel pogrąża się w terrorystycznej rebelii*, Defence24, 30 IX 2023 r., https://defence24.pl/geopolityka/sahel-pograza-sie-w-terrorystycznej-rebelii [dostęp: 12 XII 2024].

Powinna ona obejmować działania na rzecz bezpieczeństwa, wsparcie instytucjonalne oraz integrację działań politycznych i gospodarczych służących rozwojowi regionu. Warto wziąć pod uwagę także możliwość organizacji przez UE misji szkoleniowej, która przygotuje kraje Afryki do przeciwdziałania terroryzmowi przede wszystkim na poziomie politycznym, ale obejmie również specjalistyczne treningi dla grup antyterrorystycznych.

Obecność w Sahelu państw spoza regionu

Od 2013 r. Francja przez ponad dekadę odgrywała najważniejszą rolę w przeciwdziałaniu terroryzmowi i stabilizacji sytuacji w Sahelu, głównie dzięki operacji „Barkhane" oraz misji „Takuba". Zaangażowanie to obejmowało Mali, Niger, Czad i Burkinę Faso, gdzie Francuzi szkolili lokalne siły i wspierali ich walkę z dżihadystami. Jednak napięcia dyplomatyczne, zwłaszcza po wojskowych zamachach stanu w Mali w 2020 r. i 2021 r., doprowadziły w 2022 r. do wycofania francuskich wojsk[72]. Francja obecnie przewartościowuje swoją strategię, kładąc nacisk na partnerstwa europejskie i ograniczoną obecność wojskową w Afryce.

Wysiłki Niemiec na rzecz stabilizacji sytuacji w Sahelu koncentrują się na misjach pokojowych ONZ oraz inicjatywach dyplomatycznych, takich jak Sahel Plus. Niemcy współpracują z sąsiednimi krajami regionu, w tym Senegalem, Ghaną i Togo, aby ograniczyć migrację i promować pokój. Berlin rozważa dalsze zaangażowanie wojskowe, chociaż jego priorytetem jest koordynacja działań w ramach UE[73]. Niemcy stawiają na dialog i negocjacje, co może pomóc w utrzymaniu stabilności w regionie.

Hiszpania dzięki misji „EUTM Mali" odegrała znaczącą rolę w szkoleniu sił zbrojnych Mali, gdzie wysłała ponad 8300 żołnierzy oraz wspierała operacje antyterrorystyczne[74]. Chociaż Madryt ma bogate doświadczenie militarne i dyplomatyczne w regionie, współpracuje z krajami Maghrebu,

[72] A. Olech, *French Operation Barkhane in Africa – success or failure?*, Stosunki Międzynarodowe – International Relations, 18 XII 2023 r., https://internationalrelations-publishing.org/articles/3-17 [dostęp: 3 XII 2024]. https://doi.org/10.12688/stomiedintrelat.17737.1.

[73] *The Federal Government realigns its Sahel policy*, Federal Foreign Office, 3 V 2023 r., https://www.auswaertiges-amt.de/en/newsroom/news/2595298-2595298 [dostęp: 4 XII 2024].

[74] L.M. Sanjuan, *Los soldados más temidos del mundo: hay una unidad española*, AS, 24 X 2024 r., https://as.com/actualidad/politica/los-soldados-mas-temidos-del-mundo-n [dostęp: 4 XII 2024].

np. w sprawie byłej kolonii w Saharze Zachodniej, kontestowanej dziś przez Maroko i organizację Front Polisario, to obecnie skupia się na zabezpieczaniu Morza Śródziemnego i utrzymaniu wpływów gospodarczych w Afryce. Brak jasnej strategii powrotu do Sahelu sugeruje, że zaangażowanie Hiszpanii w tym regionie będzie maleć.

Włochy stopniowo zwiększały swoją obecność w Afryce przez otwieranie nowych ambasad i intensyfikację wizyt dyplomatycznych. W 2023 r. w obliczu destabilizacji politycznej ograniczyły swoje siły w Nigrze, ale pozostały tam i reprezentują UE oraz starają się utrzymać wpływy w państwie pomimo jego agresywnej postawy wobec Zachodu. Pozostają także w Czadzie i uczestniczą w szkoleniu lokalnych jednostek oraz we współpracy z europejskimi partnerami. Ich strategia obejmuje ograniczenie nielegalnej migracji i zacieśnianie relacji z państwami Maghrebu[75]. Włochy łączą pomoc humanitarną z dyplomacją, co sprzyja ich pozytywnemu odbiorowi w regionie.

Turcja zwiększa swoje wpływy w Sahelu. Dostarcza drony i pomaga w walce z terroryzmem, przez co wspiera starania NATO[76]. Jednocześnie prywatna firma wojskowa Sadat wysyła najemników do regionów, w których toczą się konflikty, i chroni infrastrukturę krytyczną, np. w Nigrze. Ankara stawia na rozwój gospodarczy, inwestuje w projekty infrastrukturalne i rozbudowuje sieć ambasad[77]. Jej strategia, która jest mniej zależna od rozwiązania przez państwa w Sahelu kwestii praw człowieka, czyni ją atrakcyjnym partnerem dla afrykańskich rządów, szukających alternatywy dla partnerstwa Zachodu.

Zjednoczone Emiraty Arabskie (ZEA) zacieśniają współpracę z Czadem, do którego dostarczają sprzęt wojskowy i gdzie stacjonują ich wojska. Rola ZEA jako nowego partnera w zapewnianiu bezpieczeństwa w regionie jest istotna zwłaszcza dla lokalnych liderów, którzy potrzebują zastąpienia tradycyjnego sojuszu z Francją. Emiraty mogą się stać wzorem dla innych

[75] J. Renoult, *L'Italie, dernier partenaire occidental du Niger*, Le Monde, 23 VII 2024 r., https://www.lemonde.fr/afrique/article/2024/07/23/l-italie-ultime-partenaire-occidental-du-niger_6256111_3212.html [dostęp: 6 XII 2024].

[76] *Sahel Showdown: How Türkiye Can Help NATO With Russian and Chinese Advances*, TRT World Research Centre, 29 VII 2024 r., https://researchcentre.trtworld.com/featured/perspectives/sahel-showdown-how-turkiye-can-help-nato-with-russian-and-chinese-advances/ [dostęp: 10 XII 2024].

[77] B. Roger, T. Eydoux, *Drones turcs, avions russes… au Sahel, la guerre des airs est déclarée*, Le Monde, 20 XI 2024 r., lemonde.fr/afrique/article/2024/11/20/drones-turcs-avions-russes-au-sahel-la-guerre-des-airs-est-declaree_6405083_3212.html [dostęp: 7 XII 2024].

państw arabskich, np. Arabii Saudyjskiej. Mogą również wypełnić lukę, która powstała po wycofaniu się Francji.

Estonia wysłała swoich żołnierzy do Mali w ramach operacji „Barkhane", aby we współpracy z partnerami międzynarodowymi wesprzeć działania antyterrorystyczne. Zaangażowanie tego państwa w Afryce obejmuje również inicjatywy w zakresie cyfryzacji i e-governance, będące elementem szerszej strategii polityki zagranicznej Estonii na lata 2020–2030[78]. Pomimo wycofania kontyngentu wojskowego Tallinn pozostaje otwarty na przyszłe misje wojskowe oraz rozwój współpracy z Unią Afrykańską – ze szczególnym uwzględnieniem innowacyjnych partnerstw w obszarach technologii cyfrowych, zrównoważonego rozwoju i transformacji energetycznej.

Stany Zjednoczone skupiły się na przeciwdziałaniu terroryzmowi. Wybudowały bazę lotniczą w Agadezie i inwestują miliony dolarów w szkolenie lokalnych sił. Zamach stanu w Nigrze w 2023 r. doprowadził do wycofania amerykańskich wojsk, co osłabiło wpływy USA w regionie[79]. Tę sytuację wykorzystała Rosja. Przez współpracę militarną i ulokowanie prywatnych firm wojskowych w byłych koloniach francuskich, zazwyczaj rządzonych przez autorytarne rządy, próbuje ona podważać dominację USA w Afryce.

Francja i USA, mimo wspólnego celu, jakim była walka z terroryzmem, często działały niezależnie, co osłabiało ich skuteczność. Brak koordynacji sprawił, że region pozostał niestabilny, mimo ogromnych inwestycji w bezpieczeństwo. Oba kraje powinny zacieśnić współpracę, aby skuteczniej reagować na zagrożenia w Sahelu, zwłaszcza w obliczu rosnących wpływów Rosji i Chin[80].

Chińczycy stali się głównym dostawcą broni dla Burkiny Faso[81]. Zwykle trafia ona w ręce Al-Kaidy, co sprawia, że ta grupa ma więcej zasobów do realizacji swoich planów. Państwa UE powinny więc rozważyć różne

[78] *Estonia's strategy for Africa*, Republic of Estonia Ministry of Foreign Affairs, 7 V 2021 r., https://vm.ee/en/estonias-strategy-africa [dostęp: 11 XII 2024].

[79] M.M. Phillips, B. Faucon, *U.S. Forces Try to Regroup as al Qaeda, Islamic State Sow Terror in West Africa*, The Wall Street Journal, 11 IX 2024 r., https://www.wsj.com/world/africa/u-s-moves-aircraft-commandos-into-west-africa-in-fight-against-islamist-militants-0b15c41b [dostęp: 11 XII 2024].

[80] A. Olech, *Francja i USA będą ponownie wojskowo współpracować w Afryce*, Defence24, 20 II 2024 r., https://defence24.pl/geopolityka/francja-i-usa-beda-ponownie-wojskowo-wspolpracowac-w-afryce [dostęp: 11 XII 2024].

[81] G. Martin, *Burkina Faso receives huge batch of Chinese military equipment*, Defence Web, 27 VI 2024 r., https://www.defenceweb.co.za/land/land-land/burkina-faso-receives-huge-batch-of-chinese-military-equipment [dostęp: 12 XII 2024].

formy wsparcia dla krajów Zatoki Gwinejskiej, w najgorszym przypadku przez ponowne nawiązanie relacji z rządzącymi tam juntami.

Rosja i Iran wyraziły zainteresowanie rozwijaniem bliższych relacji z Nigrem, posiadającym największe na świecie złoża uranu. Potencjał, który kraje Sahelu mogłyby wykorzystać do własnego rozwoju, może zostać przejęty przez obce państwa, wrogo nastawione do Zachodu.

Rola NATO w Sahelu

Region Sahelu pozostaje jednym z najbardziej niedocenianych i marginalizowanych obszarów w politykach bezpieczeństwa UE[82] i NATO[83]. Dynamika zmian, jakie zaszły tam od 2021 r., w połączeniu z geopolityczną bliskością Maghrebu powinny skłonić Europę do ponownego przemyślenia swojego zaangażowania i do intensyfikacji działań w regionie. W latach 2021–2023 większość unijnych i międzynarodowych inicjatyw dotyczących Sahelu została zawieszona, mimo że wyzwania w zakresie bezpieczeństwa, migracji i radykalizacji systematycznie narastają. Sytuacja ta wymaga nie tylko głębokiej analizy potencjalnych zagrożeń, lecz także opracowania długofalowej, spójnej strategii bezpieczeństwa, dostosowanej do realiów regionu.

Do obecnej powściągliwości państw zachodnich przyczyniły się zarówno negatywne doświadczenia związane z interwencją NATO w Libii, jak i porażka francuskiej misji wojskowej w Sahelu. Kraje UE i NATO są więc niechętne do angażowania się w kolejną, długo trwającą operację, która wymagałaby skoordynowanej odpowiedzi na złożone wyzwania w regionie.

Pomimo zaangażowania licznych aktorów krajowych, regionalnych i międzynarodowych, w tym sił zbrojnych państw Sahelu, Unii Afrykańskiej, ECOWAS, ONZ, UE oraz partnerów spoza kontynentu, działania te wciąż nie są skoordynowane. Niespójność podejść, konkurujące interesy oraz ograniczone mechanizmy współpracy sprawiają, że wysiłki stabilizacyjne

[82] European Parliament, *New EU strategic priorities for the Sahel. Addressing regional challenges through better governance*, https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/696161/EPRS_BRI%282021%29696161_EN.pdf [dostęp: 14 XII 2024].

[83] NATO, *Strategic foresight analysis. Regional perspectives report on North Africa and the Sahel*, https://www.act.nato.int/wp-content/uploads/2023/05/NU_SFA_Report_North_Africa_and_the_Sahel_SACT_approved_final_edited_version.pdf [dostęp: 14 XII 2024].

są fragmentaryczne i często nieskuteczne. Chociaż część państw członkowskich NATO, zwłaszcza tych utrzymujących historyczne więzi z regionem, przez lata inwestowała w bezpieczeństwo i rozwój Sahelu, zakończenie operacji „Barkhane" stworzyło w przestrzeni militarnej poważną lukę, która do dziś pozostaje niewypełniona[84].

W ostatnich latach wysiłki NATO w zakresie bezpieczeństwa koncentrowały się głównie na zagrożeniach występujących w rejonie Morza Śródziemnego. Sojusz realizował kampanie szkoleniowe wewnątrz państw członkowskich, a także wzmacniał współpracę z partnerami z Afryki Północnej[85]. Tymczasem stale rosnąca liczba incydentów terrorystycznych w Sahelu powinna skłonić NATO do ponownej oceny strategicznych priorytetów i zwrócenia większej uwagi na ten niestabilny region. Szczególnie niepokojący jest rozwój struktur Państwa Islamskiego w Nigrze, Burkinie Faso i Mali, co powinno być sygnałem alarmowym dla decydentów oraz dla analityków zajmujących się bezpieczeństwem transregionalnym[86].

Charakter działania ISIS sprawia, że jego obecność stanowi zagrożenie nie tylko dla państw, w których ma bezpośrednie struktury, lecz także dla krajów południowej Europy, zwłaszcza tych z licznymi diasporami marokańskimi, algierskimi i tunezyjskimi. W ostatnim czasie pojawiły się doniesienia sugerujące, że ISIS nie tylko prowadzi aktywną rekrutację wśród tych społeczności, lecz także nadzoruje działania potencjalnych sprawców ataków terrorystycznych na terytorium Hiszpanii[87].

[84] C. Doxsee, J. Thompson, M. Harris, *The End of Operation Barkhane and the Future of Counterterrorism in Mali*, Center for Strategic & International Studies, 2 III 2022 r., https://www.csis.org/analysis/end-operation-barkhane-and-future-counterterrorism-mali [dostęp: 19 XII 2024].

[85] A. Olech, *Współpraca państw Maghrebu z NATO na rzecz bezpieczeństwa w regionie*, Instytut Nowej Europy, 12 X 2021 r., https://ine.org.pl/wspolpraca-panstw-maghrebu-z-nato-na-rzecz-bezpieczenstwa-w-regionie/ [dostęp: 19 XII 2024].

[86] R. Grammer, *Top counterterrorism official warns of ISIS' rapid rise in Africa*, Politico, 25 XI 2024 r., https://www.politico.com/news/2024/11/25/top-counterterrorism-official-warns-of-isiss-rapid-rise-in-africa-00191571 [dostęp: 20 XII 2024].

[87] L. Breton, *Terrorisme: l'État islamique avait des projets d'attentats visant les Jeux olympiques de Paris et l'Euro de football*, La Depeche, 17 VI 2024 r., https://www.ladepeche.fr/2024/06/17/terrorisme-letat-islamique-avait-des-projets-dattentats-visant-les-jeux-olympiques-de-paris-et-leuro-de-football-12022418.php [dostęp: 21 XI 2024].

Sahel jako przedłużenie południowej flanki NATO. Implikacje dla Sojuszu

W przyszłej strategii NATO powinno traktować południową i wschodnią flankę jako obszary, które są ze sobą powiązane. Przyjęcie tej perspektywy wymaga minimalizacji wewnętrznych sporów i promowania głębszej integracji politycznej dotyczącej dwutorowych działań. Wojna w Ukrainie ożywiła struktury NATO, o czym świadczy przystąpienie do Sojuszu Finlandii i Szwecji. Powodem, który skłonił te kraje do akcesji, była obawa o potencjalną agresję ze strony Rosji[88].

Ta sytuacja powinna skłonić do dyskusji na temat rozwijania strategii NATO w kierunku południowym. Skuteczność nowej koncepcji będzie zależała od zdolności Sojuszu do podjęcia działań na rzecz Sahelu, zanim dojdzie tam do znacznego rozrostu organizacji terrorystycznych[89]. Podczas szczytu NATO w Wilnie w 2023 r., na którym najważniejszą kwestią była wojna w Ukrainie, opublikowano oddzielny dokument dotyczący południowej Europy oraz zidentyfikowano dwa najważniejsze zagrożenia dla Sojuszu – Rosję i organizacje terrorystyczne[90].

W przeszłości aktywność NATO na południowej flance była dominowana przez wydarzenia na flance wschodniej. Państwa członkowskie prezentowały różne podejścia do budowania potencjału obronnego od strony Afryki, a wojna w Ukrainie w jeszcze większym stopniu skupiła uwagę na wschodzie. Nie powinno to jednak zmniejszać zaangażowania i rozwijania strategii na południu. Wojna w Ukrainie ma konsekwencje dla Morza Śródziemnego, Bliskiego Wschodu i Afryki. Geopolityczne zakusy Rosji

[88] Y. Atalan, *The Future of NATO's Southern Flank*, Center for Strategic & International Studies, 10 VII 2024 r., https://www.csis.org/analysis/future-natos-southern-flank [dostęp: 23 XII 2024]; J. Davidson, *Four steps that NATO's southern flank strategy needs to succeed*, Atlantic Council, 25 VI 2024 r., https://www.atlanticcouncil.org/blogs/new-atlanticist/four-steps-that-natos-southern-flank-strategy-needs-to-succeed/ [dostęp: 23 XII 2024]; A. Polyakova i in., *A New Vision for the Transatlantic Alliance: The Future of European Security, the United States, and the World Order after Russia's War in Ukrain*e, Center for European Policy Analysis, 30 XI 2023 r., https://cepa.org/comprehensive-reports/a-new-vision-for-the-transatlantic-alliance-the-future-of-european-security-the-united-states-and-the-world-order-after-russias-war-in-ukraine/ [dostęp: 23 XII 2024].

[89] S. Colombo, I. Fakir, *NATO, North Africa, and the Sahel: Squaring the triangle of insecurity*, Middle East Institute, 5 VII 2024 r., https://www.mei.edu/publications/nato-north-africa-and-sahel-squaring-triangle-insecurity [dostęp: 23 XII 2024].

[90] *Vilnius Summit Communiqué*, NATO, 11 VII 2023 r., https://www.nato.int/cps/en/natohq/official_texts_217320.htm [dostęp: 23 XII 2024].

oraz rosnąca konkurencja ze strony Chin ujawniły w ciągu ostatniej dekady kwestie bezpieczeństwa wspólne dla wschodu i południa[91].

Aktualne priorytety i wyzwania dla NATO

Geopolityczna stabilność południowej flanki NATO jest bardzo ważna dla bezpieczeństwa państw członkowskich: Francji, Stanów Zjednoczonych, Włoch, Hiszpanii, Turcji i Grecji. Jej utrzymanie wymaga zwiększonej koordynacji i interoperacyjności między sojusznikami operującymi w regionie, zwłaszcza w odniesieniu do najbardziej niestabilnych obszarów, takich jak Maghreb – z wyraźnym naciskiem na sytuację w Libii – oraz Sahel. Narastający wpływ Rosji i Chin na Bliskim Wschodzie oraz w Afryce, a także rozwój organizacji terrorystycznych i sieci przestępczych wskazują na pilną potrzebę przyjęcia przez NATO długoterminowej, zintegrowanej strategii wobec tych regionów. W centrum takiego podejścia powinny się znaleźć działania mające na celu przeciwdziałanie terroryzmowi oraz efektywne zarządzanie migracją. To jedne z najistotniejszych wyzwań dla państw południowej flanki Sojuszu.

Skuteczność działań NATO na tej flance może być osłabiona przez napięcia w relacjach grecko-tureckich, a także przez rozbieżności pomiędzy Francją, Hiszpanią i Włochami w kwestii zaangażowania w kolejne misje wojskowe w Afryce. Brak spójności politycznej i ograniczona gotowość do współpracy mogą utrudniać wypracowanie skoordynowanej odpowiedzi na wyzwania bezpieczeństwa w regionie.

Państwa Afryki Zachodniej, m.in. Senegal, Wybrzeże Kości Słoniowej, Ghana, Togo i Benin, dostrzegają narastające zagrożenie ze strony organizacji terrorystycznych i coraz mocniej apelują o pilne wsparcie ze strony społeczności międzynarodowej. W tym kontekście dla NATO i UE priorytetem powinno być budowanie trwałych więzi politycznych i gospodarczych z krajami położonymi na obrzeżach Sahelu oraz zapewnienie bezpieczeństwa w regionie. Takie podejście nie tylko ograniczyłoby ich zależność od inwestycji strategicznych realizowanych przez Chiny, lecz także utrudniłoby działalność rosyjskich najemników oraz przeciwdziałało wojnie informacyjnej prowadzonej przez państwa trzecie. W szerszej perspektywie działania te przyczyniłyby się do realnego wzmocnienia lokalnych społeczności i zwiększenia odporności całego regionu.

[91] Y. Atalan, *The Future of NATO's Southern Flank*...

Pomimo wysiłków podejmowanych w ciągu ostatnich dziesięciu lat działania NATO jako gwaranta bezpieczeństwa w regionie Sahelu pozostają niespójne i mają ograniczony wpływ. Wynika to przede wszystkim z rozproszonego i trudnego do jednoznacznego zdefiniowania charakteru zagrożeń, które obejmują nie tylko aktywność wielu grup terrorystycznych, lecz także głęboko zakorzenione problemy polityczne, społeczne i gospodarcze. Dodatkowymi wyzwaniami są niejasne ambicje Sojuszu wobec regionu, brak wewnętrznego konsensusu wśród jego członków oraz relatywnie ograniczone wykorzystanie zasobów militarnych.

Relacje NATO z partnerami z Afryki Północnej i Sahelu, w tym z Algierią, Egiptem, Mauretanią, Marokiem i Tunezją, koncentrowały się głównie na zwalczaniu transnarodowej przestępczości oraz wzmacnianiu regionalnych zdolności wojskowych. Chociaż współpraca ta przyczyniła się do częściowego ograniczenia działań ugrupowań terrorystycznych w obszarze śródziemnomorskim, to miała również niezamierzony skutek w postaci przesunięcia aktywności bojowników do środka kontynentu i wzmocnienia struktur terrorystycznych w centralnym Sahelu.

Sytuację utrudnia niejasna i niesprecyzowana polityka państw Europy Zachodniej, która komplikuje wysiłki NATO przez brak konsultacji przy podejmowaniu działań politycznych. Na przykład Francja i Hiszpania prowadzą odmienną politykę wobec Maroka i Algierii, konfrontując się przy problemie Sahary Zachodniej i utrudniając kontakt, który mógłby zostać wykorzystany do stabilizacji sytuacji w Sahelu.

W nadchodzących latach NATO będzie musiało wypracować spójną, realistyczną strategię wobec regionu Sahelu, opartą na współpracy z legalnymi rządami, wybranymi prywatnymi firmami wojskowymi działającymi na ich zlecenie (to może wydawać się niebezpieczne, ale to są realne struktury wojskowe) oraz lokalnymi społecznościami. Tylko takie podejście może doprowadzić do sformułowania skutecznej wizji strategicznej, uwzględniającej złożoność wyzwań charakterystycznych dla tego regionu[92]. Sojusz znajduje się obecnie w punkcie zwrotnym, jeśli chodzi o kształtowanie misji zagranicznych, po zakończeniu zaangażowania w Afganistanie i Iraku, a także wobec ograniczonej obecności w Libii, Syrii i Sahelu. Konieczne jest przemyślenie roli NATO w obszarach niestabilnych i wypracowanie nowych

[92] S. D'Amato, E. Baldaro, *Does the Sahel need NATO?*, ICCT, 26 VIII 2024 r., https://icct.nl/publication/does-sahel-need-nato-0 [dostęp: 24 XII 2024].

modeli działania, które nie będą jedynie powieleniem wcześniejszych interwencji, lecz realną odpowiedzią na zagrożenia XXI w.

Państwa Sahelu, stojące w obliczu narastającego zagrożenia ze strony organizacji terrorystycznych, znajdują się obecnie w sytuacji, w której muszą dokonywać strategicznych wyborów: albo skonfrontują się z Zachodem i strukturami NATO, albo zmierzą się samotnie z rosnącą falą dżihadystycznej przemocy, której ani Rosja, ani Chiny, mimo rosnącej obecności w regionie, nie są w stanie skutecznie powstrzymać. Ta sytuacja stwarza realną szansę dla państw zachodnich na odbudowanie wpływów i zwiększenie swojej wiarygodności jako partnera bezpieczeństwa. W obliczu zmieniającej się architektury zagrożeń NATO powinno rozważyć reorganizację swojej misji w regionie, rozszerzenie zakresu operacji oraz bardziej zdecydowane zaangażowanie wojskowe w państwach zmagających się z długo trwającymi powstaniami dżihadystycznymi.

Migracja

Afryka doświadcza bezprecedensowych przemian demograficznych jako region o najszybszym wzroście liczby ludności na świecie. Do 2050 r. populacja kontynentu wzrośnie z obecnych 1,2 mld do ok. 2,5 mld osób[93]. Co roku na rynek pracy wchodzi od 10 mln do 12 mln młodych Afrykańczyków. Daje to zarówno ogromne możliwości rozwojowe, jak i stwarza poważne wyzwania dla systemów gospodarczych i edukacyjnych. Ponad 60% populacji Afryki to osoby poniżej 25. roku życia i te młode społeczeństwa muszą zmagać się z wieloma trudnościami, takimi jak: terroryzm, represyjna władza czy skrajne ubóstwo. Wyjątkowy profil demograficzny kontynentu czyni Afrykę bardzo ważnym punktem globalnej debaty o przyszłości zatrudnienia, edukacji i mobilności młodych ludzi. Ze względu na brak perspektyw w regionie coraz większa ich liczba poszukuje lepszych warunków życia poza kontynentem. Kierują się głównie do Europy.

Jednym z głównych czynników kryzysu migracyjnego stało się zagrożenie dżihadystyczne. Nasila je wojna prowadzona przez sojusz AES przeciwko Al-Kaidzie i ISIS. Po zerwaniu porozumień z UE przez rządy wojskowe Mali, Nigru i Burkiny Faso szlaki migracyjne wiodące do Maghrebu

[93] *Forecast of the total population of Africa from 2020 to 2050*, Statista, 22 III 2024 r., https://www.statista.com/statistics/1224205/forecast-of-the-total-population-of-africa [dostęp: 27 XII 2024].

i południowych granic Europy zostały ponownie aktywowane. Mimo że administracje Tunezji i Algierii, wspierane finansowo przez UE, podejmują działania mające na celu zawracanie migrantów, nowe trasy przerzutowe nieustannie się rozwijają. Duży niepokój budzi to, że wśród osób przemieszczających się w kierunku Europy znajdują się również bojownicy powiązani z organizacjami terrorystycznymi. Stanowi to poważne zagrożenie dla bezpieczeństwa wewnętrznego państw europejskich.

Wraz z nasilaniem się zmian klimatycznych sytuacja w Afryce, zwłaszcza w regionie Sahelu, coraz bardziej się pogarsza. Pustynnienie i susze zmuszają miliony ludzi do opuszczenia swoich domów, co dodatkowo osłabia i tak już kruchą strukturę społeczno-polityczną. Ta ekologiczna katastrofa tworzy idealne warunki dla grup ekstremistycznych, które rekrutują nowych członków wśród przesiedlonych, zdesperowanych społeczności. Grupy terrorystyczne przekształcają ogromne obszary Sahelu w swoje terytoria, przy czym wykorzystują nieudolność junt wojskowych, które siłą przejęły rządy. Te tereny stały się niemożliwe do kontrolowania przez władze. Europa, która już teraz zmaga się z wyzwaniami związanymi z migracją, stoi przed podwójnym zagrożeniem – kryzysem humanitarnym oraz narastającym terroryzmem, którego skutki coraz częściej ją dotykają.

Droga przez Maghreb i Morze Śródziemne do Hiszpanii, Włoch i Francji jest najbardziej obciążonym szlakiem migracyjnym[94]. Ze względu na rosnącą presję na tę trasę migranci coraz częściej korzystają z alternatywnych korytarzy. Jednym z nich jest szlak wiodący przez Rosję i Białoruś, skąd próbują przekroczyć granice UE i dotrzeć na Litwę, Łotwę oraz do Polski[95]. Ten kierunek, wykorzystywany przez reżimy w Mińsku i Moskwie jako narzędzie politycznego nacisku, stawia graniczne kraje UE w obliczu zarówno kryzysu migracyjnego, jak i zagrożeń związanych z bezpieczeństwem.

Stawka dla Europy i NATO nigdy nie była wyższa. Brak skoordynowanej międzynarodowej strategii wobec złożonych wyzwań Sahelu niesie ryzyko eskalacji kryzysów i braku kontroli nad nimi. Obecna sytuacja będzie prowadzić do większych ruchów migracyjnych oraz bardziej zaawansowanych operacji terrorystycznych wymierzonych w europejskie miasta.

[94] V. Malingre, P. Jacqué, *European Union wants to toughen fight against illegal immigration,* Le Monde, 18 X 2024 r., https://www.lemonde.fr/en/international/article/2024/10/18/european-union-wants-to-toughen-fight-against-illegal-immigration_6729757_4.html [dostęp: 12 XII 2024].

[95] Z. Śliwa, A. Olech, *Wyzwania w kontekście migracji i kryzys na granicy polsko-białoruskiej,* „Wiedza Obronna" 2022, t. 278, nr 1, s. 87–105. https://doi.org/10.34752/2022-d278.

Bez odpowiednich mechanizmów kontroli granic i współpracy międzynarodowej ruchy migracyjne mogą przekształcić się w kryzys, który zdestabilizuje system ochrony nie tylko w państwach granicznych, lecz także w całej UE. Migracja to również rodzaj broni. Tysiące niezidentyfikowanych osób, wśród których są członkowie grup terrorystycznych, mają bezpośredni wpływ na bezpieczeństwo państw UE i NATO, a w tym przypadku możliwość reakcji militarnej jest ograniczona. Dlatego Sojusz jest zobowiązany do ochrony granic[96].

Podsumowanie

W nadchodzących latach deterioracja sytuacji w Sahelu będzie postępować. Wzrost zagrożenia dżihadystycznego, brutalność reżimów wojskowych, zmiany klimatyczne i ruchy migracyjne to kwestie, które będą stanowić źródło wyzwań zarówno dla Afryki, jak i Europy. Obecny stan bezpieczeństwa w Sahelu wskazuje na degradację życia społecznego, ekonomicznego i politycznego. Lokalne armie nie są w stanie kontrolować więcej niż 60% własnego terytorium[97]. Nie ma mowy o inwestycjach czy rozwoju społeczeństw, tak bardzo przecież różniących się od siebie.

Pomoc finansowa dla państw regionu jest zbyt mała. Sahel potrzebuje nowej strategii rozwoju gospodarczego oraz bezpośredniej pomocy wojskowej, takiej jak wsparcie z powietrza, stałe bazy wojskowe czy specjalne operacje przeciw terrorystom realizowane na terytorium Afryki. Pozostawienie terrorystów i rebeliantów samym sobie może wydawać się łatwym i bezpiecznym rozwiązaniem, ale w następnych dziesięcioleciach słabo przygotowane państwa Afryki Zachodniej będą celem dla organizacji terrorystycznych, m.in. ISIS i Al-Kaidy, promujących głównie islamski fundamentalizm.

Państwa Sahelu coraz częściej nawiązują nowe partnerstwa, szczególnie z Chinami, Rosją oraz krajami Półwyspu Arabskiego. W przeciwieństwie do wsparcia finansowego oferowanego przez państwa zachodnie, które często stawiają warunki dotyczące przejrzystości, demokratyzacji i przestrzegania praw człowieka, nowi partnerzy nie wymagają zmian politycznych. Co więcej, zapewniają natychmiastowe korzyści finansowe, co dla junt

[96] Tamże.

[97] A. Antil, *Un an après sa création, une Alliance des États du Sahel qui se cherche*, IFRI, 16 IX 2024 r., https://www.ifri.org/fr/presse-contenus-repris-sur-le-site-presse-lien-externe-avec-citation/un-apres-sa-creation-une [dostęp: 28 XII 2024].

wojskowych rządzących w regionie stanowi istotny czynnik wspierający utrzymanie władzy i kontroli[98].

W obliczu trudnej sytuacji strategią dla NATO jest współpraca z krajami regionu. To oznacza kooperację z państwami położonymi w pobliżu Sahelu, tj. sojuszniczymi dla NATO i Zachodu, aby tam szkolić wojska krajów Afryki i uniemożliwić grupom terrorystycznym rozrost. Nawet jeśli te działania nie będą bezpośrednio związane z krajami Sahelu, NATO i UE i tak będą niedługo zmuszone do interakcji z państwami i organizacjami w Maghrebie i Sahelu.

Z militarnego punktu widzenia ważne jest utrzymanie obecności sił międzynarodowych w Afryce, w pobliżu regionów, gdzie działalność prowadzą ISIS oraz Al-Kaida, a co za tym idzie – tam, gdzie władze wojskowe współpracują z Rosją. Dotyczy to zwłaszcza Mali, Burkiny Faso i Nigru.

Działania militarne powinny być uzupełnione wsparciem ze strony rządów innych krajów Afryki, w tym z Unii Afrykańskiej, które są zaangażowane w regionie. Należy zadbać o pozytywne relacje z ludnością cywilną, co może skutkować większym poszanowaniem prawa konfliktów zbrojnych i praworządności. Siły zbrojne muszą być przykładem wartości promowanych przez państwa regionu i cieszyć się zaufaniem ludności cywilnej. Tego brakuje w Afryce. Utrudnieniem jest kulturowa i etniczna różnorodność tego kontynentu, ale nawet niewielki wspólny mianownik powinien zostać wykorzystany do budowania porozumienia.

Niepokojące jest to, że po ponad dekadzie przemocy pojawia się nowa faza kryzysu. Mimo że istnieją podobieństwa do sytuacji z 2012 r. (przed pojawieniem się wojsk z państw NATO i UE, na czele z operacją „Barkhane"), to obecnie sytuacja bezpieczeństwa w centralnym Sahelu jest bardziej skomplikowana. Region jest coraz bardziej niestabilny i jednocześnie maleje w nim wpływ organizacji międzynarodowych. Niedocenienie powagi sytuacji i zlekceważenie narastania złożonych problemów w Sahelu sprawi, że za kilka lat decyzje, które NATO będzie podejmowało w odniesieniu do tego regionu, będą miały tylko wymiar misji wojskowych. Współczesny kryzys w Sahelu nie może więc pozostać bez odpowiedzi. Pierwszym krokiem powinno być wypracowanie politycznej obecności w regionie, następnie szkolenie afrykańskich żołnierzy, a później wdrożenie środków mających na celu skuteczne monitorowanie sytuacji i zarządzanie nią, żeby minimalizować straty, przede wszystkim w ludziach.

[98] A. Olech, *Grupa Wagnera w Afryce. Pozorowana walka rosyjskich najemników z terroryzmem*, „Terroryzm – studia, analizy, prewencja" 2024, nr 5, s. 53–89. https://doi.org/10.4467/27204383TER.24.002.19390.

Trzeba wykorzystać istniejącą szansę, ponieważ w Europie wzrasta zagrożenie terroryzmem. Federacja Rosyjska i inne wrogie Sojuszowi państwa realizują bardzo aktywną politykę w regionie Sahelu, co wymaga zdecydowanej odpowiedzi ze strony NATO i partnerów. Wyzwanie w postaci jednoczesnego zaangażowania na wschodniej i południowej flance może się okazać dla Sojuszu i UE zbyt duże.

Bibliografia

As-Sazid S., *Emerging Security Challenges in the Sahel and the Need for an Adaptative Approach towards Peacebuilding*, „International Day of United Nations Peacekeepers Journal" 2023, t. 9, nr 9, s. 17–34.

Benjaminsen T.A., Svarstad H., *Climate Change, Scarcity and Conflicts in the Sahel*, w: T.A. Benjaminsen, H. Svarstad, *Political Ecology. A Critical Engagement with Global Environmental Issues*, bmw 2021, s. 183–205. https://doi.org/10.1007/978-3-030-56036-2_8.

Lounnas D., *Le djihadisme au Sahel après la chute de Daech*, „Politique étrangère" 2019, nr 2, s. 105–114.

Olech A., *Grupa Wagnera w Afryce*, Defence24.

Olech A., *Grupa Wagnera w Afryce. Pozorowana walka rosyjskich najemników z terroryzmem*, „Terroryzm – studia, analizy, prewencja" 2024, nr 5, s. 53–89. https://doi.org/10.4467/27204383TER.24.002.19390.

Śliwa Z., Olech A., *Wyzwania w kontekście migracji i kryzys na granicy polsko-białoruskiej*, „Wiedza Obronna" 2022, t. 278, nr 1, s. 87–105. https://doi.org/10.34752/2022-d278.

Źródła internetowe

Al Qaeda affiliate says 200 soldiers killed in Burkina Faso attack, Reuters, 16 V 2025 r., https://www.reuters.com/world/africa/al-qaeda-affiliate-says-200-soldiers-killed--attack-burkina-military-site-reports-2025-05-15/ [dostęp: 16 V 2025].

Antil A., *Un an après sa création, une Alliance des États du Sahel qui se cherche*, IFRI, 16 IX 2024 r., https://www.ifri.org/fr/presse-contenus-repris-sur-le-site-presse-lien--externe-avec-citation/un-apres-sa-creation-une [dostęp: 28 XII 2024].

Atalan Y., *The Future of NATO's Southern Flank*, Center for Strategic & International Studies, 10 VII 2024 r., https://www.csis.org/analysis/future-natos-southern-flank [dostęp: 23 XII 2024].

Banchereau M., *US hands over its last military base in Niger to the ruling junta*, The Associated Press, 7 VIII 2024 r., https://apnews.com/article/niger-united-states-troops-army-military-bases-junta-sahel-coup-1ae5334bc68eb6b45e1e2d612bfb2b6f [dostęp: 5 I 2025].

Bhattacharya S., *China's Great Game in the Sahel*, Vivekananda International Foundation, 12 X 2022 r., https://www.vifindia.org/article/2022/china-s-great-game-in-the-sahel [dostęp: 7 XII 2024].

Bihan J. le, *Former Niger minister launches movement to overthrow junta*, The Africa Report, 27 IX 2024 r., https://www.theafricareport.com/363047/former-niger-minister-launches-movement-to-overthrow-junta/ [dostęp: 5 I 2025].

Borrell J., *Together for the security, stability and development of the Sahel*, European Union External Action, 8 V 2020 r., https://www.eeas.europa.eu/eeas/together-security-stability-and-development-sahel_en [dostęp: 27 V 2025].

Breton L., *Terrorisme: l'État islamique avait des projets d'attentats visant les Jeux olympiques de Paris et l'Euro de football*, La Depeche, 17 VI 2024 r., https://www.ladepeche.fr/2024/06/17/terrorisme-letat-islamique-avait-des-projets-dattentats-visant-les-jeux-olympiques-de-paris-et-leuro-de-football-12022418.php [dostęp: 21 XI 2024].

Burkina Faso: Unlawful Killings, 'Disappearances' by the Army, Human Rights Watch, 29 VI 2023 r., https://www.hrw.org/news/2023/06/29/burkina-faso-unlawful-killings-disappearances-army [dostęp: 5 I 2025].

Center for Preventive Action, *Violent Extremism in the Sahel*, Council on Foreign Relations, 23 X 2024 r., https://www.cfr.org/global-conflict-tracker/conflict/violent-extremism-sahel [dostęp: 16 XII 2024].

Colombo S., Fakir I., *NATO, North Africa, and the Sahel: Squaring the triangle of insecurity*, Middle East Institute, 5 VII 2024 r., https://www.mei.edu/publications/nato-north-africa-and-sahel-squaring-triangle-insecurity [dostęp: 23 XII 2024].

Crisis in Burkina Faso: What you need to know and how you can help, International Rescue Committee, 14 II 2024 r., https://www.rescue.org/article/crisis-burkina-faso-what-you-need-know-and-how-you-can-help [dostęp: 5 I 2025].

Czerep J., *Konsekwencje powołania Konfederacji Państw Sahelu*, Polski Instytut Spraw Międzynarodowych, 14 VIII 2024 r., https://www.pism.pl/publikacje/konsekwencje-powolania-konfederacji-panstw-sahelu [dostęp: 15 I 2025].

D'Amato S., Baldaro E., *Does the Sahel need NATO?*, ICCT, 26 VIII 2024 r., https://icct.nl/publication/does-sahel-need-nato-0 [dostęp: 24 XII 2024].

David T., *Troops Foil Boko Haram, ISWAP Drone Attack In Buni Gari*, Leadership, https://leadership.ng/troops-foil-boko-haram-iswap-drone-attack-in-buni-gari/ [dostęp: 5 I 2025].

Davidson J., *Four steps that NATO's southern flank strategy needs to succeed*, Atlantic Council, 25 VI 2024 r., https://www.atlanticcouncil.org/blogs/new-atlanticist/four-steps-that-natos-southern-flank-strategy-needs-to-succeed/ [dostęp: 23 XII 2024].

Deaths Linked to Militant Islamist Violence in Africa Continue to Spiral, Africa Center for Strategic Studies, 29 I 2024 r., https://africacenter.org/spotlight/mig2024-deaths-militant-islamist-violence-africa-rise/ [dostęp: 5 I 2025].

Defining a New Approach to the Sahel's Military-led States, International Crisis Group, 22 V 2025 r., https://www.crisisgroup.org/africa/sahel/burkina-faso-mali-niger/defining-new-approach-sahels-military-led-states [dostęp: 27 V 2025].

Desert to Power initiative, African Development Bank Group, https://www.afdb.org/en/topics-and-sectors/initiatives-partnerships/desert-power-initiative [dostęp: 15 XII 2024].

Dieng A., *The Sahel: Challenges and opportunities*, „International Review of the Red Cross" 2021, t. 103, nr 918, s. 765–779, https://international-review.icrc.org/articles/editorial-the-sahel-challenges-opportunities-adama-dieng-918 [dostęp: 15 XII 2024]. https://doi.org/10.1017/S1816383122000339.

Douce S., *Burkina Faso's Djibo city struggles under jihadist siege*, La Croix International, 7 XI 2024 r., https://international.la-croix.com/world/burkina-fasos-djibo-city-struggles-under-jihadist-siege [dostęp: 5 I 2025].

Doxsee C., Thompson J., Harris M., *The End of Operation Barkhane and the Future of Counterterrorism in Mali*, Center for Strategic & International Studies, 2 III 2022 r., https://www.csis.org/analysis/end-operation-barkhane-and-future-counterterrorism-mali [dostęp: 19 XII 2024].

Duhamel J., *Central Sahel – Map of jihadist militant groups activity (Jan–May 2024)*, Jules Duhamel, 21 VI 2024 r., https://www.julesduhamel.com/central-sahel-map-of-jihadist-militant-groups-activity-jan-may-2024/ [dostęp: 15 I 2025].

Ecological Threat Report 2024. Analysing ecological threats, resilience & peace, The Institute for Economics & Peace, https://www.economicsandpeace.org/wp-content/uploads/2024/10/ETR-2024-web.pdf [dostęp: 15 XII 2024].

Ehl D., *How the Russian Wagner Group is entrenching itself in Africa*, Deutsche Welle, 27 X 2024 r., https://www.dw.com/en/russia-kremlin-wagner-group-influence-in-central-african-republic-sudan-mali/a-70599853 [dostęp: 5 I 2025].

Estonia's strategy for Africa, Republic of Estonia Ministry of Foreign Affairs, 7 V 2021 r., https://vm.ee/en/estonias-strategy-africa [dostęp: 11 XII 2024].

European Parliament, *New EU strategic priorities for the Sahel. Addressing regional challenges through better governance*, https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/696161/EPRS_BRI%282021%29696161_EN.pdf [dostęp: 14 XII 2024].

Fakhry A., *More than borders: effects of EU interventions on migration in the Sahel*, Institute for Security Studies, 16 VIII 2023 r., https://issafrica.org/research/west-africa-report/more-than-borders-effects-of-eu-interventions-on-migration-in-the-sahel [dostęp: 30 XII 2024].

Fleming L., Issoufou T.I., *Niger confirms anti-junta rebels behind oil attack*, BBC, 22 VI 2024 r., https://www.bbc.com/news/articles/c511n4edl7lo [dostęp: 5 I 2025].

Forecast of the total population of Africa from 2020 to 2050, Statista, 22 III 2024 r., https://www.statista.com/statistics/1224205/forecast-of-the-total-population-of-africa [dostęp: 27 XII 2024].

G5 Sahel Region: Country Climate and Development Report – Annex, World Bank Group, https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099150106302237600/p1773430dc79a10c09f600cf2ac1e0e9f3 [dostęp: 27 V 2025].

Global Terrorism Index 2025, Institute for Economics & Peace, https://www.visionofhumanity.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf [dostęp: 27 V 2025].

Grammer R., *Top counterterrorism official warns of ISIS' rapid rise in Africa*, Politico, 25 XI 2024 r., https://www.politico.com/news/2024/11/25/top-counterterrorism-official-warns-of-isiss-rapid-rise-in-africa-00191571 [dostęp: 20 XII 2024].

Hauchard A., *In Violence-shattered Central Mali, Victims Recount Their Lives*, Barron's, 9 II 2022 r., https://www.barrons.com/news/in-violence-shattered-central-mali-victims-recount-their-lives-01644458408 [dostęp: 5 I 2025].

Ibrahim H.O., *The Sahel – a Land of Opportunity*, United Nations, 10 VI 2019 r., https://unpartnerships.un.org/news/2019/sahel-land-opportunity [dostęp: 14 XII 2024].

Independent expert group supporting NATO's comprehensive and deep reflection process on the southern neighbourhood. Final Report. May 2024, NATO, https://nato.int/nato_static_fl2014/assets/pdf/2024/5/pdf/240507-NATO-South-Report.pdf [dostęp: 16 XII 2024].

Islamic State group nearly doubled its Mali territory in under a year, UN says, France 24, 26 VIII 2023 r., https://www.france24.com/en/africa/20230826-islamic-state-group-doubled-controlled-territory-in-mali-in-under-a-year-un-experts-say [dostęp: 5 I 2025].

Jadoon A., Sayed A., Webber L., Valle R., *From Tajikistan to Moscow and Iran: Mapping the Local and Transnational Threat of Islamic State Khorasan*, „CTC Sentinel" 2024, t. 17, nr 5, https://ctc.westpoint.edu/from-tajikistan-to-moscow-and-iran-mapping-the-local-and-transnational-threat-of-islamic-state-khorasan/ [dostęp: 5 I 2025].

Jeannin M., *Ghana worries about rise of terrorist threat in Gulf of Guinea*, Le Monde, 7 VI 2022 r., https://www.lemonde.fr/en/le-monde-africa/article/2022/06/07/ghana-concerned-about-extension-of-terrorist-threat-to-coastal-states-of-gulf-of-guinea_5985936_124.html [dostęp: 5 I 2025].

Joscelyn T., *Analysis: Al Qaeda groups reorganize in West Africa*, FDD's Long War Journal, 13 III 2017 r., https://www.longwarjournal.org/archives/2017/03/analysis-al-qaeda-groups-reorganize-in-west-africa.php [dostęp: 5 I 2025].

Kadivar J., *Exploring Takfir, Its Origins and Contemporary Use: The Case of Takfiri Approach in Daesh's Media*, „Sage Journals" 2020, t. 7, nr 3, https://journals.sagepub.com/doi/full/10.1177/2347798920921706 [dostęp: 5 I 2025]. https://doi.org/10.1177/2347798920921706.

Karr L., *Africa File, April 24, 2025: JNIM's Growing Pressure on Benin; Turkey to Somalia; Salafi-Jihadi Cells Continue to Grow Across Nigeria*, Critical Threats, 24 IV 2025 r., https://www.understandingwar.org/backgrounder/africa-file-april-24-2025-jnim%E2%80%99s-growing-pressure-benin-turkey-somalia-salafi-jihadi/ [dostęp: 20 V 2025].

Kasroui S., *Morocco's BCIJ Foils Terrorist Plot, Arrests 4 ISIS-Affiliated Suspects Near Casablanca*, Marocco World News, 26 I 2025 r., https://www.moroccoworldnews.com/2025/01/367913/morocco-s-bcij-foils-terrorist-plot-arrests-4-isis-affiliated--suspects-near-casablanca [dostęp: 20 V 2025].

Kum P., *Niger: L'ancien rebelle nigérien, Rhissa Ag Boula, annonce son intention de reprendre les armes pour chasser les putschistes*, Alwihda Info, 21 VIII 2023 r., https://www.alwihdainfo.com/Niger-L-ancien-rebelle-nigerien-Rhissa-Ag-Boula-annonce-son-intention-de-reprendre-les-armes-pour-chasser-les_a125857.html [dostęp: 5 I 2025].

Maclean R., Jammeh S., *Africa Received Billions in U.S. Aid. Here's What It Will Lose*, The New York Times, 8 III 2025 r., https://www.nytimes.com/2025/03/08/world/africa/africa-usaid-funds.html/ [dostęp: 20 IV 2025].

Mali and Niger rebels met to 'strengthen' ties amid political turmoil, Al Arabiya News, 2 IX 2024 r., https://english.alarabiya.net/News/world/2024/09/02/mali-and-niger--rebels-met-to-strengthen-ties-amid-political-turmoil [dostęp: 5 I 2025].

Malingre V., Jacqué P., *European Union wants to toughen fight against illegal immigration*, Le Monde, 18 X 2024 r., https://www.lemonde.fr/en/international/article/2024/10/18/european-union-wants-to-toughen-fight-against-illegal-immigration_6729757_4.html [dostęp: 12 XII 2024].

Marangio R., *Sahel reset: time to reshape the EU's engagement*, European Union Institute for Security Studies, 5 II 2024 r., https://www.iss.europa.eu/publications/briefs/sahel-reset-time-reshape-eus-engagement [dostęp: 15 XII 2024].

Martin G., *Burkina Faso receives huge batch of Chinese military equipment*, Defence Web, 27 VI 2024 r., https://www.defenceweb.co.za/land/land-land/burkina-faso-receives-huge-batch-of-chinese-military-equipment [dostęp: 12 XII 2024].

McMakin W., *UN food agency says 40 million people are struggling to feed themselves in West and Central Africa*, AP, 20 XII 2024 r., https://apnews.com/article/africa-food--insecurity-hunger-304b66ef7b9b56262fe1114a4b28c7e6 [dostęp: 26 XII 2024].

Military juntas in Africa's 'coup belt' fail to contain extremist violence, Financial Times, 24 XI 2024 r., https://www.ft.com/content/d0af5533-ecdd-4be0-bbb8-e5b3e-4bb11b4 [dostęp: 30 XII 2024].

Mintoiba F., *Footsteps of change: Rising influence of China and Russia in Africa*, Daily Sabah, 3 X 2024 r., https://www.dailysabah.com/opinion/op-ed/footsteps-of-change-rising-influence-of-china-and-russia-in-africa [dostęp: 7 XII 2024].

More than 50 million in West and Central Africa at risk of hunger, United Nations, 9 V 2025 r., https://news.un.org/en/story/2025/05/1163086 [dostęp: 30 V 2025].

Morocco: ISIS-instigated plot foiled, 12 suspects arrested, The North Africa Post, 19 II 2025 r., https://northafricapost.com/84516-morocco-isis-instigated-terror-plot-foiled-12-suspects-arrested.html [dostęp: 20 V 2025].

Moscow's winning return to Africa, Le Monde, 21 VIII 2024 r., https://www.lemonde.fr/en/international/article/2024/08/21/moscow-s-winning-return-to-africa_6719241_4.html [dostęp: 7 XII 2024].

Nasr W., *ISIS in Africa: The End of the „Sahel Exception"*, New Lines Institute, 2 VI 2020 r., https://newlinesinstitute.org/nonstate-actors/isis-in-africa-the-end-of-the-sahel-exception/ [dostęp: 10 I 2025].

NATO, *Strategic foresight analysis. Regional perspectives report on North Africa and the Sahel*, https://www.act.nato.int/wp-content/uploads/2023/05/NU_SFA_Report_North_Africa_and_the_Sahel_SACT_approved_final_edited_version.pdf [dostęp: 14 XII 2024].

Nsaibia H., *Actor Profile: Jama'at Nusrat al-Islam wal-Muslimin (JNIM)*, Armed Conflict Location & Event Data, 13 XI 2023 r., https://acleddata.com/2023/11/13/actor-profile-jamaat-nusrat-al-islam-wal-muslimin-jnim/ [dostęp: 5 I 2025].

Nsaibia H., *Actor Profile: Volunteers for the Defense of the Homeland (VDP)*, Armed Conflict Location & Event Data, 26 III 2024 r., https://acleddata.com/2024/03/26/actor-profile-volunteers-for-the-defense-of-the-homeland-vdp/ [dostęp: 5 I 2025].

Nsaibia H., Weiss C., *The End of the Sahelian Anomaly: How the Global Conflict between the Islamic State and al-Qa`ida Finally Came to West Africa*, „CTC Sentinel" 2020, t. 13, nr 7, s. 1–14, https://ctc.westpoint.edu/wp-content/uploads/2020/07/CTC-SENTINEL-072020.pdf [dostęp: 5 I 2025].

Olech A., *Francja i USA będą ponownie wojskowo współpracować w Afryce*, Defence24, 20 II 2024 r., https://defence24.pl/geopolityka/francja-i-usa-beda-ponownie-wojskowo-wspolpracowac-w-afryce [dostęp: 11 XII 2024].

Olech A., *French Operation Barkhane in Africa – success or failure?*, Stosunki Międzynarodowe – International Relations, 18 XII 2023 r., https://internationalrelations-publishing.org/articles/3-17 [dostęp: 3 XII 2024]. https://doi.org/10.12688/stomiedintrelat.17737.1.

Olech A., *Współpraca państw Maghrebu z NATO na rzecz bezpieczeństwa w regionie*, Instytut Nowej Europy, 12 X 2021 r., https://ine.org.pl/wspolpraca-panstw-maghrebu-z-nato-na-rzecz-bezpieczenstwa-w-regionie/ [dostęp: 19 XII 2024].

Olech A., Wójcik P., *Wojna o Sahel [Raport]*, Defence24, 17 XI 2024 r., https://defence24.pl/geopolityka/wojna-o-sahel-raport [dostęp: 15 XII 2024].

Olech A., Wójtowicz B., *Rywalizacja o surowce w Sahelu – region konfliktu mocarstw*, Trimarium.pl, 18 XI 2022 r., https://trimarium.pl/projekt/rywalizacja-o-surowce-w-sahelu-region-konfliktu-mocarstw/ [dostęp: 7 XII 2024].

Pertier E., *After Military Took Power, Terrorist Attacks Only Got Worse*, The New York Times, 22 XII 2024 r., https://www.nytimes.com/2024/12/22/world/africa/niger-war-coup.html [dostęp: 5 I 2025].

Phillips M.M., Faucon B., *U.S. Forces Try to Regroup as al Qaeda, Islamic State Sow Terror in West Africa*, The Wall Street Journal, 11 IX 2024 r., https://www.wsj.com/world/africa/u-s-moves-aircraft-commandos-into-west-africa-in-fight-against-islamist-militants-0b15c41b [dostęp: 11 XII 2024].

Polyakova A., Lucas E., Boulègue M., Sendak C., Kindsvater S., Kuz I., Stone S., *A New Vision for the Transatlantic Alliance: The Future of European Security, the United States, and the World Order after Russia's War in Ukrain*e, Center for European Policy Analysis, 30 XI 2023 r., https://cepa.org/comprehensive-reports/a-new-vision-for-the-transatlantic-alliance-the-future-of-european-security-the-united-states-and-the-world-order-after-russias-war-in-ukraine/ [dostęp: 23 XII 2024].

Portillo L.V. del, *Challenges in the Sahel: Opportunities for Europe*, Eurodefense Network, 21 II 2021 r., https://eurodefense.eu/2021/02/21/challenges-in-the-sahel-opportunities-for-europe/ [dostęp: 18 XII 2024].

Raineri L., Strazzari F., *Jihadism in Mali and the Sahel: evolving dynamics and patterns*, European Union Institute for Security Studies, 29 VI 2017 r., https://www.iss.europa.eu/publications/briefs/jihadism-mali-and-sahel-evolving-dynamics-and-patterns [dostęp: 16 XII 2024].

Renoult J., *L'Italie, dernier partenaire occidental du Niger*, Le Monde, 23 VII 2024 r., https://www.lemonde.fr/afrique/article/2024/07/23/l-italie-ultime-partenaire-occidental-du-niger_6256111_3212.html [dostęp: 6 XII 2024].

Roger B., Eydoux T., *Drones turcs, avions russes… au Sahel, la guerre des airs est déclarée*, Le Monde, 20 XI 2024 r., lemonde.fr/afrique/article/2024/11/20/drones-turcs-avions-russes-au-sahel-la-guerre-des-airs-est-declaree_6405083_3212.html [dostęp: 7 XII 2024].

Sahel, Britannica, https://www.britannica.com/place/Sahel [dostęp: 14 XII 2024].

Sahel Showdown: How Türkiye Can Help NATO With Russian and Chinese Advances, TRT World Research Centre, 29 VII 2024 r., https://researchcentre.trtworld.com/featured/perspectives/sahel-showdown-how-turkiye-can-help-nato-with-russian--and-chinese-advances/ [dostęp: 10 XII 2024].

Sanjuan L., *Los soldados más temidos del mundo: hay una unidad española*, AS, 24 X 2024 r., https://as.com/actualidad/politica/los-soldados-mas-temidos-del-mundo-n [dostęp: 4 XII 2024].

Tesfaye B., *Climate Change and Conflict in the Sahel*, Council on Foreign Relations, November 2022, https://www.cfr.org/report/climate-change-and-conflict-sahel [dostęp: 27 V 2025].

The Federal Government realigns its Sahel policy, Federal Foreign Office, 3 V 2023 r., https://www.auswaertiges-amt.de/en/newsroom/news/2595298-2595298 [dostęp: 4 XII 2024].

Toutate I., *BCIJ Links 'Highly Dangerous' Foiled Terror Plot to Sahel Terrorist Groups*, Morocco World News, 24 II 2025 r., https://www.moroccoworldnews.com/2025/02/174948/bcij-links-highly-dangerous-foiled-terror-plot-to-sahel-terrorist-groups/ [dostęp: 20 V 2025].

Tuareg rebels driven out of Timbuktu, Al Jazeera, 29 VI 2012 r., https://www.aljazeera.com/news/2012/6/29/tuareg-rebels-driven-out-of-timbuktu [dostęp: 5 I 2025].

US military says withdrawal from Niger is complete, France24, 16 IX 2024 r., https://www.france24.com/en/live-news/20240916-us-military-says-withdrawal-from-niger-is-complete [dostęp: 5 I 2025].

US troops pull out of Niger's Air Base 101, Reuters, 8 VII 2024 r., https://www.reuters.com/world/africa/us-troops-pull-out-nigers-air-base-101-2024-07-07/ [dostęp: 5 I 2025].

Vilnius Summit Communiqué, NATO, 11 VII 2023 r., https://www.nato.int/cps/en/natohq/official_texts_217320.htm [dostęp: 23 XII 2024].

Weiss C., *AQIM's Imperial Playbook. Understanding al-Qa'ida in the Islamic Maghreb's Expansion into West Africa*, bmw, April 2022, https://ctc.westpoint.edu/wp-content/uploads/2022/04/AQIMs-Imperial-Playbook.pdf [dostęp: 5 I 2025].

Weiss C., *Tuareg rebels, JNIM each claim victory over Russia's Wagner Group in Mali*, Foundation for Defense of Democracies, 29 VII 2024 r., https://www.fdd.org/analysis/op_eds/2024/07/29/tuareg-rebels-jnim-each-claim-victory-over-russias-wagner-group-in-mali/ [dostęp: 5 I 2025].

Wójcik J., *Sahel pogrąża się w terrorystycznej rebelii*, Defence24, 30 IX 2023 r., https://defence24.pl/geopolityka/sahel-pograza-sie-w-terrorystycznej-rebelii [dostęp: 12 XII 2024].

Wójcik P., wpis na portalu X, 19 I 2025 r., https://x.com/SaladinAlDronni/status/1881013944443363547 [dostęp: 24 I 2025].

Zelin A.Y., *The Islamic State on the March in Africa*, The Washington Institute for Near East Policy, 1 III 2024 r., https://www.washingtoninstitute.org/policy-analysis/islamic-state-march-africa [dostęp: 5 I 2025].

Zelin A.Y., Cahn S., *Exploiting a „Vast jihad Arena": The Islamic State Takes Territory in Mali*, The Washington Institute for Near East Policy, 26 IX 2023 r., https://www.washingtoninstitute.org/policy-analysis/exploiting-vast-jihad-arena-islamic-state-takes-territory-mali [dostęp: 5 I 2025].

Zenn J., *Brief: JNIM Attacks in Benin Represented Group's Growing Operational Strength in Periphery*, The Jamestown Foundation, 11 XII 2024 r., https://jamestown.org/program/brief-jnim-attacks-in-benin-represented-groups-growing-operational-strength-in-periphery/ [dostęp: 5 I 2025].

Dr Aleksander Olech

Szef Działu Współpracy Międzynarodowej w Defence24 oraz redaktor naczelny Defence24.com. Wykładowca na uczelniach krajowych i zagranicznych, współpracownik NATO, analityk i publicysta. Były zastępca dyrektora Departamentu Afryki i Bliskiego Wschodu Ministerstwa Spraw Zagranicznych. Absolwent Europejskiej Akademii Dyplomacji oraz Akademii Sztuki Wojennej. Główne zainteresowania badawcze: relacje francusko-rosyjskie, wyzwania w Afryce oraz polityka bezpieczeństwa NATO.

Kontakt: a.olech@defence24.pl

Paweł Wójcik

Badacz terroryzmu islamskiego. Ekspert w Opportunity Institute for Foreign Affairs. Specjalizuje się w tematyce dotyczącej Państwa Islamskiego i Al-Kaidy oraz w ocenie ryzyka związanego z działalnością tych organizacji. Jego zainteresowania badawcze obejmują także politykę w Syrii, linię Duranda oraz region Sahelu.

Kontakt: chrzestogniapl@gmail.com

Terroryzm – studia, analizy, prewencja, 2025, nr 7: 139–177

https://doi.org/10.4467/27204383TER.25.028.21805

Artykuł

Ochrona biologiczna towarów i usług mogących zostać użytych jako broń lub środek terroru

Biosecurity of dual-use items

ANNA BIELECKA-ODER https://orcid.org/0009-0002-6952-0023

Polskie Towarzystwo Bezpieczeństwa Narodowego

Abstrakt

Większość czynników biologicznych wykorzystywanych w charakterze wrogim jest jednocześnie czynnikami chorób szczególnie niebezpiecznych i wysoce zakaźnych, stanowiących zagrożenie zdrowia publicznego. Sposób, w jaki te czynniki zostaną wykorzystane, jest determinowany głównie przez czynnik ludzki. Postęp w naukach biotechnologicznych z jednej strony przyczynił się m.in. do zakończenia pandemii COVID-19 (szczepionki mRNA), z drugiej jednak otworzył drogę dla prowadzenia zaawansowanych badań z wykorzystaniem czynników biologicznych w nieetycznych celach. Praca stanowi wprowadzenie do problematyki ochrony biologicznej. Przedstawia pojęcie ochrony biologicznej w sposób przekrojowy, w ujęciu międzynarodowych porozumień rozbrojeniowych i nieproliferacyjnych w zakresie broni biologicznej i toksynowej oraz nawiązujących do nich przepisów. Autorka dokonuje przeglądu i analizy środków służących zabezpieczeniu i ochronie czynników biologicznych oraz związanych z nimi technologii, w odniesieniu do działalności szczególnie podatnych na nadużycia w obszarze tego rodzaju ochrony. Skuteczne przeciwdziałanie zagrożeniom biologicznym wymaga interdyscyplinarnego podejścia do kwestii ochrony biologicznej. Stawką jest zapobieżenie użyciu materiałów biologicznych o potencjale podwójnego zastosowania w charakterze broni lub środka terroru.

Słowa kluczowe

ochrona biologiczna, traktaty międzynarodowe, produkty podwójnego zastosowania

Abstract

Most of biological warfare agents are simultaneously serious biological threats for public health. The way in which these factors are used is mainly determined by the anthropogenic factor. Accelerated progress in life sciences and biological engineering stopped the COVID-19 pandemic (mRNA vaccine), on the other hand, opened the way for advanced research using biological agents for unethical purposes. The paper provides an introduction to biological security issues. It presents the concept of biological security in a cross-cutting manner, in terms of international disarmament, non-proliferation agreements on biological and toxin weapons as well as the regulations referring to them. The author reviews and analyses measures to secure and protect biological agents and related technologies, with reference to activities particularly vulnerable to abuse in the area of such protection. Effective countering of biological threats requires an interdisciplinary approach to biosecurity. At stake is the prevention of the use of biological materials with dual-use potential as a weapon or terrorist agent.

Keywords

biosecurity, multilateral treaties, dual-use items

Zagrożenie biologiczne

Przyjęło się powszechnie, że zagrożenie biologiczne powodują głównie czynniki biologiczne – bakterie, wirusy, toksyny biologiczne[1]. Źródłami zagrożenia mogą być np. bakteria *Bordetella pertusis*, która wywołuje krztusiec – chorobę wysoce zakaźną, stanowiącą zagrożenie zdrowia publicznego, oraz bakteria *Bacillus anthracis* będąca przyczyną wąglika. Z uwagi na wiele czynników (m.in. środowiskowych, biologicznych, epidemiologicznych, zdrowotnych, medycznych, społecznych, socjalnych, behawioralnych, etnograficznych, geopolitycznych) i ich zmiennych wąglik może stwarzać zagrożenie na różnym poziomie. Może stanowić zagrożenie

[1] Artykuł bazuje na zagadnieniach analizowanych w rozprawie doktorskiej autorki. W artykule dokonano aktualizacji tekstu oraz uzupełnień o wątki dotyczące zdarzeń, które zaistniały po wrześniu 2018 r.

epidemiczne lub zdrowia publicznego, jeśli dotyczy zachorowań wśród ludzi, a także zagrożenie endemiczne, jeśli dotyczy określonej populacji albo powszechnie występuje w danym regionie geograficznym. Laseczka wąglika może ponadto powodować zagrożenie epizootyczne, jeśli dotyczy zachorowań wśród zwierząt, jak również zagrożenie terrorystyczne w przypadku celowego spowodowania zachorowań wśród ludzi i/lub zwierząt. Ze względu na możliwość występowania różnych postaci wąglika wśród ludzi (płucna, skórna, żołądkowo-jelitowa), wymagających zastosowania nieco odmiennych rodzajów terapii i działań poekspozycyjnych, ocena ryzyka zachorowania na tę chorobę jest złożona i wykracza poza właściwość pojedynczej dyscypliny naukowej.

Następstwem istnienia zagrożenia powodowanego przez czynniki biologiczne może być to, że technologia stosowana do selekcji, proliferacji czy modyfikacji mikroorganizmów lub aparatura przeznaczona do syntez biologicznych czy biotransformacji stosowanych w produkcji, izolacji i oczyszczaniu produktów pochodzenia organicznego (białek, w tym toksyn) mogą zostać wykorzystane niewłaściwie. Na przykład bioreaktor (fermentor) stosowany do produkcji bakterii w warunkach hodowli ciągłej na dużą skalę może być wykorzystywany dwojako w zależności od jego przeznaczenia, tj. jako sprzęt zakazany przez prawo międzynarodowe, jeśli używa się go do produkcji czynników biologicznych dla celów bojowych, i jako sprzęt dozwolony do stosowania i rozpowszechniania, jeśli używa się go do wytwarzania czynników biologicznych dla celów pokojowych, np. ochrony zdrowia (produkcji szczepionek, antybiotyków, leków przeciwwirusowych, białek terapeutycznych) czy ochrony środowiska (produkcji środków ochrony roślin). W obu tych przypadkach podczas wytwarzania są stosowane ta sama technologia i oprzyrządowanie. Dlatego też w czasie wstępnych oględzin miejsca zdarzenia niejednokrotnie trudno rozstrzygnąć, czy działalność, której przedmiotem jest produkcja mikroorganizmów lub toksyn biologicznych, jest prowadzona w celach pokojowych, wrogich czy jednych i drugich. Z uwagi na dualistyczną naturę technologii wykorzystującej żywe układy biologiczne w produkcji przemysłowej określa się ją mianem technologii podwójnego zastosowania. Niewielka jej modyfikacja może sprawić, że zacznie służyć celom ofensywnym zamiast defensywnym[2].

[2] Przy złej intencji do powstania zagrożenia biologicznego może dojść za pośrednictwem urządzeń wykorzystywanych również przez inne gałęzie przemysłu, np. urządzeń służących do produkcji paliw czy instalacji przeznaczonych do prowadzenia fermentacji napojów

Zapewnienie skutecznej ochrony biologicznej jest dużym wyzwaniem. Wynika to z wielości czynników, które mają na to wpływ. Należą do nich m.in.: profil działalności człowieka i cele, jakie mu przyświecają, różnorodność czynników biologicznych, możliwość ich modyfikowania na różnych etapach ekspresji genów, wielorakość procesów i metod biotechnologicznych, zmienność uwarunkowań środowiskowych wpływających na rozmieszczenie i dostępność nie tylko samych czynników, lecz także wektorów (nośników) chorób zakaźnych, różne sposoby ich uwolnienia, swoistość uwarunkowań osobniczych na poziomie komórkowym, mających bezpośredni wpływ na podatność na zachorowanie.

Międzynarodowe porozumienia w zakresie ochrony biologicznej

Szerokie spektrum działalności prowadzonych przez człowieka oraz zagrożeń biologicznych będących ich następstwem powoduje, że pomimo wspólnego celu, jakim jest skuteczna ochrona biologiczna, środki mające służyć jej zapewnieniu mogą być odmienne. Nad koncepcjami tej ochrony debatowali interesariusze z wielu środowisk, w tym specjaliści z zakresu prawa międzynarodowego zajmujący się zakazem stosowania broni biologicznej i toksynowej, z zakresu ochrony środowiska i różnorodności biologicznej, zdrowia publicznego i epidemiologii, ochrony zdrowia zwierząt, ochrony fitosanitarnej, ochrony zdrowia personelu w laboratorium, reagowania na wypadek kryzysu zdrowotnego, a także przedstawiciele wielu środowisk akademickich. Każde z tych środowisk za wiodące wskazywało te postulaty, które były zbieżne z jego subiektywnymi celami. Cele te obejmowały m.in.: rozbrojenie i nieproliferację broni masowego rażenia (dalej: BMR), przeciwdziałanie bioterroryzmowi, ochronę zdrowia ludzi i reagowanie kryzysowe w sytuacji epidemii, ochronę bioróżnorodności, ochronę zdrowia zwierząt i roślin uprawnych, bezpieczeństwo i higienę pracy ze szkodliwymi czynnikami biologicznymi, budowanie świadomości na temat zagrożeń biologicznych.

Koncepcja ochrony biologicznej wywodzi się z porozumień międzynarodowych w zakresie rozbrojenia i nieproliferacji broni biologicznej i toksynowej. Pierwszym porozumieniem wprowadzającym zakaz używania

spożywczych. Ponadto w ciągu kilku godzin można oczyścić taką aparaturę lub rozmontować instalację, co sprawia, że przestępcy mogą szybko ukryć oznaki swoich działań.

bojowych środków biologicznych był *Protokół dotyczący zakazu używania na wojnie gazów duszących, trujących lub podobnych oraz środków bakteriologicznych*, zwany potocznie protokołem genewskim[3]. W prace nad tym dokumentem była zaangażowana również Polska. Był to ogromny krok naprzód w kierunku usankcjonowania tego zakazu, mimo że w protokole objęto nim jedynie stosowanie tych środków w czasie wojny. Nie zabroniono natomiast badań nad bronią biologiczną, jej produkcji i gromadzenia. Ponadto niektórzy sygnatariusze (Francja, Stany Zjednoczone, Wielka Brytania) zastrzegli sobie prawo do jej wykorzystania w ramach odwetu, jeśli przeciwnik użyje tego środka jako pierwszy, co było dodatkowym ograniczeniem wprowadzonego zakazu. Pomimo to protokół genewski nigdy nie stracił na znaczeniu, czego dowodem jest odwoływanie się do niego w preambułach dwóch późniejszych porozumień: *Konwencji o zakazie prowadzenia badań, produkcji i gromadzenia zapasów broni bakteriologicznej (biologicznej) i toksycznej oraz ich zniszczeniu* z 1972 r., zwanej potocznie konwencją o zakazie broni biologicznej i toksynowej (dalej: konwencja BTWC)[4], oraz *Konwencji o zakazie prowadzenia badań, produkcji, składowania i użycia broni chemicznej oraz o zniszczeniu jej zapasów* z 1993 r., zwanej potocznie konwencją o zakazie broni chemicznej (dalej: konwencja CWC)[5].

Konwencja BTWC jest kluczowym porozumieniem w zakresie bezpieczeństwa biologicznego i ochrony biologicznej. Ten temat został podjęty również w Rezolucji Rady Bezpieczeństwa Organizacji Narodów Zjednoczonych Nr 1540 z 2004 r.[6] dotyczącej globalnego zakazu stosowania wszystkich czterech rodzajów BMR. Międzynarodowe reżimy kontrolne nad bronią biologiczną i toksynową wprowadzone przez członków Grupy Australijskiej (The Australia Group, AG)[7], w tym Polskę, służą kontroli transferu i eksportu czynników biologicznych, toksyn i technologii podwójnego zastosowania.

[3] *Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare*, 1925.

[4] *The Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction*, 1972.

[5] *Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction*, 1993.

[6] *Resolution 1540 (2004) / adopted by the Security Council at its 4956th meeting, on 28 April 2004*, 2004.

[7] *Fighting the spread of chemical and biological weapons*, https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/index.html [dostęp: 22 II 2025].

Temat ochrony biologicznej został podjęty także w innych międzynarodowych porozumieniach, których Polska jest państwem-stroną. Są to m.in.: konwencja o różnorodności biologicznej[8] i jej dwa protokoły – dotyczący nadzoru nad żywymi organizmami modyfikowanymi genetycznie[9] oraz dotyczący ochrony różnorodności biologicznej i naturalnych ekosystemów Ziemi[10], Międzynarodowe Przepisy Zdrowotne (ang. *International Health Regulations,* IHRs)[11] opracowane przez Światową Organizację Zdrowia (World Health Organization, WHO), a także umowy w zakresie transportu towarów niebezpiecznych[12]. Cennym źródłem wiedzy o ochronie biologicznej są również podręczniki i rekomendacje dotyczące bezpieczeństwa i ochrony biologicznej w laboratoriach, repozytoriach, podczas transportu, prowadzenia prac badawczo-rozwojowych czy na wypadek intencjonalnego użycia środków o charakterze chemicznym, biologicznym, radiologicznym i nuklearnym (ang. *chemical, biological, radiological,* and *nuclear*, CBRN).

Konwencja o zakazie broni biologicznej i toksynowej (1972)

Tekst konwencji BTWC obejmuje 15 artykułów. To pierwsze wielostronne porozumienie prawnie wiążące i obecnie najważniejszy na świecie traktat w dziedzinie nieproliferowania broni biologicznej i toksynowej. Stanowi podstawę dla późniejszych uwarunkowań w zakresie bezpieczeństwa i ochrony biologicznej, dlatego wymaga szczególnej uwagi.

Przedstawiciele państw-stron, w tym Polska, od 1980 r. spotykają się co ok. 5 lat i obradują podczas konferencji przeglądowych. Celem tych obrad jest dokonanie przeglądu dotychczasowego funkcjonowania konwencji BTWC oraz wypracowanie dokumentu końcowego. Są w nim prezentowane nowo przyjęte ustalenia służące lepszemu zinterpretowaniu i zrozumieniu założeń tej konwencji w kontekście aktualnie obowiązujących dokumentów normatywnych, postępu wiedzy i techniki oraz działań podejmowanych na forach międzynarodowych w przedmiotowym zakresie.

---

8 *The Convention on Biological Diversity*, 1993.

9 *The Cartagena Protocol on Biosafety to the Convention on Biological Diversity*, 2003.

10 *The Nagoya Protocol on Access to Genetic Resources and the Fair and Equitable Sharing of Benefits Arising from their Utilization to the Convention on Biological Diversity*, 2014.

11 *The International Health Regulations*, World Health Organization 2005.

12 *European Agreement Concerning the International Carriage of Dangerous Goods by Road* (ADR); *The Regulation concerning the International Carriage of Dangerous Goods by Rail* (RID); *The European Agreement concerning the International Carriage of Dangerous Goods by Inland Waterways* (ADN); *The IATA Dangerous Goods Regulations* (IATA DGR).

Dodatkowo państwa-strony konwencji BTWC są zobowiązane każdego roku przedkładać tzw. środki budowy zaufania (ang. *confidence-building measures*, CBMs) w postaci sprawozdań. Ich celem jest eliminowanie ewentualnych wątpliwości czy podejrzeń w zakresie prac prowadzonych w celach pokojowych w obszarze nauk biologicznych, jak również promowanie transparentności i wymiany informacji. Sprawozdanie obejmuje takie informacje, jak:

1) dane o krajowych ośrodkach badawczych i laboratoriach, w których obowiązują najwyższe standardy bezpieczeństwa biologicznego, ustanowione po to, aby wysoce niebezpieczne czynniki biologiczne były wykorzystywane do celów dozwolonych przez konwencję BTWC;
2) informacje o epidemiach chorób zakaźnych i zdarzeniach spowodowanych przez toksyny biologiczne w ostatnim roku;
3) aktualny wykaz publikacji naukowych oraz informacje o inicjatywach planowanych na kolejny rok;
4) wykaz krajowych aktów prawnych bądź innych zalegalizowanych instrumentów nawiązujących do konwencji BTWC;
5) informacje na temat programów badawczo-rozwojowych w dziedzinie biologii na rzecz działań ofensywnych i/lub defensywnych prowadzonych po 1 stycznia 1946 r.;
6) dane o państwowych i prywatnych zakładach produkujących szczepionki dla ludzi[13].

Konwencja BTWC jako pierwsza podjęła temat bezpieczeństwa biologicznego i ochrony biologicznej, szczególnie w artykułach I, III, IV, VII, IX i X. Podczas konferencji przeglądowych w ciągu ostatnich 44 lat sukcesywnie uszczegóławiano zapisy w tym zakresie.

Artykuł I

Konwencja BTWC nie określa środków biologicznych i toksyn, które mogą zostać wykorzystane jako broń, co jest jej zaletą i wadą jednocześnie. Dzięki temu może obejmować szeroką grupę czynników biologicznych stwarzających zagrożenie dla ludzi, zwierząt i roślin oraz pozyskanych w różny sposób. Przykładowo, w dokumentach końcowych z konferencji przeglądowych przyjęto, że artykuł I dotyczy ogółu szkodliwych drobnoustrojów

[13] *Confidence Building Measures*, United Nations, Office for Disarmament Affairs, https://disarmament.unoda.org/biological-weapons/confidence-building-measures/ [dostęp: 13 X 2024].

lub innych czynników mikrobiologicznych lub toksyn występujących naturalnie oraz sztucznie wytworzonych lub zmodyfikowanych[14]. Uwzględnia ponadto cząstki oraz elementy komórkowe czynników i toksyn, w tym syntetyczne odpowiedniki otrzymane na drodze chemicznej bądź analogi strukturalne naturalnie występujących związków, bez względu na ich źródło czy metodę produkcji, typ i ilość, których tworzenie nie ma profilaktycznego, ochronnego ani pokojowego uzasadnienia[15], a także toksyny pochodzenia bakteryjnego, zwierzęcego oraz roślinnego, w tym ich syntetycznie wytworzone analogi[16].

W odniesieniu do wyposażenia sprzętowego i technologii sytuacja jest identyczna. Konwencja nie wprowadza nazw urządzeń ani specyfikacji technicznej, co umożliwia objęcie zakazem wszystkich urządzeń i technologii mogących potencjalnie służyć proliferacji bojowych środków biologicznych lub ich uwolnieniu[17].

Artykuł III

Stosuje się bezpośrednio do kwestii ochrony biologicznej, gdyż zobowiązuje do zaniechania przekazywania czynników biologicznych lub środków ich przenoszenia w celach wrogich, pomagania w pracach na rzecz ich rozwoju i wpływania na nie. Podczas konferencji przeglądowych uszczegółowiono ten przepis i zobowiązano państwa-strony do zapewnienia ochrony podczas transferu wszystkim środkom ujętym w artykule I. Postulowano, aby odbywało się to m.in. w drodze krajowej implementacji konwencji BTWC, unormowań prawnych w zakresie transferu czynników biologicznych i urządzeń, które mogą zostać wykorzystane do ich produkcji, obowiązku nadzoru i kontroli nad tymi transferami. W 1996 r. dyskutowano nad sposobami zapobiegania pozyskaniu tych czynników przez szeroką grupę potencjalnych odbiorców (osobę fizyczną, państwo, grupę państw bądź organizację międzynarodową) oraz ich transferowaniu w obrębie terytorium danego państwa[18]. Niestety, okazało się to problematyczne, gdyż na mocy tej

[14] *Final Document of the Sixth Review Conference,* Geneva 2006. BWC/CONF.VI.I.1.

[15] *Final Document of the Third Review Conference,* Geneva 1991. BWC/CONF.III.I.3; *Final Document of the Fourth Review Conference,* Geneva 1996. BWC/CONF.IV.I.5.

[16] *Final Document of the Second Review Conference,* Geneva 1986. BWC/CONF.II.I.5.

[17] *Final Document of the Seventh Review Conference,* Geneva 2011. BWC.CONF.VII.I.1; *Final Document of the Eighth Review Conference,* Geneva 2016. BWC/CONF.VIII.I.1; *Final Document of the Ninth Review Conference,* Geneva 2022. BWC/CONF.IX/CRP.2/Rev.1.II.I.

[18] *Final Document of the Fourth Review Conference*... BWC/CONF.IV.III.3.

samej konwencji państwa-strony są zobowiązane umożliwić jak najszerszą wymianę sprzętu, materiałów i wiedzy naukowo-technicznej w zakresie pokojowego wykorzystania czynników biologicznych, toksyn i techniki (artykuł X). Z tego powodu niejednokrotnie apelowano o stworzenie instrumentów służących ustanowieniu reżimu kontrolnego nad wszystkimi czynnikami biologicznymi, toksynami biologicznymi, urządzeniami podwójnego zastosowania oraz ich elementami składowymi, w przypadku których istnieje ryzyko, że mogłyby zostać wykorzystane do ofensywnych programów nad rozwojem broni biologicznej i toksynowej[19].

Wnioskowano, aby w ramach kontroli eksportu wydawać licencje lub zezwolenia, które byłyby udzielane po uzyskaniu pewności, że dany towar trafi do wcześniej zatwierdzonego odbiorcy i zostanie wykorzystany w celach zgodnych z porozumieniem[20]. Zalecano, aby państwa-strony stworzyły system zabezpieczenia i ochrony każdego ze środków stosujących się do artykułu[21], co było problematyczne z uwagi na brak przez długi czas arbitralnego wykazu tych środków.

Po atakach terrorystycznych w 2001 r. wzrosło zainteresowanie uregulowaniem kwestii związanych z ochroną środków objętych zakazem w artykule I konwencji BTWC. Stwierdzono, że zagrożenie wynikające z terroryzmu biologicznego powinno implikować konieczność wprowadzenia skuteczniejszych środków kontroli przewozu i transferu tych środków. Dotyczyło to w szczególności krajów niebędących stronami konwencji BTWC, bez względu na to, czy transfer byłby kierowany do osoby indywidualnej czy członków ugrupowań reprezentujących poglądy określonych narodowości czy innych grup. Wzbudzało to ożywioną dyskusję. Obawiano się bowiem, że zaproponowane działania mogą zaszkodzić tradycyjnej wymianie handlowej i utrudnić współpracę pomiędzy państwami-stronami w celach pokojowych[22].

Polaryzacja stanowisk w tej kwestii jest nadal widoczna. Dużą rozbieżność obserwuje się pomiędzy krajami wysoko rozwiniętymi, mającymi

[19] *Final Document of the Third Review Conference*... BWC/CONF.III.III.1; *Final Document of the Fourth Review Conferenc*e... BWC/CONF.IV.III.2; *Final Document of the Sixth Review Conference*... BWC/CONF.VI.III.8-9; *Final Document of the Seventh Review Conference*... BWC/CONF.VII.III.9; *Final Document of the Eighth Review Conference*... BWC/CONF/VIII.III.9.

[20] *Final Document of the Sixth Review Conference*... BWC/CONF.VI.III.8.

[21] Tamże. BWC/CONF.VI.III.9.

[22] *Final Document of the Fifth Review Conference*, Geneva 2001–2002. BWC/CONF.V.COW/CRP.1.III – *Annex to the draft report of the Committee of the Whole.*

odpowiednie zdolności, zaplecze naukowo-techniczne, szeroko wykorzystującymi czynniki biologiczne w sferze ochrony zdrowia (komercyjnej), a państwami niemającymi dostatecznej wiedzy i zdolności. Apelują one o zapewnienie im nieskrępowanego dostępu do materiałów i technologii oraz udzielenie daleko idącej pomocy zamiast uprzedniego wprowadzenia mechanizmów kontroli i nadzoru nad czynnikami wrażliwymi[23].

Artykuł IV

Zobowiązuje państwa-strony do podjęcia wszelkich działań służących zapobieżeniu produkcji broni biologicznej i toksynowej, ale nie precyzuje tych działań wprost, co tym samym daje możliwość wprowadzania dowolnych narzędzi i środków. W dokumentach końcowych z konferencji przeglądowych przyjęto, że przedsięwzięcia powinny wynikać z instrumentów prawnych obowiązujących w danym kraju, zarówno z przepisów penalnych służących realizacji na terytorium danego kraju zakazu prowadzenia prac rozwojowych, produkowania, przechowywania, nabywania i utrzymywania czynników biologicznych i sprzętu wymienionych w artykule I, jak i z przepisów związanych z zapobieganiem tego rodzaju działaniom przez sprawowanie kontroli nad nimi[24].

W celu skutecznego wypełniania zobowiązań wynikających z artykułu IV podczas konferencji przeglądowych wielokrotnie podejmowano kwestię ochrony środków biologicznych. Na przykład za szczególnie istotne uznano implementowanie międzynarodowych standardów w zakresie zarządzania bezpieczeństwem biologicznym i ochrony biologicznej[25], wdrażanie regulacji prawnych dotyczących ochrony fizycznej mienia oraz zabezpieczenia obiektów, w których są wykorzystywane szczególnie niebezpieczne czynniki biologiczne i toksyny. Podkreślano, że ustanowienie przepisów w tym zakresie istotnie wpłynie nie tylko na bezpieczeństwo zdrowia publicznego na wypadek zagrożeń epidemicznych, lecz także na zabezpieczenie czynników zakaźnych i toksyn przed ich uwolnieniem

[23] *Biological Weapons Convention – Ninth Review Conference*, United Nations, Office for Disarmament Affairs, https://meetings.unoda.org/bwc-revcon/biological-weapons-convention-ninth-review-conference-2022 [dostęp: 8 III 2025].

[24] *Final Document of the Second Review Conference*... BWC/CONF.II.IV.4; *Final Document of the Third Review Conference*... BWC/CONF.III.IV.3; *Final Document of the Fourth Review Conference*... BWC/CONF.IV.IV.1-4; *Final Document of the Sixth Review Conference*... BWC/CONF.VI.IV.11.i; *Final Document of the Seventh Review Conference*... BWC/CONF.VII.IV.11.i; *Final Document of the Eighth Review Conference*... BWC/CONF.VIII.IV.11.a-b.

[25] *Final Document of the Seventh Review Conference*... BWC/CONF.VII.IV.13a.

albo wrogim przejęciem[26]. W ramach zwiększania skuteczności tego artykułu wskazywano na potrzebę ochrony czynników biologicznych, środków i toksyn biologicznych nie tylko w laboratoriach czy miejscach ich przechowywania, lecz także podczas transportu[27]. Gdy w 2005 r. WHO opublikowało IHRs podejmujące kwestie budowania krajowej gotowości w zakresie wykrywania i identyfikowania zagrożeń zdrowotnych o zasięgu transgranicznym oraz reagowania na nie, dostrzeżono bliską korelację tego instrumentu prawnego z artykułem IV konwencji BTWC. Państwa-strony konwencji BTWC, będące w dużej mierze jednocześnie państwami członkowskimi WHO, zaczęły postulować podjęcie krajowych środków w kierunku doskonalenia metod diagnostycznych, wzmacniania nadzoru epidemiologicznego i zdolności wykrywania ognisk chorób zakaźnych na poziomie krajowym, regionalnym i międzynarodowym w celu jednoczesnego realizowania obu porozumień. Uznano przy tym, że przez stałe monitorowanie zachorowalności w ramach krajowych sieci nadzoru będzie możliwe dużo szybsze wykrycie zachorowań nietypowych, podejrzanych lub niewiadomego pochodzenia, mogących być skutkiem prac sprzecznych z konwencją BTWC[28].

Na podstawie artykułu IV postulowano również wdrożenie instrumentów prawnych w zakresie kontroli i reglamentacji osób mających do czynienia z czynnikami patogennymi, popularyzowanie wśród nich wiedzy oraz promowanie postaw etycznych. Uznano, że edukacja i podnoszenie świadomości w zakresie możliwości wykorzystania szczególnie niebezpiecznych czynników biologicznych, toksyn biologicznych oraz urządzeń i środków służących do ich transmisji w zamiarze sprzecznym z postanowieniami konwencji BTWC mogłyby zwiększyć skuteczność działań wynikających z artykułu IV. Sugerowano, aby w programach szkoleniowych oraz materiałach edukacyjnych przeznaczonych dla studentów medycyny, nauk przyrodniczych i kierunków wojskowych zawrzeć treści o konwencji BTWC

[26] *Final Document of the Second Review Conference*... BWC/CONF.II.IV.4ii; *Final Document of the Third Review Conference*... BWC/CONF.III.IV.3ii; *Final Document of the Fourth Review Conference*... BWC/CONF.IV.IV.3; *Final Document of the Sixth Review Conference*... BWC/CONF.VI.IV.11.iii; *Final Document of the Seventh Review Conference*... BWC/CONF.VII.IV.11.iii; *Final Document of the Eighth Review Conference*... BWC/CONF.VIII.IV.11.b-c.

[27] *Final Document of the Seventh Review Conference*... BWC/CONF.VII.IV.11.

[28] *Final Document of the Sixth Review Conference*... BWC/CONF.VI.IV.13; *Final Document of the Seventh Review Conference*... BWC/CONF.VII.IV.13vi; *Final Document of the Eighth Review Conference*... BWC/CONF.VIII.IV.13f.

i protokole genewskim[29]. W 2022 r. wnioskowano o rozszerzenie grupy odbiorców o osoby działające w sektorze publicznym, prywatnym i środowisko akademickie oraz o aktywniejsze włączenie się w działania służące wczesnemu rozpoznawaniu zagrożeń związanych z nieprzestrzeganiem konwencji BTWC, w tym aktów bioterrorystycznych. Szczególnej kontroli powinny podlegać osoby, które uzyskały dostęp do szkodliwych czynników biologicznych i toksyn mających zastosowanie do konwencji BTWC, oraz specjaliści, którzy dzięki swej wiedzy i umiejętnościom są zdolni dokonać modyfikacji czynników biologicznych i zwiększyć zjadliwość patogenów czy zaostrzyć przebieg chorób przez nie wywoływanych. Uznano to za jedno z możliwych działań służących zapobieżeniu produkcji broni biologicznej i toksynowej[30].

Artykuł VII

Zobowiązuje państwa-strony traktatu, organizacje międzynarodowe, rządowe i pozarządowe do udzielania wsparcia krajom, wobec których Rada Bezpieczeństwa ONZ potwierdziła naruszenie konwencji BTWC. Artykuł obliguje do wzajemnej pomocy w dochodzeniu na wypadek popełnienia lub podejrzenia popełnienia czynu zabronionego przez tę konwencję. W celu skutecznego wypełniania zapisów tego artykułu podczas konferencji przeglądowych rekomendowano, aby koordynującą rolę w śledztwie odgrywała ONZ, przy wsparciu odpowiednich organizacji międzynarodowych, w tym WHO, która jest międzynarodową organizacją właściwą w sprawach zdrowia ludzi na świecie, w tym dochodzeń epidemiologicznych. Uznano, że zaangażowanie epidemiologów, obok innych organizacji, w tym właściwych w kwestii prowadzenia dochodzenia na wypadek popełnienia i/lub podejrzenia popełnienia czynu zabronionego przez konwencję, usprawniłoby wykrywanie i identyfikowanie źródła choroby, opisywanie dróg transmisji czynnika zakaźnego i wskazanie właściwego sposobu postępowania, jeśli dany czynnik zostałby wykorzystany w charakterze broni lub środka terroru[31]. W 2006 r. rozszerzono listę tych organizacji, gdyż przyjęto,

[29] *Final Document of the Second Review Conference*... BWC/CONF.II.IV.4iii; *Final Document of the Third Review Conference*... BWC/CONF.III.IV.3iii; *Final Document of the Fourth Review Conference*... BWC/CONF.IV.IV.3iii.

[30] *Final Document of the Seventh Review Conference*... BWC/CONF.VII.IV.13ii-iv; *Final Document of the Eighth Review Conference*... BWC/CONF.VIII.IV.13b-d; *Final Document of the Ninth Review Conference*... BWC/CONF.IX/CRP.2/Rev.1.II.IV.

[31] *Final Document of the Third Review Conference*... BWC/CONF.III.VII.4; *Final Document of the Fourth Review Conference*... BWC/CONF. IV.VII.5.

że wzajemna pomoc wzmocni globalne bezpieczeństwo i zminimalizuje skutki podobnych zdarzeń[32].

Ponadto apelowano, podobnie jak w przypadku artykułu IV, o podjęcie krajowych działań na rzecz wzmocnienia nadzoru nad chorobami zakaźnymi oraz zdolności wykrywania i identyfikowania czynników biologicznych mogących stanowić źródło ognisk chorób zakaźnych[33].

Artykuł IX

Zobowiązuje do ustanowienia zakazu stosowania broni chemicznej oraz środków mogących przyczynić się do jej produkcji i rozprzestrzenienia, co z pozoru słabo koreluje z zagadnieniami ochrony biologicznej. Należy jednak pamiętać, że podczas obrad nad konwencją BTWC wielokrotnie podejmowano problematykę bojowych środków trujących i zgłaszano potrzebę ustanowienia konwencji o zakazie broni chemicznej. Skutkiem tego było powstanie zaraz po jej ogłoszeniu 181 dokumentów ratyfikacyjnych i wniosków o przystąpienie[34].

To właśnie w kontekście artykułu IX konwencji BTWC zaczęto dostrzegać problem narastającej konwergencji biologii i chemii oraz wyzwań związanych z bezpieczeństwem biologiczno-chemicznym. Podczas konferencji przeglądowej w 2011 r. uznano, że zagrożenia na styku biologii i chemii oraz zbieżność biologicznych i chemicznych technologii stosujących się do bezpieczeństwa biologicznego oraz ochrony ludzi i środowiska powinny sugerować wspólne działania na rzecz zapobiegania zagrożeniom biologicznym i chemicznym w odniesieniu do obu traktatów, tj. konwencji BTWC i konwencji CWC[35].

Ma to znaczenie o tyle, że bardzo często zacierają się różnice między patogenami chemicznie zsyntetyzowanymi a związkami chemicznymi wyprodukowanymi z wykorzystaniem organizmów żywych. Wykorzystując układy chemiczne, można stworzyć niebezpieczny patogen, a wykorzystując

[32] *Final Document of the Sixth Review Conference*... BWC/CONF.VI.VII.34; *Final Document of the Seventh Review Conference*... BWC/CONF.VII.VII.36.

[33] *Final Document of the Sixth Review Conference*... BWC/CONF.VI.VII.35; *Final Document of the Seventh Review Conference*... BWC/CONF.VII.VII.38; *Final Document of the Eighth Review Conference*... BWC/CONF.VIII.VII; *Final Document of the Ninth Review Conference*... BWC/CONF.IX/CRP.2/Rev.1.II.VII.

[34] *Final Document of the Fourth Review Conference*... BWC/CONF.IV.IX.45; *Final Document of the Seventh Review Conference*... BWC/CONF.VII.IX.48.

[35] *Final Document of the Seventh Review Conference*... BWC/CONF.VII.IX.49.

hodowle bakterii, można wyprodukować toksyny biologiczne, w tym ich syntetycznie wytworzone analogi[36].

Artykuł X

W głównej mierze dotyczy szeroko rozumianej współpracy państw-stron na rzecz badań naukowych, prac bioinżynieryjnych, transferu wiedzy i technologii. Zobowiązuje do prowadzenia prac rozwojowych oraz wykorzystywania nauk biologicznych i technologii dla dobra ludzkości i środowiska. Zobowiązanie to powinno być realizowane przez umożliwienie wymiany urządzeń, materiałów, informacji naukowych i technicznych dotyczących wykorzystania środków bakteriologicznych (biologicznych) i toksyn w możliwie najszerszym zakresie, pod warunkiem że będą one służyć celom pokojowym. Artykuł ten obliguje do współpracy w przyczynianiu się do dalszego rozwoju i wykorzystywania odkryć naukowych w dziedzinie bakteriologii na rzecz zapobiegania chorobom lub innych celów o charakterze pokojowym.

Wnioskowano, aby państwa-strony konwencji BTWC, zwłaszcza kraje rozwinięte, rozszerzały współpracę naukowo-technologiczną z krajami rozwijającymi się. Współpraca miałaby obejmować m.in.: transfer wiedzy, doświadczeń i rozwiązań technologicznych w zakresie pokojowego wykorzystania czynników biologicznych i toksyn, przekazywanie i wymianę informacji, szkolenia naukowców i ekspertów oraz transfer materiałów i środków[37]. Dostęp do wiedzy specjalistycznej miałby obejmować bakteriologię, biotechnologię, inżynierię genetyczną, mikrobiologię oraz pokrewne dziedziny nauki i techniki[38].

Podczas konferencji przeglądowej w 2016 r. szczególnie dyskusyjna, obok wprowadzenia prawnie wiążącego mechanizmu weryfikacyjnego, była sprawa współpracy, odmiennie postrzeganej przez państwa zachodnie i kraje rozwijające się. Na potrzebę jej wzmocnienia w ramach artykułu X zwracały uwagę przede wszystkim kraje rozwijające się (m.in. Iran, Wenezuela, Kuba) skupione w grupie państw niezaangażowanych (ang. Non-Aligned Movement and other States, NAM). Domagały się szerszego dostępu do

[36] *Final Document of the Second Review Conference*... BWC/CONF.II.I.5.

[37] Tamże. BWC/CONF.II.X.3ii-iv; *Final Document of the Third Review Conference*... BWC/CONF.III.X.3ii-iv; *Final Document of the Fourth Review Conference*... BWC/CONF.IV.X.12ii-iv, viii; *Final Document of the Sixth Review Conference*... BWC/CONF.VI.X.49; *Final Document of the Seventh Review Conference*... BWC/CONF.VII.X.58.

[38] *Final Document of the Second Review Conference*... BWC/CONF.II.X.2; *Final Document of the Third Review Conference*... BWC/CONF.III.X.2; *Final Document of the Fourth Review Conference*... BWC/CONF.IV.X.2.

nowoczesnych osiągnięć biotechnologii i sprzętu, know-how, szkoleń oraz wymiany naukowej i akademickiej, co nie spotkało się z przychylnością innych państw (m.in. USA, Wielkiej Brytanii, Szwecji i Niemiec)[39]. Dopiero podczas uzgadniania dokumentu końcowego z ostatniej konferencji przeglądowej w 2022 r. podjęto decyzję o powołaniu grupy roboczej ekspertów. Jej celem będzie m.in. opracowanie mechanizmu przeglądu oraz oceny osiągnięć naukowych i technologicznych istotnych dla konwencji BTWC[40].

Koncepcja ochrony biologicznej

Anglojęzyczne terminy *biosafety* (bezpieczeństwo biologiczne) i *biosecurity* (ochrona biologiczna) wielokrotnie traktowano jako terminy tożsame albo bliskoznaczne. Termin *biosafety* pojawił się wcześniej niż *biosecurity* i przez dłuższy czas obejmował także zagadnienia związane z ochroną biologiczną. W związku z tym w niektórych krajach (np. Francja, Niemcy, Rosja i Chiny) termin ochrona biologiczna w ogóle nie funkcjonował, co często powodowało trudności natury praktycznej.

Aby lepiej zrozumieć różnice pomiędzy tymi terminami, uczestnicy konwencji BTWC w 2003 r. zaproponowali ich nieformalną interpretację. Przyjęli, że bezpieczeństwo biologiczne to zabezpieczenie ludzi przed drobnoustrojami, ochrona biologiczna natomiast skupia się na ochronie i zabezpieczeniu drobnoustrojów przed wrogim działaniem ludzi. Pięć lat później doprecyzowano, że bezpieczeństwo biologiczne powinno koncentrować się na działaniach służących stworzeniu bezpiecznych warunków pracy ze szkodliwymi czynnikami biologicznymi oraz zapewnieniu ochrony ludziom i środowisku przed ich przypadkowym uwolnieniem. Z kolei ochronę biologiczną należy rozumieć jako różne środki i sposoby zabezpieczenia czynników biologicznych oraz technologii podwójnego zastosowania przed kradzieżą bądź bezprawnym przejęciem czy pozyskaniem i ich użyciem w celu wyrządzenia szkody. Składa się na nią: ochrona fizyczna pomieszczeń oraz obiektów, w których przechowuje się szczególnie niebezpieczne patogeny i toksyny, kontrola transferu produktów i technologii podwójnego zastosowania, właściwe pakowanie, znakowanie i ochrona podczas transportu przesyłek zawierających materiał zakaźny, ochrona wiedzy, technologii i wyników prac naukowo-badawczych mogących być potencjalnym źródłem informacji, jak wyprodukować broń biologiczną i toksynową, przeciwdziałanie terroryzmowi biologicznemu. W ramach

[39] *Final Document of the Eighth Review Conference*... BWC/CONF.VIII/4.X.59.

[40] *Final Document of the Ninth Review Conference*... BWC/CONF.IX/CRP.2/Rev.1.X.71.

ochrony biologicznej są podejmowane również zagadnienia dotyczące egzekwowania przestrzegania międzynarodowych porozumień, przeciwdziałania agroterroryzmowi (ochrona środowiska przed celowym uwolnieniem gatunków obcych lub inwazyjnych w celu wyrządzenia szkód w uprawach rolnych), prowadzenie dochodzeń z wykorzystaniem śladów biologicznych jako materiału dowodowego oraz działań śledczych w celu ujęcia sprawców aktów bioterrorystycznych[41].

Rezolucja Rady Bezpieczeństwa ONZ nr 1540 (2004)

Rezolucja Rady Bezpieczeństwa ONZ nr 1540 (dalej: rezolucja 1540)[42] to pierwszy międzynarodowy instrument prawnie wiążący, kompleksowo ujmujący kwestie wszystkich trzech rodzajów BMR. Jej implementacja oznacza wdrożenie i realizację zapisów trzech porozumień: konwencji BTWC, konwencji CWC oraz traktatu o nierozprzestrzenianiu broni jądrowej (NPT)[43].

Założenia rezolucji 1540 bezpośrednio wspierają wykonywanie zobowiązań wynikających z konwencji BTWC, gdyż uszczegóławiają i precyzują środki ochrony biologicznej służące przeciwdziałaniu nielegalnemu posiadaniu, wytwarzaniu, przechowywaniu, transportowi, tranzytowi materiałów i technologii wykorzystywanych do produkcji broni biologicznej i toksynowej oraz handlowi nimi. Działania są realizowane w czterech obszarach:

1) przyjęcia i egzekwowania prawa karnego w zakresie nieprzestrzegania zakazu wytwarzania broni biologicznej i toksynowej oraz środków służących jej rozprzestrzenianiu,
2) przyjęcia środków służących zapobieżeniu nielegalnemu obrotowi BMR i materiałami stosowanymi do jej produkcji,
3) nieutrudniania wymiany handlowej i świadczenia komercyjnych usług zdrowotnych prowadzonych zgodnie z obowiązującymi przepisami,
4) zachęcania krajów do prowadzenia dialogu i wymiany doświadczeń w zakresie stosowanych środków bezpieczeństwa i ochrony granic terytorialnych oraz kontroli eksportu.

[41] *Biosafety and Biosecurity – Submitted by the Implementation Support Unit,* 24 June 2008, BWC/MSP/2008/MX/INF.1; A. Bielecka-Oder, *Safety and Security Regulations Against Biological Threats,* w: *Defence Against Bioterrorism,* V. Radosavljevic, I. Banjari, G. Belojevic (red.), Springer Netherlands 2018.

[42] *Resolution 1540 (2004)*...

[43] *The Nuclear Non-Proliferation Treaty* (NPT), 1968.

W celu weryfikowania skuteczności krajowej implementacji tych założeń Komitet Rezolucji 1540 (ang. 1540 Committee) opracował matryce (ang. *1540 Matrices*) opisujące stopień jej wdrożenia[44]. W części dotyczącej broni biologicznej i toksynowej oraz związanych z nią materiałów każdy kraj jest zobowiązany:

- określić przynależność do porozumień międzynarodowych i regionalnych,
- wskazać krajowe instrumenty prawnie wiążące i niewiążące zabraniające świadczenia usług, pomocy i finansowania wymienionych w matrycy działań, m.in. produkowania, pozyskiwania, przechowywania, prowadzenia prac rozwojowych, transportowania, transferowania własności na inne podmioty gospodarcze i/lub osoby fizyczne,
- wskazać rodzaj środków stosowanych wobec krajowych mechanizmów kontroli nad przestrzeganiem bezpieczeństwa i ochrony biologicznej w zakresie produkcji, użytkowania, przechowywania, transportowania oraz innych metod pozyskiwania czynników biologicznych, toksyn i środków ich rozprzestrzeniania oraz licencjonowania obiektów zajmujących się wyżej wspomnianymi aktywnościami, rejestrowania osób mających do czynienia z wyżej wymienionymi materiałami, sprawdzania ich wiarygodności, stosowania ochrony fizycznej, przestrzegania uregulowań prawnych wobec prac w dziedzinie inżynierii genetycznej oraz innych regulacji w zakresie bezpieczeństwa i ochrony biologicznej,
- zamieścić krajowe regulacje, procedury, środki, w tym wymienić instytucje odpowiedzialne m.in. za sprawowanie kontroli nad handlem, prowadzenie negocjacji w zakresie sprzedaży dóbr i technologii oraz za pośrednictwo, prowadzenie czynności dochodzeniowo-śledczych i/lub wywiadowczych, sprawdzanie posiadanych uprawnień i licencji, przeprowadzanie kontroli eksportu na podstawie list kontrolnych czynników biologicznych, toksyn i technologii podwójnego zastosowania oraz kontroli ich źródeł finasowania.

Rezolucja 1540 stanowi jeden z głównych filarów międzynarodowego porządku w zakresie nieproliferacji i kontroli obrotu BMR, czemu dano wyraz w 2022 r. w sprawozdaniu z postępów w realizacji strategii UE przeciw rozprzestrzenianiu BMR. Wskazano w nim, że kraje UE uznają ją za jeden

[44] *Approved 1540 Committee Matrix of [State]*, https://www.un.org/en/sc/1540/Documents/Matrix%20Template%202013%20(E).pdf [dostęp: 17 XI 2024].

z (...) *kluczowych elementów globalnych wysiłków na rzecz zapobiegania rozpowszechnianiu tego rodzaju broni wśród terrorystów i innych podmiotów niepaństwowych*[45].

Grupa Australijska (1985)

Obecnie na świecie funkcjonuje kilka wielostronnych systemów kontroli wywozu materiałów i środków o znaczeniu strategicznym dla bezpieczeństwa (np. porozumienie z Wassenaar, Komitet Zanggera, Grupa Australijska, Grupa Dostawców Jądrowych, System Kontroli Technologii Rakietowych). Najważniejszym ugrupowaniem w obszarze kontroli eksportu bojowych czynników biologicznych i technologii podwójnego zastosowania, istotnie przyczyniającym się do przeciwdziałania proliferacji i rozprzestrzenianiu czynników broni biologicznej i toksynowej, jest Grupa Australijska[46]. Jej działalność bezpośrednio wspiera realizację postanowień konwencji BTWC przez koordynowanie przez jej członków polityk eksportowych towarów o charakterze strategicznym oraz wzmacnianie skuteczności działania krajowych środków w zakresie licencjonowania towarów podwójnego zastosowania. Członkowie AG, w tym Polska, są jednocześnie państwami-stronami konwencji BTWC oraz CWC[47].

W ramach sprawowania reżimu kontrolnego nad bronią biologiczną i toksynową AG opracowała trzy listy kontrolne: a) listę biologicznego sprzętu, technologii i oprogramowania o charakterze podwójnego zastosowania, b) listę patogenów ludzkich i zwierzęcych oraz toksyn, c) listę patogenów roślinnych, które z uwagi na możliwość ich wykorzystania do produkcji broni biologicznej i toksynowej są poddawane szczególnej kontroli eksportowej. Są to ważne wykazy, gdyż jako pierwsze wskazują konkretne nazwy gatunkowe oraz specyfikację techniczną sprzętu o potencjale podwójnego zastosowania, które powinny podlegać szczególnej kontroli. Wykazy te powinny stać się punktem odniesienia dla regulacji krajowych[48].

---

[45] *Sprawozdanie roczne z postępów w realizacji strategii Unii Europejskiej przeciw rozprzestrzenianiu broni masowego rażenia (2022 r.)*, Prawo.pl, https://www.prawo.pl/akty/dz-u-ue-c-2023-383,72216862.html [dostęp: 28 IX 2024].

[46] *Introduction*, The Australia Group, https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/introduction.html [dostęp: 21 IX 2024].

[47] *Participants*, The Australia Group, https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/participants.html [dostęp: 21 IX 2024].

[48] *Australia Group Common Control Lists*, The Australia Group, https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/controllists.html [dostęp: 30 XI 2024].

Podczas analizy poszczególnych pozycji tych list należy mieć na uwadze, że przykładowo reżim kontrolny nie ma zastosowania do czynników biologicznych, które stanowią składnik szczepionek ochronnych (cel pokojowy). Miałby zastosowanie, gdyby te czynniki były eksportowane w formie czystych żywych kultur bądź w przypadku toksyn – czystych izolatów (możliwość podwójnego zastosowania).

Zarówno konwencja BTWC, jak i rezolucja 1540 nie doczekały się tak konkretnych rozwiązań. Można domniemywać, że jest to konsekwencją uniwersalności tych porozumień, co wymusiło określony poziom ogólności i konieczność konsensusu. Nie dotyczy to AG, która jest ugrupowaniem niezależnym i dzięki temu być może jest skuteczniejsza w realizacji swoich postanowień.

Warto nadmienić, że członkowie AG często podejmują tematy potencjalnych zagrożeń będących konsekwencją zmieniających się warunków geopolitycznych i uwarunkowań na arenie międzynarodowej. Na przykład podczas posiedzenia plenarnego w 2022 r. dyskutowano o możliwości użycia środków broni chemicznej i biologicznej przez Federację Rosyjską. Nie wykluczono możliwości ataków na ukraińskie obiekty cywilne, w których są wykorzystywane bądź deponowane środki biologiczne i chemiczne. Debatowano również o zagrożeniu globalnym wynikającym z dezinformacji na ten temat[49]. Wątek ten podejmowano także w latach 2023–2024. Podkreślano, że z powodu zagrożenia terroryzmem chemicznym i biologicznym należy zachować szczególną czujność w przypadku realizacji zamówień, które mogłyby wspierać wrogie działania, a ponadto trzeba chronić się przed niewłaściwym wykorzystaniem technologii oraz sprzętu chemicznego i biologicznego przez podmioty niepaństwowe. Zwrócono również uwagę na ryzyko płynące z przekazywania zasobów intelektualnych i wiedzy specjalistycznej w dziedzinach nauk mogących mieć zastosowanie do porozumień nieproliferacyjnych lub udostępniania tych zasobów i wiedzy za pomocą środków masowego przekazu czy innych kanałów wymiany oraz na konieczność skutecznej kontroli nad niematerialnymi transferami technologii (ang. *intangible transfer of technology*, ITT)[50].

[49] *Statement by the Chair of the 2022 Australia Group Plenary*, The Australia Group, https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/2021-ag-plenary-statement.html [dostęp: 22 IX 2024].

[50] *Statement by the Chair of the 2023 Australia Group Plenary*, Paris 2023; *Statement by the Chair of the 2024 Australia Group Plenary*, Paris 2024; K. Hyuk, *Intangible Transfer of Technology (ITT): Open-source Information Analysis for the Implementation of Sanctions on North Korea*,

Członkowie AG uczestniczą w spotkaniach państw-stron konwencji BTWC i wspierają wypełnianie jej postanowień. W 2024 r. wskazano, że z niecierpliwością oczekują na rozwój dwóch nowych mechanizmów – dotyczącego współpracy i pomocy międzynarodowej oraz odnoszącego się do rozwoju naukowo-technologicznego, jak również progresu we wdrażaniu środków ochrony biologicznej[51].

Konwencja o różnorodności biologicznej (1993)

Konwencja o różnorodności biologicznej (dalej: konwencja CBD)[52] jest najważniejszym porozumieniem międzynarodowym poświęconym ochronie różnorodności biologicznej środowiska naturalnego przed zagrożeniami będącymi następstwem wykorzystywania nowoczesnych biotechnologii. Jej celami, poza ochroną, są zrównoważone użytkowanie elementów bioróżnorodności, uczciwy i sprawiedliwy podział korzyści wynikających z wykorzystywania zasobów genetycznych, respektowanie praw wobec nich oraz odpowiednie finansowanie[53]. Przez protokoły wynikające z realizacji jej celów pośrednio nawiązuje ona do problematyki bezpieczeństwa i ochrony biologicznej w kontekście konwencji BTWC.

Protokół z Kartageny o bezpieczeństwie biologicznym (2003)

Jest instrumentem prawnie wiążącym, realizującym pierwszy cel konwencji CBD, czyli ochronę różnorodności biologicznej, w tym ochronę zdrowia ludzi, zwierząt, roślin i środowiska naturalnego przed szkodliwym wpływem produktów nowoczesnej biotechnologii[54].

Wiadomo, że obok wielu korzyści płynących z osiągnięć współczesnej biotechnologii, szczególnie technik biologii molekularnej i inżynierii genetycznej, istnieje wąski margines zastosowań potencjalnie wrogich. Dlatego zgodnie z konwencją BTWC zabrania się produkowania i wykorzystywania bakterii, wirusów i ich toksyn oraz stosowania technologii w celach innych niż pokojowe czy ochronne, a co za tym idzie, zabrania się

38 North, 10 III 2023 r., https://www.38north.org/2023/03/intangible-transfer-of-technology-itt-open-source-information-analysis-for-the-implementation-of-sanctions-on-north-korea/ [dostęp: 9 III 2025].

51 *Statement by the Chair of the 2024 Australia Group Plenary…*, pkt 14.

52 *The Convention on Biological Diversity*, 1993.

53 Tamże, art. 1.

54 *Protokół z Kartageny o bezpieczeństwie biologicznym do Konwencji o różnorodności biologicznej*.

wprowadzania do środowiska i rozprzestrzeniania środków biologicznych, które mogłyby zostać wykorzystane jako broń, wywołać zachorowania wśród ludzi (bioterroryzm), wyrządzić szkody w gospodarce rolnej (agroterroryzm) – czy to przez zamierzone skażenie żywności (bioterroryzm żywnościowy), czy celowe niszczenie zasobów środowiska naturalnego. Dlatego umyślne modyfikowanie mikroorganizmów o potencjale podwójnego zastosowania w celu ich uwolnienia do środowiska bądź stworzenia zagrożenia zdrowia ludzi, zwierząt i przyrody wpisuje się w problematykę ochrony biologicznej w kontekście konwencji BTWC.

Powodem powstawania protokołu kartageńskiego była potrzeba ustanowienia reguł bezpiecznego wykorzystywania żywych organizmów genetycznie modyfikowanych (ang. *living modified organisms*, LMOs), w tym mikroorganizmów genetycznie modyfikowanych (ang. *genetically modified microorganisms*, GMMs), oraz uregulowania kwestii związanych z międzynarodowym handlem nimi. Brak tych reguł mógłby wywrzeć negatywny wpływ na zachowanie bądź zrównoważone użytkowanie bioróżnorodności środowiska, a w konsekwencji stworzyć zagrożenie zdrowia publicznego[55]. Protokół określa ponadto działania zapobiegawcze konieczne do podjęcia w sytuacji uwolnienia LMOs. W myśl tej umowy kraje będące stronami protokołu mają pełne prawo ograniczać import albo użytkowanie tych organizmów, zakazać ich, jeśli nie ma dowodów naukowych lub pewności co do bezpieczeństwa ich stosowania[56].

Ingerencja w materiał genetyczny żywych czynników zakaźnych może wpłynąć na stworzenie broni wyposażonej w nowy ładunek, tj. w znany gen, ale niewystępujący w danym czynniku, gdyż włączony do genomu sztucznie, bądź w ładunek o charakterze innowacyjnym, czyli wyposażony w nowo stworzony gen. Dlatego za wymagające szczególnej uwagi uznano takie procesy, jak transferowanie genów oporności lekowej na mikroorganizmy wcześniej jej nieposiadające w celu zmniejszenia wrażliwości patogenu na lek oraz celowe zmienianie powierzchniowych struktur białkowych patogenów odpowiedzialnych za powstawanie przeciwciał w organizmie (obronę), czyli modyfikowanie właściwości antygenowych bakterii chorobotwórczych. Dyskusyjne są również prace służące modyfikacji struktur lipopolisacharydowych bakterii w taki sposób, aby utrudnić ich wczesną detekcję i rozpoznanie przez układ odpornościowy, oraz

[55] Tamże, art. 4.

[56] Tamże, art. 16–18.

polegające na addycji genów odpowiedzialnych za produkcję toksyn. Potencjalnie niebezpieczne mogą być modyfikacje bakterii służące zwiększeniu ich stabilności w środowisku zewnętrznym, np. zwiększające ich odporność na niekorzystne warunki atmosferyczne (promieniowanie UV emitowane przez Słońce) bądź stres mechaniczny (wytrzymałość), będące następstwem ich uwolnienia do środowiska, a także długotrwałego i silnego mieszania podczas prowadzenia hodowli bioreaktorowych. Podobnie potencjalnie groźne może być przekształcanie mikroorganizmów niechorobotwórczych w patogenne przez celowe transferowanie do nich genów odpowiedzialnych za właściwości chorobotwórcze, a ponadto zmiany służące „zaprogramowaniu" ich do produkcji określonych związków chemicznych, w tym toksyn, które mogą zostać użyte w charakterze broni[57].

Zarówno konwencja BTWC, jak i protokół z Kartageny regulują kwestie transferów. Artykuł III konwencji w zakresie sprawowania kontroli nad transferem czynników broni biologicznej i toksynowej oraz urządzeń ich dotyczących, a artykuł X – w zakresie transferu materiałów i technologii oraz wzajemnej współpracy na rzecz pokoju. Protokół kartageński natomiast w zakresie transgranicznego przemieszczania LMOs oraz transferu wiedzy i technologii. Oba porozumienia akcentują ponadto potrzebę wspierania wymiany informacji na temat prowadzonych doświadczeń oraz strategii krajowych realizowanych w celu przeciwdziałania zagrożeniom będących następstwem biotechnologii. W przypadku protokołu jest to System Wymiany Informacji o Bezpieczeństwie Biologicznym[58], a konwencji BTWC – CBMs. Należy jednak zaznaczyć, że cele obu tych dokumentów są odmienne[59].

Pomimo odległych obszarów regulacji zakresy treści obu porozumień – konwencji BTWC i protokołu kartageńskiego – są zbieżne pod względem oceny skutków modyfikacji genetycznej. Wszystkie czynniki biologiczne poddane modyfikacjom zmieniającym ich genotyp kwalifikują się jako czynniki objęte zakazem wyrażonym w konwencji BTWC, o ile celem tych modyfikacji jest wrogie wykorzystanie tych czynników, gdyż zakaz obejmuje wszystkie czynniki biologiczne, w tym wyprodukowane z wykorzystaniem metod nowoczesnej biotechnologii.

[57] K. Nixdorff, D. Schilling, M. Hotz, *Critical Aspects of Biotechnology in Relation to Proliferation*, w: *The Implementation of Legally Binding Measures to Strengthen the Biological and Toxin Weapons Convention*, M. Chevrier i in. (red.), NATO Science Series II, t. 150, 2004.

[58] *The Convention on Biological Diversity…*, art. 20.

[59] Tamże, art. 22.

Protokół z Nagoi o wykorzystaniu zasobów genetycznych (2014)

Przedmiotem regulacji jest ochrona zasobów genetycznych przed ich nielegalnym pozyskaniem i wykorzystaniem, co określa się mianem piractwa biologicznego[60]. Dotyczy głównie bezprawnego pozyskiwania i wykorzystywania dzikich roślin, egzotycznych zwierząt, endemicznych mikroorganizmów, ich puli genowych oraz wiedzy tradycyjnej z nimi związanej[61] pozyskanych z ich regionu przez koncerny farmaceutyczne w celu prowadzenia badań nad nowymi środkami leczniczymi, ich opatentowania, a potem czerpania z tego tytułu korzyści materialnych.

Protokół z Nagoi wdraża cel trzeci konwencji CBD, czyli (...) *sprawiedliwy i równy podział korzyści wynikających z wykorzystania zasobów genetycznych, w tym przez odpowiedni dostęp do zasobów genetycznych oraz przez odpowiedni transfer właściwych technologii – z uwzględnieniem wszystkich praw do tych zasobów i technologii, a także poprzez odpowiednie finansowanie, tym samym wnosząc wkład w ochronę różnorodności biologicznej i zrównoważone wykorzystanie jej elementów*[62].

Państwa-strony protokołu z Nagoi to w większości kraje rozwijające się, którym przepis daje możliwość legalnego podniesienia swojego statusu gospodarczego przez czerpanie korzyści majątkowych i niematerialnych[63]. Wnosi, że zasoby genetyczne to pule genów gatunków występujących naturalnie w przyrodzie (łac. *in situ*), jak również zbiory zasobów utworzone przez człowieka (łac. *ex situ*) – banki genów oraz mikrobiologiczne kolekcje kultur, w tym zarówno żywy, jak i martwy materiał biologiczny w postaci DNA lub RNA.

I chociaż protokół z Nagoi nie obejmuje swoim zakresem ludzkiego materiału genetycznego, to stosuje się do mikroorganizmów lub drobnoustrojów patogennych wyizolowanych z tkanek ludzkich, krwi bądź płynów ustrojowych człowieka. Analogicznie jest w przypadku towarów żywnościowych – protokół nie dotyczy ich bezpośrednio, ale stosuje się do patogenów

[60] *Collins English Dictionary – Complete and Unabridged*, 12th edition, Collins 2014; E. Hammond, *Biopiracy Watch: A compilation of some recent cases*, t. 1, Third World Network 2013.

[61] Wiedzę tradycyjną należy rozumieć jako wiedzę ludową, tubylczą.

[62] *Protokół z Nagoi do Konwencji o różnorodności biologicznej o dostępie do zasobów genetycznych oraz sprawiedliwym i równym podziale korzyści wynikających z wykorzystania tych zasobów*, art. 1.

[63] E. Martyniuk, *Nowe uregulowania prawne dotyczące dostępu do zasobów genetycznych zwierząt i ich potencjalny wpływ na prace hodowlane i badania naukowe*, „Przegląd Hodowlany" 2016, nr 5, s. 10–14.

wyizolowanych z żywności[64]. Dodatkowo wprowadza pojęcia ważne z punktu widzenia ochrony biologicznej oraz ochrony własności intelektualnej[65].

Protokół z Nagoi ma pośrednie znaczenie dla ochrony biologicznej, gdyż jego głównym celem jest ochrona praw państw do zasobów biologicznych oraz własności intelektualnej na ich temat. Ochronę zbiorów biologicznych, w tym czynników niebezpiecznych dla zdrowia, traktuje pośrednio. Jednak jego zapisy przekładają się na konieczność ustanowienia środków zabezpieczenia w obiektach, gdzie są gromadzone i przechowywane zasoby genetyczne czynników patogennych oraz wiedza na ich temat, aby zapobiec ich kradzieży bądź innemu nielegalnemu wykorzystaniu. Ma to pośrednie przełożenie na ograniczanie ryzyka bezprawnego ich użycia w celach wrogich określonych w art. I konwencji BTWC[66].

Międzynarodowe Przepisy Zdrowotne (2005)

Międzynarodowe Przepisy Zdrowotne to opracowany przez WHO instrument prawnie wiążący, który ma na celu wzmacnianie krajowych zdolności w zakresie zapobiegania, nadzoru epidemiologicznego, wykrywania oraz wczesnego ostrzegania i reagowania na transgraniczne zagrożenia zdrowia publicznego (ang. Public Health Emergency of International Concern, PHEIC).

Państwa będące stronami tego porozumienia, w tym Polska, są zobowiązane do implementacji IHRs oraz budowania bądź doskonalenia krajowych zdolności w zakresie detekcji, identyfikacji, nadzoru, profilaktyki, zapobiegania rozprzestrzenianiu się chorób zakaźnych, oceny ryzyka biologicznego oraz gotowości do reagowania na poważne zagrożenia zdrowia publicznego o zasięgu międzynarodowym, przy skoordynowanej współpracy służb krajowych zaangażowanych w reagowanie (w przypadku braku takich zdolności – we współpracy ze służbami innych państw). Obostrzenia IHRs nie powinny jednak zakłócać transgranicznego ruchu pasażerskiego i handlu oraz powinny opierać się na środkach krajowych (legislacyjnych,

[64] G. Verkley, M. Dunja, D. Smith, *The Nagoya Protocol and mBRCs: towards a MIRRI Best Practice for Access and Benefit Sharing (ABS)* – prezentacja podczas ECCO 34 Conference, Session 2 BRCs and Regulations, Paryż, 28 V 2015 r.

[65] *Protokół z Nagoi do Konwencji o różnorodności biologicznej o dostępie do zasobów genetycznych…*, art. 2c i 2d.

[66] *The Workshop on Nagoya Protocol for "Collection Holders"*, Brussels 2017.

prawnych, organizacyjnych, szkoleniowych)[67]. Zawarto w nich m.in. zalecenia dotyczące wprowadzania środków zabezpieczających zdrowie ludzi przy przekraczaniu przejść granicznych, stosujące się do osób podróżujących, ich bagażu, kontenerów, środków lokomocji, towarów i przesyłek[68]. Każdego roku podczas Światowego Zgromadzenia Zdrowia (ang. World Health Assembly, WHA) jest omawiany postęp prac wśród państw członkowskich w zakresie implementacji IHRs[69].

Co ważne, IHRs stosują się do mogących rozprzestrzeniać się poza granice administracyjne państw chorób zakaźnych oraz zagrożeń zdrowia, których zwalczanie może wymagać skoordynowanej odpowiedzi kilku krajów. Dotyczy to m.in. zagrożeń biologicznych, chemicznych, radiologicznych, o nieznanej etiologii, mających potencjał spowodowania znacznych szkód dla populacji ludzkiej, a także ognisk chorób naturalnie występujących, przypadkowych zdarzeń z udziałem czynników biologicznych i toksyn na skutek wypadku przy pracy czy zaniedbania, aktów wandalizmu bądź sabotażu oraz zamierzonego ich użycia w celach przestępczych[70]. To powoduje, że IHRs również pośrednio nawiązują do konwencji BTWC.

W IHRs kwestie bezpieczeństwa biologicznego i ochrony biologicznej odnoszą się przede wszystkim do krajowych zdolności w zakresie zapewnienia bezpieczeństwa zdrowotnego obywateli. Każdy kraj powinien mieć własne zdolności diagnostyczne, a w przypadku ich braku powinien nawiązać współpracę z ośrodkiem innego kraju, aby zapewnić optymalny dla wszystkich państw poziom bezpieczeństwa zdrowotnego[71]. Jest także zobowiązany rozwijać, umacniać i utrzymywać gotowość do szybkiego i skutecznego reagowania na zagrożenia zdrowia oraz stany nagłe o zasięgu międzynarodowym[72]. Powinien również zapewnić bezpieczne warunki pracy w laboratoriach z udziałem czynników biologicznych[73], procedury reagowania na naturalne, przypadkowe i zamierzone użycie czynników biologicznych i toksyn mogących wywrzeć szkodliwy wpływ na stan zdrowia

[67] *The International Health Regulations*..., art. 2, 12–13.

[68] Tamże, art. 15–22, 23–39.

[69] *Implementation of the International Health Regulations (2005): Report by the Director-General*, World Health Organization 2024, https://apps.who.int/gb/ebwha/pdf_files/WHA77/A77_8-en.pdf [dostęp: 8 III 2025].

[70] *The International Health Regulations*..., Appendix II, 2005.

[71] Tamże, art. 5.1, 14, Annex 1, paragraph 6(b), 2005.

[72] Tamże, art. 13.1, 2005.

[73] The World Health Assembly Resolution 58.29, *Enhancement of laboratory biosafety*, 2005.

społeczeństwa[74] oraz sposoby zapobiegania i kontroli transgranicznego szerzenia się chorób zakaźnych i innych zagrożeń zdrowotnych[75]. Podobnie konwencja BTWC w art. IV wzywa państwa-strony do krajowej implementacji wszelkich możliwych środków bezpieczeństwa i ochrony biologicznej, w tym do doskonalenia metod detekcji i sposobów nadzoru nad chorobami zakaźnymi. Podkreślano to podczas konferencji przeglądowych w 2011 r. i 2016 r. Także w okresie międzysesyjnym w latach 2007–2010 poruszano zagadnienia związane z ochroną pracowników w laboratoriach, ochroną patogenów, toksyn i sprzętu, mające zastosowanie do zapisów konwencji (2008 r.), oraz kwestie dotyczące usprawniania zdolności reagowania w zakresie rozpoznawania, wykrywania, diagnozowania i zwalczania chorób zakaźnych (2009 r.).

Zagrożenia zdrowotne, które się pojawiły w czasie dwóch ostatnich dekad, w tym pandemia COVID-19, skłoniły do rewizji i aktualizacji IHRs w niektórych obszarach (m.in. ochrona danych osobowych, stosowanie dokumentów cyfrowych). W maju 2024 r. przyjęto poprawki dostosowujące IHRs do obecnych i przyszłych wyzwań w zakresie bezpieczeństwa zdrowotnego.

Warto wspomnieć również o aktualnie procedowanym przez WHO traktacie pandemicznym, którego celem jest lepsze przygotowanie państw na przyszłe zagrożenia zdrowotne. Tu także, podobnie jak przy konwencji BTWC, w trakcie procesu negocjacyjnego dało się zauważyć dwukierunkowość stanowisk krajów rozwijających się i rozwiniętych. Dotyczyło to zwłaszcza kwestii dostępu do materiału genetycznego czynników biologicznych o potencjale pandemicznym, technologii biomedycznej, wyników prac naukowych oraz ochrony własności intelektualnej w zakresie wyrobów medycznych wykorzystywanych podczas pandemii[76].

Bezpieczeństwo transportu substancji biologicznych

Substancje zakaźne są zaliczane do towarów niebezpiecznych, których niekontrolowane przejęcie lub uwolnienie może spowodować skażenie biologiczne środowiska i stworzyć zagrożenie zdrowia. Główne ramowe regulacje odnośnie do klasyfikowania, pakowania i transportu materiałów

[74] The World Health Assembly Resolution 55.16, *Global public health response to natural occurrence, accidental release or deliberate use of biological and chemical agents or radionuclear material that affect health*, 2002.

[75] The World Health Assembly Resolution 58.3, *Revision of the International Health Regulations*, 2005.

[76] *Intergovernmental Negotiating Body*, World Health Organization, https://apps.who.int/gb/inb/index.html [dostęp: 17 XI 2024].

niebezpiecznych zostały określone przez Komitet Ekspertów ONZ ds. Transportu Materiałów Niebezpiecznych (ang. Committee of Experts on the Transport of Dangerous Goods, UNCETDG). Na ich podstawie oraz przy wsparciu organizacji międzynarodowych odgrywających wiodącą rolę w odniesieniu do poszczególnych typów zagrożeń i rodzajów transportu (drogowego, kolejowego, lotniczego i morskiego) opracowano przepisy szczegółowe. WHO doradzało ONZ w tworzeniu regulacji dotyczących transportu substancji trujących i zakaźnych.

Głównym aktem prawnym dotyczącym międzynarodowego przewozu drogowego towarów niebezpiecznych, w tym materiałów zakaźnych, jest *Umowa dotycząca międzynarodowego przewozu drogowego towarów niebezpiecznych* – ADR[77]. Wprowadza ona m.in. obowiązek zapewnienia bezpieczeństwa przewozu materiałów zakaźnych i określa obowiązki nadawcy przesyłki, przewoźnika i kierowcy.

Pomocny w zakresie zagadnień związanych z transportem jest także przewodnik WHO do spraw transportu materiałów zakaźnych[78], w którym zestawiono obowiązujące regulacje oraz zawarto wiele praktycznych rad na temat zasad klasyfikowania przesyłki, sposobu bezpiecznego jej pakowania, znakowania i postępowania z nią podczas załadunku i przewozu. Wszystkie substancje stanowiące zagrożenie biologiczne zostały zaklasyfikowane do klasy 6 – substancje trujące i zakaźne i podklasy 6.2 – substancje zakaźne. Poszczególnym materiałom klasy 6.2 nadano numery kodów klasyfikujących: I1 – materiały niebezpieczne dla ludzi, I2 – materiały niebezpieczne tylko dla zwierząt, I3 – odpady kliniczne, I4 – próbki diagnostyczne. Na czas transportu powinny one zostać dodatkowo oznaczone jednym z kodów UN: UN 2814 – substancje zakaźne działające na ludzi, UN 2900 – substancje zakaźne działające na zwierzęta, UN 3373 – preparaty diagnostyczne, preparaty kliniczne lub substancje pochodzenia biologicznego, UN 3291 – odpady medyczne. Poszczególne kody determinują sposób pakowania. Na przykład towary oznaczone UN 2814 i UN 2900 powinny być pakowane zgodnie z instrukcją P620, UN 3291 według P621, a w przypadku UN 3373 obowiązuje instrukcja pakowania P650. Z kolei czynniki biologiczne modyfikowane genetycznie niespełniające definicji „substancja trująca" bądź „substancja zakaźna" są zaliczane do klasy 9 – różne substancje

[77] *ADR 2023 – Agreement concerning the International Carriage of Dangerous Goods by Road*, United Nations 2022.

[78] *Guidance on regulations for the transport of infectious substances, 2023–2024*, World Health Organization 2024.

i artykuły niebezpieczne, w tym substancje niebezpieczne dla środowiska, które należy oznaczyć jako UN 3245 i pakować według instrukcji P904.

Oprócz tego w zakresie transportu zakaźnych materiałów biologicznych obowiązuje podział na kategorię A i kategorię B. Kategoria A to materiał zakaźny, o którym wiadomo lub podejrzewa się, że może powodować u człowieka lub zwierząt chorobę śmiertelną, chorobę zagrażającą życiu lub mogącą powodować trwały uszczerbek na zdrowiu. Kategoria B to materiał zakaźny niespełniający kryteriów kategorii A, np. próbki kliniczne przewożone do laboratorium w celach diagnostycznych.

Zgodnie z zaleceniami WHO to nadawca przesyłki jest odpowiedzialny za właściwe klasyfikowanie materiału pochodzenia biologicznego, zapakowanie i oznakowanie paczki tak, aby dotarła ona do miejsca przeznaczenia i nie stworzyła podczas przewozu zagrożenia dla ludzi, zwierząt i środowiska. W obowiązku nadawcy jest dołączenie dokumentacji przewozowej, dobranie odpowiedniego środka transportu oraz powiadomienie odbiorcy przesyłki o terminie jej wysłania, co ma gwarantować jej ochronę na każdym etapie podróży.

Przewóz materiałów zakaźnych uszczegóławiają dodatkowo przepisy stosowne dla danego typu środka transportu. Polska także jest zobowiązana ich przestrzegać.

Międzynarodowe rekomendacje w zakresie ochrony biologicznej

Konwencja BTWC w art. IV zobowiązuje państwa-strony do podjęcia wszelkich możliwych środków i działań w celu zapobieżenia rozwijaniu i produkcji czynników biologicznych, toksyn i biotechnologii, które mogą zostać użyte jako broń lub środek bioterroru. Zapis ten zobowiązuje nie tylko do ustanawiania prawa karnego, lecz także do wdrożenia działań prewencyjnych, które pozwoliłyby bezpiecznie prowadzić pokojowe prace z mikroorganizmami oraz ochronić je przed wrogim wykorzystaniem. Szeroki zakres miejsc i działań, w których są wykorzystywane czynniki biologiczne i toksyny szkodliwe dla zdrowia (działalność medyczna, w tym podmioty lecznicze, medyczne laboratoria diagnostyczne, zakłady inżynierii genetycznej, laboratoria stacji sanitarno-epidemiologicznych, działalność weterynaryjna, w tym wiwaria, lecznice weterynaryjne, działalność naukowo-badawcza, sektor farmaceutyczny, biotechnologiczny, sektor rolno-spożywczy) wymagał zastosowania, obok prawnie wiążących regulacji, narzędzi wspomagających. Skuteczne

okazały się podręczniki, instrukcje, wytyczne i inne środki, w których zostały omówione sposoby właściwego postępowania z czynnikami biologicznymi w celu ochrony zdrowia i obiektów ich wykorzystania. Ważną rolę odegrały także międzynarodowe organizacje, ośrodki, instytucje i stowarzyszenia specjalizujące się w wąskich obszarach bezpieczeństwa i ochrony biologicznej w różnych sferach działalności.

Co więcej, niewiążące instrumenty prawne okazały się czytelniejsze niż akty normatywne i łatwiejsze do wykorzystania w praktyce. Znacznie krótsza i prostsza, w porównaniu z nowelizacją obowiązujących aktów prawnych, była droga nanoszenia w nich poprawek w celu dostosowania ich do zmieniających się warunków, w tym do aktualnych zagrożeń biologicznych i postępów w nauce.

Bezpieczeństwo i ochrona biologiczna w laboratorium

Obok ochrony zdrowia osób narażonych na szkodliwe czynniki biologiczne w miejscu pracy nie mniej ważne z punktu widzenia konwencji BTWC jest zapobieganie działalności przestępczej, w której te czynniki są wykorzystywane (bioterroryzm, sabotaż itp.).

Jedną z ważniejszych rekomendacji jest podręcznik WHO dotyczący bezpieczeństwa biologicznego w laboratorium[79], którego pierwsze wydanie zostało opublikowane w 1983 r.[80] Przyjęto w nim, że czynniki biologiczne to główna przyczyna ryzyka, i wskazano warunki bezpiecznej pracy w laboratorium oraz zasady klasyfikowania czynników biologicznych, określono poziomy hermetyczności pozwalające odgraniczyć narażenie oraz omówiono wyposażenie sprzętowo-aparaturowe i dobre praktyki w odniesieniu do poszczególnych grup niebezpiecznych czynników i toksyn. Opisano standardowe procedury operacyjne uwzględniające zdarzenia losowe, środki ochrony osobistej, zasady postępowania z odpadami pochodzenia biologicznego i materiałem zakaźnym, środki dezynfekcji i techniki sterylizacji. W kolejnych edycjach podręcznika rozwinięto tematy związane z indywidualną odpowiedzialnością osób za bezpieczeństwo i ochronę, podjęto aspekt bioetyczny, problematykę nowych osiągnięć nauk przyrodniczych i biotechnologii, zagadnienia dotyczące bezpiecznego transportu przesyłek. Dodano rozdział o ochronie fizycznej obiektu oraz pomieszczeń wykorzystywania czynników biologicznych, rozwinięto wątek potrzeby

[79] *Laboratory biosafety manual. Fourth edition*, World Health Organization 2020.

[80] *Laboratory biosafety manual. First edition*, World Health Organization 1983.

inwentaryzacji mikroorganizmów i sprzętu, ochrony informacji i zasobów wiedzy oraz kontroli personelu mającego do nich dostęp.

Po przeanalizowaniu podejścia WHO do laboratoryjnej ochrony biologicznej, poczynając od 1983 r., a kończąc na najnowszej wersji podręcznika, która ukazała się w 2020 r., można dostrzec, że postanowiono odejść od pierwotnego założenia i przyjęto, że czynniki przynależące do danej grupy ryzyka nie muszą podlegać ściśle regułom przypisanym do danego poziomu bezpieczeństwa biologicznego. Uzasadniono to tym, że na faktyczne ryzyko ma wpływ nie tyle czynnik biologiczny, ile okoliczności towarzyszące (kompetencje personelu, dyscyplina w przestrzeganiu wewnętrznych procedur laboratoryjnych). W rezultacie, po uwzględnieniu założeń trzech wcześniejszych edycji podręcznika i by wyjść naprzeciw krajom rozwijającym się, przyjęto, że ocena ryzyka zagrożenia powinna uwzględniać okoliczności jednostkowe, specyficzne dla danego miejsca i sytuacji (m.in. sytuację epidemiczną w regionie czy kraju, poziom hermetyczności danego laboratorium, jego wyposażenie, kwalifikacje pracowników, dostępność i rodzaj środków ochrony indywidualnej, a także sytuację geopolityczną, w tym prawdopodobieństwo napadu na tle rabunkowym, obecność ugrupowań ekstremistycznych).

W 2024 r. WHO opublikowało wytyczne w publikacji pt. *Laboratory biosecurity guidance*[81]. To kontynuacja wyżej wspomnianego podręcznika i uzupełnienie go o zagadnienia związane z ochroną biologiczną w laboratorium. Zawiera ona przegląd praktyk i zasad pomocnych w zapobieganiu poważnym zdarzeniom biologicznym oraz omawia potencjalne przyczyny tych zdarzeń i możliwe do podjęcia działania na poziomie instytucjonalnym, krajowym i międzynarodowym. Obejmuje takie tematy, jak:

a) ocena ryzyka w zakresie ochrony biologicznej przy wykorzystaniu metodyki zarządzania ryzykiem, m.in. warunki przechowywania czynników biologicznych, transport oraz możliwe sposoby wykorzystania mikroorganizmów i technologii w badaniach eksperymentalnych z podziałem na rodzaj działalności (diagnostyczna, badawcza, repozytorium, biobank),
b) pojawiające się i nowe technologie oraz potencjalne zagrożenia z nimi związane (inżynieria genetyczna, w tym technologia edycji

[81] *Laboratory biosecurity guidance*, World Health Organization 2024.

genomu[82], napęd genowy[83], modyfikacje epigenetyczne[84], biologia syntetyczna, sztuczna inteligencja, ochrona informacji i cyberbezpieczeństwo, techniki „zrób to sam" (ang. *do it yourself*, DIY), publikowanie wyników prac badawczych mogących stanowić źródło informacji, jak wyprodukować broń biologiczną i toksynową,

c) obowiązujące regulacje w tym zakresie oraz wytyczne dla tworzenia krajowych uregulowań (prawo międzynarodowe i krajowe),
d) wzmocnienie roli i odpowiedzialności instytucjonalnych komisji ds. bezpieczeństwa biologicznego,
e) sytuacje krytyczne – wojna, niepokoje społeczne, klęski żywiołowe.

Analizując te wytyczne, warto zwrócić uwagę również na tło, mianowicie na afiliację autorów publikacji oraz ekspertów merytorycznych, którzy wnieśli wkład. Nietrudno wówczas o interpretację zamysłu tego przedsięwzięcia, zwłaszcza gdy się spojrzy przez pryzmat takich zmiennych, jak: sytuacja epidemiczna danego regionu, choroby endemiczne, ryzyko występowania poważnych zagrożeń zdrowia publicznego o zasięgu transgranicznym, aktualna sytuacja geopolityczna, stanowiska krajowe prezentowane podczas posiedzeń dotyczących międzynarodowych porozumień rozbrojeniowych i nieproliferacyjnych, a także uwzględni kraj pochodzenia i profil działalności podmiotu udzielającego wsparcia finansowego. Daje to nadzieję, że opracowane wytyczne dzięki bazowaniu na doświadczeniach krajów rozwiniętych skuteczniej trafią do właściwych adresatów w krajach rozwijających się i tym samym, przez promowanie ochrony biologicznej u źródeł potencjalnego zagrożenia, wzmocnią w skali globalnej bezpieczeństwo i ochronę zasobów biologicznych i technologii.

[82] Technologia edycji genomu (ang. *genome editing*) – polega na wycięciu jednego lub kilku genów i zastąpieniu go innym bądź innymi lub na dezaktywacji genu. Technologia ta jest wykorzystywana w wielu dziedzinach nauk biologicznych oraz jako innowacyjna metoda terapeutyczna niektórych wcześniej nieuleczalnych chorób genetycznych.

[83] Napęd genowy (ang. *gene drive*) – technika polegająca na projektowaniu genetycznym osobników tak, aby w sposób celowy wprowadzały nowe geny do całej populacji gatunku, które następnie są przekazywane w kolejnych pokoleniach. Jest wykorzystywana głównie w celu zmiany całej wolno żyjącej populacji lub jej zniszczenia, np. szkodników upraw, ale także regulowania niektórych gatunków komarów będących wektorami chorób zakaźnych, np. malarii czy endemicznych gorączek krwotocznych.

[84] Modyfikacje epigenetyczne – zmiany chemiczne wpływające na dziedziczne mechanizmy regulacji aktywności genów m.in. patogenność, odpowiedź immunologiczną gospodarza, patogenezę i/lub obraz kliniczny choroby.

Promowaniem zasad bezpieczeństwa i ochrony biologicznej zajmują się również inne światowe ośrodki. Ciekawą pozycją jest podręcznik pt. *Biosafety in Microbiological and Biomedical Laboratories*[85] wydany przez amerykańskie Narodowe Instytuty Zdrowia (National Institutes of Health, NIH), w którym poszerzono omawianie tych zagadnień o laboratoria biomedyczne, placówki weterynaryjne oraz wiwaria wykorzystywane w celach badawczych.

Z kolei inny podręcznik, autorstwa Petera Clevestiga, pt. *Handbook of Applied Biosecurity for Life Science Laboratories*[86] stanowi źródło wiedzy na temat sposobów zabezpieczeń obiektów, w których wykorzystuje się szczególnie niebezpieczne czynniki biologiczne. Dostarcza on wielu użytecznych instrukcji na temat laboratoryjnej ochrony biologicznej. Przystępnie opisuje m.in., jak przeprowadzić ocenę ryzyka dla zabezpieczeń czynników biologicznych i jej wyniki zastosować w praktyce, czym jest odpowiedzialność pracownika za czynniki, z którymi pracuje, w jaki sposób sprawować kontrolę jakościową i ilościową nad zasobami laboratorium, jak chronić informacje wrażliwe dotyczące wykazów posiadanych czynników zakaźnych, aparatury i wyposażenia znajdujących się na terenie obiektu, danych osobowych pacjentów, od których wyizolowano patogeny, i danych personalnych pracowników, jak zabezpieczać transfer i transport szczególnie niebezpiecznych patogenów, aby zminimalizować ryzyko ich nielegalnego przejęcia.

Z kolei wytyczne w zakresie ochrony zasobów biologicznych opracowane przez Organizację Współpracy Gospodarczej i Rozwoju (Organisation for Economic Co-operation and Development, OECD) podejmują aspekt ochrony kolekcji kultur bakteryjnych, ich puli genowych, biotechnologii oraz bezpieczeństwa pracowników laboratoriów i naukowców potencjalnie narażonych na ekspozycję na szkodliwe czynniki biologiczne. Tym bardziej że definicje bezpieczeństwa biologicznego i ochrony biologicznej wypracowane przez delegatów państw-stron biorących udział w spotkaniach dotyczących konwencji BTWC są tożsame z tymi stosowanymi w publikacjach OECD[87]. Dodatkowym wsparciem merytorycznym i praktycznym

[85] P.J. Meechan, J. Potts, *Biosafety in Microbiological and Biomedical Laboratories. 6th edition*, Centers for Disease Control and Prevention, National Institutes of Health 2020.

[86] P. Clevestig, *Handbook of Applied Biosecurity for Life Science Laboratories*, Stockholm International Peace Research Institute 2009.

[87] OECD, *Biological Resource Centres: Underpinning the Future of Life Sciences and Biotechnology*, Paris 2001. https://doi.org/10.1787/9789264193550-en; OECD, *OECD Best Practice Guidelines for Biological Resource Centres*, Paris 2007. https://doi.org/10.1787/9789264128767-en.

w zabezpieczeniu światowych kultur bakteryjnych i wzmacnianiu ochrony biologicznej są wytyczne specjalistycznych organizacji i federacji (Światowej Federacji Kolekcji Kultur – World Federation for Culture Collections, WFCC[88]; Światowej Kolekcji Referencyjnych Szczepów – World Data Centre for Microorganism, WDCM[89]; Europejskiej Organizacji Kolekcji Kultur – European Culture Collections' Organisation, ECCO[90]).

Działalność medyczna i weterynaryjna to jedne z ważniejszych obszarów wykorzystywania czynników biologicznych, dlatego ochrona biologiczna w tych miejscach ma szczególne znaczenie. Do nieuprawnionego przejęcia czynników biologicznych i technologii może dojść także w innych newralgicznych miejscach. Rozpowszechnianie wyników badań naukowych o podwójnym zastosowaniu (ang. *dual use research of concern*, DURC) to kolejny obszar wymagający nadzorowania i ochrony, dlatego tak istotne jest edukowanie i uświadamianie osób mających do czynienia ze szkodliwymi czynnikami biologicznymi na temat ryzyka, jak również budowanie postaw odpowiedzialności[91]. Ochrona biologiczna to także ważny element przeciwdziałania zagrożeniom intencjonalnym i aktom bioterroru[92], zabezpieczenia zasobów żywnościowych przed celową kontaminacją (terroryzm żywnościowy) oraz umyślnym wyrządzeniem szkód w uprawach i hodowli zwierząt (agroterroryzm)[93].

[88] *Guidelines for the Establishment and Operation of Collections of Cultures of Microorganisms. 3rd edition*, World Federation for Culture Collections 2010.

[89] World Data Centre for Microorganisms, https://www.wdcm.org/ [dostęp: 24 XI 2024].

[90] The European Culture Collections' Organisation (ECCO), https://www.eccosite.org/ [dostęp: 24 XI 2024].

[91] *Biosecurity – Freedom and Responsibility of Research*, Deutscher Ethikrat 2014; *Responsible Conduct in the Global Research Enterprise*, The InterAcademy Partnership (IAP) 2012; *Research and methods*, Robert Koch Institut, https://www.rki.de/EN/Content/infections/Dual_Use/code_of_conduct.html [dostęp: 29 XI 2024]; *Dual-use research*, RIVM / Bureau Biosecurity, https://www.bureaubiosecurity.nl/en/dual-use [dostęp: 29 XI 2024].

[92] *Preparedness for the deliberate use of biological agents: a rational approach to the unthinkable*, World Health Organization 2001; *Mental health of populations exposed to biological and chemical weapons*, World Health Organization 2005; *Public health response to biological and chemical weapons: WHO guidance*, World Health Organization 2004.

[93] *Terrorist threats to food: Guidance for establishing and strengthening prevention and response systems*, World Health Organization 2002.

Podsumowanie

Celem ochrony biologicznej jest zapobieganie zagrożeniom biologicznym, w tym intencjonalnym. Z uwagi na szeroki wachlarz potencjalnych zagrożeń (mikroorganizmy, toksyny biologiczne, sprzęt i technologia biologiczna, wiedza specjalistyczna), źródeł ich pochodzenia (naturalne, przypadkowe, intencjonalne) oraz możliwości wykorzystywania czynników biologicznych i technologii biologicznej (rodzaj prowadzonej działalności) do kwestii ochrony biologicznej należy podchodzić wielopłaszczyznowo. Porozumienia rozbrojeniowe i nieproliferacyjne oraz reżimy kontrolne w zakresie BMR (konwencja BTWC, rezolucja 1540, konwencja CWC, AG) wskazują wprost, co powinno być wspólnym mianownikiem skutecznej ochrony środków biologicznych o potencjale podwójnego zastosowania i jak te środki ustanowić na poziomie krajowym[94]. Uregulowania nawiązujące do nich pośrednio (konwencja CBD i jej protokoły, IHRs, umowy w zakresie transportu) mogą wzmacniać ochronę biologiczną, mimo że realizują zupełnie inne cele. Z kolei rekomendacje i wytyczne ośrodków wiodących w przedmiotowym zakresie dostarczają cenną wiedzę i wskazówki dotyczące ich praktycznego wdrażania na poziomie nie tylko instytucjonalnym i resortowym, lecz także krajowym. Przyczyniają się tym samym do wzmocnienia bezpieczeństwa i ochrony biologicznej w skali globalnej.

[94] Mianowicie: a) zapewnić ochronę fizyczną laboratoriów oraz miejsc przechowywania i gromadzenia środków biologicznych, o których mowa w artykule I konwencji BTWC, przed dostępem osób nieuprawnionych oraz przed nielegalnym przejęciem tych środków; b) podjąć odpowiednie środki w celu zapewnienia ochrony czynnikom biologicznym, toksynom i technologii istotnym z punktu widzenia konwencji BTWC, w tym za pomocą środków kontroli dostępu, właściwego postępowania z takimi czynnikami i specjalistycznym sprzętem podczas ich wykorzystywania oraz transportu; c) przyjąć, zgodnie z uregulowaniami konstytucyjnymi państw-stron, środki legislacyjne, administracyjne, sądowe i inne, w tym ustawodawstwo penalne, mające na celu zapewnienie bezpieczeństwa i ochrony czynnikom biologicznym, toksynom i technologii w laboratoriach, obiektach ich wykorzystywania oraz podczas ich transportu; d) ustanowić kompleksowe i konkretne krajowe środki kontroli wykorzystania czynników biologicznych, toksyn i technologii do celów pokojowych; e) dokonywać okresowego przeglądu tych czynników, toksyn i technologii i tam, gdzie to konieczne, uchwalać lub aktualizować prawo krajowe, w tym środki regulacyjne i karne, zapewniające skuteczną realizację zakazu ujętego w artykule I konwencji BTWC, a także aktualizować wykazy czynników biologicznych i urządzeń istotnych dla zapewnienia bezpieczeństwa, ochrony i zachowania reżimów podczas transferu tych czynników.

Bibliografia

Bielecka-Oder A., *Safety and Security Regulations Against Biological Threats*, w: *Defence Against Bioterrorism*, V. Radosavljevic, I. Banjari, G. Belojevic (red.), Springer Netherlands 2018.

Biosecurity – Freedom and Responsibility of Research, Deutscher Ethikrat 2014.

Clevestig P., *Handbook of Applied Biosecurity for Life Science Laboratories*, Stockholm International Peace Research Institute 2009.

Collins English Dictionary – Complete and Unabridged, 12th edition, Collins 2014.

Guidance on regulations for the transport of infectious substances, 2023–2024, World Health Organization 2024.

Guidelines for the Establishment and Operation of Collections of Cultures of Microorganisms. 3rd edition, World Federation for Culture Collections 2010.

Hammond E., *Biopiracy Watch: A compilation of some recent cases*, t. 1, Third World Network 2013.

Laboratory biosafety manual. First edition, World Health Organization 1983.

Laboratory biosafety manual. Fourth edition, World Health Organization 2020.

Laboratory biosecurity guidance, World Health Organization 2024.

Martyniuk E., *Nowe uregulowania prawne dotyczące dostępu do zasobów genetycznych zwierząt i ich potencjalny wpływ na prace hodowlane i badania naukowe*, „Przegląd Hodowlany" 2016, nr 5, s. 10–14.

Meechan P.J., Potts J., *Biosafety in Microbiological and Biomedical Laboratories. 6th edition*, Centers for Disease Control and Prevention, National Institutes of Health 2020.

Nixdorff K., Schilling D., Hotz M., *Critical Aspects of Biotechnology in Relation to Proliferation*, w: *The Implementation of Legally Binding Measures to Strengthen the Biological and Toxin Weapons Convention*, M. Chevrier i in. (red.), NATO Science Series II – t. 150, 2004.

OECD, *Biological Resource Centres: Underpinning the Future of Life Sciences and Biotechnology*, Paris 2001. https://doi.org/10.1787/9789264193550-en.

OECD, *OECD Best Practice Guidelines for Biological Resource Centres*, Paris 2007. https://doi.org/10.1787/9789264128767-en.

Preparedness for the deliberate use of biological agents: a rational approach to the unthinkable, World Health Organization 2001.

Public health response to biological and chemical weapons: WHO guidance, World Health Organization 2004.

Responsible Conduct in the Global Research Enterprise, The InterAcademy Partnership (IAP) 2012.

Terrorist threats to food: Guidance for establishing and strengthening prevention and response systems, World Health Organization 2002.

Źródła internetowe

Approved 1540 Committee Matrix of [State], https://www.un.org/en/sc/1540/documents/Matrix%20Template%202013%20(E).pdf [dostęp: 17 XI 2024].

Australia Group Common Control Lists, The Australia Group, https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/controllists.html [dostęp: 30 XI 2024].

Biological Weapons Convention – Ninth Review Conference, United Nations, Office for Disarmament Affairs, https://meetings.unoda.org/bwc-revcon/biological-weapons-convention-ninth-review-conference-2022 [dostęp: 8 III 2025].

Confidence Building Measures, United Nations, Office for Disarmament Affairs, https://disarmament.unoda.org/biological-weapons/confidence-building-measures/ [dostęp: 13 X 2024].

Dual-use research, RIVM / Bureau Biosecurity, https://www.bureaubiosecurity.nl/en/dual-use [dostęp: 29 XI 2024].

Fighting the spread of chemical and biological weapons, https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/index.html [dostęp: 22 II 2025].

Hyuk K., *Intangible Transfer of Technology (ITT): Open-source Information Analysis for the Implementation of Sanctions on North Korea*, 38 North, 10 III 2023 r., https://www.38north.org/2023/03/intangible-transfer-of-technology-itt-open-source-information-analysis-for-the-implementation-of-sanctions-on-north-korea/ [dostęp: 9 III 2025].

Implementation of the International Health Regulations (2005): Report by the Director-General, World Health Organization 2024, https://apps.who.int/gb/ebwha/pdf_files/WHA77/A77_8-en.pdf [dostęp: 8 III 2025].

Intergovernmental Negotiating Body, World Health Organization, https://apps.who.int/gb/inb/index.html [dostęp: 17 XI 2024].

Introduction, The Australia Group, https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/introduction.html [dostęp: 21 IX 2024].

Participants, The Australia Group, https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/participants.html [dostęp: 21 IX 2024].

Research and methods, Robert Koch Institut, https://www.rki.de/EN/Content/infections/Dual_Use/code_of_conduct.html [dostęp: 29 XI 2024].

Sprawozdanie roczne z postępów w realizacji strategii Unii Europejskiej przeciw rozprzestrzenianiu broni masowego rażenia (2022 r.), Prawo.pl, https://www.prawo.pl/akty/dz-u-ue-c-2023-383,72216862.html [dostęp: 28 IX 2024].

Statement by the Chair of the 2022 Australia Group Plenary, The Australia Group, https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/2021-ag-plenary-statement.html [dostęp: 22 IX 2024].

The European Culture Collections' Organisation (ECCO), https://www.eccosite.org/ [dostęp: 24 XI 2024].

World Data Centre for Microorganisms, https://www.wdcm.org/ [dostęp: 24 XI 2024].

Akty prawne

ADR 2023 – Agreement concerning the International Carriage of Dangerous Goods by Road, United Nations 2022.

Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction, 1993.

European Agreement Concerning the International Carriage of Dangerous Goods by Road (ADR).

Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, 1925.

Protokół z Kartageny o bezpieczeństwie biologicznym do Konwencji o różnorodności biologicznej (Dz. Urz. UE L 201/50 z 31 VII 2002 r.).

Protokół z Nagoi do Konwencji o różnorodności biologicznej o dostępie do zasobów genetycznych oraz sprawiedliwym i równym podziale korzyści wynikających z wykorzystania tych zasobów (Dz. Urz. UE L 150/234 z 20 V 2014 r.).

Resolution 1540 (2004) / adopted by the Security Council at its 4956th meeting, on 28 April 2004, 2004.

The Convention on Biological Diversity, 1993.

The Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction, 1972.

The European Agreement concerning the International Carriage of Dangerous Goods by Inland Waterways (ADN).

The IATA Dangerous Goods Regulations (IATA DGR).

The International Health Regulations, World Health Organization 2005.

The Nuclear Non-Proliferation Treaty (NPT), 1968.

The Regulation concerning the International Carriage of Dangerous Goods by Rail (RID).

Oficjalne stanowiska i dokumenty

Biosafety and Biosecurity – Submitted by the Implementation Support Unit, 24 June 2008.

Final Document of the Ninth Review Conference, Geneva 2022.

Final Document of the Eighth Review Conference, Geneva 2016.

Final Document of the Seventh Review Conference, Geneva 2011.

Final Document of the Sixth Review Conference, Geneva 2006.

Final Document of the Fifth Review Conference, Geneva 2001–2002.

Final Document of the Fourth Review Conference, Geneva 1996.

Final Document of the Third Review Conference, Geneva 1991.

Final Document of the Second Review Conference, Geneva 1986.

Mental health of populations exposed to biological and chemical weapons, World Health Organization 2005.

Statement by the Chair of the 2023 Australia Group Plenary, Paris 2023.

Statement by the Chair of the 2024 Australia Group Plenary, Paris 2024.

The Workshop on Nagoya Protocol for "Collection Holders", Brussels 2017.

The World Health Assembly Resolution 58.29, *Enhancement of laboratory biosafety*, 2005.

The World Health Assembly Resolution 58.3, *Revision of the International Health Regulations*, 2005.

The World Health Assembly Resolution 55.16, *Global public health response to natural occurrence, accidental release or deliberate use of biological and chemical agents or radionuclear material that affect health*, 2002.

Verkley G., Dunja M., Smith D., *The Nagoya Protocol and mBRCs: towards a MIRRI Best Practice for Access and Benefit Sharing (ABS)* – prezentacja podczas ECCO 34 Conference, Session 2 BRCs and Regulations, Paryż, 28 V 2015 r.

Dr Anna Bielecka-Oder

Biolog w zakresie mikrobiologii, epidemiolog, doktor nauk medycznych i nauk o zdrowiu. Specjalizuje się w obszarze bezpieczeństwa i ochrony biologicznej oraz w szczególnie niebezpiecznych i wysoce zakaźnych czynnikach biologicznych, w tym środkach biologicznych używanych w charakterze broni. Zajmuje się również zagadnieniami związanymi z planowaniem działań służących wzmacnianiu gotowości i zdolności do reagowania na zdarzenia z udziałem tego rodzaju czynników i środków.

Kontakt: a.bieleckaoder@gmail.com

ARTYKUŁY RECENZYJNE / RECENZJE

Terroryzm – studia, analizy, prewencja, 2025, nr 7: 181–198

https://doi.org/10.4467/27204383TER.25.029.21806

Recenzja

Kim Ghattas, Czarna fala. Arabia Saudyjska, Iran i czterdziestoletnia rywalizacja, która odmieniła kultury, religię i pamięć zbiorową na Bliskim Wschodzie[1]

Krzysztof Izak
Autor niezależny
https://orcid.org/0000-0001-9815-6035

Kim Ghattas to dziennikarka i pisarka, która urodziła się i dorastała w Libanie, a obecnie mieszka na przemian w Bejrucie i Waszyngtonie. Przez 20 lat relacjonowała i komentowała wydarzenia na Bliskim Wschodzie dla BBC i „Financial Times". Autorka jest stypendystką think tanku Carnegie Endowment for International Peace w Waszyngtonie i członkiem rady powierniczej Uniwersytetu Amerykańskiego w Bejrucie (American University of Beirut).

Recenzowana publikacja ukazała się w wersji anglojęzycznej w 2020 r. Na tle licznych prac dotyczących Bliskiego Wschodu jest

[1] K. Ghattas, *Czarna fala. Arabia Saudyjska, Iran i czterdziestoletnia rywalizacja, która odmieniła kultury, religię i pamięć zbiorową na Bliskim Wschodzie*, Warszawa 2023, Czarna Owca, 496 s.

to pozycja wybitna i unikatowa, ponieważ szczegółowo przedstawia rywalizację między Arabią Saudyjską a Iranem. Wkrótce po wydaniu „The New York Times" uznał ją za jedną z najlepszych książek w dziedzinie literatury faktu.

W publikacji autorka wykorzystała wiele różnych rodzajów źródeł, m.in.: dokumenty archiwalne, prace naukowe i artykuły prasowe. Godna uwagi jest zwłaszcza liczba przeprowadzonych przez nią wywiadów, w tym ze znanymi osobistościami, takimi jak: saudyjski książę Turki al-Faisal, lider tunezyjskiej Partii Odrodzenia (arab. Hizb an-Nahda) Raszid al-Ghannuszi czy zamordowany w 2018 r. saudyjski dziennikarz Dżamal Chaszukdżi. Ghattas ukazała historię nie przez pryzmat jedynie ważnych osobistości, lecz uwzględniła w niej udział wielu mniej znanych lub wręcz nieznanych graczy politycznych, których wpływ na wydarzenia był istotny. Warto zauważyć, że takie podejście jest rzadko spotykane.

Książka *Czarna fala*... ułatwia zrozumienie wydarzeń na Bliskim Wschodzie z lat 1979–2019. To, że zostały opisane różne kraje i okresy, z pewnością komplikowało pracę nad nią, ale dzięki temu czytelnik ma możliwość ujrzenia szerszej perspektywy, obejmującej cały region. Autorka umiejętnie połączyła tematykę historyczną, religijną, kulturową i geopolityczną i przekazała w ten sposób obszerną wiedzę na temat stosunkowo mało znanej (poza specjalistami) rywalizacji pomiędzy Arabią Saudyjską a Iranem. Od momentu zwycięstwa rewolucji islamskiej w 1979 r. rywalizacja ta często była inspirowana przez Stany Zjednoczone. W recenzowanej książce polityka zagraniczna USA na Bliskim Wschodzie została przedstawiona jednak jako drugorzędna w stosunku do sytuacji w regionie, do decyzji zapadających w Teheranie, Rijadzie, Kairze i innych stolicach oraz do ambicji lokalnych decydentów. Tamtejsi obywatele nie są – zdaniem autorki – jedynie ofiarami polityki Zachodu, lecz ponoszą konsekwencje decyzji własnych władz. Relacje między sunnicko-wahabicką Arabią Saudyjską i szyickim Iranem przekładają się na stosunki międzynarodowe w świecie muzułmańskim i stają się źródłem wielu napięć, mordów na tle politycznym, terroryzmu i konfliktów zbrojnych. Autorka w mistrzowski sposób połączyła zagadnienia historyczne z informacjami pochodzącymi od świadków wydarzeń. Książka konfrontuje czytelników z trudnymi realiami, z jakimi mierzą się zwykli ludzie na Bliskim Wschodzie, doświadczający tragicznych konsekwencji antagonizmów w Libanie, Syrii, Iraku i Jemenie oraz fanatyzmu religijnego w Egipcie i Pakistanie. Cierpienia

będące udziałem milionów stanowią dowód tego, jak geopolityczna rywalizacja przekłada się na ludzkie nieszczęście.

Ghattas przedstawiła fascynującą galerię postaci, których losy często się przeplatały. Wiele z nich zakończyło życie tragicznie, inni musieli uciekać ze swojego kraju, aby się ratować. Wykaz wraz z krótkim opisem 59 najważniejszych osób, spośród setek wymienionych w tekście decydentów, dysydentów, uczestników i świadków wydarzeń, znajduje się na początku książki. Dzięki temu podczas lektury można wrócić do notki o postaci, o której się właśnie czyta. Lista została podzielona na kraje. Są to kolejno: Liban, Iran, Arabia Saudyjska, Irak, Syria, Pakistan i Egipt.

Wprowadzenie zaczyna się od pytania: *Co się z nami stało?* (s. 19), które zadaje sobie racjonalnie myśląca część arabskiego społeczeństwa. Należy do niej autorka, a także jej rozmówcy, pamiętający czasy przed czarną falą[2] i diametralną zmianę życia, gdy ta fala rozlała się w ich krajach. Pytanie to ma skłonić do refleksji nad tym, kiedy i dlaczego fanatyzm religijny, zabójstwa na tle religijnym i wojny amorficzne rozprzestrzeniły się w świecie arabskim i muzułmańskim. Podtytuł książki: *Arabia Saudyjska, Iran i czterdziestoletnia rywalizacja, która odmieniła kultury, religię i pamięć zbiorową na Bliskim Wschodzie* może sugerować jedną z odpowiedzi. To samo pytanie autorka powtarza pod koniec (s. 450) i stara się na nie udzielić odpowiedzi, przeprowadzając krótkie podsumowanie przedstawionych wydarzeń.

Książka składa się z trzech części zatytułowanych: *Rewolucja*, *Współzawodnictwo* i *Zemsta*. Tytuły te, podobnie jak tytuły większości rozdziałów, np.: *Mrok*, *Zabiłem faraona*, *Żadnej dupatty* czy *Kain i Abel*, wyraźnie wskazują, że Ghattas nie pisała jej z myślą o ekspertach od Bliskiego Wschodu, lecz chciała dotrzeć do szerokiego grona czytelników. Moim zdaniem doskonale jej się to udało. Na początku każdego rozdziału, oprócz tytułu i motta, są wymienione kraje i przedział czasowy, których dotyczą opisywane wydarzenia.

Część I książki zawiera cztery rozdziały. W pierwszym, noszącym tytuł *Rewolucja kasetowa*, autorka przedstawiła wydarzenia rozgrywające się w latach 1977–1979 w Libanie, Iranie, Iraku i Francji. Rozdział drugi poświęciła Iranowi w latach 1979–1980, trzeci – Arabii Saudyjskiej w 1979 r., a w czwartym skoncentrowała się na krwawych wydarzeniach rozgrywających się w latach 1979–1980 w Arabii Saudyjskiej, Iraku, Iranie, Syrii

[2] Określenie pochodzi od koloru flag używanych przez muzułmańskie organizacje terrorystyczne, takie jak Al-Kaida czy Państwo Islamskie. Bojownicy tej drugiej organizacji powiewali nimi, kiedy zajmowali kolejne miasta w Iraku i Syrii.

i Afganistanie. Historia rozpoczyna się w Libanie w 1977 r., kiedy w ojczyźnie Ghattas toczyła się wojna domowa. Zanim do niej doszło, państwo to było siedzibą opozycjonistów, rewolucjonistów i terrorystów z różnych krajów. Wśród nich byli palestyńscy bojownicy z Al-Fatah (arab. Harakat at-Tahrir al-Filastinijja) i Organizacji Wyzwolenia Palestyny (OWP, arab. Munazzamat at-Tahrir al-Filastinijja), lokalnych zbrojnych ugrupowań nacjonalistycznych i religijnych oraz świeccy nacjonaliści z Ruchu Wyzwolenia Iranu (pers. Nehzat-e Azadi-e Iran) z Mostafą Czamranem na czele, który nawiązał kontakty z miejscowymi szyitami. Wzywał on szacha Iranu Mohammada Rezę Pahlawiego, aby zrzekł się tronu. Czamran odegrał bardzo ważną rolę w późniejszej rewolucji islamskiej i był pierwszym ministrem obrony w porewolucyjnym Iranie. Inny uciekinier z Iranu, Musa al-Sadr, założył w Libanie organizację Ruch Poniżonych (arab. Harakat al-Mahrumin), aby bronić interesów ludności szyickiej, stanowiącej najbiedniejszą wspólnotę religijną w tym kraju. Powołał też Najwyższą Radę Szyicką (arab. Al-Madżlis al-Alam asz-Szia). Irańska rewolucja, której towarzyszyły masowe wystąpienia na ulicach, zaktywizowała nie tylko uciśnionych szyitów w Libanie, lecz także francuskich intelektualistów marksistowskich, takich jak Michel Foucault czy Jean-Paul Sartre. Zastanawiali się oni, czy słabnąca fala arabskiej i europejskiej rewolucji socjalistycznej jest teraz wspierana przez perskie odrodzenie.

W październiku 1978 r. do Francji przyjechał ajatollah Ruhollah Chomeini wraz z kilkoma działaczami Ruchu Wyzwolenia Iranu, którzy byli zmuszeni opuścić Irak. Przejął tam władzę Saddam Husajn i ponownie wzniecił wrogość między Arabami i Persami oraz sunnitami i szyitami, a w 1980 r. wypowiedział wojnę Iranowi. We Francji Chomeini mógł korzystać z wolności słowa i nieograniczonego dostępu do światowej prasy. Nagrywał tam wezwania do obalenia szacha, przesyłane następnie do Iranu i odtwarzane w meczetach. Jego pobyt w Neauphle-le-Château na przedmieściach Paryża trwał niespełna cztery miesiące. W dniu 16 stycznia 1979 r. szach wraz z rodziną opuścił Iran i udał się na emigrację. Dwa tygodnie później triumfalnie powrócił tam Chomeini i po dziesięciu dniach ogłosił zwycięstwo rewolucji islamskiej. Pierwszym zagranicznym przywódcą, który się z nim spotkał, był Jaser Arafat – przewodniczący Al-Fatah i OWP. Przyleciał do Teheranu 17 lutego samolotem użyczonym mu przez prezydenta Syrii Hafeza al-Asada. Przebieg tej wizyty Ghattas opisuje z interesującymi szczegółami.

Saudyjczycy byli bardzo zaniepokojeni rewolucją w Iranie. Duże obawy wśród członków dynastii panującej i przedstawicieli władz religijnych wzbudzały również wydarzenia w ich własnym kraju. W dniu 20 listopada 1979 r. kilkuset islamskich ekstremistów, dowodzonych przez Dżuhajmana ibn Muhammada al-Utajbiego i Muhammada ibn Abdullaha al-Kahtaniego, opanowało Wielki Meczet w Mekce (arab. Al-Masdżid al-Haram). Al-Utajbi poddał krytyce politykę Rijadu – oskarżył monarchię o apostazję i sojusz z chrześcijanami. Domagał się, aby Arabię Saudyjską opuścili eksperci, inżynierowie i doradcy wojskowi z zagranicy. Nawoływał do wprowadzenia „czystego" wahhabizmu, który – jak twierdził – Saudowie oraz prorządowi uczeni muzułmańscy porzucili. Głosił, że jego towarzysz, Al-Kahtani, jest *mahdim*, czyli mesjaszem. Rebelia została brutalnie stłumiona przez władze. Siłom rządowym, wspieranym przez francuskich komandosów, odbicie meczetu zajęło dwa tygodnie. Zgodę na wkroczenie niewiernych Francuzów do świątyni wydał wielki mufti Arabii Saudyjskiej i jej najwyższy autorytet religijny Abdel Aziz bin Baz, którego wizja islamu była nie mniej konserwatywna niż wizja Chomeiniego. Francuscy żołnierze musieli oczywiście najpierw przyjąć islam. Bin Baz wykorzystał potem całe zdarzenie, by zmusić rodzinę królewską i społeczeństwo do życia zgodnie z nakazami islamu, czego domagali się rebelianci okupujący meczet. Po wydarzeniach w Wielkim Meczecie, w wyniku których zginęli wszyscy rebelianci (część podczas szturmu na świątynię, pozostali w egzekucjach), władze Arabii Saudyjskiej, w obawie przed kolejnymi rewoltami fanatyków religijnych, zaczęły realizować postulaty ich przywódców i dokonały wielu zmian w systemie prawnym zgodnie z regułami szariatu. Po 1979 r. odsunięto kobiety od prowadzenia programów telewizyjnych, zakazano publikowania zdjęć w gazetach i reklam z ich udziałem oraz zatrudniania ich, zmuszono je też do zakrywania całego ciała w przestrzeni publicznej. Zamknięto kluby i kina. Policja religijna, czyli funkcjonariusze Komitetu Krzewienia Cnoty i Zapobiegania Występkom (arab. Hajat al-Amr bi al-Maaruf wa al-Nahi an al-Munkar), otrzymała duże fundusze i autonomię działania. Radykalni imamowie i kaznodzieje, którzy zainspirowali Al-Utajbiego, a później Osamę bin Ladena i innych terrorystów, doprowadzili do utrwalenia zasad wahhabickich w saudyjskim społeczeństwie – od podręczników szkolnych promujących nietolerancję wobec odmiennych przekonań religijnych po cofnięcie praw człowieka dla kobiet i mniejszości religijnych, podobnie jak w Iranie. Władze tego kraju interesowały się saudyjskimi elitami rządzącymi. Chomeini był zagorzałym krytykiem dynastii Saudów i wzywał do ich

obalenia. „Eksport rewolucji" islamskiej stał się centralnym tematem irańskiej polityki zagranicznej. Ze względu na aktywne działania nowych przywódców Iranu Saudyjczycy zaczęli promować za granicą własną wersję radykalnego islamu, aby nie tylko chronić, lecz także zwiększać swoje wpływy. Rijad wydał miliardy dolarów na budowę meczetów i szkół religijnych za granicą oraz na finansowanie charytatywnych organizacji religijnych wiernych radykalnej ideologii wahhabickiej i uważających szyitów za heretyków. Irańczycy to samo zrobili w krajach o dużej liczbie szyitów, takich jak Liban, Afganistan i Pakistan. Starali się przedstawić Iran oraz jego przywódców jako prawdziwą awangardę islamu, występującą przeciwko wszystkim jego wrogom, w tym Saudyjczykom.

Dnia 25 grudnia 1979 r. nastąpiła inwazja wojsk ZSRR na Afganistan. Trzy wydarzenia z 1979 r.: rewolucja w Iranie, opanowanie meczetu w Mekce i wkroczenie radzieckich sił do Afganistanu nie miały nic wspólnego ze sobą, ale ich zaistnienie doprowadziło do katastrofy. Upadek szacha początkowo poparli kupcy, nacjonaliści oraz irańska lewica, ale zwolennicy Chomeiniego i teokratycznego państwa szyickiego szybko zyskali przewagę. Atak na Mekkę przeprowadzili ekstremiści, którzy postrzegali dynastię Saudów jako zdrajców rygorów islamu wahhabickiego. Afganistan stał się pierwszym w czasach nowożytnych polem bitwy międzynarodowego dżihadu. Wydarzenia te na zawsze zmieniły Bliski Wschód i zapoczątkowały proces reislamizacji świata muzułmańskiego w duchu radykalnego islamu.

Rewolucja islamska w Iranie i zajęcie meczetu w Mekce wywołały daleko idące zmiany w Arabii Saudyjskiej, polegające na powolnej, ale zdecydowanej ekspansji salafickiego purytanizmu. Przyspieszyły je radziecka okupacja Afganistanu oraz atak wojsk Iraku na Iran 22 września 1980 r. Był to początek ośmioletniej wojny, którą obie strony nazwały arabsko-perską, odwołując się do podziału sięgającego VII w.[3] Ghattas dostrzegła nierównowagę w sposobie relacjonowania ówczesnych wydarzeń w Iranie, Afganistanie i Arabii Saudyjskiej. Podczas gdy informacje z tych dwóch pierwszych państw trafiały na pierwsze strony gazet na całym świecie, wydarzeniom w Arabii Saudyjskiej nie poświęcano uwagi w mediach. Tymczasem według autorki: *W 1979 r. wybuchły dwie islamskie rewolucje.* (…) *Obydwie zostały źle zrozumiane. Jedna z nich polegała na gwałtownym, dramatycznym zawróceniu z drogi postępu i odrzuceniu wielowiekowej tradycji, druga – na powolnym,*

[3] Podział wyznawców islamu na sunnitów i szyitów nastąpił w VII w. Po śmierci w 656 r. trzeciego kalifa z dynastii sprawiedliwych, Usmana Ibn Affana, rozpoczęła się konfrontacja między nimi.

ale zdecydowanym umacnianiu salafickiego purytanizmu. Każda z nich miała przekształcić kraj, w których się wydarzyła, a następnie w kolejnych dekadach rozejść się jak fala po całym świecie arabskim i muzułmańskim (s. 112). To – zdaniem Ghattas – stało się źródłem czarnej fali, która w następnych latach przetoczyła się w świecie muzułmańskim.

Autorka książki ciekawie opisuje zmiany zachodzące w dwóch krajach stanowiących kolebkę czarnej fali, tj. w Iranie i Arabii Saudyjskiej. Stawały się one coraz bardziej opresyjne wobec swoich obywateli. Po ogłoszeniu zwycięstwa rewolucji islamskiej w Iranie rozpoczął się terror. Zamknięto wszystkie uniwersytety. Ich działalność została wznowiona po trzech latach, ale już z inną obsadą kadrową. Dokonano czystek wśród wykładowców, ale też w społeczności studentów. Przeprowadzono je również w armii i instytucjach państwowych. Z czasem „rewolucja zaczęła pożerać własne dzieci". Zginęły tysiące ludzi. Rewolta w Iranie zainspirowała przeciwników prezydenta Syrii Hafiza al-Asada i w 1982 r. doszło do rebelii zorganizowanej przez Braci Muzułmanów (arab. Al-Ichwan al-Muslimin) w mieście Hama. Oba powstania zostały krwawo stłumione przez siły rządowe. Bracia Muzułmanie nigdy nie wybaczyli Chomeiniemu i Iranowi, że zostali przez nich porzuceni. Said Hawwa – jeden z przywódców syryjskich Braci Muzułmanów, który początkowo wychwalał Chomeiniego i jego rewolucję – zaczął potępiać ajatollaha jako zagrożenie dla sunnickiego świata muzułmańskiego. Świat islamu ponownie wkroczył, podobnie jak w średniowieczu, w fazę zwalczania się różnych nurtów religijnych.

Część II książki liczy osiem rozdziałów. Pierwszy i siódmy zostały poświęcone wydarzeniom w Egipcie (lata 1977–1995), drugi i czwarty – w Pakistanie (lata 1978–1988), trzeci – w Libanie (lata 1980–1988), piąty i ósmy – w Arabii Saudyjskiej (lata 1987–2001). W szóstym rozdziale, pt. *Wojny kulturowe*, autorka opisała zmiany, które zaszły w wymienionych państwach w latach 1988–1990. Transformacja pod wpływem radykalnego islamu nastąpiła szybko i objęła wszystkie dziedziny życia. Ghattas dużo miejsca poświęciła Egiptowi. W 1928 r. powstało w tym kraju i z powodzeniem rozwijało się wspomniane wcześniej Stowarzyszenie Braci Muzułmanów (arab. Dżamijjat al-Ichwan al-Muslimin)[4], które w ciągu następnych dekad objęło cały świat muzułmański i stało się źródłem wielu organizacji

[4] Organizacja, która powstała w Egipcie, nosiła nazwę Stowarzyszenie Braci Muzułmanów. Z upływem lat nabrała ona międzynarodowego charakteru, co doprowadziło do zaniku słowa „stowarzyszenie" w nazwie i pojawienia się krótszej formy – Bracia Muzułmanie.

terrorystycznych[5]. Zanim to jednak nastąpiło, rozwijały się nauka, kultura i sztuka o charakterze świeckim. Egipcjanki były pionierkami i głównymi postaciami arabskiego feminizmu. Piosenkarka Umm Kulsum robiła międzynarodową karierę i cieszyła się sławą, a prezydent Egiptu Gamal Abdel Naser traktował ją jak dobro narodowe. Zdaniem Ghattas Egipt jest doskonałym przykładem przyspieszenia i zaostrzenia radykalnej reislamizacji w wyniku rewolucji w Iranie i odrodzenia saudyjskiego wahhabizmu. Przejawem tej reislamizacji było m.in. powstanie organizacji Egipski Islamski Dżihad (arab. Al-Dżihad al-Islami al-Misri), założonej w 1978 r. przez Muhammada Abd as-Salama Faradża, głównego ideologa i stratega ugrupowania, oraz Abbuda Abd al-Latifa az-Zummura, oficera armii egipskiej. Głównym celem tej organizacji było obalenie władz w Egipcie. Nową wykładnią dżihadu stała się książka Faradża pt. *Al-Farida al-Ghajba* (pol. *Zaniedbany obowiązek*), wydana w konspiracji w 1980 r. Autor stwierdził w niej między innymi, że środkiem do osiągnięcia ostatecznego celu w postaci odtworzenia państwa muzułmańskiego jest walka zbrojna i zabicie tych, którzy sprzeniewierzyli się zasadom islamu. Przedstawiona przez Faradża koncepcja świętej wojny stała się apologią terroryzmu i legitymizowała zamach na prezydenta Egiptu Anwara as-Sadata, który zdradził islam, podpisując w marcu 1979 r. porozumienie pokojowe z Izraelem. Do zamachu na As-Sadata doszło 6 października 1981 r. w Kairze. Podczas parady wojskowej, zorganizowanej z okazji rocznicy wojny z Izraelem w 1973 r., czterech członków Egipskiego Islamskiego Dżihadu pod dowództwem por. Chalida Ahmeda Szawkiego al-Islambuliego, uzbrojonych w automatyczne karabiny szturmowe oraz granaty, odłączyło się od defilującego pododdziału i zaatakowało trybunę, na której znajdował się prezydent wraz z gośćmi honorowymi. Oprócz As-Sadata zginęło osiem osób, a ok. 30 zostało rannych, w tym oficerowie armii USA[6]. Czterech bezpośrednich zamachowców oraz Faradża skazano na karę śmierci, wielu innych otrzymało kary więzienia. Wśród nich znajdował się lekarz Ajman az-Zawahiri. Oskarżono go o udział

[5] Od lat 70. XX w. w narodowych strukturach Braci Muzułmanów dużą rolę zaczęły odgrywać frakcje, które swoje cele, m.in. obalenie rządów niewiernych i islamizację, postanowiły osiągnąć nie przez kontynuowanie pracy organicznej, ale przez walkę zbrojną. W Egipcie z Braci Muzułmanów wyłoniła się Egipska Grupa Islamska, w Libanie – Ruch Zjednoczenia Islamu, w Gazie – Hamas, w Sudanie – Islamski Front Narodowy.

[6] Autorka książki błędnie przypisała zamach Grupie Islamskiej (arab. Al-Dżama'a al-Islamijja). Dokonał go Islamski Dżihad (arab. Al-Dżihad al-Islami). Autor recenzji krótko doprecyzował przebieg i skutki tego zamachu. Zob. K. Izak, *Leksykon organizacji i ruchów islamistycznych*, Warszawa 2014, s. 158–159.

w planowaniu zamachu i handel bronią. Został skazany na trzy lata więzienia. Po zwolnieniu w 1984 r. wyjechał do Peszawaru w Pakistanie, gdzie podjął współpracę z Osamą bin Ladenem.

W drugiej połowie lat 80. XX w. doszło do wielu ataków na egipskich polityków i intelektualistów. W 1987 r. ciężko raniono byłego ministra spraw wewnętrznych Hassana Abu Baszę oraz zamordowano Makrama Muhammada Ahmeda – redaktora naczelnego tygodnika „Al-Musawar" (pol. Fotograf). W 1989 r. ofiarą zamachu padł były minister spraw wewnętrznych Zaki Badr, a w 1990 r. – przewodniczący parlamentu Rifat Mahdżub. W 1992 r. zginął Faradż Foda – znany intelektualista oraz przeciwnik islamskiego radykalizmu. W czasie procesu zabójców Fody powołany na świadka obrony Muhammad al-Ghazali, czołowy uczony muzułmański i charyzmatyczny kaznodzieja, stwierdził, że gdy osoba urodzona jako muzułmanin walczy z szariatem, tak jak Foda, popełnia występek apostazji podlegający karze śmierci. Ghattas pisze: (…) *wykonanie wyroku śmierci na apostatach należało do państwa, ale ponieważ państwo nie zdołało powstrzymać Fody, wyrok mogli wykonać prawi muzułmanie. Ghazali oświadczył, że nie powinno być żadnej kary dla muzułmanina, który podejmuje wykonanie takiego śmiercionośnego obowiązku* (s. 270). W 1993 r. ekstremiści podjęli próbę zamachu na premiera Atefa Sidkiego, ministra spraw wewnętrznych Hassana Muhammada al-Alfiego oraz ministra informacji Safwata al-Szarifa. Zaatakowano również laureata literackiej Nagrody Nobla Nadżiba Mahfuza, który w 1994 r. został ugodzony nożem w szyję. Przeżył, ale jego ręka została poważnie uszkodzona. Kolejną ofiarą był wykładowca uniwersytecki Nasr Abu Zajd. W jego dziełach znaleziono nieodpowiednie treści i okrzyknięto go apostatą. Sąd wbrew jego woli rozwiódł go z żoną, gdyż zgodnie z zasadami islamu muzułmanka nie może być poślubiona innowiercy (Abu Zajd stał się nim jako apostata). Jego małżonka nie podporządkowała się wyrokowi i w 1995 r. oboje wyjechali do Europy. Osiedlili się w Lejdzie, w zachodniej Holandii, gdzie Abu Zajdowi zaproponowano pracę w miejscowym uniwersytecie. Wydarzenia te dobitnie pokazały, że radykalny islam miał wpływy w egipskich kręgach prawniczych, i to nie tylko wśród adwokatów, nad których związkiem Bracia Muzułmanie przejęli kontrolę już w 1992 r., lecz także wśród sędziów. Okazało się, że umiarkowani i radykalni islamiści zaczęli działać wspólnie – ci drudzy mordowali ofiary wskazane przez tych pierwszych. Kierowanie ataków na świeckich intelektualistów służyło pogłębieniu fanatyzmu religijnego.

Czarna fala dotarła również do Pakistanu. Autorka rozpoczyna narrację poświęconą temu państwu od historii Mahtab Channy (po mężu: Mahtab Akbar Rashdi), znanej prezenterki telewizyjnej i radiowej, wykładowczyni na Uniwersytecie Sindh (University of Sindh), która wyjechała do Stanów Zjednoczonych, aby studiować stosunki międzynarodowe. Do Pakistanu wróciła w 1978 r., rok po tym, jak wprowadzono tam dyktaturę. W lipcu 1977 r. został aresztowany popularny i charyzmatyczny premier Zulfikar Ali Bhutto, wyznawca islamu szyickiego w jego umiarkowanej wersji. Obalił go dowódca sił zbrojnych gen. Mohammad Zia ul-Hak, który obiecywał, że sytuacja powstała po zamachu będzie tymczasowa. Oświadczył on: *Moim jedynym celem jest zorganizowanie wolnych i uczciwych wyborów, które odbędą się w październiku tego roku. Zaraz po wyborach władza zostanie przekazana wybranym przedstawicielom narodu. Uroczyście zapewniam, że nie odstąpię od tego harmonogramu* (s. 162). Wybory jednak nigdy się nie odbyły, a we wrześniu 1977 r. generał ogłosił się prezydentem. W kwietniu 1979 r. pomimo protestów całego świata Zulfikar Ali Bhutto został stracony. Ghattas poświęca dużo uwagi wydarzeniom rozgrywającym się w Pakistanie. Przypomina, że islamistyczne ugrupowania aktywnie działały tam od dziesięcioleci. Największe i najbardziej znane, Stowarzyszenie Muzułmańskie (ur. Dżama'at-e Islami), zostało powołane już w 1941 r., a więc sześć lat przed powstaniem Pakistanu. Założył je w mieście Lahaur znany radykalny uczony muzułmański Abu Al al-Maududi. Jednak zmiany w kraju prowadzące do jego islamizacji następowały powoli. Przyspieszenia nabrały po przejęciu władzy przez Zia ul-Haka, który nazwał się żołnierzem islamu. Był on głęboko wierzącym, ortodoksyjnym muzułmaninem, uzurpującym sobie moralne prawo do podjęcia szeroko zakrojonej polityki islamizacji państwa. Jego ambicją było uczynienie z każdego Pakistańczyka gorliwego i bogobojnego muzułmanina. Dnia 10 lutego 1979 r., dzień przed ogłoszeniem zwycięstwa rewolucji islamskiej w Iranie, Zia ul-Hak wprowadził surowe prawa szariatu. Mahtab Channa obserwowała te zmiany z przerażeniem. Została zwolniona z telewizji, ponieważ nie zgodziła się z nakazem zakrywania włosów na wizji. Nakaz ten wkrótce zaczął dotyczyć kobiet przebywających w miejscach publicznych. Jednocześnie od początku lat 80. w Pakistanie zwiększały się wpływy religijne Arabii Saudyjskiej. Przez kraj płynęła pomoc, głównie amerykańska i saudyjska, dla afgańskich mudżahedinów walczących z Rosjanami. Rosło również saudyjskie wsparcie finansowe dla szkół koranicznych kształcących dzieci i młodzież, które uciekły z Afganistanu. To młode pokolenie dało początek talibom.

W tamtym czasie ważną rolę odgrywało miasto Peszawar, nazywane „miniarabistanem" i stanowiące rodzaj tygla międzynarodowego dżihadu. Zbierali się w nim ochotnicy przybywający z całego świata, aby w sąsiednim Afganistanie walczyć z Armią Czerwoną. Przebywali tam również założyciele Al-Kaidy – Abdullah Azzam, Osama bin Laden i Ajman az-Zawahiri. Z kolei Dżamal Chaszukdżi, któremu Ghattas poświęciła ostatni rozdział książki, był korespondentem w Peszawarze, wysyłającym do saudyjskich gazet pełne zachwytu depesze. Był on zafascynowany dżihadystyczną międzynarodówką, w której widział jedność ummy, czyli światowej społeczności muzułmańskiej. W jego oczach afgańscy mudżahedini prowadzili sprawiedliwą i chwalebną wojnę przeciwko niewiernym, tzn. radzieckim najeźdźcom. Za zgodą pakistańskich służb specjalnych powstawały zbrojne ugrupowania i milicje, których celem było atakowanie mniejszości szyickiej. W 1987 r. afgańscy i pakistańscy bojownicy zaatakowali wioski należące do szyickiego plemienia Turi w regionie Kurram, przy granicy z Afganistanem. Szyici odparli atak. W trwających dwa tygodnie walkach zginęło 52 szyitów i 120 sunnitów, a 14 wiosek częściowo lub całkowicie zniszczono. Według Ghattas: *Było to epicentrum nowoczesnego rozlewu krwi na tle religijnym, pierwszego tego rodzaju w czasach współczesnych. Konflikt religijny przybrał zbrojną postać. Następnie zaczęły się zamachy* (s. 230). Rywalizacja między Arabią Saudyjską i Iranem przeniosła się do Pakistanu, gdzie sunnici i szyici zaczęli się systematycznie mordować. Nienawiść ta była umiejętnie podsycana przez władze Arabii Saudyjskiej, które w swoim kraju prześladowały szyitów i zatrzymywały ich przywódców religijnych.

Saudowie wyłożyli wiele milionów dolarów na odbudowę kompleksu świątynnego w Mekce, zniszczonego podczas wydarzeń w 1979 r., i wzniesienie wokół hoteli dla pielgrzymów. Zadanie to zlecono Saudi Binladin Group, holdingowi budowlanemu założonemu w 1931 r. przez Muhammada bin Ladena, ojca Osamy. Jego wykonanie wiązało się ze zburzeniem wielu zabytków pamiętających czasy pierwszych muzułmanów. Z tych działań najbardziej zadowolony był wahhabicki establishment religijny, walczący z wszelkimi przejawami upamiętniania przodków. Jednocześnie nasilał się rygoryzm religijny. Aby przeprowadzić reformy w Arabii Saudyjskiej, odwrócić uwagę od własnego, zachodniego stylu życia i zapewnić sobie legitymizację sprawowania władzy u muzułmańskich uczonych, Saudowie stopniowo zwiększali ich przywileje i możliwości kontrolowania życia społecznego. W 1984 r. król Fahd otworzył Kompleks Drukowania Świętego Koranu nazwany jego imieniem (arab. Madżma al-Malik Fahd al-Itibit

al-Mushaf al-Szarifi), jedną z największych drukarni na świecie, będącą w stanie wypuścić 8 mln sztuk Koranu rocznie. Drukowano w niej nową, rzekomo doskonałą, wersję świętej księgi, zaopatrzoną w adnotacje i komentarze, oraz jej przekład na język angielski. Mnóstwo egzemplarzy tej wersji Koranu (oraz jej kolejnych dodruków), zawierającej m.in. agresywne treści wymierzone w Żydów i chrześcijan, rozdano pielgrzymom oraz rozprowadzono za granicą za pośrednictwem saudyjskich ambasad.

W 1986 r. – jak pisze Ghattas – (...) *król Fahd ogłosił, że oficjalnie zastępuje tytuł Jego Królewskiej Mości tytułem Strażnika Dwóch Świętych Meczetów. Tytułu tego, wprowadzonego przez Saladyna w czasach wypraw krzyżowych, nigdy nie używano oficjalnie aż do czasu, gdy pojawił się król Fahd* (s. 241). Przez cały okres wojny iracko-irańskiej (1980–1988) Fahd wspierał Bagdad miliardami dolarów. Ideologia wahhabicka, która inspirowała Saudyjczyków i innych muzułmanów do walki z radziecką okupacją Afganistanu, stała się narzędziem do szerzenia w świecie islamu idei nietolerancji, radykalizacji i terroryzmu. Rząd w Rijadzie inaczej postrzegał saudyjskich bojowników dżihadu w kraju i za granicą. Tych pierwszych zwalczał, a tych drugich traktował jak wahhabickich męczenników. Na oderwaniu Saudów od wahhabizmu zależało Amerykanom. Nie było to jednak możliwe. Ta ideologia wyniosła ich do władzy i wywodzili z niej swoją legitymizację. Elita religijna kraju cieszyła się patronatem wielu książąt i konflikt z wahhabitami mógł pozbawić Saudów władzy.

Po ataku USA na Afganistan w październiku 2001 r. i Irak w 2003 r. w Arabii Saudyjskiej pojawiła się nowa fala radykalizacji, podobna do tej, która nastąpiła po wojnie w Iraku w 1991 r. Inne były jednak zarzuty kierowane pod adresem rodziny królewskiej. W latach 90. XX w. członkowie fundamentalistycznego odrodzenia zwanego przebudzeniem (arab. *sahwa*) zarzucali królowi Fahdowi, że wezwał niewiernych w celu wyzwolenia Kuwejtu. Na początku XXI w. sympatycy dżihadu Al-Kaidy oskarżali Saudów o udzielanie pomocy niewiernym z Zachodu w ich wojnie z Irakiem oraz z rządzonym przez talibów Afganistanem, który dał schronienie Bin Ladenowi i jego zwolennikom. Podkreślano bezprawność sprawowania władzy przez dynastię Saudów i konieczność wypędzenia z kraju Amerykanów. Pomimo wielu starań i uległości wobec władz religijnych, krzewienia w świecie muzułmańskim ideologii wahhabickiej, Saudowie mieli więc wrogą, radykalną opozycję poza granicami swojego państwa.

Podobnie jak w latach 80. XX w. Peszawar był „miniarabistanem", tak libański Baalbek i Dolina Bekaa stały się placówką Teheranu. Właśnie w tym

regionie został utworzony Hezbollah (arab. Hizb Allah – Partia Boga). Bezpośredni wpływ na powstanie tej organizacji miały wkroczenie 6 czerwca 1982 r. wojsk izraelskich do Libanu oraz działania ambasadora Iranu w Bejrucie – ajatollaha Alego Akbara Mohtaszemiego. Na jego prośbę z Teheranu przerzucono do Doliny Bekaa ok. 1500 żołnierzy Korpusu Strażników Rewolucji Islamskiej (pers. Sepah-e Pasdaran-e Inqelab-e Eslami) z zadaniem szkolenia libańskich bojowników szyickich. Głównymi postaciami związanymi z realizacją tego przedsięwzięcia byli znany szyicki duchowny Raghib Harb i pierwszy przywódca Hezbollahu Subhi al-Tufajli. Jego zastępcą został Naim Kasim, który wcześniej działał w Oddziałach Libańskiego Oporu (arab. Afwadż al-Mukawama al-Lubnanija, Amal). Oprócz nich trzon Hezbollahu tworzyła grupa szyickich duchownych, na czele z Sajjidem Hassanem Nasrallahem. Zbrojnymi skrzydłami Hezbollahu były Islamski Opór (arab. Al-Mukawama al-Islamijja) oraz Islamski Dżihad (arab. Al-Dżihad al-Islami), który zorganizował zamachy samobójcze na kwatery wojsk Izraela, USA i Francji. Były to pierwsze tego typu ataki na Bliskim Wschodzie. Ludzi żyjących pod kontrolą Hezbollahu zmuszano do znoszenia ograniczeń społecznych i prawnych oraz poddawano ideologicznej indoktrynacji, co dotąd było obce Libanowi. Autorka książki przykuwa uwagę czytelnika opisem pierwszych ośmiu lat terrorystycznej działalności Hezbollahu i losów jego przywódców.

Ghattas ciekawie opisuje również sprawę książki Salmana Rushdiego pt. *Szatańskie wersety*, o której było głośno w momencie wycofywania sił radzieckich z Afganistanu na początku 1989 r.[7] Gdy powieść ukazała się we wrześniu 1988 r., ajatollah Chomeini nie wnosił żadnego sprzeciwu. Wywołała ona natomiast burzliwe protesty w Wielkiej Brytanii. Wspierały je Arabia Saudyjska oraz różne organizacje muzułmańskie. Mimo to książkę przetłumaczono na język perski i sprzedawano w Teheranie. Sytuacja zmieniła się, gdy do kampanii przeciwko *Szatańskim wersetom* bezpośrednio włączyła się Arabia Saudyjska jako strażnik islamu. Przy udziale swojej ambasady w Londynie zorganizowała akcję na rzecz zakazu rozpowszechniania tej powieści i postawienia jej autora przed sądem. Chomeini

[7] Tytuł książki nawiązuje do słów zachęcających do czczenia pogańskich bogiń Al-Lat, Manat i Al-Uzza, które to słowa rzekomo szatan podszepnął prorokowi Muhammadowi. Prorok miał stwierdzić, że miejsce tych bogiń jest przy Allahu. Dzięki tej wypowiedzi Muhammad zyskał sojuszników we wrogim mu plemieniu Kurajszytów, ale kilka dni potem zaprzeczył tej narracji. Jej treść miała się jednak znaleźć w pierwotnej wersji 53. sury Koranu zatytułowanej *Gwiazda* (arab. *An-Nadżm*).

nie mógł pozostać bierny wobec działań Królestwa. Wezwał nie tylko do zakazu sprzedaży książki, lecz także do zabicia jej autora i każdej osoby zaangażowanej w publikację tego dzieła. Za głowę Rushdiego wyznaczył nagrodę w wysokości 3 mln dolarów. Saudyjskie władze religijne, „pokonane" przez irańską fatwę, ogłosiły, że tamtejsze sądy powinny spróbować zaocznie skazać Rushdiego za bluźnierstwo. Autor *Szatańskich wersetów* nie stanął jednak przed sądem i uniknął śmierci[8]. Zamordowani zostali natomiast tłumacze jego powieści na japoński i turecki oraz wydawca norweskiego tłumaczenia. Wyścig nietolerancji religijnej między Arabią Saudyjską i Iranem to tylko jeden z wątków książki Ghattas. Pisze ona: *Śmierć jako kara za bluźnierstwo pojawiła się w świecie muzułmańskim w wyniku dziwnego zwrotu w rywalizacji między Iranem a Arabią Saudyjską o pozycję światowego przywódcy islamu* (s. 256). Od tej pory w wielu krajach muzułmańskich zaczęli ginąć ludzie oskarżani o bluźnierstwo. Muzułmańscy radykałowie egzekucje przeprowadzali najczęściej na ulicach.

Część III książki składa się z siedmiu rozdziałów i obejmuje lata 2003–2019. Poświęcono je wydarzeniom oraz losom mieszkańców w krajach będących tematem poprzednich rozdziałów oraz dodatkowo Syrii i Turcji. W ostatniej części publikacji autorka w interesujący sposób ukazała dalszy przebieg saudyjsko-irańskiej rywalizacji ideologiczno-religijnej i walki o rząd dusz na Bliskim Wschodzie oraz przejęcie kontroli przez ekstremistów muzułmańskich w Syrii i Jemenie. Walka ta w dużej mierze przekształciła się w wojny zastępcze między Rijadem i Teheranem.

W pierwszym rozdziale, dotyczącym Iraku, Ghattas wróciła do lat 90., w których reżim Saddama Husajna krwawo rozprawił się z szyitami i zgładził ich przywódców religijnych. Wkroczenie do tego kraju w 2003 r. amerykańskich wojsk wzbudziło nadzieje na pozytywne zmiany społeczne. Stało się jednak inaczej. Iraccy żołnierze zwolnieni z wojska przez Amerykanów oraz funkcjonariusze byłego reżimu utworzyli tajne ugrupowanie Powrót (arab. Al-Awda). Większość sunnitów uważała, że delegalizacja irackiej partii Baas (pol. Odrodzenie)[9] oraz demobilizacja i zwolnienie z pracy w instytucjach publicznych członków tej partii były niesprawiedliwe.

[8] W sierpniu 2022 r. muzułmański radykał zaatakował Salmana Rushdiego nożem. Do zdarzenia doszło podczas spotkania autorskiego w mieście Chautauqua niedaleko Buffalo w stanie Nowy Jork. W wyniku odniesionych obrażeń pisarz stracił wzrok w jednym oku i władzę w lewej ręce.

[9] Nazwa partii to skrót od Hizb al-Baas al-Arabi al-Isztiraki (Partia Socjalistycznego Odrodzenia Arabskiego).

Co więcej, działania te zostały odebrane jako cios we wszystkich wyznawców sunnizmu, a nie tylko tych, którzy należeli do Baas. Wykluczeni z życia publicznego, bezrobotni członkowie partii zaczęli organizować się w grupy rebelianckie, walczące z Amerykanami i występujące przeciwko irackim szyitom. Za rządów Saddama Husajna byli oni prześladowani, ale po jego obaleniu zaczęli dominować w życiu politycznym, gdyż mieli przewagę liczebną w społeczeństwie (stanowili 60%). Rozczarowani, zwłaszcza dawni wojskowi, szybko dołączyli do antyamerykańskiego ruchu oporu. Błędy, które wówczas popełniono[10], wywołały falę przemocy oraz doprowadziły do wybuchu sunnickiego powstania i krwawych walk między szyicką Armią Mahdiego (arab. Dżajsz al-Mahdi) i sunnitami, na czele z członkami organizacji Zwolennicy Islamu (arab. Ansar al-Islam). W ciągu kilku pierwszych lat po inwazji Saudyjczycy stanowili prawie połowę zagranicznych bojowników biorących udział w powstaniu, a saudyjscy dżihadyści przeprowadzili więcej zamachów samobójczych niż islamscy ochotnicy z jakiegokolwiek innego kraju. Ghattas pisze: *Saudyjczycy ostrzegali Amerykanów przed inwazją i przekonywali, że nie posłuży ona niczyim interesom i spowoduje odrodzeniem się fundamentalizmu, który dotrze aż do Stanów Zjednoczonych i Europy. Ostrzegali przed zniszczeniem Iraku, ale tak naprawdę obawiali się, że Irakiem rządzonym przez szyitów kierować będzie Iran. Sunnickie powstanie stało się zabójczym antidotum* (s. 326–327).

Z organizacji powiązanych wówczas z Al-Kaidą powstało Państwo Islamskie, które okazało się największą, najbogatszą i najbardziej morderczą organizacją terrorystyczną na świecie. Zyskała ona zwolenników i stworzyła filie w wielu państwach muzułmańskich. Arabia Saudyjska nawet wtedy nie przestała wspierać rozprzestrzeniania się ekstremizmu wahhabickiego. Jego ofiarą padł w Pakistanie Salman Taseer, gubernator prowincji Pendżab, który w styczniu 2011 r. został zamordowany przez własnego ochroniarza. Zabójca nie mógł się pogodzić z tym, że polityk sprzeciwiał się prawu dotyczącemu bluźnierstwa i stanął w obronie chrześcijanki Asii Bibi oskarżonej o ten występek. Mordercę skazano na karę śmierci i powieszono w 2016 r. Uznano go za męczennika, a meczet wybudowany ku jego czci na przedmieściach Islamabadu gromadzi tysiące

[10] Paul Bremer, amerykański cywilny administrator Iraku, skupił całość władzy w tym państwie i rozwiązał iracką armię, co spowodowało, że rzesza mężczyzn znalazła się bez pracy. To było jedno ze źródeł rebelii. Opóźniając przejmowanie odpowiedzialności za kraj przez Irakijczyków, Bremer przyczynił się do uznania Amerykanów za okupantów, a nie wyzwolicieli.

wiernych. Ghattas stwierdza: *Od zakończenia wojny z ZSRR w Afganistanie wpływy saudyjskie w Pakistanie stały się mniej wyraźne, ale być może bardziej podstępne. Funkcjonariusze saudyjskiego wywiadu nie musieli już latać do Peszawaru dwa razy w miesiącu z torbami gotówki, jak miało to miejsce w latach osiemdziesiątych. Mieli dobrze rozwiniętą sieć kontaktów, zarówno formalną, jak i nieformalną* (s. 357).

Autorka książki zbyt pobieżnie podeszła do sytuacji w Syrii. Za jej problemy obwiniła Iran, podobnie jak winą za powstanie Państwa Islamskiego obarczyła Arabię Saudyjską. Tymczasem przyczyny wybuchu wojny domowej w Syrii w 2011 r. były bardziej złożone, a główną rolę odegrał reżim w Damaszku. Znaczący wpływ na przebieg wojny w Syrii miały Stany Zjednoczone, które wysłały tam duże ilości broni i wspierały rebeliantów, o czym autorka nie wspomniała. Milczeniem pominęła również udział Turcji w syryjskim konflikcie. W książce zabrakło ponadto komentarza dotyczącego Libii. Ghattas wspomina o tym kraju jedynie marginesowo, w odniesieniu do opisywanych przez nią różnych postaci, które spędziły tam trochę czasu. Tymczasem podczas Arabskiej Wiosny w 2011 r. doszło w Libii do antyrządowej rebelii. Wspierało ją lotnictwo NATO, wbrew postanowieniu Rady Bezpieczeństwa ONZ, które zezwalało jedynie na strefy lotów, a nie na bombardowanie z powietrza i wspomaganie rebeliantów. Autorka nie napisała ponadto o ataku na konsulat USA w Bengazi przeprowadzonym 11 września 2012 r. przez islamskich ekstremistów powiązanych z Al-Kaidą. Zginął wówczas amerykański ambasador Chris Stevens i cztery inne osoby. Ciekawie natomiast został opisany przebieg Arabskiej Wiosny w Egipcie. Doprowadziła ona do upadku prezydenta Hosniego Mubaraka i wyboru na to stanowisko w 2012 r. Muhammada Mursiego, wywodzącego się z Braci Muzułmanów. Zmiany w Egipcie z dużym niepokojem obserwowali Saudowie, gdyż polityczny sukces Braci Muzułmanów w tym kraju mógł stać się inspiracją do zorganizowania przewrotu w Arabii Saudyjskiej. Jednak po roku urzędowania „kłopotliwy" prezydent został obalony przez wojsko.

Sofana Dahlan, saudyjska prawniczka i jedna z rozmówczyń autorki, stwierdziła, że chciała wierzyć, (...) *że Muhammad ibn Salman jest bohaterem, na którego jej pokolenie od dawna czekało* (s. 434). Młody Salman, zwany także MbS[11], po objęciu tronu w 2015 r. przez ojca, króla Salmana, został ministrem obrony, a wkrótce potem również następcą tronu sprawującym

[11] MbS jest akronimem stworzonym od nazwiska księcia, w którym słowo „ibn" zostało zastąpione przez „bin". Oba wyrazy oznaczają w języku arabskim 'syn'.

rzeczywistą władzę w kraju. Zniósł zakaz prowadzenia samochodów przez kobiety i uwolnił dla nich wiele zawodów. Nakazał ponowne otwarcie kin i sal koncertowych oraz przypuścił atak propagandowy na religijny konserwatyzm Królestwa, czym zyskał poklask młodych Saudyjczyków. Jego wypowiedzi i działania przyciągały uwagę mediów na całym świecie. Ghattas pisze: *Kiedy ogłosił, że epoka roku 1979 dobiegła końca, miał rację pod jednym względem: religia już nie wystarczała, by motywować społeczeństwo i mobilizować masy* (s. 440). Za tą pozą reformatora kryła się jednak postać okrutnego tyrana, nieznoszącego sprzeciwu i krytyki. Stąd porwania i aresztowania przeciwników saudyjskiego reżimu, w tym głośna śmierć wspomnianego wcześniej dziennikarza Dżamala Chaszukdżiego. Autorka poświęciła mu ostatni rozdział, zatytułowany *Morderstwo nad Bosforem*. Chaszukdżi został zamordowany 2 października 2018 r. w konsulacie swojego kraju w Stambule, a jego zwłoki poćwiartowano. Życie dziennikarza i jego śmierć mogą stanowić epilog książki w odniesieniu do Arabii Saudyjskiej i jej postrzegania przez zamordowanego – od wczesnego poparcia dla afgańskich mudżahedinów po jego późniejsze, fatalne w skutkach uświadomienie sobie, że reformy następcy tronu zostały tak pomyślane, aby utrzymać dynastię Saudów przy władzy. W 2019 r. pięciu zabójców Chaszukdżiego sąd w Rijadzie skazał na karę śmierci. Jednak ich mocodawcy i ci, którzy nadzorowali zabójstwo dziennikarza, nigdy nie stanęli przed sądem. Wśród nich był sam książę Salman i jego prawa ręka od czarnej roboty – Saud al-Kahtani. Po okresie dyplomatycznej izolacji Królestwa, a nawet po opublikowaniu raportu Wysokiego Komisarza Narodów Zjednoczonych ds. Praw Człowieka, w którym uznano odpowiedzialność Arabii Saudyjskiej za „pozasądową egzekucję z premedytacją" Chaszukdżiego, wszystko wróciło do normy, a Zachód był gotów przystąpić do udziału w realizacji projektu „Wizja 2030", ogłoszonego przez MbS w kwietniu 2016 r.

Podsumowując, Iran i Arabia Saudyjska przez 40 lat używały religii jako broni w celu konsolidacji państwa, sprawowania wewnętrznej kontroli nad społeczeństwem i dyskredytowania opozycji. Jednocześnie udzielały wsparcia władzom innych krajów i organizacjom pozarządowym, aby propagować wojowniczą ideologię religijną. Należałoby się jednak zastanowić, czy czarna fala mogłaby powstać bez oportunistycznego wykorzystania konfliktu arabsko-izraelskiego przez ajatollaha Chomeiniego czy Osamę bin Ladena. Autorka nie poświęciła jednak Izraelowi zbyt wiele uwagi.

Książka Kim Ghattas może być fascynującą lekturą zarówno dla naukowców i specjalistów zawodowo poświęcających czas analizowaniu

sytuacji na Bliskim Wschodzie, jak i dla osób po prostu interesujących się tym regionem i pragnących zrozumieć złożoność problemów, które go dotykają. W zakończeniu autorka stwierdza: *Napisałam ją dla tych, którzy wierzą, że świat arabski i muzułmański to coś więcej niż nieustannie pojawiające się w nagłówkach gazet informacje o terroryzmie, ISIS czy Korpusie Strażników Rewolucji. Może przede wszystkim napisałam ją dla tych mieszkańców i mieszkanek regionu, z mojego pokolenia i młodszych, którzy wciąż pytają: „Co się z nami stało?" i zastanawiają się, dlaczego ich rodzice nie zrobili lub nie mogli zrobić nic, by powstrzymać katastrofę*. Poza szukaniem odpowiedzi na to pytanie czytelnicy *Czarnej fali…* znajdą w książce Ghattas wyjaśnienia dotyczące źródeł wielu konfliktów w tej części świata oraz przejmujące opisy nadziei i pragnień ludzi, którzy tam żyją. Czyta się to jak dobrą powieść. Gorąco zachęcam do lektury.

Krzysztof Izak

Emerytowany funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego, pełniący służbę m.in. w pionach realizujących zadania w zakresie przeciwdziałania zagrożeniom terrorystycznym. Autor ponad 20 artykułów o tematyce terroryzmu, które ukazały się na łamach wielu czasopism naukowych. Twórca *Leksykonu organizacji i ruchów islamistycznych* wydanego przez ABW.

Kontakt: lizior3@wp.pl

Terroryzm – studia, analizy, prewencja, 2025, nr 7: 199–205

https://doi.org/10.4467/27204383TER.25.030.21807

Recenzja

Waldemar Zubrzycki, Jarosław Cymerski, Terroryzm i sposoby jego finansowania[1]

Jakub Grelewicz
Autor niezależny
https://orcid.org/0009-0006-3310-8976

Oliwia Łubowska
Autorka niezależna
https://orcid.org/0009-0006-8659-1690

Wnikliwa analiza i interpretacja występowania terroryzmu we współczesnym świecie, związanych z nim zagrożeń oraz metod jego finansowania pomagają w zrozumieniu istoty problemu oraz w opracowaniu skutecznych strategii przeciwdziałania temu zjawisku.

Profesor Waldemar Zubrzycki oraz doktor Jarosław Cymerski połączyli siły, aby stworzyć kompleksowe opracowanie na temat terroryzmu i jego finansowania. Pierwszy z autorów jest emerytowanym policjantem, pełnomocnikiem Komendanta

[1] W. Zubrzycki, J. Cymerski, *Terroryzm i sposoby jego finansowania*, Szczytno 2022, Wydawnictwo Wyższej Szkoły Policji w Szczytnie, 185 s.

Głównego Policji do utworzenia Biura Operacji Antyterrorystycznych oraz praktykiem z ogromnym doświadczeniem w Ministerstwie Spraw Wewnętrznych i Administracji. Drugi jest absolwentem Wyższej Szkoły Policji (obecnie Akademia Policji) w Szczytnie i Akademii Obrony Narodowej w Warszawie, specjalistą w dziedzinie nauk o polityce, a od 28 lat funkcjonariuszem – najpierw Biura Ochrony Rządu, a obecnie Służby Ochrony Państwa. Ich kompetencje i osiągnięcia zawodowe pozwalają na nadanie im miana ekspertów w obszarze badań nad terroryzmem. Książka pt. *Terroryzm i sposoby jego finansowania* to charakterystyka współczesnego terroryzmu, szczegółowa analiza funkcjonowania organizacji terrorystycznych oraz metod ich finansowania. Publikacja została poddana recenzji naukowej prof. dr. hab. Bernarda Wiśniewskiego oraz dr. hab. Aleksandra Babińskiego, co jest jej dodatkowym atutem. Wydawcą książki jest Wydawnictwo Wyższej Szkoły Policji w Szczytnie.

Książka składa się ze wstępu, czterech części podzielonych na rozdziały z ich podsumowaniem, zakończenia oraz bibliografii, które tworzą spójną i logiczną konstrukcję. W pierwszej części scharakteryzowano różne aspekty współczesnego terroryzmu. Autorzy omawiają jego źródła oraz wskazują trudności w definiowaniu tego typu zagrożeń. W drugiej części skupiają się na wybranych elementach funkcjonowania organizacji terrorystycznych, m.in. na kategoriach wydatków, działaniach propagandowych, metodach rekrutacji i szkoleniu członków. W części trzeciej analizują finansowanie działalności organizacji terrorystycznych, w tym legalne i nielegalne źródła przychodów. Zilustrowaniem tych zagadnień jest czwarta część książki, w której zaprezentowano przykłady pozyskiwania środków przez wybrane organizacje terrorystyczne.

W pierwszej części pt. *Charakterystyka zjawiska współczesnego terroryzmu* autorzy skrupulatnie analizują to zagadnienie. Dzielą źródła współczesnego terroryzmu na polityczne, społeczne i religijne. Swoje obserwacje przekazują w sposób, który pomaga czytelnikowi zrozumieć złożoność motywacji stojących za działaniami terrorystycznymi. Kolejnym elementem tej części książki jest rozdział dotyczący definicji pojęcia terroryzmu. Autorzy przytaczają i porównują wykładnie różnych badaczy oraz opisują, jak ten termin ewoluował w ciągu dziesięcioleci. Omawiają również definicje proponowane przez organizacje międzynarodowe i pokazują różnice w podejściu do tego typu działalności. Przywołują definicje sformułowane przez Komisję Europejską oraz wybrane służby specjalne na świecie, co pozwala na porównanie perspektyw różnych instytucji. Zauważają trudności

w jednoznacznym zdefiniowaniu tego zjawiska oraz jego złożoność. Rozważają możliwość określania terroryzmu z uwzględnieniem metod działania zamachowców, co z kolei akcentuje techniczne i taktyczne aspekty ich aktywności. Zwracają uwagę na społeczny wymiar terroryzmu przez analizę jego wpływu na społeczeństwo i jednostkę. Następnie prezentują typologię terroryzmu przez pryzmat metod działania oraz motywacji sprawców, np. politycznych czy religijnych. Po podsumowaniu tych rozważań przechodzą do rozdziału o sposobach działania terrorystów. Wprowadzają czytelnika w tematykę pozyskiwania środków na działalność terrorystyczną, wskazują różne metody jej finansowania. Szczegółowo opisują formy ataków z wykorzystaniem: broni palnej i białej, ładunków wybuchowych, statków powietrznych oraz z wzięciem zakładników. Omawiają również użycie w nich broni masowego rażenia i bezzałogowych platform mobilnych, podkreślając innowacyjność i adaptacyjność metod stosowanych przez organizacje terrorystyczne. Nie pomijają ataków cybernetycznych i zamachów symultanicznych, które stanowią coraz większe wyzwanie dla współczesnych systemów bezpieczeństwa. Następnie autorzy relacjonują wybrane zamachy terrorystyczne. Rozpoczynają od przeprowadzonego na Bali w 2002 r., a następnie opisują zamachy, w kórych wykorzystano fałszywe informacje. Szczególną uwagę poświęcają atakom we Francji, Belgii i Niemczech, które wstrząsnęły światową opinią publiczną. Dokładnie analizują zamachy w Paryżu z 13 listopada 2015 r., będące jednymi z największych ataków terrorystycznych we współczesnej Europie. W ich wyniku 130 osób zginęło, a ponad 350 zostało rannych. Następnie omawiają skoordynowane ataki bombowe w Brukseli z 22 marca 2016 r. – dwa na lotnisku w Zaventem i jeden przy stacji metra Maelbeek, w których zginęło 35 osób, w tym trzech zamachowców, a ok. 340 zostało rannych – oraz zamach na jarmarku bożonarodzeniowym w Berlinie z 19 grudnia 2016 r., podczas którego kierowca ciężarówki wjechał w tłum i zabił 12 osób, a kilkadziesiąt ranił. Na koniec opisują zamach w Londynie z 7 lipca 2005 r., kiedy to trzy eksplozje w metrze i jedna w autobusie miejskim spowodowały śmierć ponad 50 osób i obrażenia u kilkuset, a także sparaliżowały centrum miasta w porannych godzinach szczytu. Przywołane przykłady mają zilustrować różnorodność form i metod działania sprawców.

Druga część książki, zatytułowana *Wybrane elementy funkcjonowania organizacji terrorystycznych*, rozpoczyna się od analizy kategorii wydatków organizacji terrorystycznych. Autorzy wyszczególniają w nich takie obszary, jak: operacje, propaganda, rekrutacja, szkolenia, wynagrodzenia

i rekompensaty dla członków, opieka społeczna, zarządzanie danym obszarem oraz administracja. Taki podział pomaga czytelnikowi zrozumieć, jak złożone i rozbudowane są struktury służące finansowaniu terroryzmu, co z kolei świadczy o profesjonalizmie terrorystów i zdolności do efektywnego zarządzania zasobami. Następnie badacze skupiają się na działaniach propagandowych prowadzonych przez grupy terrorystyczne, przywołują przy tym wiele przykładów. Ukazują, jak dużą rolę odgrywa propaganda nie tylko w szerzeniu ideologii, lecz także w rekrutacji nowych członków i budowaniu wizerunku organizacji na arenie międzynarodowej.

Istotnym zagadnieniem tej części książki jest pozyskiwanie zwolenników. Autorzy opisują wybrane sposoby werbunku i zwracają uwagę na różnorodność metod stosowanych przez organizacje terrorystyczne. Omawiają rekrutację pasywną, rekrutację w więzieniach oraz koszty z tym związane. Zwracają uwagę, jak ważny dla ciągłości i rozwoju organizacji jest nabór nowych członków, a także jak wykorzystuje się manipulację i ideologię do przyciągania sympatyków. Opisują też wybrane elementy szkolenia członków organizacji terrorystycznych, a szczególną rolę w tym procesie przypisują manipulacji psychicznej. Wskazują, jak przez indoktrynację i oddziaływanie psychologiczne są kształtowane postawy i przekonania przyszłych terrorystów. Przedstawiają cechy dobrze wyszkolonego zawodowca, przede wszystkim jego zdolność do działania w skrajnych warunkach, dużą odporność psychiczną oraz wysoki poziom przygotowania fizycznego i taktycznego. W podsumowaniu autorzy zwracają uwagę na złożoność i profesjonalizm działań organizacji terrorystycznych. Dzięki tej analizie czytelnik może lepiej zrozumieć mechanizmy funkcjonowania tych grup oraz wyzwania, jakie ich działalność stawia przed służbami bezpieczeństwa i społecznością międzynarodową w kontekście przeciwdziałania terroryzmowi.

Trzecia część książki nosi tytuł *Finansowanie działalności organizacji terrorystycznych*. Na początku autorzy definiują pojęcie finansowania terroryzmu z przytoczeniem terminów zaproponowanych przez Bank Światowy i Międzynarodowy Fundusz Walutowy. Następnie przedstawiają międzynarodowy wymiar walki z finansowaniem terroryzmu i stanowisko Organizacji Narodów Zjednoczonych wobec tej kwestii. Autorzy przyglądają się również regulacjom polskiego prawa i temu, jak Polska wpisuje się w te globalne wysiłki. Oceniają skuteczność polskich przepisów w przeciwdziałaniu przepływom finansowym na rzecz organizacji terrorystycznych. W dalszych rozdziałach skupiają się na różnych metodach pozyskiwania

funduszy przez organizacje terrorystyczne. Omawiają wykorzystanie organizacji non profit, które często są przykrywką dla nielegalnych działań finansowych. Zgłębiają kwestię wsparcia udzielanego organizacjom terrorystycznym przez ich sympatyków, podkreślają przy tym rolę ideologii i propagandy w mobilizacji zasobów. Kolejnym istotnym elementem finansowania organizacji terrorystycznych są podmioty gospodarcze. Autorzy ukazują, jak legalne przedsiębiorstwa mogą być wykorzystywane do prania brudnych pieniędzy i transferu środków finansowych. Następnie przechodzą do szczegółowego opisu nielegalnych źródeł przychodów terrorystów. Wśród nich znajdują się takie działania, jak: produkcja narkotyków i handel nimi, przemyt towarów i handel nimi, w tym diamentami, oraz handel ludźmi. Istotnym źródłem finansowania dla wielu organizacji są – także omówione w książce – wymuszenia, porwania i drobna przestępczość. Autorzy zwracają uwagę na wykorzystanie instytucji bankowych do transferu i ukrywania środków finansowych, podkreślają przy tym konieczność wzmożonej kontroli i regulacji sektora finansowego. Analizują również rolę współczesnych technologii w ułatwianiu przepływu funduszy i komunikacji między członkami organizacji terrorystycznych. Innymi wskazanymi w książce metodami pozyskiwania środków przez terrorystów są handel dziełami sztuki, oszustwa podatkowe oraz eksploatacja surowców naturalnych. Autorzy opisują także zaangażowanie wybranych państw w finansowanie terroryzmu. Rozpoczynają od Iranu i omówienia jego domniemanego wsparcia dla różnych grup terrorystycznych. Następnie skupiają się na Sudanie i Syrii i przedstawiają złożone relacje tych państw z organizacjami terrorystycznymi oraz wpływ polityki międzynarodowej na te powiązania. W podsumowaniu podkreślają złożoność problemu finansowania terroryzmu oraz konieczność międzynarodowej współpracy w celu skutecznego przeciwdziałania temu zjawisku.

W ostatniej części, pt. *Przykłady pozyskiwania środków przez wybrane organizacje terrorystyczne*, autorzy przedstawiają wyniki swoich badań nad trzema aspektami funkcjonowania wybranych organizacji terrorystycznych: strategią finansową wraz ze sposobami finansowania, rekrutacją członków i systemem szkoleń. Omawiają te aspekty w odniesieniu do Al-Kaidy, Boko Haram, Hezobollahu i Państwa Islamskiego (ISIS). Wskazują podobieństwa i różnice w funkcjonowaniu tych organizacji w kontekście pozyskiwania środków i nowych członków.

Recenzowana książka stanowi kompleksowe opracowanie na temat terroryzmu oraz metod jego finansowania. Autorzy wykorzystali swoje

bogate doświadczenie zawodowe i praktyczne do wnikliwych studiów nad problematyką aktualną i niezwykle istotną z punktu widzenia bezpieczeństwa globalnego. Praca charakteryzuje się logiczną i spójną strukturą, co ułatwia czytelnikowi zrozumienie złożoności omawianych zagadnień. Każdy temat jest starannie opracowany, z uwzględnieniem zarówno aspektów teoretycznych, jak i ilustrujących je przykładów. Szczególnie cenne są opisy konkretnych organizacji terrorystycznych, jak Al-Kaida czy ISIS, które pozwalają na lepsze zrozumienie mechanizmów ich działania oraz sposobów pozyskiwania środków. Atutami książki są także analiza różnych definicji terroryzmu oraz wskazanie trudności związanych z jednoznacznym zdefiniowaniem tego zjawiska. Autorzy podkreślają, że ten problem wynika z ewolucji samego terroryzmu oraz z różnorodności form i metod działania terrorystów.

Publikacja stanowi cenną pozycję na rynku literatury specjalistycznej ze względu na cechy, które ją wyróżniają wśród innych wartościowych, zarówno krajowych, jak i zagranicznych, ujęć problematyki terroryzmu, takich jak: monografia dr. hab. Tomasza R. Aleksandrowicza *Terroryzm międzynarodowy* (2011 r.), artykuł naukowy *Terroryzm i jego finansowanie w kontekście nowelizacji art. 165a k.k.* autorstwa dr hab. Anny Golonki (2020 r.) czy anglojęzyczna monografia dr. Magnusa Ranstorpa *Terrorism and Human Rights* (2008 r.). Na wyjątkowość recenzowanej pozycji wpływają m.in. takie czynniki, jak:

1) osadzenie analizy finansowania terroryzmu w realiach funkcjonowania polskich służb bezpieczeństwa, możliwe dzięki bogatemu doświadczeniu zawodowemu autorów w pracy operacyjnej oraz obszernej wiedzy teoretycznej;
2) kompleksowa analiza zagadnienia, obejmująca jego trzy zasadnicze elementy niezbędne do funkcjonowania organizacji terrorystycznych, tj. modele finansowania, schematy pozyskiwania członków oraz procedury szkoleniowe;
3) podjęcie problemu finansowania zjawiska w kontekście polskiego systemu prawno-instytucjonalnego, przy jednoczesnym uwzględnieniu uwarunkowań globalnych, zapewniające unikalne wnioski praktyczne, istotne dla środowiska policyjno-wojskowego oraz pozostałych badaczy polityki bezpieczeństwa.

Terroryzm i sposoby jego finansowania to pozycja godna polecenia. Stanowi wartościowe źródło wiedzy dla studentów, pracowników służb bezpieczeństwa oraz przedstawicieli różnych dziedzin nauki zainteresowanych

problematyką terroryzmu. Waldemar Zubrzycki i Jarosław Cymerski przedstawiają skomplikowane zagadnienia w wyczerpujący, a jednocześnie przystępny sposób, co sprawia, że książka może zdobyć szersze grono odbiorców. Jest ona istotnym wkładem w dyskurs na temat terroryzmu i daje solidną podstawę do dalszych badań w tym obszarze. Dzięki niej czytelnik zyskuje pełniejszy obraz zagrożeń związanych z terroryzmem, wyzwań stojących przed społecznością międzynarodową w kontekście walki z tym zjawiskiem oraz narzędzi, które mogą być w tym celu wykorzystane.

Jakub Grelewicz

Ukończył studia licencjackie na Wydziale Nauk o Polityce i Bezpieczeństwie Uniwersytetu Mikołaja Kopernika w Toruniu. Obecnie studiuje na Wydziale Nauk o Polityce i Administracji na Uniwersytecie Kazimierza Wielkiego w Bydgoszczy. Interesuje się zagadnieniami związanymi z bezpieczeństwem wewnętrznym Polski, funkcjonowaniem sił zbrojnych oraz obronnością państwa.

Kontakt: kubagrelewicz@wp.pl

Oliwia Łubowska

Absolwentka Wydziału Filologicznego Uniwersytetu Łódzkiego. Jej zainteresowania badawcze skupiają się wokół zagadnień dotyczących bezpieczeństwa wewnętrznego, stosunków międzynarodowych oraz wyzwań związanych z konfliktami.

PRACE KONKURSOWE

Terroryzm – studia, analizy, prewencja, 2025, nr 7: 209–227

https://doi.org/10.4467/27204383TER.25.031.21808

Artykuł

Ataki z 11 września 2001 roku i zmiany prawno-administracyjne w polityce bezpieczeństwa Stanów Zjednoczonych[1]

The attacks of 11 September 2001 and legal and administrative changes in US security policy

Franciszek Dziadkowiec-Wędlikowski

Autor niezależny

https://orcid.org/0009-0008-0115-4702

Abstrakt

Artykuł omawia konsekwencje ataków terrorystycznych z 11 września 2001 r. dla polityki bezpieczeństwa Stanów Zjednoczonych. Wydarzenie to zapoczątkowało wiele istotnych zmian prawno-administracyjnych, które zrewolucjonizowały podejście USA do zwalczania terroryzmu. Główne reformy, takie jak wprowadzenie ustawy *The USA PATRIOT Act of 2001*, powołanie Departamentu Bezpieczeństwa Wewnętrznego oraz zaostrzenie regulacji dotyczących bezpieczeństwa lotniczego, miały na celu zwiększenie skuteczności prewencji oraz szybszą reakcję na potencjalne zagrożenia. Choć zmiany te przyniosły istotne korzyści, wzbudziły również kontrowersje związane z naruszaniem praw obywatelskich.

[1] Artykuł powstał na podstawie pracy licencjackiej pt. *Zabójstwa celowane jako element strategii CIA w kontekście ataków terrorystycznych z 11 września 2001 roku* obronionej na Wydziale Studiów Międzynarodowych i Politycznych Uniwersytetu Jagiellońskiego. Praca została wyróżniona w XIII edycji konkursu Szefa ABW na najlepszą pracę doktorską, magisterską lub licencjacką dotyczącą bezpieczeństwa państwa w kontekście zagrożeń wywiadowczych, terrorystycznych, ekonomicznych.

Analiza reform pokazuje ewolucję polityki bezpieczeństwa oraz wskazuje na wyzwania, które stoją przed współczesnym systemem walki z terroryzmem.

Słowa kluczowe

ataki z 11 września 2001 r., *The USA PATRIOT Act of 2001*, polityka bezpieczeństwa Stanów Zjednoczonych, bezpieczeństwo lotnicze, reformy administracyjne, reformy prawne, Departament Bezpieczeństwa Wewnętrznego, ataki terrorystyczne

Abstract

This article discusses the implications of terrorist attacks of 11 September 2001 for US security policy. The event triggered a number of significant legal and administrative changes that revolutionised the US approach to counter-terrorism. Major reforms, such as the introduction of *The USA PATRIOT Act of 2001*, establishment of the Department of Homeland Security and the tightening of air safety regulations, were aimed at increasing the effectiveness of prevention and responding more quickly to potential threats. While these changes have brought significant benefits, they have also raised controversy over violations of civil rights. The analysis of the reforms shows the evolution of security policy and points to the challenges facing the contemporary counter-terrorism system.

Keywords

the attacks of 11 September 2001, *The USA PATRIOT Act*, US security policy, aviation security, administrative reforms, legal reforms, Department of Homeland Security, terrorist attacks

Wprowadzenie

Ataki terrorystyczne z 11 września 2001 r. w Stanach Zjednoczonych okazały się punktem zwrotnym w polityce bezpieczeństwa zarówno dla tego kraju, jak i większości państw szeroko pojętego Zachodu. Doświadczenia związane z terroryzmem spowodowały wprowadzenie fundamentalnych zmian w polityce i systemie bezpieczeństwa USA oraz wpłynęły na kształtowanie się nowych strategii i podejść do walki z terroryzmem na całym świecie. Po atakach z 11 września 2001 r. prezydent Stanów Zjednoczonych George W. Bush wygłosił orędzie do narodu amerykańskiego, które rozpoczął słowami: *Dziś, nasi współobywatele, nasz sposób życia, sama nasza wolność zostały zaatakowane w serii celowych i śmiercionośnych aktów*

terrorystycznych[2]. Ataki na World Trade Center (WTC), w których zginęło niemal 3000 osób, zapisały się jako jedne z najtragiczniejszych w historii Stanów Zjednoczonych. Trzy z czterech porwanych samolotów osiągnęły swoje cele – maszyna wykonująca lot nr 11 uderzyła w północną wieżę WTC o godz. 8.46, ta realizująca lot nr 175 – w południową wieżę o godz. 9.03, a lot nr 77 – w budynek Pentagonu o godz. 9.37. Samolot wykonujący lot nr 93 nie dotarł do celu w Waszyngtonie i rozbił się na polach Pensylwanii krótko po godz. 10.00. Liczba ofiar przewyższyła nawet tragiczny bilans japońskiego ataku na Pearl Harbor w 1941 r.[3]

Celem artykułu jest omówienie motywów sprawców oraz przedstawienie zmian prawno-administracyjnych, których dokonano po atakach na WTC, przede wszystkim na podstawie uchwalonej w 2001 r. ustawy *The USA PATRIOT Act of 2001*. Przeanalizowanie tych wydarzeń i ich skutków jest istotne dla zrozumienia ewolucji polityki bezpieczeństwa w Stanach Zjednoczonych oraz dla lepszego przygotowania się państw do wyzwań w dziedzinie bezpieczeństwa.

Motywy sprawców ataków z 11 września 2001 roku

Ataki terrorystyczne na WTC i Pentagon zostały przeprowadzone przez członków Al-Kaidy, organizacji terrorystycznej zarządzanej przez Osamę bin Ladena i związanej ideowo z fundamentalizmem islamskim. Przyczyny ataku zostały szeroko omówione w opublikowanym w listopadzie 2002 r. tekście *Letter to America* (pol. List do Ameryki) napisanym przez samego przywódcę organizacji[4]. W manifeście podkreślił on, że zamach był wynikiem ataków na muzułmanów w wielu regionach świata, przede wszystkim amerykańskich interwencji wojskowych w krajach arabskich, konfliktu izraelsko-palestyńskiego, drugiej wojny w Czeczenii czy wspierania

[2] W oryginale: „(...) Today, our fellow citizens, our way of life, our very freedom came under attack in a series of deliberate and deadly terrorist acts (...)". Zob. *WATCH: President George W. Bush's address to the nation after September 11, 2001 attacks*, YouTube, 19 VIII 2021 r., https://www.youtube.com/watch?v=WA8-KEnfWbQ [dostęp: 30 III 2023]. Tłumaczenia w tekście pochodzą od autora (dop. red.).

[3] W atakach 11 IX 2001 r. zginęło 2977 osób, w ataku na Pearl Harbor – 2403 po stronie amerykańskiej. Zob. *14 Interesting Pearl Harbor Facts*, Pearl Harbor Tours, https://www.pearlharbortours.com/pearl-harbor/facts-about-pearl-harbor [dostęp: 25 I 2025].

[4] O. bin Laden, *Letter to America*, https://web.archive.org/web/20040615081002/http://observer.guardian.co.uk/worldview/story/0,11581,845725,00.html [dostęp: 26 I 2025].

Indii w dyskryminacji muzułmanów na terenie Kaszmiru. Ponadto wyraził sprzeciw wobec amerykańskiego stylu życia, znacznie odbiegającego od zasad wyznaczonych przez Mahometa, oddzielających religię od władzy, oraz wobec homoseksualizmu, wykorzystywania kobiet w reklamie i sprzedaży produktów, lobbingu czy zachodniego systemu finansowań. Bardzo wyraźnie zamanifestował swoją nienawiść do Żydów i państwa Izrael oraz wsparcia udzielanego mu przez Stany Zjednoczone. Stwierdził również, że jeśli naród amerykański jest wolny i ma możliwość wyboru swojej władzy, to jest współwinny działań rządu. W ten sposób Bin Laden uzasadnił zaatakowanie przez jego organizację celów cywilnych[5].

Oprócz motywów bezpośrednio wyrażonych w manifeście można doszukać się również tych przekazanych nie wprost, nawiązujących do doktryny, które wybrzmiały w późniejszych wypowiedziach Bin Ladena i członków Al-Kaidy. Michael Scott Doran zwrócił uwagę, że: *Gdy terrorysta zabija, celem nie jest morderstwo samo w sobie, lecz coś innego – przykładowo represje policji doprowadzające do rozłamu między władzą a społeczeństwem, które terrorysta będzie mógł później wykorzystać w celach rewolucyjnych. Osama bin Laden zabiegał o międzynarodową represję wojskową i ją otrzymał. Będzie więc chciał wykorzystać ją do swojej szczególnej odmiany rewolucji*[6]. Bin Laden zamierzał wciągnąć Stany Zjednoczone do walki ze światem islamskim, a działania Al-Kaidy według niego miały być katalizatorem dla rewolucji, którą chciał wywołać. Dalej Doran stwierdził, że: *Bin Laden wyreżyserował spektakl o wysokim poziomie politycznym, który – miał nadzieję – dotrze do tych, którzy interesowali go najbardziej: ummy*[7] *czy światowej islamskiej społeczności. Scenariusz był prosty: Ameryka, obsadzona w roli złoczyńcy, miała użyć swojej potęgi militarnej, jak postać z kreskówki próbująca zabić muchę strzelbą. Media zadbałyby o to, by użycie siły przeciw cywilnej populacji Afganistanu było transmitowane na całym świecie, a umma uznałaby za szokujące, jak Amerykanie nonszalancko wywołują cierpienie i śmierć muzułmanów*[8]. Odpowiedź Stanów Zjednoczonych na wydarzenia z 11 września miała zatem odsłonić przed populacją muzułmańską prawdziwe oblicze Ameryki, a w konsekwencji pojednać tę społeczność

[5] Tamże.

[6] M.S. Doran, *Somebody Else's Civil War*, „Foreign Affairs" 2002, t. 81, nr 1, s. 22–23.

[7] *Umma* – słowo pochodzące z języka arabskiego, oznaczające społeczność, naród, wspólnotę muzułmańską.

[8] M.S. Doran, *Somebody Else's Civil War*..., s. 23.

we wspólnej walce przeciw okrucieństwom ze strony Amerykanów. Dalej Doran odwołuje się do polaryzacji, jaka miałaby pojawić się między społecznością muzułmańską a szeroko pojętym światem zachodnim (zwłaszcza państwami NATO i Unii Europejskiej), sprzymierzonym ze Stanami Zjednoczonymi. Doprowadziłaby ona do osiągnięcia głównego celu Bin Ladena – rewolucji islamskiej w państwach muzułmańskich, co jednocześnie zapewniłoby ekstremistycznej odmianie islamu możliwość przetrwania i rozwoju[9].

Według Daniela Benjamina i Stevena Simona ataki z 11 września 2001 r. były motywowane wyłącznie religijnie: *Porwania (samolotów) były spełnieniem sakramentu, którego celem było przywrócenie światu moralnego porządku odebranego mu przez wrogów islamu i muzułmańskich kolaborantów*[10]. Odpowiedź na ataki w postaci wyrażania poparcia dla islamu przez amerykański rząd, na czele z prezydentem Bushem, była zdaniem Benjamina i Simona właściwą decyzją, pokazującą wyznawcom islamu, że Ameryka jest przeciwnikiem nie ich, lecz mordowania niewinnych ludzi[11].

Skutki ataków z 11 września 2001 roku

W czasie orędzia prezydenta Busha padły słowa, które okazały się wstępem do zmiany polityki Stanów Zjednoczonych i początkiem konfliktu, znanego dziś pod nazwą globalnej wojny z terroryzmem – amerykańskiej odpowiedzi na atak ze strony Al-Kaidy: *Nie będziemy czynić rozróżnienia między terrorystami, którzy popełnili te czyny, a tymi, którzy ich ukrywają*[12]. Zaledwie tydzień po atakach Kongres Stanów Zjednoczonych wprowadził w życie rezolucję pt. *Joint Resolution to authorize the use of United States Armed Forces against those responsible for the recent attacks launched against the United States* (pol. Wspólna rezolucja zezwalająca na użycie Sił Zbrojnych Stanów Zjednoczonych przeciwko osobom odpowiedzialnym za ostatnie ataki przeprowadzone na Stany Zjednoczone). Rezolucja – skrótowo nazwana *The Authorization for Use of Military Force* (pol. Zezwolenie na wykorzystanie

[9] Tamże, s. 41.

[10] D. Benjamin, S. Simon, *The Age of Sacred Terror*, New York 2002, s. 40.

[11] Tamże.

[12] W oryginale: „We will make no distinction between the terrorists who committed these acts and those who harbor them (...)". Zob. *WATCH: President George W. Bush's address to the nation...*

Sił Zbrojnych)[13] – umożliwiła prezydentowi wykorzystanie wszelkiej niezbędnej siły przeciwko sprawcom zamachów z 11 września, osobom planującym je, pomagającym w przeprowadzeniu oraz tym, którzy udzielali tym osobom schronienia[14].

Niespełna miesiąc po zamachach, 7 października 2001 r., Stany Zjednoczone ze wsparciem Wielkiej Brytanii rozpoczęły operację „Enduring freedom", wymierzoną w talibów rządzących w Afganistanie i kryjówki Al-Kaidy rozmieszczone na terytorium tego państwa. Jej głównymi celami były: schwytanie lub zabicie czołowych przywódców Al-Kaidy, zniszczenie na terytorium Afganistanu infrastruktury należącej do terrorystów i odsunięcie talibów od władzy[15]. Wczesna faza wojny, prócz udanych nalotów przeprowadzonych przez amerykańskie i brytyjskie siły, opierała się również na użyciu amerykańskich wojsk specjalnych, wspomagających Pasztunów i Sojusz Północny w ich walce z talibami. Pierwsze amerykańskie konwencjonalne siły lądowe przybyły na miejsce 12 dni później[16].

Śledztwo wszczęte w sprawie zamachów, któremu nadano kryptonim PENTTBOMB[17], było największym w dotychczasowej historii FBI. Brało w nim udział ponad 4000 funkcjonariuszy i 3000 pracowników. Już trzy dni po feralnych wydarzeniach udało się ustalić tożsamość wszystkich 19 podejrzanych o udział w zamachu. Dnia 27 września upubliczniono ich zdjęcia. Śledczy szybko powiązali tych mężczyzn z Al-Kaidą i uzyskali dostęp do zebranych na ich temat danych wywiadowczych[18].

Zmiany prawno-administracyjne

Ataki terrorystyczne z 11 września 2001 r. wywołały gorącą debatę na temat konieczności dostosowania prawa do nowych zagrożeń terrorystycznych.

[13] *Authorization for Use of Military Force*, https://www.govinfo.gov/content/pkg/PLAW-107publ40/pdf/PLAW-107publ40.pdf [dostęp: 30 III 2023].

[14] Tamże.

[15] I.H. Daalder, J.M. Lindsay, *The Bush Revolution: The Remaking of America's Foreign Policy*, April 2003, https://www.brookings.edu/wp-content/uploads/2016/06/20030425.pdf, s. 20 [dostęp: 25 I 2025].

[16] *1999 – 2021 The U.S. War in Afghanistan*, Council on Foreign Relations, https://www.cfr.org/timeline/us-war-afghanistan [dostęp: 30 III 2023].

[17] Skrót PENTTBOMB pochodzi od Pentagon/Twin Towers Bombing Investigation.

[18] *A Review of the FBI's Handling of Intelligence Information Prior to the September 11 Attacks*, https://oig.justice.gov/sites/default/files/archive/special/0506/chapter5.htm [dostęp: 10 VI 2023].

W wyniku dyskusji i intensywnych prac legislacyjnych wprowadzono nowe ustawy i przepisy mające na celu wzmocnienie środków bezpieczeństwa oraz rozszerzenie uprawnień organów ścigania i służb specjalnych, aby zwiększyć skuteczność przeciwdziałania terroryzmowi[19].

W kolejnej części artykułu omówiono ustawę Patriot Act, która wprowadziła rozszerzenie uprawnień agencji rządowych w zakresie monitorowania i zwalczania terroryzmu, oraz utworzenie Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych. Wspomniano również o zmianach w środkach bezpieczeństwa lotniczego.

The USA PATRIOT Act of 2001

Fundamentem zmian prawnych jest przyjęty 26 października 2001 r. *The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (pol. Jednoczenie i wzmacnianie Ameryki przez dostarczanie odpowiednich narzędzi potrzebnych do zwalczania terroryzmu i przeciwdziałania mu)[20] w skrócie *The USA PATRIOT Act of 2001* (dalej: Patriot Act). Ustawa wprowadziła zmiany w kompetencjach krajowych służb wywiadowczych i organów ścigania[21]. Skupiono się w niej na czterech najważniejszych zagadnieniach:

- rozszerzeniu możliwości inwigilacji przez organy ścigania, m.in. za pomocą podsłuchiwania telefonów,
- ułatwieniu komunikacji między poszczególnymi służbami, by w celu zwalczania terroryzmu mogły skuteczniej korzystać z dostępnych zasobów,
- zaktualizowaniu prawa, by uwzględniało nowe technologie i zagrożenia,
- zaostrzeniu kar za przestępstwa o charakterze terrorystycznym, z jednoczesnym zwiększeniem zakresu czynów, które kwalifikują się jako takie przestępstwa[22].

W pierwszym rozdziale ustawy opisano utworzenie funduszu na rzecz działań antyterrorystycznych oraz nadano prokuratorowi generalnemu Stanów Zjednoczonych prawo do wystosowania prośby do Departamentu

[19] L. Fisher, *Presidential War Power*, Lawrence 2004, s. 202.

[20] *The USA PATRIOT Act of 2001*, https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf [dostęp: 30 III 2023].

[21] S. Wojciechowski, P. Osiewicz, *Zrozumieć współczesny terroryzm*, Warszawa 2017, s. 129.

[22] *The USA PATRIOT Act: Preserving Life and Liberty*, Department of Justice, https://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf [dostęp: 30 III 2023].

Obrony USA (United States Department of Defense) o pomoc ze strony wojska w przypadku nielegalnego użycia broni masowego rażenia na terytorium USA. Ponadto zlecono dyrektorowi United States Secret Service utworzenie National Electronic Crime Task Force – ogólnokrajowej grupy zadaniowej mającej na celu prewencję, wykrywanie i badanie przestępstw w sferze cyber, zwłaszcza ataków terrorystycznych na infrastrukturę krytyczną[23]. Potępiono również dyskryminację i agresję wobec muzułmanów żyjących w Stanach Zjednoczonych, do których to aktów dochodziło po atakach z 11 września. Najważniejszym zapisem tego rozdziału wydaje się sekcja 106, która zapewniła prezydentowi możliwość konfiskaty aktywów należących do osób i organizacji pochodzących z zagranicy i podejrzewanych o działalność terrorystyczną. Ponadto w przypadku gdy konfiskata jest podejmowana na podstawie niejawnych źródeł informacji, podejrzana osoba lub organizacja może nie zostać o niej poinformowana[24].

Z punktu widzenia służb wywiadowczych jednym z najważniejszych rozdziałów jest rozdział drugi. Dotyczy on inwigilacji osób podejrzanych o terroryzm, udział w oszustwach komputerowych lub nadużycia oraz szpiegów pracujących dla obcych mocarstw, którzy są zaangażowani w tajną działalność na terytorium Stanów Zjednoczonych. Agencjom rządowym umożliwiono gromadzenie informacji w ramach wywiadu zagranicznego zarówno od obywateli Stanów Zjednoczonych, jak i cudzoziemców[25].

Wcześniejsze prawo zezwalało funkcjonariuszom FBI wyższej rangi na ubieganie się o nakaz sądowy, w związku z dochodzeniem, w celu uzyskania dostępu do rejestrów przewoźników, hoteli, magazynów czy firm wynajmujących pojazdy. Sekcja 215 zmieniła te przepisy. Wnioski mogą składać funkcjonariusze FBI niższej rangi – *assistant special agent-in-charge* (czyli osoby odpowiedzialne za biura terenowe FBI). Ponadto nakazy sądowe zaczęły obejmować wszelkie przedmioty będące w posiadaniu kogokolwiek – każdej firmy czy osoby prywatnej. Poszukiwane przedmioty nie muszą, tak jak wcześniej, mieć związku ze zidentyfikowanym szpiegiem czy obcym państwem, ale można ich poszukiwać wyłącznie w ramach dochodzenia mającego na celu ochronę Stanów Zjednoczonych przed terroryzmem międzynarodowym lub tajnymi działaniami wywiadowczymi,

[23] *ECTF and FCTF*, United State Secret Service, https://www.secretservice.gov/contact/ectf-fctf [dostęp: 30 III 2023].

[24] *The USA PATRIOT Act of 2001*..., s. 6–8.

[25] Tamże, s. 8–25.

pod warunkiem że takie śledztwo jest prowadzone nie tylko na podstawie pierwszej poprawki do konstytucji Stanów Zjednoczonych, lecz ma ono także inne podstawy[26].

Sekcja 218 zmieniła wymagania (wyznaczone dotychczas przez ustawę o nadzorze nad wywiadem zagranicznym – *The Foreign Intelligence Surveillance Act of 1978*, FISA), które służby wywiadowcze miały spełnić, by móc podjąć się inwigilacji danej osoby. Dotychczasowy „cel" (ang. *the purpose*) inwigilacji w postaci gromadzenia informacji wywiadu zagranicznego zmieniono na „istotny cel" (ang. *significant purpose*). Inwigilację można było prowadzić, gdy zbieranie informacji wywiadu zagranicznego było tylko celem częściowym (istotnym), a głównym celem był inny występek. Dało to służbom możliwość inwigilacji znacznie większej części obywateli, przy powołaniu się na zapis, że zbieranie informacji wywiadu zagranicznego nie musi być głównym, a jedynie istotnym celem tej inwigilacji[27]. Rozdział drugi obejmuje również przepisy dotyczące sankcji handlowych nakładanych na talibów oraz ograniczeń w eksporcie towarów rolnych, leków i urządzeń medycznych[28].

Trzeci rozdział ustawy został podzielony na trzy podrozdziały. Pierwszy dotyczy wzmocnienia przepisów bankowych, zwłaszcza w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Drugi omawia kwestię komunikacji między organami ścigania a instytucjami finansowymi. Trzeci jest poświęcony przemytowi i fałszerstwu waluty. Celem wprowadzonych zmian, jak zaznaczył ustawodawca, było (...) *zwiększenie możliwości Stanów Zjednoczonych w zapobieganiu międzynarodowemu praniu pieniędzy i finansowaniu terroryzmu oraz jego wykrywaniu i ściganiu*[29].

Rozdział czwarty wprowadził wiele zmian w ustawie o imigracji i obywatelstwie (*Immigration and Nationality Act of 1965*). Zapewnił on więcej uprawnień w zakresie dochodzeń i egzekwowania prawa prokuratorowi

[26] Tamże, s. 17. Pierwsza poprawka odnosi się do nienaruszalności wolności słowa. W tłumaczeniu Andrzeja Pułły: „Kongres nie ustanowi ustaw wprowadzających religię lub zabraniających swobodnego wykonywania praktyk religijnych; ani ustaw ograniczających wolność słowa lub prasy, lub naruszających prawo do pokojowych zgromadzeń i wnoszenia do rządu petycji o naprawę krzywd". Zob. *Konstytucja Stanów Zjednoczonych Ameryki*, A. Pułło (tłum. i wstęp), Warszawa 2002, s. 55.

[27] S.H. Rackow, *How the USA Patriot Act Will Permit Governmental Infringement upon the Privacy of Americans in the Name of „Intelligence" Investigations*, „University of Pennsylvania Law Review" 2002, t. 150, nr 5, s. 1676–1677. https://doi.org/10.2307/3312949.

[28] *The USA PATRIOT Act of 2001*..., s. 21.

[29] Tamże, s. 27.

generalnemu Stanów Zjednoczonych oraz Służbie Imigracji i Naturalizacji (Immigration and Naturalization Service, INS). Ten rozdział również został podzielony na trzy podrozdziały. Pierwszy dotyczy kwestii bezpieczeństwa północnej granicy państwa – zlikwidowano limit dotyczący maksymalnej liczby pracowników na tej granicy, przygotowano środki (zarówno finansowe, jak i infrastrukturę), które umożliwiłyby potrojenie liczby funkcjonariuszy Straży Granicznej (Border Patrol), Służby Celnej (Customs Service) oraz INS. Umożliwiono także INS oraz Departamentowi Stanu USA dostęp do danych Krajowego Centrum Informacji Kryminalnej (National Crime Information Center) prowadzonego przez FBI. W drugim podrozdziale wzmocniono przepisy imigracyjne. Szczególnie ważnym elementem tego podrozdziału jest sekcja 412, umożliwiająca przetrzymywanie przez czas nieokreślony (z koniecznością przedłużenia co sześć miesięcy) osób stanowiących zagrożenie dla Stanów Zjednoczonych (z uwagi na powiązania z grupami terrorystycznymi lub wspieranie działalności terrorystycznej). Część trzecią z kolei poświęcono rodzinom osób, które zostały poszkodowane w zamachach z 11 września. Zwrócono uwagę na fakt, że niektórzy poszkodowani lub ich rodziny byli imigrantami, a dokumenty potwierdzające legalność ich pobytu na terytorium Stanów Zjednoczonych mogły stracić ważność niedługo po zamachu. Dla tych osób postanowiono zrobić wyjątek i wydłużyć czas potrzebny na złożenie do urzędu odpowiednich dokumentów[30].

Piąty rozdział Patriot Act zwiększył górny limit nagród, które mogą być wypłacane przez państwo za pomoc w ujęciu terrorystów. Ponadto potwierdzono możliwość współpracy federalnych służb wywiadowczych z innymi organami ścigania oraz rozszerzono uprawnienia United States Secret Service w kwestii oszustw i innych działań przestępczych wymierzonych w instytucje finansowe objęte ubezpieczeniem federalnym.

Sekcja 505 zmieniła trzy ustawy: ustawę o prywatności elektronicznej (*The Electronic Communications Privacy Act of 1986*), ustawę o prawie do prywatności finansowej (*The Right to Financial Privacy Act of 1978*) oraz ustawę o uczciwej sprawozdawczości kredytowej (*The Fair Credit Reporting Act of 1970*) i upoważniła strony trzecie do ujawniania w celach wywiadowczych, na pisemny wniosek FBI, poufnych zapisów transakcji, raportów finansowych i informacji kredytowych[31]. Przed tą zmianą prawną FBI było zobowiązane do zapewnienia, że poszukiwane informacje dotyczyły

[30] Tamże, s. 72–93.

[31] S.H. Rackow, *How the USA Patriot Act*..., s. 1689.

obcego państwa, obcego funkcjonariusza wywiadu, terrorysty międzynarodowego lub osoby zaangażowanej w tajne działania wywiadowcze. Po tej zmianie FBI musi jedynie zapewnić, że dane, które mają zostać udostępnione, są istotne w dochodzeniu mającym na celu zapobieganie terroryzmowi międzynarodowemu lub w tajnej działalności wywiadowczej. Stwarza to poważne ryzyko wystąpienia nadużyć ze strony FBI[32].

W rozdziale szóstym zapewniono pomoc rodzinom funkcjonariuszy poszkodowanym w atakach terrorystycznych (m.in. zwiększono wypłaty z wcześniejszych 100 000 dolarów do 250 000 dolarów). Zmieniono zapisy ustawy o ofiarach przestępstw z 1984 r. (*The Victims of Crime Act of 1984*)[33].

Rozdział siódmy omawia kwestię zmian dotyczących wymiany informacji między agencjami rządowymi, mających na celu usprawnienie komunikacji organów ścigania poszczególnych szczebli (federalnego, stanowego i lokalnego) w przypadku ataków terrorystycznych[34]. Wprowadzone zmiany miały usprawnić pracę i wymianę informacji w przypadku dochodzeń prowadzonych pod nadzorem kilku organów jednocześnie[35].

Kolejnym bardzo istotnym rozdziałem ustawy jest rozdział ósmy. W sekcji 801 uzupełniono luki prawne dotyczące ataków na środki transportu zbiorowego. Dotychczasowe zapisy prawa nie uwzględniały kar za ataki skierowane na środki transportu zbiorowego. Sekcja 802 uzupełniła z kolei definicję terroryzmu krajowego, zgodnie z którą są to (...) *czyny przestępcze niebezpieczne dla życia ludzkiego, popełnione głównie na terytorium Stanów Zjednoczonych, których domniemanym celem jest zastraszenie lub wywarcie nacisku na ludność cywilną, lub wywarcie wpływu na politykę rządu poprzez zastraszenie, lub przymus, lub wpłynięcie na działania rządu poprzez masowe zniszczenie, zabójstwo lub porwanie*[36]. Sekcja 803 wprowadziła, zapowiedziany już 11 września, zakaz ukrywania terrorystów pod karą więzienia lub grzywny. Kolejne sekcje (804 i 805) dodały odpowiednio: zmiany związane z eksterytorialnością przepisów (uwzględniając w nich ataki na ambasady, konsulaty i bazy wojskowe) oraz zakaz udzielania terrorystom wsparcia materialnego. Zgodnie z sekcją 806, dotyczącą zagadnienia majątku należącego

[32] *The USA PATRIOT Act of 2001*..., s. 93–98.

[33] Tamże, s. 99.

[34] Tamże, s. 104.

[35] Tamże.

[36] Ch. Doyle, *Terrorism: Section by Section Analysis of the USA PATRIOT Act*, https://www.arl.org/wp-content/uploads/2001/12/patriot-act-analysis-2001.pdf, s. 50–55 [dostęp: 30 III 2023].

do terrorystów i organizacji terrorystycznych, cały taki majątek, niezależnie od tego, czy znajduje się na terytorium Stanów Zjednoczonych czy za granicą, podlega przepadkowi. Ten przepis ma na celu wykluczyć jedno z głównych źródeł finansowania aktów terrorystycznych. Następnym istotnym punktem rozdziału jest sekcja 808, wprowadzająca zmiany w definicji federalnego przestępstwa terrorystycznego. Z definicji usunięto kilka mniej poważnych przestępstw, takich jak napaść czy zniszczenie mienia, umieszczono w niej natomiast poważniejsze przestępstwa, takie jak: ataki na samoloty i lotniska, użycie broni biologicznej i chemicznej oraz zabójstwa i uprowadzenia członków Kongresu Stanów Zjednoczonych, Gabinetu Stanów Zjednoczonych czy sędziów Sądu Najwyższego Stanów Zjednoczonych. Sekcja 809 wprowadziła brak przedawnienia dla przestępstw o charakterze terrorystycznym. Zgodnie z sekcjami 810 i 811 znacznie zwiększono kary za popełnienie aktów terroru lub pomoc w ich przeprowadzeniu. Przykładowo najwyższa kara za doprowadzenie do uszkodzenia elektrowni jądrowej, jeśli w ataku nie było żadnych ofiar śmiertelnych, wzrosła z 10 do 20 lat pozbawienia wolności. Kolejne sekcje m.in. zezwoliły na nadzór nad osobami oskarżonymi o terroryzm po wypuszczeniu ich z więzienia, zwiększyły kary za przestępstwo cyberterroryzmu oraz podniosły nakłady finansowe na rzecz rozwoju krajowego cyberbezpieczeństwa, a także zaostrzyły przepisy dotyczące broni biologicznej (wprowadzając m.in. kary do 10 lat pozbawienia wolności za dysponowanie środkami biologicznymi lub toksynami[37], których posiadania nie da się uzasadnić pokojowymi zamiarami)[38].

[37] Zgodnie z Kodeksem Stanów Zjednoczonych termin „czynnik biologiczny" oznacza „dowolny mikroorganizm (w tym m.in. bakterie, wirusy, grzyby lub pierwotniaki) lub substancję zakaźną, lub dowolny naturalnie występujący, bioinżynieryjny lub zsyntetyzowany składnik takiego mikroorganizmu lub substancji zakaźnej, zdolny do spowodowania: (A) śmierci, choroby lub innej biologicznej dysfunkcji u człowieka, zwierzęcia, rośliny lub innego żywego organizmu; (B) pogorszenie jakości żywności, wody, sprzętu, zaopatrzenia lub wszelkiego rodzaju materiałów; albo (C) szkodliwe zmiany w środowisku". Termin „toksyna" oznacza natomiast „toksyczny materiał lub produkt roślin, zwierząt, mikroorganizmów (w tym między innymi bakterii, wirusów, grzybów lub pierwotniaków) lub substancji zakaźnych, lub rekombinowaną lub zsyntetyzowaną cząsteczkę, niezależnie od ich pochodzenia i metody produkcji, i obejmuje: (A) każdą trującą substancję lub produkt biologiczny, który może zostać opracowany w wyniku biotechnologii wytwarzanej przez żywy organizm; albo (B) każdy trujący izomer lub produkt biologiczny, homolog lub pochodną takiej substancji". Za: https://www.govinfo.gov/content/pkg/USCODE-2023-title18/pdf/USCODE-2023-title18.pdf [dostęp: 20 II 2025] – przyp. red.

[38] *The USA PATRIOT Act of 2001*..., s. 104–116.

Zmiany zawarte w rozdziale dziewiątym miały usprawnić działanie wywiadu, zwłaszcza w związku ze zbieraniem informacji wywiadu zagranicznego. Dyrektorowi Centralnej Agencji Wywiadowczej (Central Intelligence Agency, CIA), na mocy sekcji 901, powierzono odpowiedzialność za ustanowienie wymagań i priorytetów dotyczących informacji wywiadu zagranicznego, które mają być gromadzone na mocy FISA, oraz za pomoc prokuratorowi generalnemu w rozpowszechnianiu informacji wywiadowczych. Ustawa Patriot Act ograniczyła jednak uprawnienia dyrektora CIA. Nie miał on już możliwości podejmowania, opartych na FISA, operacji nadzoru elektronicznego lub przeszukania fizycznego ani kierowania i zarządzania nimi, chyba że zezwolono na nie przez ustawę lub rozporządzenie wykonawcze prezydenta[39]. Sekcja 902 uzupełniła definicję informacji wywiadu zagranicznego o informacje dotyczące międzynarodowej działalności terrorystycznej. Zgodnie z sekcją 903 członkowie społeczności wywiadowczej powinni dokładać wszelkich starań na rzecz zdobycia informacji o terrorystach i organizacjach terrorystycznych. Sekcja 904 zezwoliła służbom wywiadowczym na odroczenie do 1 lutego 2002 r. składania Kongresowi wymaganych raportów wywiadowczych. W sekcji 905 prokuratorowi generalnemu, w porozumieniu z dyrektorem CIA, polecono opracowanie, w czasie nie dłuższym niż 180 dni od wejścia ustawy w życie, wytycznych dotyczących rozpowszechnienia wśród społeczności wywiadowczej informacji wywiadu zagranicznego ujawnionych w trakcie dochodzenia karnego. Wytyczne te miały pozwalać na raportowanie amerykańskiej wspólnocie wywiadowczej (ang. Intelligence Community) o podjętych lub planowanych działaniach na podstawie informacji, które agencje wspólnoty wywiadowczej przekazały Departamentowi Sprawiedliwości USA (U.S. Department of Justice). Wytyczne mogły zawierać wyjątki w przypadku istnienia zagrożenia dla toczącego się dochodzenia. Zgodnie z sekcją 907 dyrektor CIA został zobowiązany zgłosić, w porozumieniu z dyrektorem FBI, utworzenie krajowego wirtualnego centrum tłumaczeń (co nastąpiło w lutym 2003 r.) w celu zapewnienia terminowych i dokładnych przekładów wywiadu zagranicznego. Sekcja 908 zezwoliła na przyznanie niezbędnych środków na szkolenie urzędników federalnych, którzy zwykle nie zajmują się sprawami wywiadu zagranicznego, oraz urzędników władz stanowych i lokalnych, którzy w trakcie ataku terrorystycznego

[39] A. Siegler, *The Patriot Act's Erosion of Constitutional Rights*, „Litigation" 2006, t. 32, nr 2, s. 18–21.

mogą napotkać członków obcego wywiadu. Szkolenie pomogłoby urzędnikom identyfikować informacje wywiadu zagranicznego i wykorzystywać je w wykonywaniu obowiązków[40].

Zmiany, których nie udało się przyporządkować do wcześniejszych rozdziałów, zawarto w ostatnim – dziesiątym. Na przykład zgodnie z sekcją 1006 cudzoziemcy, którzy brali udział w praniu brudnych pieniędzy, nie mogą wjechać do Stanów Zjednoczonych. Na podstawie sekcji 1009 przekazano FBI 250 000 dolarów w celu zbadania możliwości zapewnienia liniom lotniczym komputerowego dostępu do nazwisk osób podejrzanych przez rząd federalny o terroryzm, a zgodnie z sekcją 1014 zapewniono poszczególnym stanom pieniądze na zakup sprzętu i szkolenia dla służb ratowniczych (policji, straży pożarnej i pogotowia ratunkowego)[41].

Wprowadzeniu tak szerokich zmian w ustawodawstwie towarzyszyły liczne kontrowersje. Przeciwnicy ustawy twierdzili, że została ona uchwalona z pobudek oportunistycznych, z zamysłem, że w świetle wydarzeń z 11 września nie będzie szeroko dyskutowana i szybko przejdzie proces legislacyjny. Ponadto stwierdzono, że sekcja 215 łamie czwartą poprawkę konstytucji[42], sekcja 505 natomiast – zarówno pierwszą, jak i czwartą poprawkę[43]. W przypadku sekcji 215 przeciwnicy dostrzegli jawną ingerencję w nietykalność mienia. Dotyczyło to przeszukiwania przez służby bez nakazu sądowego miejsc zamieszkania czy pracy osoby podejrzanej, a także podsłuchiwania rozmów czy zdobywania informacji bez jej wiedzy. W przypadku sekcji 505 zarzucano ponadto naruszanie wolności słowa. Kontrowersje wzbudziła również sekcja 412, umożliwiająca zatrzymywanie na czas nieokreślony osób stanowiących zagrożenie dla państwa bez stawiania im zarzutów[44].

[40] *The USA PATRIOT Act of 2001*..., s. 117–121.

[41] Tamże, s. 121–132.

[42] Czwarta poprawka odnosi się do nietykalności osób i mienia. W tłumaczeniu Andrzeja Pułły: „Prawa ludu do nietykalności osobistej, mieszkania, dokumentów i mienia nie wolno naruszać przez nieuzasadnione rewizje i zatrzymanie; nakaz w tym przedmiocie można wystawić tylko wówczas, gdy zachodzi wiarygodna przyczyna potwierdzona przysięgą lub zastępującym ją oświadczeniem. Miejsce podlegające rewizji oraz osoby i rzeczy podlegające zatrzymaniu powinny być w nakazie szczegółowo określone". Zob. *Konstytucja Stanów Zjednoczonych Ameryki*..., s. 55–56.

[43] *Myths and Realities About the Patriot Act*, ACLU, 22 I 2005 r., https://www.aclu.org/other/myths-and-realities-about-patriot-act [dostęp: 31 V 2023].

[44] Tamże.

Znaczna część drugiego rozdziału Patriot Act wstępnie miała wygasnąć ostatniego dnia 2005 r., zgodnie z wpisaną w ustawę *sunset clause*, czyli zaplanowaną z góry datą wygaśnięcia przepisów, które dokonuje się automatycznie, chyba że zostanie przegłosowane przedłużenie. Do takiego przegłosowania doszło w marcu 2006 r. Prezydent Bush podpisał je i utrzymał większość najważniejszych elementów rozdziału bez zmian. Za rządów Baracka Obamy również przegłosowano przedłużenie ustawy (w 2012 r.), a w 2015 r. w ustawie USA FREEDOM Act podtrzymano większość zapisów wygasającego Patriot Act prócz sekcji 215, co miało uniemożliwić Agencji Bezpieczeństwa Narodowego (National Security Agency) masowe zbieranie informacji z telefonów komórkowych Amerykanów podejrzanych o działalność terrorystyczną.

Departament Bezpieczeństwa Krajowego Stanów Zjednoczonych

W odpowiedzi na ataki z 11 września prezydent Bush ogłosił utworzenie Biura Bezpieczeństwa Wewnętrznego (Office of Homeland Security) w celu koordynowania działań na rzecz bezpieczeństwa wewnętrznego. Dnia 25 listopada 2002 r. zgodnie z ustawą o bezpieczeństwie wewnętrznym (*The Homeland Security Act of 2002*) powołano Departament Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych (U.S. Department of Homeland Security, DHS) w celu konsolidacji organów władzy wykonawczej Stanów Zjednoczonych związanych z bezpieczeństwem wewnętrznym[45]. Dnia 1 marca 2003 r. 22 agencje zjednoczyły się w ramach jednego departamentu ze wspólną misją ochrony narodu amerykańskiego, co stanowi najbardziej zróżnicowane połączenie funkcji i obowiązków federalnych[46]. Misja DHS, najmłodszego, trzeciego co do wielkości departamentu, obejmuje m.in.: zapobieganie terroryzmowi, egzekwowanie prawa, zapewnianie bezpieczeństwa granic lądowych i morskich oraz transportu, prowadzenie polityki imigracyjnej, zarządzanie kryzysowe, zapewnianie cyberbezpieczeństwa. Powołanie DHS oznaczało zmianę amerykańskiego sposobu myślenia o zagrożeniach. Wprowadzenie terminu „ojczyzna" (ang. *homeland*) zarówno do systemu prawnego, jak i do nomenklatury służb było wyrazem skoncentrowania się rządzących na ochronie ludności nie tylko przed

[45] *The Homeland Security Act of 2002*, https://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf [dostęp: 31 V 2023].

[46] *Creation of the Department of Homeland Security*, Homeland Security, https://www.dhs.gov/creation-department-homeland-security [dostęp: 12 V 2023]; S. Wojciechowski, P. Osiewicz, *Zrozumieć współczesny terroryzm*..., s. 104.

sytuacjami kryzysowymi wywołanymi czynnikami naturalnymi, takimi jak klęski żywiołowe, lecz także przed rozproszonymi zagrożeniami ze strony osób czy organizacji[47].

Bezpieczeństwo lotnicze

Wydarzenia z 11 września miały olbrzymi wpływ na bezpieczeństwo lotnictwa cywilnego. W tym zakresie wprowadzono znaczne ograniczenia dotyczące przedmiotów, które można wnieść na pokład samolotu (m.in. zakazano wnoszenia noży – to nimi posłużono się podczas ataków Al-Kaidy), zakaz wstępu do kabiny pilotów (wprowadzono więcej zabezpieczeń, aby utrudnić dostanie się do niej osób postronnych), w związku z którym piloci przeszli dodatkowe szkolenia. Zmiany dotyczyły także usprawnień w bezpieczeństwie na samych lotniskach[48]. Po zamachach z 11 września utworzono Administrację Bezpieczeństwa Transportu (Transportation Security Administration), a także znacznie zwiększono budżet i liczbę etatów w Federal Air Marshal Service – federalnej policji lotniczej[49].

Podsumowanie

Zmiany wprowadzone po atakach na WTC miały daleko idące konsekwencje zarówno w polityce wewnętrznej, jak i w stosunkach międzynarodowych Stanów Zjednoczonych. Rozszerzenie uprawnień służb specjalnych, nowe regulacje dotyczące bezpieczeństwa lotniczego oraz powołanie DHS przyczyniły się do poprawy zdolności Stanów Zjednoczonych w zakresie prewencji zagrożeń terrorystycznych i reagowania na nie. Przyjęta polityka bezpieczeństwa wyznaczyła nowe standardy w walce z terroryzmem[50]. Niemniej jednak, jak wspomniano, zmiany te spotkały się również z krytyką ze strony obrońców praw człowieka i organizacji międzynarodowych, podkreślających, że wprowadzenie tych środków w pewnym stopniu

[47] E. Alterman, M. Green, *The Book on Bush: How George W. (Mis)leads America*, New York 2004, s. 244.

[48] *Bezpieczeństwo i ochrona lotnictwa cywilnego*, A.K. Siadkowski, A. Tomasik (red.), Poznań 2012, s. 152–154.

[49] A.K. Siadkowski, *Bezpieczeństwo i ochrona w cywilnej komunikacji lotniczej na przykładzie Polski, Stanów Zjednoczonych i Izraela*, Szczytno 2013, s. 296–302.

[50] *The Lessons Learned for U.S. National Security Policy in the 20 Years Since 9/11*, CAP, 10 IX 2021 r., https://www.americanprogress.org/article/lessons-learned-u-s-national-security-policy-20-years-since-911/ [dostęp: 27 I 2025].

naruszyło podstawowe prawa obywatelskie, takie jak prawo do prywatności i swobód obywatelskich[51]. Tym samym stało się konieczne znalezienie równowagi między skutecznością w zwalczaniu zagrożeń a ochroną wartości demokratycznych.

Mimo że wprowadzone zmiany przyniosły wiele korzyści w zakresie bezpieczeństwa, zdaniem autora ich długoterminowe skutki dla społeczeństwa oraz systemu politycznego wymagają dalszych analiz. Rozwój technologii oraz ewolucja metod walki z terroryzmem skłaniają do stawiania nowych pytań o etykę, efektywność działań prewencyjnych oraz przestrzeganie związanego z nimi prawa. Konieczne jest dostosowywanie środków do dynamicznie zmieniającej się natury zagrożeń, z jednoczesnym poszanowaniem praw obywatelskich i międzynarodowych standardów prawnych. W przeciwnym razie walka z terroryzmem może prowadzić do podkopania fundamentów, które powinna chronić.

Bibliografia

Alterman E., Green M., *The Book on Bush: How George W. (Mis)leads America*, New York 2004.

Benjamin D., Simon S., *The Age of Sacred Terror*, New York 2002.

Bezpieczeństwo i ochrona lotnictwa cywilnego, A.K. Siadkowski, A. Tomasik (red.), Poznań 2012.

Doran M.S., *Somebody Else's Civil War*, „Foreign Affairs" 2002, t. 81, nr 1, s. 22–42.

Fisher L., *Presidential War Power*, Lawrence 2004.

Konstytucja Stanów Zjednoczonych Ameryki, A. Pułło (tłum. i wstęp), Warszawa 2002.

Rackow S.H., *How the USA Patriot Act Will Permit Governmental Infringement upon the Privacy of Americans in the Name of „Intelligence" Investigations*, „University of Pennsylvania Law Review" 2002, t. 150, nr 5, s. 1651–1696. https://doi.org/10.2307/3312949.

[51] M. Carlisle, *How 9/11 Radically Expanded the Power of the U.S. Government*, Time, 11 IX 2021 r., https://time.com/6096903/september-11-legal-history/ [dostęp: 27 I 2025].

Siadkowski A.K., *Bezpieczeństwo i ochrona w cywilnej komunikacji lotniczej na przykładzie Polski, Stanów Zjednoczonych i Izraela*, Szczytno 2013.

Siegler A., *The Patriot Act's Erosion of Constitutional Rights*, „Litigation" 2006, t. 32, nr 2, s. 18–24.

Wojciechowski S., Osiewicz P., *Zrozumieć współczesny terroryzm*, Warszawa 2017.

Źródła internetowe

14 Interesting Pearl Harbor Facts, Pearl Harbor Tours, https://www.pearlharbortours.com/pearl-harbor/facts-about-pearl-harbor [dostęp: 25 I 2025].

1999 – 2021 The U.S. War in Afghanistan, Council on Foreign Relations, https://www.cfr.org/timeline/us-war-afghanistan [dostęp: 30 III 2023].

A Review of the FBI's Handling of Intelligence Information Prior to the September 11 Attacks, https://oig.justice.gov/sites/default/files/archive/special/0506/chapter5.htm [dostęp: 10 VI 2023].

Carlisle M., *How 9/11 Radically Expanded the Power of the U.S. Government*, Time, 11 IX 2021 r., https://time.com/6096903/september-11-legal-history/ [dostęp: 27 I 2025].

Creation of the Department of Homeland Security, Homeland Security, https://www.dhs.gov/creation-department-homeland-security [dostęp: 12 V 2023].

Daalder I.H., Lindsay J.M., *The Bush Revolution: The Remaking of America's Foreign Policy*, April 2003, https://www.brookings.edu/wp-content/uploads/2016/06/20030425.pdf [dostęp: 25 I 2025].

Doyle Ch., *Terrorism: Section by Section Analysis of the USA PATRIOT Act*, https://www.arl.org/wp-content/uploads/2001/12/patriot-act-analysis-2001.pdf [dostęp: 30 III 2023].

ECTF and FCTF, United State Secret Service, https://www.secretservice.gov/contact/ectf-fctf [dostęp: 30 III 2023].

Laden O. bin, *Letter to America*, https://web.archive.org/web/20040615081002/http://observer.guardian.co.uk/worldview/story/0,11581,845725,00.html [dostęp: 26 I 2025].

Myths and Realities About the Patriot Act, ACLU, 22 I 2005 r., https://www.aclu.org/other/myths-and-realities-about-patriot-act [dostęp: 31 V 2023].

The Lessons Learned for U.S. National Security Policy in the 20 Years Since 9/11, CAP, 10 IX 2021 r., https://www.americanprogress.org/article/lessons-learned-u-s-national-security-policy-20-years-since-911/ [dostęp: 27 I 2025].

The USA PATRIOT Act: Preserving Life and Liberty, Department of Justice, https://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf [dostęp: 30 III 2023].

WATCH: President George W. Bush's address to the nation after September 11, 2001attacks, YouTube, 19 VIII 2021 r., https://www.youtube.com/watch?v=WA8-KEnfWbQ [dostęp: 30 III 2023].

Akty prawne

The Authorization for Use of Military Force, https://www.govinfo.gov/content/pkg/PLAW-107publ40/pdf/PLAW-107publ40.pdf [dostęp: 30 III 2023].

The Homeland Security Act of 2002, https://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf [dostęp: 31 V 2023].

The USA PATRIOT Act of 2001, https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf [dostęp: 30 III 2023].

Franciszek Dziadkowiec-Wędlikowski

Student kierunku bezpieczeństwo narodowe na Uniwersytecie Jagiellońskim w Krakowie. Jego zainteresowania naukowe obejmują Stany Zjednoczone oraz funkcjonowanie służb specjalnych w Polsce i na świecie.

Kontakt: franciszek.dw@gmail.com

VARIA

Terroryzm – studia, analizy, prewencja, 2025, nr 7: 231–254

https://doi.org/10.4467/27204383TER.25.032.21809

Varia

Sektor ochrony i bezpieczeństwa w świetle nowych trendów

Wnioski z badań

Adam Tatarowski
Zakład Rozwoju Technicznej Ochrony Mienia TECHOM
https://orcid.org/0009-0007-5503-6819

W sierpniu i wrześniu 2024 r. na zlecenie Zakładu Rozwoju Technicznej Ochrony Mienia TECHOM sp. z o.o. (dalej: TECHOM) przeprowadzono przekrojowe badania sektora ochrony i bezpieczeństwa mienia i osób. Ich efektem jest stworzenie przez zespół badaczy z MABEA sp. z o.o.: Annę Araminowicz, Piotra Klattę, Tomasza Radochońskiego i Magdę Sierżyńską pierwszego kompleksowego raportu pt. *Ochrona i Bezpieczeństwo Mienia i Osób – analiza sektora. Raport z badania*, który uwzględnia szeroki kontekst prawno-normatywny i specyfikę tego sektora. Jest to bezpłatny raport przeznaczony do powszechnego użytku. Jego pierwsza edycja została wydana w październiku 2024 r.[1] Drugą edycję, poszerzoną o najnowsze

[1] A. Araminowicz, P. Klatta, T. Radochoński, M. Sierżyńska, *Ochrona i Bezpieczeństwo Mienia i Osób – analiza sektora. Raport z badania*, Kraków 2024, MABEA sp. z o.o., https://www.mabea.pl/wp-content/uploads/2024/11/Ochrona-i-bezpieczenstwo-mienia-i-osob-analiza-sektora.Raport-z-badania2024_do-pobrania.pdf [dostęp: 28 I 2025].

dane statystyczne, opublikowano w marcu 2025 r. na stronie internetowej TECHOM[2].

Inspiracją do realizacji badań była informacja podana w lipcu 2024 r. przez Polską Agencję Rozwoju Przedsiębiorczości (PARP) o konkursie na powierzenie organizacji i prowadzenia sektorowych rad ds. kompetencji – organów zdefiniowanych w art. 4c ust. 1 pkt 2 ustawy o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości[3]. Sektorowe rady ds. kompetencji służą budowaniu współpracy między administracją publiczną, instytucjami edukacyjnymi i organizacjami biznesowymi i skupiają przedstawicieli tych sektorów. Odgrywają ważną rolę na rynku pracy przez wsparcie kształcenia osób dorosłych. Sektorową radę ds. kompetencji utworzono m.in. w sektorze ochrony i bezpieczeństwa mienia i osób (nazwa zaproponowana przez PARP).

Idea utworzenia sektorowych rad wynikła z tendencji w UE do unifikacji rozumienia kompetencji i kwalifikacji. Już konwencja lizbońska o uznawaniu kwalifikacji, jako międzynarodowe porozumienie pod patronatem UNESCO i Rady Europy, umożliwiła uznawanie kwalifikacji akademickich w Europie i poza jej granicami[4]. Należy wspomnieć również o dyrektywie 2005/36/WE[5], która dotyczy uznawania kwalifikacji zawodowych w UE i umożliwia specjalistom uprawianie swojego zawodu lub świadczenie usług za granicą. Dyrektywa ta stanowiła podstawę do wprowadzenia w 2008 r. Europejskiej Ramy Kwalifikacji (ERK), która następnie została znowelizowana w 2017 r.[6] Zgodnie z zaleceniem Rady Europy w sprawie propagowania automatycznego wzajemnego uznawania kwalifikacji uzyskanych w ramach kształcenia i szkolenia na poziomie wyższym

---

[2] A. Araminowicz, P. Klatta, T. Radochoński, M. Sierżyńska, *Ochrona i Bezpieczeństwo Mienia i Osób – analiza sektora. Raport z badania. Wydanie II zaktualizowane*, Kraków 2025, MABEA sp. z o.o., https://www.techom.com/wp-content/uploads/2025/04/Raport_MABEA_TECHOM_2025.pdf [dostęp: 21 V 2025].

[3] *Ustawa z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości* (t.j. DzU z 2025 r. poz. 98).

[4] *Konwencja o uznaniu kwalifikacji związanych z uzyskaniem wyższego wykształcenia w Regionie Europejskim, sporządzona w Lizbonie dnia 11 kwietnia 1997 r.* (DzU z 2004 r. nr 233 poz. 2339).

[5] *Dyrektywa 2005/36/WE Parlamentu Europejskiego i Rady z dnia 7 września 2005 r. w sprawie uznawania kwalifikacji zawodowych* (Dz. Urz. UE L 255/22 z 30 IX 2005 r.).

[6] *Zalecenie Rady z dnia 22 maja 2017 r. w sprawie europejskich ram kwalifikacji dla uczenia się przez całe życie i uchylające zalecenie Parlamentu Europejskiego i Rady z dnia 23 kwietnia 2008 r. w sprawie ustanowienia europejskich ram kwalifikacji dla uczenia się przez całe życie* (Dz. Urz. UE C 189/15 z 15 VI 2017 r.).

i średnim II stopnia oraz efektów uczenia się osiągniętych w okresach nauki za granicą[7], ERK ma promować przejrzystość krajowych systemów kształcenia i szkolenia oraz budować wzajemne zaufanie. Sektorowe rady zgodnie z ustawą o Zintegrowanym Systemie Kwalifikacji[8] odgrywają zasadniczą rolę w nadzorze nad Polską Ramą Kwalifikacji (czyli polskiej implementacji ERK) dla poszczególnych sektorów.

Podstawę prawną działania sektorowych rad określają:

1) ustawa o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości,
2) ustawa o Zintegrowanym Systemie Kwalifikacji,
3) ustawa Prawo oświatowe[9].

Co więcej, w projekcie nowelizacji ustawy o zarządzaniu kryzysowym[10] rada sektorowa ds. kompetencji w sektorze ochrony i bezpieczeństwa jest wskazana jako organ wydający opinie dotyczące certyfikatów lub innych dokumentów, których żądają operatorzy infrastruktury krytycznej (IK) przy realizacji rozwiązań organizacyjno-technicznych mających na celu zapewnienie bezpieczeństwa zarządzanej przez nich IK i zwiększenie jej odporności.

Wniosek konkursowy o organizację i prowadzenie rady w tym sektorze, złożony przez TECHOM we współpracy z Polską Platformą Bezpieczeństwa Wewnętrznego, Polskim Towarzystwem Bezpieczeństwa Narodowego i Ogólnopolskim Stowarzyszeniem Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem „POLALARM" (dalej: POLALARM), uzyskał pozytywną opinię prezes PARP. To ogromne wyróżnienie stwarza możliwości działania na wielu płaszczyznach, czemu sprzyja specyficzne ulokowanie sektorowych rad ds. kompetencji w ekosystemie publiczno-prywatnym.

Poniżej przedstawiono syntetyczną prezentację raportu, w której uwzględniono różne dane, w tym statystyczne.

---

[7] *Zalecenie Rady z dnia 26 listopada 2018 r. w sprawie propagowania automatycznego wzajemnego uznawania kwalifikacji uzyskanych w ramach kształcenia i szkolenia na poziomie wyższym i średnim II stopnia oraz efektów uczenia się osiągniętych w okresach nauki za granicą* (Dz. Urz. UE C 444/1 z 10 XII 2018 r.).

[8] *Ustawa z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji* (t.j. DzU z 2024 r. poz. 1606).

[9] *Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe* (t.j. DzU z 2024 r. poz. 737, ze zm.).

[10] Projekt ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw, https://legislacja.rcl.gov.pl/docs//2/12386961/13069020/13069024/dokument711601.pdf [dostęp: 4 IV 2025].

Sektor ochrony i bezpieczeństwa mienia i osób – omówienie wyników badania

Sektor ochrony i bezpieczeństwa mienia i osób odgrywa szczególną rolę w zapewnieniu stabilności państwa, a jego znaczenie stale rośnie w obliczu nowych wyzwań technologicznych, regulacyjnych i geopolitycznych. Współczesne zagrożenia wymagają nowych rozwiązań legislacyjnych, organizacyjnych, skuteczniejszych metod zabezpieczeń oraz – przede wszystkim – wykwalifikowanych kadr, zdolnych do przeciwdziałania zarówno tradycyjnym, jak i nowym formom zagrożeń, w tym cyberprzestępczości czy zagrożeniom hybrydowym.

Autorzy raportu skoncentrowali się na trzech najważniejszych aspektach funkcjonowania sektora:

1. Struktura i regulacje – analiza kontekstu prawno-normatywnego, z uwzględnieniem specyfiki sektora.
2. Potrzeby kompetencyjne – identyfikacja luk w kwalifikacjach kadr oraz rekomendacje dotyczące kształcenia i walidacji umiejętności.
3. Nowe wyzwania i technologie – omówienie trendów geopolitycznych, legislacyjnych i technologicznych, które będą kształtować przyszłość sektora.

Przeprowadzone badania miały na celu kompleksowe zdiagnozowanie aktualnej sytuacji w sektorze, określenie najważniejszych problemów oraz wskazanie kierunków rozwoju, które pozwolą na lepsze dostosowanie usług ochrony do współczesnych realiów.

Metodologia badań i zakres analiz

Badania sektora ochrony i bezpieczeństwa mienia i osób zostały przeprowadzone w sierpniu i wrześniu 2024 r. Celami tych badań były:

- analiza otoczenia społeczno-gospodarczego i instytucjonalno-prawnego sektora ochrony i bezpieczeństwa mienia i osób,
- analiza oferty edukacyjno-szkoleniowej na potrzeby sektora,
- analiza trendów wpływających na rynek pracy i potrzeby kompetencyjne w sektorze,
- identyfikacja potrzeb kompetencyjnych w sektorze,

– identyfikacja wyzwań stojących przed sektorem w kontekście działań mających na celu zapewnienie kadr posiadających kompetencje adekwatne do potrzeb rynku pracy w sektorze[11].

Badania objęły analizę danych zastanych, badanie jakościowe i badanie ankietowe.

W ramach analizy danych zastanych uwzględniono:
– akty prawne regulujące działania w sektorze,
– dane statystyczne,
– raporty i analizy dotyczące sektora,
– artykuły naukowe,
– artykuły w mediach drukowanych i elektronicznych oraz komunikaty prasowe,
– informacje zamieszczone na stronach internetowych podmiotów (np. instytucji regulujących działanie sektora, organizacji branżowych, uczelni),
– informacje zamieszczone na portalach branżowych[12].

Badanie jakościowe stanowiło istotne uzupełnienie analizy danych zastanych i umożliwiło rozpoznanie specyfiki sektora. Zostało przeprowadzone w formie dwóch zogniskowanych wywiadów grupowych oraz panelu eksperckiego. Łącznie w badaniu wzięło udział 29 osób, w tym cenieni eksperci z administracji publicznej (regulatorzy rynku), stowarzyszeń i izb branżowych, uczelni wyższych, specjalistycznych placówek kształcenia ustawicznego, a także przedstawiciele przedsiębiorców, zarówno tych, którzy działają w sektorze (agencje ochrony, firmy projektujące systemy zabezpieczeń i instalujące je), jak i tych, którzy zamawiają usługi ochrony (m.in. w obszarach IK, handlu, logistyki).

Badanie ankietowe zostało przeprowadzone metodą CAWI (ang. Computer-Assisted Web Interview) na grupie 46 respondentów reprezentujących m.in. przedsiębiorstwa świadczące usługi ochrony, zleceniodawców i użytkowników usług ochrony, organizacje branżowe, instytucje edukacyjne, administrację publiczną[13].

Na podstawie zgromadzonych danych opracowano scenariusze rozwoju sektora, uwzględniające wpływ nowych regulacji prawnych, rozwój

[11] A. Araminowicz, P. Klatta, T. Radochoński, M. Sierżyńska, *Ochrona i Bezpieczeństwo Mienia i Osób – analiza sektora. Raport z badania*, Kraków 2024..., s. 8.

[12] Tamże, s. 9.

[13] Tamże, s. 11.

technologii oraz zmieniające się potrzeby rynku pracy. Metodologia badawcza pozwoliła na wielowymiarową analizę sektora oraz zintegrowanie perspektyw: regulacyjnej, biznesowej i edukacyjnej.

Charakterystyka sektora

Sektor ochrony i bezpieczeństwa mienia i osób zaczął się intensywnie rozwijać w Polsce po transformacji ustrojowej w 1989 r. Bardzo szybko zyskał ogromne znaczenie w gospodarce wolnorynkowej. Pierwszym aktem prawnym, który umożliwił działalność w sektorze, była ustawa o działalności gospodarczej[14]. Regulowała ona konieczność uzyskania koncesji w zakresie usług w ochronie osób i mienia, a także detektywistycznych. Fundament funkcjonowania branży stanowi natomiast ustawa o ochronie osób i mienia[15]. Przez niemal dekadę sektor funkcjonował bez właściwych regulacji, co generowało liczne niejasności prawne. Obecnie podlega on wielu dodatkowym regulacjom, jednak znaczna część usług ochrony funkcjonuje poza ramami prawnymi, ponieważ nie ma wymagań dla usługodawców działających poza ramami wyznaczanymi przez ustawę o ochronie osób i mienia. To charakterystyczne dla tej branży zjawisko ma praktyczne konsekwencje dla całego rynku usług ochrony. Stwarza wyzwania zarówno stricte legislacyjne, jak i oddolne, wynikające z dynamicznych zmian rynkowych oraz rosnących oczekiwań wobec pracowników ochrony. Wymaga to od nich dostosowania się do nowych technologii oraz zdobywania specjalistycznych kompetencji, obejmujących m.in. zarządzanie bezpieczeństwem, zarządzanie ryzykiem czy zarządzanie sytuacjami kryzysowymi. W związku z rosnącą rolą ochrony IK agencje ochrony i inne firmy stanowiące trzon sektora muszą sprostać coraz bardziej wymagającym standardom, co jest wyzwaniem nie tylko regulacyjnym, lecz także edukacyjnym i w zakresie weryfikowania kompetencji.

Zdefiniowanie sektora na potrzeby raportu – zgodnie z wytycznymi PARP – oparto na kodach Polskiej Klasyfikacji Działalności (PKD). Wybrane podklasy przedstawiono w tabeli 1[16].

[14] *Ustawa z dnia 23 grudnia 1988 r. o działalności gospodarczej* (DzU z 1988 r. nr 41 poz. 324, ze zm.).

[15] *Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia* (t.j. DzU z 2025 r. poz. 532).

[16] Wszystkie tabele i wykresy w tym artykule pochodzą z publikacji: A. Araminowicz, P. Klatta, T. Radochoński, M. Sierżyńska, *Ochrona i Bezpieczeństwo Mienia i Osób – analiza sektora. Raport z badania*, Kraków 2024… (przyp. red.).

Tabela 1. Opis wybranych podklas Polskiej Klasyfikacji Działalności 2007.

Podklasa	Podklasa obejmuje
74.90.Z – Pozostała działalność profesjonalna, naukowa i techniczna, gdzie indziej niesklasyfikowana	• pośrednictwo w interesach, tj. organizowanie zaopatrzenia lub sprzedaży dla małych i średnich firm, z wyłączeniem pośrednictwa w handlu nieruchomościami, pośrednictwo w zakupie lub sprzedaży patentów, działalność związaną z wyceną, z wyłączeniem wyceny nieruchomości i wyceny dla towarzystw ubezpieczeniowych (antyki, biżuteria itp.), kontrolę dokumentów przewozowych, informacje dotyczące stawek za fracht, działalność związaną z prognozowaniem pogody, • **doradztwo w zakresie bezpieczeństwa**, • działalność agronomów i ekonomistów rolnych, doradztwo w sprawach środowiska naturalnego, pozostałe doradztwo techniczne, doradztwo inne niż doradztwo z zakresu architektury lub inżynierii oraz doradztwo w zakresie zarządzania, działalność związaną z opracowywaniem kosztorysów, działalność agentów lub agencji występujących w imieniu indywidualnych osób, w celu zaangażowania do filmu, teatru oraz innej działalności artystycznej lub sportowej, wydania książek, nagrań muzycznych, scenariuszy sztuk, prac artystycznych i fotografii przez wydawców, producentów itp.
80.10.Z – Działalność ochroniarska, z wyłączeniem obsługi systemów bezpieczeństwa	• wykonywanie działalności w zakresie ochrony i patrolowania, działalności ochroniarskiej związanej z transportem pieniędzy, papierów wartościowych lub innych wartościowych rzeczy, • działalność ochroniarską w zakresie przewozów samochodami opancerzonymi, • działalność usługową w zakresie ochrony osobistej, • działalność usługową w zakresie wykrywacza kłamstw, • działalność usługową związaną z pobieraniem i identyfikacją odcisków palców, • pozostałą działalność ochroniarską, z wyłączeniem obsługi systemów bezpieczeństwa
80.20.Z – Działalność ochroniarska w zakresie obsługi systemów bezpieczeństwa	• działalność ochroniarską w zakresie obsługi i monitorowania elektronicznych systemów bezpieczeństwa, takich jak: alarmy przeciwwłamaniowe czy przeciwpożarowe, włączając ich instalację i konserwację, • instalację, naprawę, przebudowę oraz regulację mechanicznych lub elektronicznych urządzeń zamykających, sejfów i skarbców w powiązaniu z późniejszym monitoringiem. Jednostki prowadzące niniejszą działalność mogą prowadzić również sprzedaż ww. urządzeń, tj. elektronicznych systemów bezpieczeństwa, mechanicznych lub elektronicznych urządzeń zamykających, sejfów i skarbców
80.30.Z – Działalność detektywistyczna	• działalność dochodzeniową i detektywistyczną, • działalność prywatnych detektywów, niezależnie od typu klienta czy celu dochodzenia

Opisy PKD korespondują ze sposobem rozumienia systemu bezpieczeństwa dla IK. W ramach Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK) funkcjonuje tzw. sześciopak opisujący system ochrony IK. Działania podejmowane na rzecz zapewnienia bezpieczeństwa obejmują:

1) zapewnienie bezpieczeństwa fizycznego, z uwzględnieniem środków technicznych wspomagających ochronę fizyczną,
2) zapewnienie bezpieczeństwa technicznego, w tym ochrony przeciwpożarowej,
3) zapewnienie bezpieczeństwa osobowego,
4) zapewnienie bezpieczeństwa teleinformatycznego,
5) zapewnienie bezpieczeństwa prawnego,
6) plany ciągłości działania i odtwarzania[17].

Struktura sektora jest silnie zróżnicowana. Dominują mikro-, małe i średnie przedsiębiorstwa świadczące usługi ochrony fizycznej, jednak coraz większą rolę odgrywają firmy specjalizujące się w systemach zabezpieczeń technicznych (popularność zyskuje wykorzystanie nowych technologii opartych na sztucznej inteligencji). Istotne są również duże korporacje zajmujące się ochroną, z których większość ma zasięg międzynarodowy.

Według danych rejestru REGON (stan na czerwiec 2024 r.) w sektorze było zarejestrowanych 7595 podmiotów deklarujących prowadzenie działalności w ramach działu PKD 80 – Działalność detektywistyczna i ochroniarska[18]. W tabeli 2 zaprezentowano liczbę tych podmiotów w latach 2015–2024, z podziałem ze względu na liczbę osób zatrudnionych.

Tabela 2. Liczba podmiotów w latach 2015–2024 deklarujących prowadzenie działalności detektywistycznej i ochroniarskiej, z podziałem na liczbę zatrudnionych (na podstawie danych z rejestru REGON).

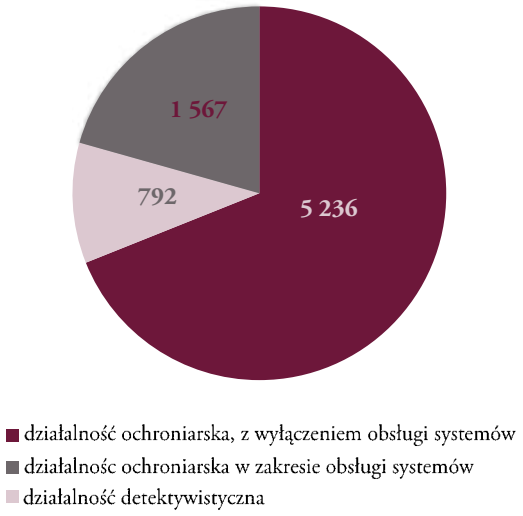
Stan na	0–9	10–49	50–249	250+	ogółem
31.12.2015	4 822	734	288	112	5 956
31.12.2016	5 259	732	275	116	6 382

[17] *Narodowy Program Ochrony Infrastruktury Krytycznej*, Rządowe Centrum Bezpieczeństwa, 2023. Tekst programu jest dostępny na stronie: https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej.

[18] A. Araminowicz, P. Klatta, T. Radochoński, M. Sierżyńska, *Ochrona i Bezpieczeństwo Mienia i Osób – analiza sektora. Raport z badania*, Kraków 2024..., s. 51.

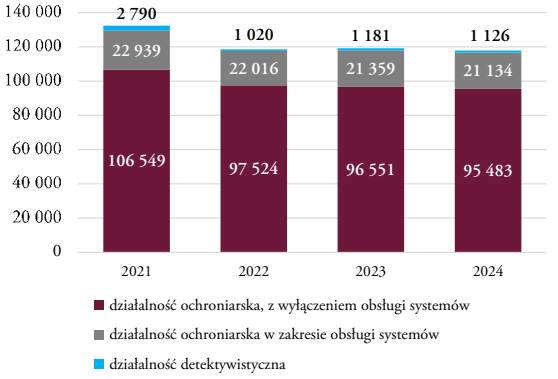
Stan na	0–9	10–49	50–249	250+	ogółem
31.12.2017	5 482	741	265	115	6 603
31.12.2018	5 546	697	247	113	6 603
31.12.2019	5 656	663	247	112	6 678
31.12.2020	5 913	637	240	112	6 902
31.12.2021	6 173	620	234	109	7 136
31.12.2022	6 410	606	228	107	7 351
31.12.2023	6 529	583	228	105	7 445
30.06.2024	6 690	578	223	104	7 595

Na wykresie 1 został przedstawiony podział podmiotów deklarujących prowadzenie w 2024 r. działalności detektywistycznej i ochroniarskiej, z uwzględnieniem podklas działu PKD 80.



Wykres 1. Liczba podmiotów deklarujących w 2024 r. prowadzenie działań w sektorze ochrony i bezpieczeństwa, z podziałem na podklasy działu PKD 80 (na podstawie danych z rejestru REGON).

Według danych Głównego Urzędu Statystycznego dotyczących zatrudnienia w ramach działu PKD 80 sektor zatrudnia 117 743 pracowników (stan na 31 marca 2024 r.)[19]. Widoczny jest spadek zatrudnienia w tym sektorze w latach 2021–2024 (wykres 2). Może to być skutek pandemii COVID-19, pełnoskalowej inwazji Rosji na Ukrainę, a także nowych trendów polegających na odchodzeniu od bezpośredniej ochrony fizycznej na rzecz zabezpieczeń technicznych.



Wykres 2. Liczba osób zatrudnionych w sektorze ochrony i bezpieczeństwa w latach 2021–2024, z podziałem na podklasy działu PKD 80 (na podstawie danych Głównego Urzędu Statystycznego).

Wartość rynku ochrony i bezpieczeństwa mienia i osób w 2023 r. była szacowana na ok. 16 mld zł, z czego największą część – ponad 11,7 mld zł – stanowiły przychody z działalności ochroniarskiej, z wyłączeniem obsługi systemów bezpieczeństwa (dział PKD 80.10.Z)[20].

Uprawnienia i kwalifikacje

Znaczna część działalności zawodowej w sektorze ochrony i bezpieczeństwa mienia i osób podlega przestarzałym regulacjom, które nie przystają do współczesnej rzeczywistości i mają w dużej mierze charakter koncesyjny – w praktyce pomijają etap nabywania kompetencji. Nie uwzględniają także realnej walidacji kompetencji.

[19] Tamże, s. 59.

[20] Tamże, s. 46.

Podstawowym aktem prawnym, który reguluje tę tematykę, jest ustawa o ochronie osób i mienia. Kwestię dopuszczenia do posiadania broni reguluje z kolei ustawa o broni i amunicji[21].

W tabeli 3 zaprezentowano liczbę osób wpisanych na listy kwalifikowanych pracowników sektora w latach 2015–2023, które mają uprawnienia zgodne z ustawą o ochronie osób i mienia.

Tabela 3. Liczba osób wpisanych na listy kwalifikowanych pracowników sektora w latach 2015–2023 (na podstawie danych Komendy Głównej Policji).

Stan na	Liczba osób wpisanych na listę kwalifikowanych pracowników ochrony fizycznej	Liczba osób wpisanych na listę kwalifikowanych pracowników zabezpieczenia technicznego
31.12.2015	90 059	17 405
31.12.2016	91 230	18 066
31.12.2017	92 943	18 633
31.12.2018	95 238	19 212
31.12.2019	95 413	19 644
31.12.2020	99 235	20 137
31.12.2021	103 323	20 801
31.12.2022	108 261	21 338
31.12.2023	112 459	22 039

Bardzo dobrym przykładem ukazującym nieaktualność wspomnianych regulacji w kontekście nabywania i walidacji kompetencji i/lub kwalifikacji jest sposób uzyskiwania wpisu na listę kwalifikowanych pracowników zabezpieczenia technicznego opisany w art. 27 ustawy o ochronie osób i mienia. Poza warunkami formalnymi (wiek, badania lekarskie, opinia Policji) praktycznie nie ma wymagań w zakresie kompetencji i/lub kwalifikacji. Wystarczające jest, gdy osoba zainteresowana, zgodnie z art. 27 ust. 2 pkt 4, (...) *posiada wykształcenie co najmniej zawodowe techniczne o specjalności elektronicznej, elektrycznej, łączności, mechanicznej, informatycznej lub ukończyła kurs pracownika zabezpieczenia technicznego albo została przyuczona do wymienionych zawodów na podstawie przepisów ustawy z dnia 22 marca 1989 r. o rzemiośle (Dz. U. z 2020 r. poz. 2159).* Nie ma innych przepisów

[21] *Ustawa z dnia 21 maja 1999 r. o broni i amunicji* (t.j. DzU z 2024 r. poz. 485).

na poziomie ustawowym, które precyzowałyby to zagadnienie. Osoba, która taki wpis uzyska, jest uprawniona do:

- wykonywania czynności, o których mowa w art. 3 pkt. 2 ustawy o ochronie osób i mienia, tj.:
  a) *montażu elektronicznych urządzeń i systemów alarmowych, sygnalizujących zagrożenie chronionych osób i mienia, oraz eksploatacji, konserwacji i naprawach w miejscach ich zainstalowania,*
  b) *montażu urządzeń i środków mechanicznego zabezpieczenia oraz ich eksploatacji, konserwacji, naprawach i awaryjnym otwieraniu w miejscach zainstalowania;*
- wykonywania czynności, o których mowa w art. 27 ust. 4 wspomnianej ustawy, tj.:
  1) *opracowywania planu ochrony w zakresie określonym w art. 3 pkt. 2,*
  2) *organizowania i kierowania zespołami pracowników zabezpieczenia technicznego*.

Czynności, o których mowa we wspomnianym art. 3 pkt. 2 ustawy o ochronie osób i mienia, nie obejmują projektowania systemów zabezpieczeń – to aspekt de facto nieuregulowany. Każda osoba, nawet taka, która nie ma wykształcenia zawodowego, może – biorąc pod uwagę obecne zapisy ustawowe – realizować projekty systemów zabezpieczeń technicznych.

Podejście do formułowania wymagań kompetencyjno-kwalifikacyjnych wobec usługodawców realizujących czynności projektowania, montażu i konserwacji systemów zabezpieczeń technicznych[22] jest regulowane również przez wojskowe wymagania normatywne, jednak ich wpływ na cały rynek jest ograniczony. Regulacje te nie mają wystarczającej mocy, aby przełożyć je na jednolite wymagania w sektorze cywilnym. Podobnie załącznik 1 do NPOIK z 2023 r.[23] jedynie wzmiankuje o sposobach nabywania i walidacji kompetencji w tej dziedzinie. W dokumencie podkreśla się zasadność realizacji kursów pracownika zabezpieczenia technicznego w wyspecjalizowanej placówce kształcenia ustawicznego działającej w systemie oświaty, a także odwołuje się do normy PN-EN 16763 *Usługi w zakresie*

[22] *Instrukcja o ochronie obiektów wojskowych i konwojowanego mienia – DU-3.14.3(A) (Szt. Gen. 1705/2023)* – (dokument niejawny).

[23] *Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje*, załącznik 1 do Narodowego Programu Ochrony Infrastruktury Krytycznej, Rządowe Centrum Bezpieczeństwa, 2023. Tekst załącznika jest dostępny na stronie: https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej.

systemów ochrony przeciwpożarowej oraz systemów zabezpieczeń technicznych. Należy jednak podkreślić, że NPOIK pełni jedynie funkcję rekomendacji, a w polskiej praktyce przetargowej najważniejszym kryterium wyboru usługodawców jest najniższa cena. W rezultacie kompetencje i kwalifikacje wykonawców są często pomijane, o ile nie zostały jednoznacznie określone w przepisach prawa. Według autorów raportu:

> (...) określone w Ustawie o ochronie osób i mienia uprawnienia dotyczą dwóch grup osób – pracowników ochrony fizycznej oraz pracowników zabezpieczenia technicznego. Przedstawiciele sektora zwracają jednak uwagę na konieczność uwzględnienia współczesnego rozumienia procesów związanych z zapewnianiem bezpieczeństwa i ochroną oraz dostosowania przepisów dotyczących kompetencji pracowników do aktualnych rozwiązań organizacyjnych i wykorzystywanych technologii.
>
> Podkreślają również, że konieczne jest zweryfikowanie i uporządkowanie przepisów dotyczących uprawnień wymaganych do wykonywania czynności z zakresu zapewniania bezpieczeństwa i ochrony osób i mienia pod kątem sposobu uzyskiwania różnych uprawnień. Przepisy z jednej strony powinny zapewnić rzetelną weryfikację określonych przepisami wymogów, z drugiej zaś, nie ograniczać nadmiernie dostępu i zapewnić dopływ do sektora pracowników posiadających potrzebne uprawnienia.
>
> Analiza zagadnień związanych z uprawnieniami dla osób wykonujących poszczególne czynności mogłaby też stanowić jeden z istotnych elementów dyskusji związanej z określaniem typowych dla sektora procesów i zadań zawodowych. Pozwoliłoby to doprecyzować zakres sektora i określić punkty styku z innymi sektorami (np. z sektorem opieki zdrowotnej w zakresie czynności wchodzących w obszar działań związanych z ratownictwem medycznym).
>
> W związku z zachodzącymi zmianami w zakresie działań realizowanych w sektorze istotne jest też podejmowanie dyskusji nad wskazywaniem wśród nich tych, których wykonywanie wymaga posiadania uprawnień określonych przepisami prawa. W odniesieniu do pozostałych, formalne potwierdzenie posiadania przydatnych do ich wykonywania kompetencji mogłoby być dobrowolne i stanowić dobrą praktykę. Wykorzystane do tego mogłyby być rozwiązania dostępne w ramach Zintegrowanego Systemu Kwalifikacji, w formie kwalifikacji wolnorynkowych lub sektorowych. Warto byłoby rozważyć podjęcie współpracy przez przedstawicieli różnych grup interesariuszy w celu

monitorowania potrzeb sektora w tym zakresie, tak aby uprawnienia i kwalifikacje w sektorze stanowiły spójny i przejrzysty system[24].

Kształcenie na potrzeby sektora

W raporcie szczegółowo zanalizowano system kształcenia w tym sektorze, edukację formalną i pozaformalną, a także zidentyfikowano najważniejsze luki kompetencyjne i potrzeby rynku.

Kształcenie formalne dotyczy zarówno szkolnictwa branżowego, jak i szkolnictwa wyższego. Edukacja branżowa obejmuje przygotowanie do pracy w sektorze w zawodach takich jak technik ochrony osób i mienia oraz technik bezpieczeństwa i higieny pracy. Szkoły policealne oferujące te kierunki działają na terenie całego kraju, a umiejętności absolwentów są potwierdzane przez egzaminy zawodowe w kwalifikacjach BPO.02 (Ochrona osób i mienia) i BPO.01 (Zarządzanie bezpieczeństwem w środowisku pracy).

Egzaminy zawodowe mają zróżnicowaną zdawalność. Na przykład w sesji letniej w 2023 r. cały egzamin w kwalifikacji BPO.02 zdało 62,70% przystępujących (z czego do części pisemnej przystąpiło 469 osób, zdało 90,62%, a do części praktycznej przystąpiło 516 osób, zdało 63,37%)[25], w kwalifikacji BPO.01 natomiast wynik był niższy i wyniósł 40,03% (do części pisemnej przystąpiło 2087 osób, zdało 91,42%, do części praktycznej – 2794 osoby, zdało 37,62%)[26]. Dane te wskazują na wyraźne trudności ze zdaniem części praktycznej egzaminów, co może sugerować niewystarczające przygotowanie absolwentów do realnych wyzwań zawodowych.

Szkolnictwo wyższe w obszarze bezpieczeństwa obejmuje takie kierunki, jak: bezpieczeństwo narodowe, bezpieczeństwo wewnętrzne, kryminologia czy administracja i bezpieczeństwo wewnętrzne. Uczelnie oferują duży wybór specjalizacji, ale dyplomy akademickie nie wystarczają do uzyskania wpisu na listę kwalifikowanych pracowników ochrony fizycznej – potwierdzają jedynie przygotowanie teoretyczne. W sektorze ważną rolę odgrywają także uczelnie dla służb mundurowych, przygotowujące m.in. przyszłych funkcjonariuszy służb państwowych.

Oprócz formalnej edukacji istotnym elementem kształcenia w sektorze ochrony są kursy i szkolenia. Należą do nich m.in.:

[24] A. Araminowicz, P. Klatta, T. Radochoński, M. Sierżyńska, *Ochrona i Bezpieczeństwo Mienia i Osób – analiza sektora. Raport z badania*, Kraków 2024..., s. 82.

[25] Tamże, s. 86.

[26] Tamże, s. 87.

– kursy dające podstawę do wpisu na listę kwalifikowanych pracowników ochrony fizycznej, obejmujące przygotowanie teoretyczne i praktyczne z zakresu strzelectwa, technik interwencyjnych oraz prawa,
– kursy pracownika zabezpieczenia technicznego (brak w ustawie o ochronie osób i mienia precyzyjnych wymagań dotyczących ich zakresu i standardów),
– obowiązkowe kursy doskonalące dla kwalifikowanych pracowników ochrony fizycznej – co 5 lat, w wymiarze 40 godzin.

W opinii przedstawicieli sektora system kursów narzucany przez ustawę o ochronie osób i mienia nie spełnia swojej roli i powinien zostać zmieniony. Brakuje standaryzacji w zakresie programów szkoleniowych, sposobów walidacji kompetencji. Ponadto odpowiednimi wymaganiami powinny zostać objęte placówki kształcenia. Co więcej, przedstawiciele sektora stwierdzili, że niektóre kursy nie dostarczają realnych umiejętności, a ich uczestnicy traktują je jedynie jako formalność, której celem jest zdobycie odpowiedniego zaświadczenia. Przykładem są kursy organizowane przez placówki kształcenia ustawicznego działające w strukturach agencji ochrony – trudno, zdaniem autora, w takim przypadku o rzetelne prowadzenie kształcenia i walidację kompetencji. Ze względu na rosnące koszty pracy przedsiębiorstwa coraz rzadziej inwestują w rozwój pracowników, co prowadzi do obniżenia jakości usług ochroniarskich.

Wyniki badania ankietowego pokazują, że branża potrzebuje szkoleń, które będą bardziej praktyczne i dostosowane do współczesnych zagrożeń oraz będą obejmować zarówno technologie, jak i aspekty prawne oraz zarządzanie bezpieczeństwem. Bez zmian systemowych i właściwego nacisku na kontrolę jakości kursów i instytucji szkoleniowych sektor może mieć coraz większy problem z wykwalifikowaną kadrą, co wpłynie na jakość i skuteczność świadczonych usług ochrony.

Trendy wpływające na sektor

Sektor ochrony i bezpieczeństwa mienia i osób stoi przed wieloma wyzwaniami wynikającymi z dynamicznie zmieniającego się otoczenia społeczno-politycznego, technologicznego i gospodarczego. Należą do nich m.in.:

– odpływ ukraińskich pracowników ochrony oraz zwiększone zapotrzebowanie na ochronę obiektów strategicznych związane z pełnoskalową inwazją Rosji na Ukrainę,

- wzmocnienie systemów zarządzania bezpieczeństwem i podnoszenie kompetencji pracowników sektora wynikające z wojny hybrydowej obejmującej cyberataki, sabotaże IK oraz działania dezinformacyjne,
- zmiana modeli pracy po pandemii COVID-19 – powrót do pracy stacjonarnej i hybrydowej, co przekłada się na wzrost zapotrzebowania na ochronę obiektów biurowych i handlowych,
- zmiany klimatyczne wymuszające dostosowanie procedur i technologii ochrony do ekstremalnych warunków pogodowych i klęsk żywiołowych,
- postęp technologiczny wpływający na transformację branży przez automatyzację, wykorzystanie sztucznej inteligencji, systemów bezzałogowych i nowoczesnych narzędzi nadzoru, co zmienia wymagania względem pracowników ochrony,
- wdrażanie dyrektywy CER[27] wymuszającej podniesienie standardów ochrony IK, co prowadzi do konieczności certyfikacji usług, osób i rozwiązań organizacyjno-technicznych,
- rosnące koszty działalności, w tym wzrost płacy minimalnej. To sprawia, że agencje ochrony ograniczają liczbę pracowników ochrony fizycznej i kierunkują działalność na realizację systemów zabezpieczeń technicznych,
- ograniczanie ochrony fizycznej w niektórych sektorach z uwagi na wysoki poziom bezpieczeństwa w Polsce (jeden z najwyższych w Europie), wzrost przestępczości w sklepach wskazuje jednak na potrzebę ponownego przemyślenia strategii zabezpieczeń,
- zrównoważony rozwój i zielona transformacja, które wymuszają na branży dostosowanie się do norm ESG (ang. Environmental, Social and Corporate Governance), co obejmuje optymalizację zużycia energii, ekologiczne podejście do sprzętu i raportowanie działań środowiskowych.

Wszystkie te czynniki będą kształtowały sektor ochrony w najbliższych latach. Wymagają one ponadto elastyczności i innowacyjnego podejścia do zarządzania bezpieczeństwem.

[27] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE* (Dz. Urz. UE L 333/164 z 27 XII 2022 r.).

Potrzeby kompetencyjne

Wyniki analizy danych zastanych, trendów oraz badań jakościowych i ilościowych pozwoliły zidentyfikować główne obszary kompetencyjne niezbędne do zapewnienia wysokiej jakości usług w sektorze ochrony i bezpieczeństwa. Obejmują one wiedzę i umiejętności w zakresie:

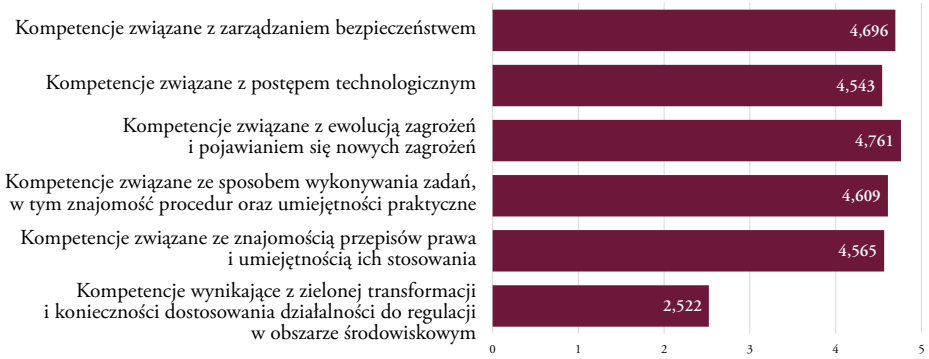
1. Zarządzania bezpieczeństwem.
   Efektywne zarządzanie bezpieczeństwem wymaga umiejętności planowania, analizy zagrożeń, oceny ryzyka oraz integracji ochrony fizycznej z systemami zabezpieczeń technicznych i aspektami cyberbezpieczeństwa. Niezbędne są znajomość nowoczesnych metod zarządzania bezpieczeństwem, skutecznej komunikacji w sytuacjach kryzysowych oraz zdolności do zarządzania dynamicznymi i nieprzewidywalnymi zagrożeniami.
2. Postępu technologicznego.
   Wzrost roli technologii w sektorze wymaga kompetencji w zakresie obsługi i wdrażania zaawansowanych systemów zabezpieczeń, w tym rozwiązań opartych na sztucznej inteligencji, automatyzacji, z uwzględnieniem nowoczesnych narzędzi nadzoru. Istotnym elementem są również rozwijające się systemy bezzałogowe i antydronowe. Ważne jest, aby zarówno specjaliści techniczni, jak i pracownicy ochrony fizycznej potrafili efektywnie wykorzystywać nowoczesne rozwiązania.
3. Ewolucji obecnych zagrożeń i pojawienia się nowych.
   Zmieniająca się sytuacja geopolityczna, rozwój wojny hybrydowej, zagrożenia terrorystyczne oraz ekstremalne zjawiska pogodowe powodują konieczność stałej aktualizacji wiedzy na temat potencjalnych zagrożeń. Pracownicy sektora powinni umieć identyfikować i analizować nowe zagrożenia oraz wdrażać skuteczne strategie prewencyjne i reagowania.
4. Sposobów wykonywania zadań z zakresu ochrony fizycznej, w tym znajomości procedur oraz umiejętności praktycznych.
   Pracownicy ochrony fizycznej muszą umieć: stosować techniki samoobrony, posługiwać się bronią, współdziałać w zespołach, rozpoznawać i neutralizować zagrożenia. Istotne jest również dostosowanie procedur operacyjnych do zmieniających się zagrożeń oraz zapewnienie odpowiedniego poziomu szkolenia dla osób o zróżnicowanym doświadczeniu zawodowym.

5. Znajomości przepisów prawa i umiejętności ich stosowania.
   Zmiany legislacyjne wymagają od pracowników sektora aktualizacji wiedzy dotyczącej regulacji prawnych. Znajomość przepisów jest niezbędna do prawidłowego wykonywania obowiązków, zwłaszcza w zakresie interwencji, ochrony IK oraz stosowania procedur bezpieczeństwa zgodnie z obowiązującymi standardami lub normami.
6. Zielonej transformacji i konieczności dostosowania działalności do regulacji w obszarze środowiskowym.
   Zrównoważony rozwój i regulacje ESG wymuszają na przedsiębiorstwach sektora wdrażanie proekologicznych rozwiązań, takich jak optymalizacja zużycia energii, redukcja śladu węglowego oraz odpowiedzialne zarządzanie zasobami. Pracownicy sektora powinni mieć wiedzę o przepisach środowiskowych oraz umiejętność ich wdrażania w codziennej działalności.

Kluczowym wymogiem w sektorze staje się interdyscyplinarność, co oznacza, że pracownicy muszą łączyć wiedzę z zakresu zarządzania, prawa, technologii, cyberbezpieczeństwa i innych obszarów. Równie ważne jest zwiększanie kompetencji osób odpowiedzialnych za zamawianie usług ochrony, ponieważ umiejętność formułowania wymagań i specyfikacji zamówień ma ogromny wpływ na jakość usług w branży. Jeden z uczestników badania jakościowego stwierdził, że (...) *bezpieczeństwo stało się mocno interdyscyplinarne. Zaciera się granica, jak daleko powinni się posunąć eksperci bezpieczeństwa w różnych dyscyplinkach nauki*[28].

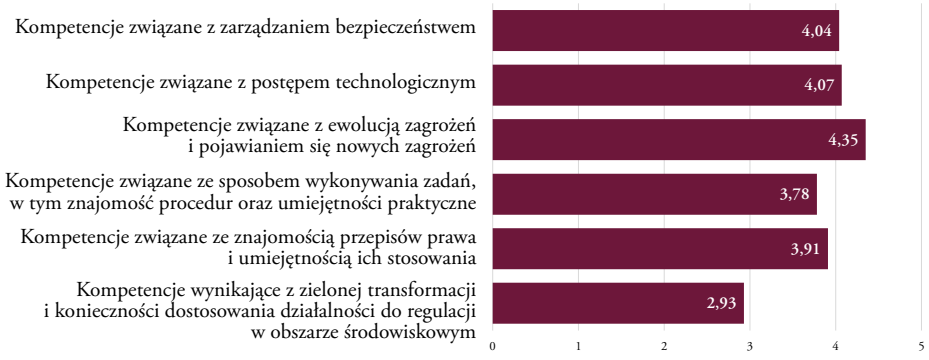
Respondenci, którzy wzięli udział w badaniu ankietowym, zostali poproszeni o dokonanie oceny w skali od 1 (mało istotny) do 5 (kluczowy) każdego z obszarów kompetencji. Ocena istotności jest średnią arytmetyczną z udzielonych odpowiedzi. Najbardziej istotnym obszarem kompetencyjnym, według uczestników badania, są wiedza i umiejętności związane z ewolucją obecnych zagrożeń i pojawianiem się nowych. Wysokie oceny dotyczące istotności uzyskały też takie obszary, jak: zarządzanie bezpieczeństwem czy sposób wykonywania zadań, w tym znajomość procedur oraz umiejętności praktyczne. Najmniej istotne w opinii respondentów są kompetencje związane z zieloną transformacją, co może wynikać z niskiej świadomości wpływu regulacji ESG na sektor (wykres 3).

[28] A. Araminowicz, P. Klatta, T. Radochoński, M. Sierżyńska, *Ochrona i Bezpieczeństwo Mienia i Osób – analiza sektora. Raport z badania*, Kraków 2024..., s. 132.



Wykres 3. Ocena istotności kompetencji.

W kolejnym pytaniu respondenci mieli dokonać oceny stopnia niedoboru kompetencji w skali od 1 (nie brakuje) do 5 (bardzo brakuje). Ocena stopnia jest średnią arytmetyczną z udzielonych odpowiedzi. Największy niedobór dotyczy według nich kompetencji związanych z ewolucją zagrożeń i pojawianiem się nowych zagrożeń, związanych z postępem technologicznym oraz związanych z zarządzaniem bezpieczeństwem (wykres 4).



Wykres 4. Ocena stopnia niedoboru kompetencji.

Przeprowadzone badania potwierdzają, że rozwój kompetencji w sektorze ochrony i bezpieczeństwa mienia i osób jest niezbędny, zwłaszcza w kontekście dynamicznych zmian technologicznych, ewolucji zagrożeń oraz nowych regulacji prawnych. Szczególnie ważne obszary wymagające wsparcia szkoleniowego to kompetencje związane z ewolucją zagrożeń

i pojawianiem się nowych zagrożeń, z postępem technologicznym, a także z zarządzaniem bezpieczeństwem. Braki kompetencyjne w tych obszarach stanowią duże wyzwanie, wpływają na efektywność i skuteczność systemów ochrony.

Badania wskazują ponadto, że największe niedobory dotyczą umiejętności analizowania nowych zagrożeń i przeciwdziałania im, w tym cyberatakom i dezinformacji. Duże znaczenie ma również podnoszenie kwalifikacji w zakresie integracji ochrony fizycznej z zabezpieczeniami technicznymi oraz obsługi nowoczesnych systemów bezpieczeństwa.

Ważnym kierunkiem rozwoju są także kompetencje związane ze znajomością przepisów prawa i umiejętnością ich stosowania, które pozwalają na podejmowanie w sytuacjach kryzysowych skutecznych i zgodnych z prawem działań. W obliczu rosnących wymagań regulacyjnych, zwłaszcza wynikających z implementacji dyrektywy CER, szkolenia powinny obejmować również procedury dotyczące ochrony IK.

Ważne będzie ponadto wprowadzenie szkoleń dotyczących zielonej transformacji, obejmujących dostosowanie działalności do regulacji środowiskowych i raportowania ESG, pomimo że respondenci ocenili ten temat jako najmniej istotny. Ponadto w sektorze ochrony często współpracują ze sobą osoby o bardzo zróżnicowanych kompetencjach, co wskazuje na konieczność ujednolicania standardów i doskonalenia umiejętności praktycznych w zakresie ochrony fizycznej, takich jak: posługiwanie się bronią, stosowanie technik interwencji czy współpracy zespołowej.

Rekomenduje się także zwiększenie świadomości osób odpowiedzialnych za zamawianie usług ochrony oraz ich szkolenie w zakresie formułowania wymagań dotyczących jakości usług bezpieczeństwa. Skuteczne programy szkoleniowe powinny być dostosowane do specyfiki sektora i uwzględniać interdyscyplinarność kompetencji przez łączenie wiedzy z obszarów zarządzania, technologii, prawa i ochrony fizycznej.

Ocena potrzeb szkoleniowych została przedstawiona na wykresie 5. Respondenci mogli wskazać maksymalnie trzy obszary. Najczęściej wskazywane były kompetencje związane z zarządzaniem bezpieczeństwem (34 wskazania), kompetencje związane z ewolucją zagrożeń i pojawianiem się nowych zagrożeń (33 wskazania) oraz kompetencje związane z postępem technologicznym (28 wskazań).

Wykres 5. Ocena potrzeb szkoleniowych.

Aby skutecznie uzupełnić luki kompetencyjne, konieczne są szczegółowe opracowanie i standaryzacja wymagań dotyczących poszczególnych obszarów kompetencyjnych. Warto rozważyć wdrożenie sektorowej ramy kwalifikacji, czym mogłaby zająć się sektorowa rada ds. kompetencji, oraz rozwój programów szkoleniowych, które pozwolą na podniesienie kwalifikacji pracowników i dostosowanie sektora do nowych wyzwań.

Dalsze analizy powinny uwzględniać zarówno krajowe, jak i zagraniczne rozwiązania w zakresie kształtowania kompetencji w sektorze ochrony i bezpieczeństwa, co umożliwi wypracowanie skutecznych narzędzi wspierających rozwój branży.

Podsumowanie

Sektor ochrony i bezpieczeństwa mienia i osób stoi przed koniecznością dostosowania się do dynamicznych zmian, kompleksowo opisanych w raporcie. Wymaga to nie tylko wdrażania nowych rozwiązań organizacyjnych, lecz także systemowego podejścia do współpracy, edukacji i uregulowań prawnych. Wyzwaniem jest zacieśnienie współpracy pomiędzy organizacjami branżowymi (krajowymi i międzynarodowymi), przedsiębiorcami, instytucjami edukacyjnymi i administracją publiczną. Z uwagi na trudną historię branży i negatywny wpływ wywierany na nią przez niektóre organizacje branżowe ten element jest szczególnie istotny z perspektywy działań rady ds. kompetencji. Uwzględnienie różnych perspektyw w procesie tworzenia standardów i regulacji może przyczynić się do skuteczniejszego

reagowania na pojawiające się zagrożenia oraz poprawy jakości świadczonych usług. W tym kontekście ważne jest wykorzystanie doświadczeń zagranicznych organizacji branżowych oraz aktywny udział w kształtowaniu europejskich standardów kompetencyjnych w sektorze ochrony.

Zmiany legislacyjne i organizacyjne odgrywają ważną rolę w kształtowaniu przyszłości sektora. Wiele obowiązujących regulacji prawnych nie przystaje do współczesnych realiów, np. niespójność wymagań kompetencyjnych dla kwalifikowanych pracowników zabezpieczenia technicznego, co powoduje trudności w interpretacji przepisów oraz ich praktycznym zastosowaniu. Istotne są więc uspójnienie i aktualizacja przepisów, aby odpowiadały one rzeczywistym wymaganiom rynku. Wprowadzenie przejrzystych regulacji dotyczących uprawnień zawodowych w sektorze ochrony pozwoliłoby zarówno na podniesienie jakości świadczonych usług, jak i na ułatwienie dostępu do zawodu kompetentnym osobom. Dobrym kierunkiem jest gruntowna nowelizacja ustawy o ochronie osób i mienia, z udziałem rady ds. kompetencji. W najbliższych latach ważny będzie wpływ znowelizowanej ustawy o zarządzaniu kryzysowym, która wdraża dyrektywę CER. Należy oczekiwać konkretnych wymagań względem operatorów IK – standaryzacja obejmie kompetencje nie tylko pracowników operatorów, lecz także zewnętrznych usługodawców i rozwiązania organizacyjno-techniczne, jakie operatorzy będą zobowiązani stosować. W długiej perspektywie konieczne będzie ujednolicenie wymagań w całym sektorze, ze szczególnym uwzględnieniem kompetencji i kwalifikacji pracowników sektora.

Jednym z istotnych wyzwań jest również poprawa wizerunku pracowników sektora. Obecnie praca w ochronie często kojarzona jest z niskimi wymaganiami i niewielkimi możliwościami rozwoju, co zmniejsza dopływ wykwalifikowanych kadr. Budowanie pozytywnego wizerunku sektora jako obszaru oferującego stabilne zatrudnienie, rozwój zawodowy oraz możliwość wykonywania społecznie istotnych zadań jest konieczne dla przyciągnięcia nowych pracowników i zwiększenia prestiżu zawodu[29].

Nieodłącznym elementem profesjonalizacji branży powinno być również zapewnienie wysokiej jakości szkoleń oraz poświęcenie w edukacji większej uwagi części praktycznej. Obecne systemy kształcenia i obowiązkowe kursy doszkalające nie zawsze spełniają swoją funkcję, a wiele firm

[29] Warto wspomnieć, że POLALARM od wielu lat zabiega o to, aby zawód pracownika zabezpieczenia technicznego miał status zawodu zaufania publicznego. Dzięki partnerstwu w sektorowej radzie ds. kompetencji realizacja takich pomysłów stanie się możliwa.

z powodów finansowych i formalnych ogranicza wydatki na rozwój pracowników.

Wprowadzenie bardziej efektywnych mechanizmów kontroli jakości szkoleń oraz instytucji szkoleniowych, a także ściślejsza współpraca między uczelniami a pracodawcami mogłyby znacznie poprawić przygotowanie kandydatów do pracy w sektorze. Kluczowe jest dostosowanie oferty edukacyjnej do nowoczesnych technologii i zmieniających się zagrożeń.

Ważny jest Zintegrowany System Kwalifikacji (ZSK), którego znaczenie wzrośnie w najbliższych latach. Mimo że w sektorze jest wiele uregulowanych kwalifikacji, to żadna z nich nie została dotąd włączona do ZSK. Takie działanie zwiększyłoby przejrzystość wymagań zawodowych i ułatwiłoby ich porównywanie. Konieczny jest przegląd istniejących kwalifikacji oraz dostosowanie ich do współczesnych potrzeb sektora.

Odpowiedzią na te wyzwania powinno być również dalsze badanie kompetencji wymaganych w sektorze oraz identyfikacja narzędzi wspierających rozwój zawodowy pracowników. Stworzenie sektorowej ramy kwalifikacji oraz doprecyzowanie standardów kompetencyjnych poszczególnych ról zawodowych pozwoliłoby na lepsze zarządzanie ścieżkami kariery w branży. Ponadto analiza dotychczasowych rozwiązań stosowanych w innych sektorach oraz krajach mogłaby dostarczyć cennych wskazówek dotyczących skutecznych metod kształcenia i walidacji umiejętności.

Sektorowa rada ds. kompetencji w sektorze ochrony i bezpieczeństwa mienia i osób stanowi narzędzie umożliwiające skuteczne reagowanie na wyzwania opisane w raporcie. Rada będzie działać na rzecz profesjonalizacji sektora przez integrację środowiska ekspertów, przedsiębiorców, przedstawicieli administracji publicznej oraz edukacji. Jej nadrzędnym celem będzie dostosowanie kwalifikacji i kompetencji pracowników sektora do dynamicznie zmieniających się realiów. Rada skupi grono wybitnych ekspertów z wiedzą fachową i doświadczeniem, których zadaniem będzie wypracowywanie rozwiązań systemowych podnoszących jakość usług ochrony i bezpieczeństwa. Przez współpracę z instytucjami publicznymi oraz organizacjami branżowymi będzie nie tylko monitorować potrzeby rynku, lecz także inicjować działania legislacyjne, certyfikacyjne oraz edukacyjne. Sektorowe rady ds. kompetencji, działające w innych obszarach gospodarki, skutecznie przyczyniały się do uspójnienia standardów kompetencyjnych i kwalifikacyjnych. Ten sam efekt zamierzamy osiągnąć w sektorze ochrony.

Adam Tatarowski

Przewodniczący Rady ds. Kompetencji w Sektorze Ochrony i Bezpieczeństwa Mienia i Osób przy Polskiej Agencji Rozwoju Przedsiębiorczości. Ekspert Rządowego Centrum Bezpieczeństwa w zakresie standaryzacji i oceny zgodności rozwiązań organizacyjno-technicznych stosowanych w zapewnianiu bezpieczeństwa infrastruktury krytycznej. Prezes Zakładu Rozwoju Technicznego Ochrony Mienia TECHOM – wyspecjalizowanej jednostki certyfikującej i placówki kształcenia ustawicznego działającej w systemie oświaty. Prezes Ogólnopolskiego Stowarzyszenia Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem „POLALARM". Członek Rady Normalizacyjnej przy Polskim Komitecie Normalizacyjnym.

Kontakt: tatarowski@techom.com

Terroryzm – studia, analizy, prewencja, 2025, nr 7: 255–279

https://doi.org/10.4467/27204383TER.25.033.21810

Varia

Umiejscowienie Jednostki Wojskowej GROM w systemie bezpieczeństwa państwa

Łukasz Niemczyk
Autor niezależny
https://orcid.org/0009-0009-5759-7841

Celem niniejszego opracowania jest zasygnalizowanie trudności w skutecznym użyciu jednostek Wojsk Specjalnych (WS) na terenie Polski oraz poza jej granicami do wsparcia podmiotów układu pozamilitarnego (jednostek organizacyjnych podporządkowanych ministrowi właściwemu do spraw wewnętrznych oraz nadzorowanych przez Ministra Koordynatora Służb Specjalnych lub też Ministra Spraw Zagranicznych) w dynamicznie zmieniającym się środowisku bezpieczeństwa państwa, w związku z zagrożeniami zarówno zewnętrznymi, jak i wewnętrznymi.

Termin ustawowy Siły Zbrojne Rzeczypospolitej Polskiej (SZ RP) zaczął funkcjonować w ustawodawstwie powszechnym od 9 grudnia 1991 r., tj. od wejścia w życie ustawy o zmianie ustawy o powszechnym obowiązku obrony Polskiej Rzeczypospolitej Ludowej oraz niektórych innych ustaw[1]. W nowelizacji użyte w różnych przypadkach wyrażenie „Polska Rzeczpospolita Ludowa" zastąpiono użytym w odpowiednich przypadkach wyrażeniem

[1] *Ustawa z dnia 25 października 1991 r. o zmianie ustawy o powszechnym obowiązku obrony Polskiej Rzeczypospolitej Ludowej oraz niektórych innych ustaw* (DzU z 1991 r. nr 113 poz. 491).

„Rzeczpospolita Polska" (RP), co ma szczególne znaczenie w zmianie treści art. 3 ust. 1 nowelizowanej ustawy o powszechnym obowiązku obrony Polskiej Rzeczypospolitej Ludowej (Rzeczypospolitej Polskiej)[2], zgodnie z którym na straży suwerenności i niepodległości Narodu Polskiego oraz jego bezpieczeństwa i pokoju stoją Siły Zbrojne Polskiej Rzeczypospolitej Ludowej (Rzeczypospolitej Polskiej). Można zatem wskazać, że SZ RP istnieją od 1991 r. Jednostka Wojskowa GROM (JW GROM) powstała na mocy zarządzenia organizacyjnego nr 004 z 13 sierpnia 1990 r. Ministra Spraw Wewnętrznych z datą jej ostatecznego sformowania do 31 marca 1991 r. Funkcjonowała w resorcie spraw wewnętrznych na zaopatrzeniu materiałowo-technicznym oraz finansowym dowódcy Nadwiślańskich Jednostek Ministerstwa Spraw Wewnętrznych. Co ciekawe, ówczesny szef JW GROM – zgodnie z § 3 ust. 1 wskazanego zarządzenia – był członkiem Międzyresortowego Zespołu Antyterrorystycznego.

Wojska Specjalne jako rodzaj SZ RP to stosunkowo młoda formacja. Wprowadzono je do porządku prawnego wraz z Dowództwem Wojsk Specjalnych oraz Dowódcą Wojsk Specjalnych[3] 4 lipca 2007 r. na mocy art. 1 pkt 1 ustawy o zmianie ustawy o powszechnym obowiązku obrony RP oraz o zmianie niektórych innych ustaw[4]. Minister Obrony Narodowej – przez wykonanie delegacji ustawowej określonej w art. 13a ust. 6 ustawy o powszechnym obowiązku obrony RP[5] – określił wymagania dotyczące WS zarządzeniem nr Z-8/MON Ministra Obrony Narodowej z 15 lutego 2008 r.[6] Z uwagi na charakter niniejszego opracowania zostaną podane tylko dokumenty oraz dane stanowiące informacje powszechnie dostępne i jawne.

Wojska Specjalne, mimo że składają się na nie wysoce specjalistyczne formacje, zwłaszcza JW GROM oraz JW Komandosów i JW Formoza,

---

[2] *Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Polskiej Rzeczypospolitej Ludowej* (DzU z 1988 r. nr 30 poz. 207, ze zm.).

[3] Artykuł 1 pkt 2 *Ustawy z dnia 24 maja 2007 r. o zmianie ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej oraz o zmianie niektórych innych ustaw*, który wprowadził omawiane regulacje w nowym art. 13a ust. 4 i 5 *Ustawy z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej*.

[4] *Ustawa z dnia 24 maja 2007 r. o zmianie ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej oraz o zmianie niektórych innych ustaw* (DzU z 2007 r. nr 107 poz. 732).

[5] *Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej* (DzU z 2004 r. nr 241 poz. 2416, ze zm.).

[6] *Zarządzenie Nr Z-8/MON Ministra Obrony Narodowej z dnia 15 lutego 2008 r. w sprawie szczegółowego zakresu działania, struktury organizacyjnej oraz siedziby Dowództwa Wojsk Specjalnych* (Dz. Urz. Min. Obr. Nar. z 2008 r. nr 7 poz. 71).

zostały podporządkowane jednakowym uregulowaniom systemowym tożsamym dla jednostek wojsk konwencjonalnych. W ciągu kilku lat WS zyskały, a potem utraciły samodzielność. Wraz z wprowadzeniem WS jako nowego rodzaju SZ RP powstało bowiem Dowództwo Wojsk Specjalnych na mocy wymienionej ustawy z 24 maja 2007 r. Następnie reforma systemu kierowania i dowodzenia dokonana m.in. na podstawie ustawy o zmianie ustawy o urzędzie Ministra Obrony Narodowej oraz niektórych innych ustaw[7] zniosła 1 stycznia 2014 r. dowództwa rodzajów wojsk (w tym Dowództwo Wojsk Specjalnych). Pozostawiła jedynie Dowództwo Operacyjne Rodzajów Sił Zbrojnych i powołała Dowództwo Generalne Rodzajów Sił Zbrojnych. Zatem mimo istnienia de facto odrębnego rodzaju wojsk, jakim są WS, przestały one samodzielnie funkcjonować i zaczęły działać w ramach ogólnowojskowych regulacji, co jest powoli odwracane.

Podstawy prawne użycia Jednostki Wojskowej GROM na terenie kraju

W Konstytucji RP[8] są dwa kluczowe przepisy odnoszące się do użycia SZ RP na terenie kraju – art. 26 ust. 1 oraz art. 5. Pierwszy z nich określa zadania SZ RP i stanowi, że służą one ochronie niepodległości państwa i niepodzielności jego terytorium oraz zapewnieniu bezpieczeństwa i nienaruszalności jego granic. Drugi ze wskazanych przepisów jest uzupełnieniem pierwszego i wskazuje, że RP m.in. zapewnia bezpieczeństwo obywateli (chroni ich przed zagrożeniami zewnętrznymi i wewnętrznymi). Ustawową realizacją uregulowań konstytucyjnych jest przepis art. 11 ust. 3 ustawy z o obronie Ojczyzny[9], zgodnie z którym SZ RP mogą brać udział w zwalczaniu klęsk żywiołowych i likwidacji ich skutków, działaniach antyterrorystycznych, działaniach z zakresu ochrony mienia, akcjach poszukiwawczych, akcjach ratowania lub ochrony zdrowia i życia ludzkiego, ochronie i obronie cyberprzestrzeni, oczyszczaniu terenów z materiałów wybuchowych i niebezpiecznych pochodzenia wojskowego oraz ich unieszkodliwianiu, a także w realizacji zadań z zakresu zarządzania kryzysowego. Ustawodawca rozwinął

[7] *Ustawa z dnia 21 czerwca 2013 r. o zmianie ustawy o urzędzie Ministra Obrony Narodowej oraz niektórych innych ustaw* (DzU z 2013 r. poz. 852).

[8] *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.* (t.j. DzU z 1997 r. nr 78 poz. 483, ze zm.).

[9] *Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny* (t.j. DzU z 2024 r. poz. 248, ze zm.).

te działania o operację wojskową prowadzoną na terytorium RP w czasie pokoju, wprowadzoną na mocy art. 8 pkt 1 ustawy o zmianie niektórych ustaw w celu usprawnienia działań SZ RP, Policji oraz Straży Granicznej na wypadek zagrożenia bezpieczeństwa państwa[10]. Regulacja ta weszła w życie 31 sierpnia 2024 r. Operacja taka polega na:

a) zorganizowanym działaniu SZ RP prowadzonym w celu zapewnienia bezpieczeństwa zewnętrznego państwa, niebędącym szkoleniem lub ćwiczeniem,
b) działaniu wojsk obcych w ramach wzmocnienia wojskowego SZ RP lub wojsk państw-stron Traktatu Północnoatlantyckiego, o którym mowa w art. 3a ust. 1 ustawy o zasadach pobytu wojsk obcych na terytorium RP[11], zasadach ich przemieszczania się przez to terytorium oraz zasadach udzielania pomocy wojskom sojuszniczym i organizacjom międzynarodowym.

To działanie jest podejmowane, jeżeli okoliczności wymagają natychmiastowego działania, w szczególności w sytuacjach zagrożenia granicy państwa, obiektów infrastruktury krytycznej, bezpieczeństwa ludzi lub mienia w znacznych rozmiarach, w przypadku gdy siły i środki służb podległych ministrowi właściwemu do spraw wewnętrznych lub przez niego nadzorowanych mogą okazać się nieadekwatne ze względu na charakter zagrożenia.

Można zadać pytanie, czy ten rodzaj działań jest powiązany z reagowaniem SZ RP na zagrożenia o charakterze terrorystycznym, skoro ustawodawca nie odsyła tutaj w żadnym zakresie do działań antyterrorystycznych lub kontrterrorystycznych lub infrastruktury krytycznej definiowanych w art. 2 pkt 1, 2 i 4 ustawy o działaniach antyterrorystycznych (dalej: ustawa o działaniach AT)[12]. Ten rodzaj działań dotyczy jednak wsparcia lub wręcz zastąpienia służb odpowiedzialnych za przygotowanie do przejmowania kontroli nad zdarzeniami o charakterze terrorystycznym w drodze zaplanowanych przedsięwzięć, reagowanie w przypadku wystąpienia takich

[10] *Ustawa z dnia 26 lipca 2024 r. o zmianie niektórych ustaw w celu usprawnienia działań Sił Zbrojnych Rzeczpospolitej Polskiej, Policji oraz Straży Granicznej na wypadek zagrożenia bezpieczeństwa państwa* (DzU z 2024 r. poz. 1248).

[11] *Ustawa z dnia 23 września 1999 r. o zasadach pobytu wojsk obcych na terytorium Rzeczypospolitej Polskiej, zasadach ich przemieszczania się przez to terytorium oraz zasadach udzielania pomocy wojskom sojuszniczym i organizacjom międzynarodowym* (t.j. DzU z 2024 r. poz. 1770).

[12] *Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych* (t.j. DzU z 2024 r. poz. 92, ze zm.).

zdarzeń oraz odtwarzanie zasobów przeznaczonych do reagowania na te zdarzenia (art. 3 ust. 2).

Przy próbie odpowiedzi na postawione pytanie należy przywołać zasadnicze regulacje dotyczące zadań WS. Po pierwsze, w 2013 r. zostało wydane (na podstawie art. 12 ust. 1 pkt 1 i ust. 2 ustawy o finansach publicznych[13]) zarządzenie nr 30/MON z 4 listopada 2013 r.[14], w którym jawnie wskazano jednostki wojskowe wchodzące w skład WS oraz ich zadania. Zgodnie z treścią § 8 załącznika nr 2 do wymienionego zarządzenia podstawowym zadaniem JW GROM jest realizacja pełnego spektrum operacji specjalnych i fizycznego zwalczania terroryzmu w układzie narodowym, sojuszniczym i koalicyjnym w środowisku lądowym i morskim, najwyższego ryzyka i znaczenia strategicznego, w tym operacji uwalniania zakładników oraz prowadzenia operacji antyterrorystycznych w czasie pokoju, kryzysu i wojny. Po drugie, należy podkreślić, że nie ma jasnego i spójnego wewnętrznie systemu użycia SZ RP, w tym JW GROM, na terenie kraju w sytuacjach zagrożenia terroryzmem. Mimo że zagrożenie jest jedno, ustawodawca wprowadził aż sześć rozwiązań zawartych w tyluż ustawach, zawierających różne tryby subsydiarnego użycia SZ RP, na wniosek różnych podmiotów, z różną regulacją w zakresie użycia broni, uzbrojenia i środków przymusu bezpośredniego oraz różnymi formami kierowania tymi działaniami.

Ustawa z dnia 6 kwietnia 1990 r. o Policji

Oddziały i pododdziały SZ RP mogą być użyte do pomocy oddziałom i pododdziałom Policji, jeżeli użycie oddziałów lub pododdziałów Policji okaże się lub może okazać się niewystarczające w razie zagrożenia bezpieczeństwa publicznego lub zakłócenia porządku publicznego, zwłaszcza przez sprowadzenie:

1) niebezpieczeństwa powszechnego dla życia, zdrowia lub wolności obywateli,
2) bezpośredniego zagrożenia dla mienia w znacznych rozmiarach,
3) bezpośredniego zagrożenia obiektów lub urządzeń ważnych dla bezpieczeństwa lub obronności państwa, siedzib centralnych

[13] *Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych* (DzU z 2013 r. poz. 885 i 938).

[14] *Zarządzenie Nr 30/MON z dnia 4 listopada 2013 r. w sprawie nadania statutów Jednostkom Wojsk Specjalnych* (Dz. Urz. Min. Obr. Nar. z 2013 r. poz. 292).

organów państwowych albo wymiaru sprawiedliwości, obiektów gospodarki lub kultury narodowej oraz przedstawicielstw dyplomatycznych i urzędów konsularnych państw obcych albo organizacji międzynarodowych, a także obiektów dozorowanych przez uzbrojoną formację ochronną utworzoną na podstawie odrębnych przepisów,

4) **zagrożenia przestępstwem o charakterze terrorystycznym mogącym skutkować niebezpieczeństwem dla życia lub zdrowia uczestników wydarzeń o charakterze kulturalnym, sportowym lub religijnym, w tym zgromadzeń lub imprez masowych**[15].

Ustawa z dnia 12 października 1990 r. o Straży Granicznej

Oddziały i pododdziały SZ RP mogą być użyte do pomocy Straży Granicznej (SG), jeżeli użycie sił SG okaże się niewystarczające lub uzasadnia to stopień zagrożenia. Można ich użyć w przypadku zagrożenia bezpieczeństwa publicznego lub zakłócenia porządku publicznego w zasięgu terytorialnym przejścia granicznego oraz w strefie nadgranicznej, w szczególności:

1) bezpośredniego zagrożenia zamachem na nienaruszalność granicy państwowej lub jego dokonania,
2) sprowadzenia bezpośredniego niebezpieczeństwa powszechnego dla życia, zdrowia lub wolności obywateli,
3) bezpośredniego zagrożenia zamachem na obiekty lub urządzenia wykorzystywane przez SG,
4) **zagrożenia przestępstwem o charakterze terrorystycznym lub jego dokonania w stosunku do obiektów lub urządzeń, o których mowa w pkt 3, lub mogącym skutkować niebezpieczeństwem dla życia ludzkiego**[16].

Dodatkowo przepis art. 11c ust. 1 ustawy o SG przewiduje użycie oddziałów i pododdziałów SZ RP w formie prowadzonego samodzielnie przeciwdziałania, gdy wymagają tego względy bezpieczeństwa państwa, zapewnienia nienaruszalności granicy państwowej lub zagrożenia bezpieczeństwa publicznego w zasięgu terytorialnym przejścia granicznego oraz w strefie

[15] Artykuł 18 *Ustawy z dnia 6 kwietnia 1990 r. o Policji* (t.j. DzU z 2024 r. poz. 145, ze zm.). Wyróżnienia w tekście pochodzą od autora (dop. red.).

[16] Artykuł 11b *Ustawy z dnia 12 października 1990 r. o Straży Granicznej* (t.j. DzU z 2024 r. poz. 915, ze zm.).

nadgranicznej lub na polskich obszarach morskich, jeżeli SG nie dysponuje możliwością skutecznego przeciwdziałania zagrożeniu lub dokonaniu przestępstwa lub uzasadnia to rodzaj zagrożenia.

Ustawa z dnia 3 lipca 2002 r. – Prawo lotnicze

Bezzałogowy statek powietrzny może zostać zniszczony albo unieruchomiony albo nad jego lotem może zostać przejęta kontrola, w przypadku gdy:

1) przebieg operacji lub działanie bezzałogowego statku powietrznego:
   a) zagraża lub może zagrozić życiu lub zdrowiu ludzi lub zwierząt,
   b) stwarza lub może stworzyć zagrożenie dla chronionych obiektów, urządzeń lub obszarów,
   c) zakłóca lub może zakłócić przebieg imprezy masowej albo zagraża bezpieczeństwu jej uczestników,
   d) **stwarza lub może stworzyć uzasadnione podejrzenie, że może zostać użyty jako środek ataku terrorystycznego**,
   e) stwarza lub może stworzyć zagrożenie bezpieczeństwa ruchu lotniczego, statku powietrznego lub życia lub zdrowia załogi lub pasażerów znajdujących się na jego pokładzie,
   f) utrudnia lub może utrudnić ruch lotniczy lub powoduje lub może spowodować jego wstrzymanie lub ograniczenie;
2) bezzałogowy statek powietrzny wbrew zakazowi wykonuje operację w strefie geograficznej ustanowionej nad:
   a) chronionymi obiektami SZ RP oraz jednostek organizacyjnych podległych lub podporządkowanych Ministrowi Obrony Narodowej lub nadzorowanych przez Ministra Obrony Narodowej,
   b) obiektami, urządzeniami lub obszarami istotnymi dla bezpieczeństwa lub obronności państwa, bezpieczeństwa publicznego lub nienaruszalności granicy państwowej.

Do zniszczenia lub unieruchomienia bezzałogowego statku powietrznego albo przejęcia kontroli nad jego lotem są uprawnieni m.in. żołnierze Żandarmerii Wojskowej (pkt 1 i 2) i SZ RP (pkt 1 lit. a, b, d–f oraz pkt 2)[17].

[17] Artykuł 156ze *Ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze* (t.j. DzU z 2025 r. poz. 31, ze zm.).

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym

Jeżeli w sytuacji kryzysowej użycie innych sił i środków jest niemożliwe lub może okazać się niewystarczające, o ile inne przepisy nie stanowią inaczej, Minister Obrony Narodowej, na wniosek wojewody, może przekazać do jego dyspozycji pododdziały lub oddziały SZ RP wraz ze skierowaniem ich do wykonywania zadań z zakresu zarządzania kryzysowego, zgodnie z wojewódzkim planem zarządzania kryzysowego. Do zadań, o których mowa wyżej, należą:

1) współudział w monitorowaniu zagrożeń,
2) wykonywanie zadań związanych z oceną skutków zjawisk zaistniałych na obszarze występowania zagrożeń,
3) wykonywanie zadań poszukiwawczo-ratowniczych,
4) ewakuowanie poszkodowanej ludności i mienia,
5) wykonywanie zadań mających na celu przygotowanie warunków do czasowego przebywania ewakuowanej ludności w wyznaczonych miejscach,
6) współudział w ochronie mienia pozostawionego na obszarze występowania zagrożeń,
7) izolowanie obszaru występowania zagrożeń lub miejsca prowadzenia akcji ratowniczej,
8) wykonywanie prac zabezpieczających, ratowniczych i ewakuacyjnych przy zagrożonych obiektach budowlanych i zabytkach,
9) prowadzenie prac wymagających użycia specjalistycznego sprzętu technicznego lub materiałów wybuchowych będących w zasobach SZ RP,
10) usuwanie materiałów niebezpiecznych i ich unieszkodliwianie, z wykorzystaniem sił i środków będących na wyposażeniu SZ RP,
11) likwidowanie skażeń chemicznych oraz skażeń i zakażeń biologicznych,
12) usuwanie skażeń promieniotwórczych,
13) wykonywanie zadań związanych z naprawą i odbudową infrastruktury technicznej,
14) współudział w zapewnieniu przejezdności szlaków komunikacyjnych,
15) udzielanie pomocy medycznej i wykonywanie zadań sanitarno-higienicznych i przeciwepidemicznych[18].

[18] Artykuł 25 *Ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym* (t.j. DzU z 2023 r. poz. 122, ze zm.).

Zdjęcie 1. Żołnierze JW GROM w warszawskim metrze podczas ćwiczeń z zakresu taktyki działań kontrterrorystycznych.

Źródło: materiały własne JW GROM.

Ustawa z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich

W przypadku gdy siły i środki Policji oraz SG są niewystarczające lub mogą okazać się niewystarczające, Minister Obrony Narodowej, na wniosek ministra właściwego do spraw wewnętrznych, może podjąć decyzję o zastosowaniu SZ RP w celu zapobieżenia, ograniczenia lub usunięcia poważnego i bezpośredniego niebezpieczeństwa powstałego na skutek użycia statku lub obiektu pływającego jako środka ataku o charakterze terrorystycznym. Dotyczy to niebezpieczeństwa grożącego:

1) statkom, obiektom portowym i portom oraz związanej z nimi infrastrukturze,
2) międzysystemowemu Gazociągowi Bałtyckiemu (Baltic Pipe) stanowiącemu połączenie systemów przesyłowych RP i Królestwa Danii wraz z infrastrukturą niezbędną do jego obsługi na terenie obszarów morskich RP,
3) obiektom, urządzeniom i instalacjom wchodzącym w skład infrastruktury zapewniającej dostęp do portów o podstawowym znaczeniu dla gospodarki narodowej,

4) wykorzystywanym w wyłącznej strefie ekonomicznej sztucznym wyspom, wszelkiego rodzaju konstrukcjom i urządzeniom przeznaczonym do rozpoznawania lub eksploatacji zasobów, jak również innym przedsięwzięciom w zakresie gospodarczego badania i eksploatacji wyłącznej strefy ekonomicznej, w szczególności w celach energetycznych, w tym morskim farmom wiatrowym w rozumieniu art. 3 pkt 3 ustawy o promowaniu wytwarzania energii elektrycznej w morskich farmach wiatrowych[19] i zespołom urządzeń służącym do wyprowadzenia mocy w rozumieniu art. 3 pkt 13 powołanej ustawy, oraz podmorskim sieciom elektroenergetycznym i światłowodowym lub rurociągom, a także związanej z nimi infrastrukturze,
5) terminalowi regazyfikacyjnemu skroplonego gazu ziemnego w Świnoujściu.

Siły Zbrojne RP na polskich obszarach morskich mogą zastosować niezbędne środki do zatopienia tego statku lub obiektu pływającego włącznie[20].

Zdjęcie 2. Ćwiczenia taktyki działań kontrterrorystycznych w wewnętrznych akwenach portowych.

Źródło: materiały własne JW GROM.

[19] *Ustawa z dnia 17 grudnia 2020 r. o promowaniu wytwarzania energii elektrycznej w morskich farmach wiatrowych* (t.j. DzU z 2025 r. poz. 498).

[20] Artykuł 27 *Ustawy z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich* (t.j. DzU z 2024 r. poz. 597).

Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych

W przypadku wprowadzenia trzeciego lub czwartego stopnia alarmowego w trybie art. 16 ust. 1 ustawy o działaniach AT, jeżeli użycie oddziałów i pododdziałów Policji okaże się niewystarczające lub może okazać się niewystarczające, do pomocy oddziałom i pododdziałom Policji mogą być użyte oddziały i pododdziały SZ RP, stosownie do ich przygotowania specjalistycznego, posiadanego sprzętu i uzbrojenia oraz zaistniałych potrzeb[21]. Żołnierze mogą wchodzić w skład grupy kontrterrorystycznej, o której mowa w art. 23 ust. 4 ustawy o działaniach AT.

By móc w pełni odpowiedzieć na pytanie dotyczące reagowania SZ RP na zagrożenia o charakterze terrorystycznym, należy doprecyzować zadania zwalczania terroryzmu przez WS. Przepis art. 3 ustawy o działaniach AT ustanowił swoisty podział odpowiedzialności za działania antyterrorystyczne i kontrterrorystyczne. W ust. 1 jest mowa o odpowiedzialności Szefa Agencji Bezpieczeństwa Wewnętrznego (ABW), w ust. 2 zaś – ministra właściwego do spraw wewnętrznych (obecnie jest nim Minister Spraw Wewnętrznych i Administracji).

Zadania związane ze zwalczaniem terroryzmu wynikają bezpośrednio z brzmienia art. 1 ust. 2 pkt 3a ustawy o Policji, delegujących Policji prowadzenie działań kontrterrorystycznych w rozumieniu ustawy o działaniach AT.

W pewnym zakresie kwestie związane z antyterroryzmem zawierają się również w sferze działań SG, zgodnie z ustawą o SG. Wiąże się to z głównymi zadaniami tej służby w odniesieniu do kontroli ruchu granicznego, zwalczania nielegalnej migracji oraz nadzoru nad wjazdem i pobytem cudzoziemców na obszarze Polski, a także ścigania przestępczości z tym związanej (art. 1 ust. 2 pkt 1–2a, pkt 4 lit. a, c, i e, pkt 5–5b) oraz z obowiązkiem współdziałania z innymi organami i służbami w zakresie rozpoznawania zagrożeń terrorystycznych i przeciwdziałania tym zagrożeniom (art. 1 ust. 1 pkt 5d).

Jak wspomniano, w ustawie o obronie Ojczyzny w art. 11 ust. 3 wskazano zadania, w których mogą brać udział SZ RP. W związku z tym, że ta ustawa nie określa sposobu prowadzenia przez nie przedmiotowych działań antyterrorystycznych, należałoby doprecyzować ich konkretne zadania. Jest to także dobry punkt wyjścia do umożliwienia nawiązania i rozwinięcia współpracy wyselekcjonowanych jednostek wojskowych – zwłaszcza WS – z organami, do których zadań należą: zapobieganie zdarzeniom

[21] Artykuł 22 ustawy o działaniach AT.

o charakterze terrorystycznym, przygotowanie do przejmowania nad nimi kontroli w drodze zaplanowanych przedsięwzięć, reagowanie w przypadku wystąpienia takich zdarzeń oraz usuwanie ich skutków, w tym odtwarzanie zasobów przeznaczonych do reagowania na nie. Byłaby to zatem współpraca przede wszystkim z ABW. Pozwoliłoby to na przyjęcie holistycznego podejścia do bezpieczeństwa państwa w myśl zasady *whole-of-government approach* (WGA), co zwiększyłoby zdolności obu partnerów. Agencja Bezpieczeństwa Wewnętrznego zyskałaby na korzystaniu z potencjału logistycznego, wyposażenia, sił i środków będących w dyspozycji WS – chociażby w zakresie zagrożeń związanych z użyciem środków chemicznych, biologicznych, radiologicznych i nuklearnych (ang. *chemical, biological, radiological, and nuclear,* CBRN), dronów, integracji łączności, wiedzy z zakresu działań kontrterrorystycznych i przeciwdywersyjnych w aspekcie ochrony infrastruktury krytycznej, a WS uzyskałyby dostęp do informacji o zagrożeniach. Umożliwi to ABW i WS lepsze przygotowanie, zgodnie z jedną z zasad, „do wojny, która będzie, a nie, która była". Ponadto skoro – zgodnie z ustawą o działaniach AT – w skład grupy kontrterrorystycznej wchodzą m.in. funkcjonariusze ABW i żołnierze SZ RP (art. 23 ust. 4), można zadać pytanie, dlaczego ustawa ta nie pozwala współdziałać SZ RP bezpośrednio z tą służbą w zakresie działań antyterrorystycznych.

Podobna niekonsekwencja ustawodawcy jest widoczna w powierzeniu Żandarmerii Wojskowej (ŻW) w rozumieniu ustawy o działaniach AT tylko prowadzenia działań antyterrorystycznych na obszarach lub w obiektach należących do komórek i jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych albo administrowanych przez te komórki i jednostki organizacyjne (art. 4 ust. 1 pkt 3a ustawy o ŻW i wojskowych organach porządkowych)[22]. W związku z tym, że ustawa o ŻW w przepisie wskazującym sposób realizacji zadań ŻW oprócz czynności operacyjno-rozpoznawczych nie zawiera przepisu wskazującego na inny sposób prowadzenia wspomnianych działań antyterrorystycznych, należy się zastanowić, czy do zadań ŻW należą działania kontrterrorystyczne (art. 4 ust. 2). Takiego rodzaju zadań nie przewiduje także rozporządzenie Rady Ministrów z 2 lipca 2018 r.[23], mimo że art. 14 ust. 1 i 2 omawianej ustawy nie bierze pod

[22] *Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych* (t.j. DzU z 2025 r. poz. 12, ze zm.).

[23] *Rozporządzenie Rady Ministrów z dnia 2 lipca 2018 r. w sprawie współdziałania Żandarmerii Wojskowej z organami uprawnionymi do wykonywania czynności operacyjno-rozpoznawczych, prowadzenia dochodzeń w sprawach o przestępstwa, a także z organami, którym przysługują*

uwagę współdziałania tej formacji m.in. z Policją i ABW. Odpowiedź zawiera się w dwóch przepisach ustawy o działaniach AT. Pierwszy z nich, art. 18 pkt 2, powierza kierowanie działaniami antyterrorystycznymi – podejmowanymi przez właściwe służby lub organy w ramach ich ustawowych zadań na miejscu zdarzenia o charakterze terrorystycznym – żołnierzowi ŻW wyznaczonemu przez Ministra Obrony Narodowej, a w przypadkach niecierpiących zwłoki – przez Komendanta Głównego ŻW. Dotyczy to zdarzeń o charakterze terrorystycznym na obszarach lub w obiektach należących do komórek i jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych albo administrowanych przez te komórki i jednostki organizacyjne. Drugi przepis, czyli art. 23 ust. 4, określa, że specjalne użycie broni może być dokonane przez funkcjonariuszy Policji, SG, ABW, żołnierzy ŻW lub SZ RP, wchodzących w skład grupy wykonującej działania kontrterrorystyczne (dalej: grupa kontrterrorystyczna). Zasadne byłoby uzupełnienie ustawy pragmatycznej o ŻW o przepis analogiczny do zawartego w ustawie o Policji, gdzie w art. 1 ust. 2 pkt 3a ustawodawca wskazał, że do podstawowych zadań Policji należy m.in. prowadzenie działań kontrterrorystycznych w rozumieniu ustawy o działaniach AT. Ponadto warto rozważyć zapewnienie możliwości wsparcia ŻW w działaniach kontrterrorystycznych prowadzonych na terenie jej właściwości miejscowej (na obszarach lub w obiektach należących do komórek i jednostek organizacyjnych podległych ministrowi obrony narodowej lub przez niego nadzorowanych albo administrowanych przez te komórki i jednostki organizacyjne) przez Centralny Pododdział Kontrterrorystyczny Policji „BOA" bądź przez WS, czego nie przewiduje rozporządzenie Ministra Obrony Narodowej z 24 lipca 2012 r.[24]

Jest to uzasadniona propozycja, ponieważ jak wynika z treści uchwały nr 252 Rady Ministrów z 9 grudnia 2014 r.[25] dotyczącej *Narodowego Programu Antyterrorystycznego na lata 2015–2019*, który – co warto podkreślić – został przyjęty przed uchwaleniem ustawy o działaniach AT, (...) ***rodzajem***

uprawnienia oskarżyciela publicznego, oraz z organami uprawnionymi do nakładania grzywien w drodze mandatu karnego w sprawach o wykroczenia (DzU z 2018 r. poz. 1334).

[24] *Rozporządzenie Ministra Obrony Narodowej z dnia 24 lipca 2012 r. w sprawie zakresu i trybu współdziałania Żandarmerii Wojskowej ze Służbą Kontrwywiadu Wojskowego, Służbą Wywiadu Wojskowego, wojskowymi organami porządkowymi oraz z dowódcami jednostek wojskowych i dowódcami (komendantami) garnizonów* (DzU z 2012 r. poz. 880).

[25] *Uchwała Nr 252 Rady Ministrów z dnia 9 grudnia 2014 r. w sprawie „Narodowego Programu Antyterrorystycznego na lata 2015–2019"* (M.P. z 2014 r. poz. 1218).

Sił Zbrojnych szczególnie predysponowanym do wsparcia działań antyterrorystycznych są Wojska Specjalne, które dysponują możliwościami, zdolnościami, wyszkoleniem i wyposażeniem zwiększającymi potencjał ww. służb w reagowaniu na zagrożenia o charakterze terrorystycznym. Siły Zbrojne RP uczestniczą również w misjach stabilizacyjnych, pokojowych i międzynarodowych koalicjach antyterrorystycznych. Niestety, dokument ten nie był nowelizowany po 2019 r., a cały program został wygaszony.

Z kolei w *Strategii Bezpieczeństwa Narodowego z 2020 r*. wskazano, że należy (...) ***rozwijać zdolności operacyjne Sił Zbrojnych Rzeczypospolitej Polskiej, w szczególności Wojsk Specjalnych, do zwalczania zagrożeń, w tym o charakterze hybrydowym***[,] ***i działań kontrterrorystycznych, we wszystkich stanach nadzwyczajnych i stanach gotowości obronnej państwa***[26]. Podobne zalecenia pojawiają się w *Rekomendacjach do Strategii Bezpieczeństwa Narodowego* z 4 lipca 2024 r.: (...) ***zdolność państwa do przeciwdziałania zagrożeniom hybrydowym to ważny element budowania odporności państwa i powinien obejmować, ze względu na unikatowy charakter, m.in. rozwój zdolności operacyjnych SZ RP, w szczególności Wojsk Specjalnych – do działań kontrterrorystycznych we wszystkich stanach gotowości obronnej państwa*** (...)[27].

Niestety, wskazane dokumenty nie przełożyły się na konkretne rozwiązania, które mogłyby usprawnić użycie WS, zwłaszcza JW GROM, o czym szerzej w dalszej części tekstu.

Zadania Jednostki Wojskowej GROM

Operacje przeprowadzane przez WS mają szeroki zakres. Zadania poszczególnych jednostek WS są wymienione we wspomnianym już zarządzeniu Nr 30/MON:

1) Jednostka Wojskowa GROM – **realizacja pełnego spektrum operacji specjalnych i fizycznego zwalczania terroryzmu w układzie narodowym, sojuszniczym i koalicyjnym w środowisku lądowym i morskim, najwyższego ryzyka i strategicznego znaczenia, w tym**

[26] *Strategia Bezpieczeństwa Narodowego z 2020 r.*, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf, s. 19 [dostęp: 23 I 2025].

[27] *Rekomendacje do Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, 4 VII 2024 r., https://www.prezydent.pl/storage/file/core_files/2024/7/4/7fa9f08052b51758d6ed4e9a11a9d32d/REKOMENDACJE%20SBNRP%204%20lipca%202024.pdf, s. 28 [dostęp: 23 I 2025].

operacji uwalniania zakładników oraz prowadzenia operacji przeciwterrorystycznych, w czasie pokoju, kryzysu i wojny,

2) Jednostka Wojskowa Komandosów – realizacja pełnego spektrum operacji specjalnych w układzie narodowym, sojuszniczym i koalicyjnym w środowisku lądowym, w tym na wodach śródlądowych, dla realizacji celów o znaczeniu operacyjnym i strategicznym w czasie pokoju, kryzysu i wojny,
3) Jednostka Wojskowa Formoza – realizacja pełnego spektrum morskich operacji specjalnych w układzie narodowym, sojuszniczym i koalicyjnym dla realizacji celów o znaczeniu operacyjnym i strategicznym. Jednostka zachowuje zdolność do wsparcia komponentu morskiego w operacji połączonej oraz do wsparcia operacji uwalniania zakładników w środowisku morskim.

Zdjęcie 3. Ćwiczenia taktyki działań kontrterrorystycznych w statkach powietrznych.
Źródło: materiały własne JW GROM.

Co istotne, cały cykl rekrutacji, szkolenia, planowania i zakupów jest podporządkowany utrzymywaniu i zwiększaniu zdolności do prowadzenia ww. działań i operacji. Siły Zbrojne RP dysponują zatem jednostkami wojskowymi przeznaczonymi do działań antyterrorystycznych, w tym kontrterrorystycznych, z których – zdaniem autora – najbardziej wszechstronną i wyspecjalizowaną w fizycznym zwalczaniu terroryzmu jest JW GROM.

Jednostka Wojskowa GROM utrzymuje siły i środki do wsparcia struktur MSWiA i stanowi skuteczne narzędzie zapewnienia bezpieczeństwa wewnętrznego kraju w ramach zadań SZ RP[28], do których należą:

- wsparcie sił i środków Policji oraz SG, m.in. przez zapewnienie transportu elementów zadaniowych w czasie operacji wsparcia ochrony granicy lądowej i wód terytorialnych, w dzień i w nocy oraz w każdych warunkach atmosferycznych,
- wsparcie operacji RENEGADE (zwłaszcza M-RENEGADE), m.in. przez stałe utrzymywanie sił i środków w wysokiej gotowości do podjęcia działań,
- zabezpieczenie infrastruktury krytycznej państwa, m.in. przez prowadzenie rozpoznania powietrznego zagrożonych rejonów,
- wsparcie sił resortu spraw wewnętrznych podczas zabezpieczenia dużych imprez masowych oraz wizyt VIP, m.in. przez utrzymanie stałej gotowości elementów zadaniowych w ramach dyżurów AT, a także przez zwiększenie mobilności i zmniejszenie czasu reakcji sił i środków dedykowanych do działania, w sytuacji wystąpienia zagrożenia zdarzeniem o charakterze terrorystycznym,
- wsparcie niekinetycznego systemu zarządzania kryzysowego, np. przez ewakuację poszkodowanych z terenów dotkniętych klęskami żywiołowymi,
- prowadzenie działań poszukiwawczo-ratowniczych w środowisku przekraczającym możliwości służb cywilnych.

Jednostka Wojskowa GROM zgodnie z *Planem zarządzania kryzysowego Ministerstwa Obrony Narodowej*[29] utrzymuje siły i środki w gotowości do udzielenia pomocy Policji w prowadzeniu operacji kontrterrorystycznych. Jednostką Policji przeznaczoną do tego typu działania jest „BOA".

[28] *Rozkaz Nr Z-3/KT Dowódcy Komponentu Wojsk Specjalnych z dnia 20 stycznia 2023 r. w sprawie użycia w Dowództwie Komponentu Wojsk Specjalnych oraz podległych Dowódcy Komponentu Wojsk Specjalnych jednostkach Wojsk Specjalnych „Planu użycia sił i środków Dowódcy Komponentu Wojsk Specjalnych w sytuacjach kryzysowych"* (dokument niejawny).

[29] *„Plan zarządzania kryzysowego resortu Obrony Narodowej" zatwierdzony przez Ministra Obrony Narodowej w dniu 16 sierpnia 2022 r.*; *Rozkaz Nr Z-9 Dowódcy Generalnego Rodzajów Sił Zbrojnych z dnia 10 stycznia 2023 r. w sprawie wprowadzenia do użytku w Dowództwie Generalnym Rodzajów Sił Zbrojnych oraz podległych Dowódcy Generalnemu Rodzajów Sił Zbrojnych jednostkach organizacyjnych „Planu użycia sił i środków Dowódcy Generalnego Rodzajów Sił Zbrojnych w sytuacjach kryzysowych"*; *Rozkaz Nr Z-3/KT Dowódcy Komponentu Wojsk Specjalnych z dnia 20 stycznia 2023 r. w sprawie użycia…*

Jak zauważa się w literaturze poruszającej tematykę związaną ze zwalczaniem terroryzmu, JW GROM (...) *zajmuje bardzo ważne miejsce w systemie reagowania w sytuacjach kryzysowych. Na podkreślenie zasługuje fakt, że jest to jedyna jednostka zdolna do wykonywania zadań związanych z fizycznym zwalczaniem terroryzmu we wszelkich jego przejawach,* (...) *jest jednostką wszechstronną, potrafiącą wykonywać zadania o różnym stopniu trudności we wszystkich rejonach świata*[30].

Perspektywy rozwoju Wojsk Specjalnych, w tym Jednostki Wojskowej GROM

Kwestię rozwoju WS, w tym JW GROM, można rozpatrywać na dwóch płaszczyznach. Pierwsza z nich dotyczy odrębnego ustawodawstwa dla WS lub ich wybranych jednostek. Jak wskazuje się w literaturze, takie rozwiązanie było już wcześniej planowane. W ramach prac nad umocowaniem prawnym JW GROM w strukturach państwa zaproponowano, aby zasady jej działania regulował akt rangi ustawowej. Projekt ustawy normujący zasady funkcjonowania tej jednostki specjalnej został opracowany przez grupę prawników specjalizujących się w dziedzinie bezpieczeństwa wewnętrznego[31]. Propozycja została jednak odrzucona przez resort obrony narodowej. Jednostka znalazła się w jego strukturze 1 października 1999 r. Od czasu podporządkowania JW GROM Dowództwu Wojsk Specjalnych, później Dowództwu Komponentu Wojsk Specjalnych (podległemu Dowództwu Generalnemu Rodzajów Sił Zbrojnych) koncepcja odrębnego uregulowania dla tej formacji nie ma żadnego poparcia wśród decydentów wojskowych i politycznych. Aktualnie – zdaniem autora – takie całkowite wyłączenie JW GROM z podporządkowania strukturom wojskowym i przekazanie do bezpośredniej dyspozycji organu politycznego (np. Ministra Obrony Narodowej) nie znajduje uzasadnienia praktycznego oraz funkcjonalnego. Niewątpliwie konieczne jest jednak usprawnienie i przyspieszenie procedur użycia jednostek WS w szeroko rozumianych sytuacjach kryzysowych oraz uczynienie tych procedur w pewnym stopniu niejawnymi.

[30] *Zagadnienia fizycznej walki z zagrożeniami terrorystycznymi – aspekty prawne i organizacyjne*, K. Jałoszyński (red.), Warszawa 2010, s. 264.

[31] H. Królikowski, *Wojskowa formacja specjalna GROM im. Cichociemnych Spadochroniarzy Armii Krajowej 1990–2000*, Gdańsk 2001, s. 110–111.

Zdjęcie 4. Ćwiczenia z zakresu przeciwdziałania zagrożeniom CBRN.

Źródło: materiały własne JW GROM.

Druga płaszczyzna rozwoju to stworzenie organu bezpośrednio podporządkowanego Ministrowi Obrony Narodowej (przez sekretarza stanu bądź podsekretarza stanu, bądź szefa Sztabu Generalnego Wojska Polskiego) lub też w ramach Rządowego Centrum Bezpieczeństwa albo w strukturach gabinetu ministra – członka Rady Ministrów właściwego do spraw koordynowania działalności służb specjalnych (np. pod nazwą Biura Operacji Wysokiego Ryzyka). Zadaniem tego organu byłoby koordynowanie w resorcie obrony narodowej lub też w wymiarze międzyresortowym wymiany informacji między MON, WS, służbami specjalnymi, a także szybkie, skuteczne i niejawne wydzielanie komponentu SZ RP z wiodącą rolą WS (zwłaszcza JW GROM) do stworzenia zespołów zadaniowych funkcjonujących z udziałem służb specjalnych. Jest to o tyle uzasadnione, że zgodnie z art. 19 ust. 1 i 2 ustawy o działaniach AT minister właściwy do spraw zagranicznych, we współpracy z Ministrem Koordynatorem Służb Specjalnych, jeżeli został powołany, koordynuje działania właściwych służb i organów w przypadku zdarzenia o charakterze terrorystycznym poza granicami RP, wymierzonego przeciwko obywatelom lub mieniu RP, z wyłączeniem zdarzeń o charakterze terrorystycznym poza granicami RP, wymierzonego przeciwko personelowi lub mieniu SZ RP. Taki dychotomiczny podział nie sprawdził się i wydaje się nieefektywny, co pokazała operacja ewakuacji polskich obywateli

z Islamskiej Republiki Afganistanu[32]. W tym przypadku podjęto działania wojskowe (operacja wojskowa zarówno co do charakteru, jak i użytych sił i środków) w przypadku zagrożenia dla osób niebędących żołnierzami, obywateli RP i obywateli innych państw. Takie rozwiązanie było planowane w podobnych okolicznościach w innych zagrożonych rejonach, w których przebywali lub przebywają cywilni obywatele Polski. Ta operacja dowodzi konieczności opracowania rozwiązań prawnych dotyczących współdziałania WS oraz Agencji Wywiadu (AW). Zalążek takich rozwiązań istnieje w art. 10 ust. 2a ustawy o SKW oraz SWW[33]. Zgodnie z tym przepisem służby te przy realizacji swoich zadań współdziałają ze Sztabem Generalnym Wojska Polskiego i innymi komórkami organizacyjnymi MON oraz Dowódcą Generalnym Rodzajów Sił Zbrojnych, Dowódcą Operacyjnym Rodzajów Sił Zbrojnych, Dowódcą Wojsk Obrony Terytorialnej, Szefem Inspektoratu Wsparcia Sił Zbrojnych, dowódcami garnizonów wojskowych i jednostek wojskowych. W celu tego współdziałania, zwłaszcza dla zapewnienia bezpieczeństwa i właściwej realizacji zadań SWW poza granicami państwa, w SWW mogą być tworzone zespoły zadaniowe składające się z funkcjonariuszy tej służby, żołnierzy zawodowych wyznaczonych na stanowiska służbowe w SWW oraz żołnierzy pełniących służbę w oddziałach lub pododdziałach SZ RP.

Biorąc pod uwagę charakter potencjalnych zagrożeń bezpieczeństwa państwa związanych z działalnością terrorystyczną oraz analizę potencjalnych kierunków ich rozwoju, należy podkreślić, że sprawne oraz dyskretne (z ang. tzw. *law pro*) współdziałanie WS, zwłaszcza JW GROM, ze służbami specjalnymi, Policją i SG jest konieczne do zapewnienia bezpieczeństwa kraju na wysokim poziomie. Najbardziej pożądaną formą rozwoju WS jest stworzenie ram prawnych w poszczególnych ustawach normujących funkcjonowanie służb specjalnych, na których podstawie WS, a szczególnie JW GROM, będą mogły sprawnie wspierać organy odpowiedzialne za bezpieczeństwo wewnętrzne państwa. W przypadku konieczności użycia WS poza granicami kraju jest potrzebne także zmodyfikowanie dotychczasowego trybu. Obecnie o działaniu Sił Zbrojnych RP poza granicami kraju decyduje Prezydent RP. Jednak współdziałanie zespołów zadaniowych służb specjalnych i WS będzie podlegało wieloszczeblowej kontroli w postaci

[32] *Polscy żołnierze zakończyli misję w Afganistanie*, Ministerstwo Obrony Narodowej, 27 VIII 2021 r., https://www.gov.pl/web/obrona-narodowa/polscy-zolnierze-zakonczyli-misje-w-afganistanie [dostęp: 23 I 2025].

[33] *Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego* (t.j. DzU z 2024 r. poz. 1405, ze zm.).

Ministra Obrony Narodowej, Ministra Koordynatora oraz Prezesa Rady Ministrów. Mając na uwadze konieczność szybkości działania, nieliczny skład zespołu zadaniowego oraz przede wszystkim bezpieczeństwo operacji (ang. *operations security*), Prezydent może być o niej poinformowany, ale niekoniecznie musi o tym decydować, ponieważ taki zespół zadaniowy działałby pod kierownictwem danej służby (w tym wypadku AW). Ważne jest też usprawnienie oraz utajnienie tego procesu. W tym celu należy uregulować wiele spraw, m.in. pseudonimizację[34] oraz samodzielność planistyczną i finansową WS, tzn. stworzenie wyodrębnionego funduszu operacji specjalnych służącego do opłacania kosztów logistycznych, jak również tworzenie zespołów zadaniowych WS ze służbami specjalnymi oraz możliwości przesuwania podporządkowania ADCOM (z ang. Administrative Command) lub OPCOM (z ang. Operational Command) w celu skrócenia drogi decyzyjnej.

Przeciwdziałanie zagrożeniom hybrydowym oraz działania kontrterrorystyczne wymagają skutecznej koordynacji użycia służb odpowiedzialnych za te zadania, w myśl zasady WGA. Są do tego potrzebne:

a) szybkie przekazywanie informacji,
b) szybkie podejmowanie decyzji,
c) szybka aktywacja oraz użycie adekwatnych sił i środków.

W odniesieniu do szybkości przepływu informacji oraz podejmowania decyzji należy wskazać, że ostatnie nowelizacje pragmatyki służbowej Policji, SG i ustawy o działaniach AT wprowadzone na podstawie ustawy o zmianie niektórych ustaw w celu usprawnienia działań SZ RP, Policji oraz SG na wypadek zagrożenia bezpieczeństwa państwa umożliwiły przekazywanie wniosku lub decyzji o użyciu SZ RP przez uprawnione organy ustnie, telefonicznie, za pomocą środków komunikacji elektronicznej w rozumieniu art. 2 pkt 5 ustawy o świadczeniu usług drogą elektroniczną[35] lub za pomocą innych środków łączności. Treść wniosku lub decyzji oraz istotne motywy takiego załatwienia sprawy utrwala się w formie pisemnej w postaci papierowej (art. 1 pkt 2 lit. b, art. 2 pkt 1 lit. b, art. 7 pkt 2 lit. a). Takie rozwiązanie było wcześniej wielokrotnie postulowane przez WS i można ocenić je jak najbardziej pozytywnie. Praktyka pokaże, czy będzie właściwie wykorzystywane.

[34] Używanie numerów operacyjnych lub też pseudonimów w celu utrudnienia identyfikacji formacji lub danych osobowych żołnierzy.

[35] *Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną* (t.j. DzU z 2024 r. poz. 1513).

Propozycje i uwagi de lege ferenda

W kolejnej części tekstu zostaną przedstawione propozycje dotyczące zasad funkcjonowania WS do rozważenia przez ekspertów w dziedzinie bezpieczeństwa państwa, zwłaszcza działania służb specjalnych.

Zgodnie z obecnym porządkiem prawnym WS nie mają możliwości bezpośredniego współdziałania z AW, ABW lub też Służbą Ochrony Państwa (SOP). Wydaje się, że istnieje wola współpracy na poziomach taktycznym i operacyjnym, jednak brakuje rozwiązań prawnych rangi ustawowej, co jest konieczne w przypadku przekazywania informacji niejawnych, użycia środków przymusu bezpośredniego lub broni palnej, a także – w ograniczonym zakresie – wsparcia lub zabezpieczenia służb specjalnych w prowadzeniu czynności operacyjno-rozpoznawczych (np. przez zbieranie danych biometrycznych na potrzeby tych służb) lub ochronnych (SOP). Można rozważyć stworzenie narzędzi analogicznych jak w przypadku SWW lub SKW (art. 10 lub art. 4 ustawy o SKW oraz SWW), czyli zespoły zadaniowe składające się z funkcjonariuszy AW, ABW lub SOP, żołnierzy zawodowych wyznaczonych na stanowiska służbowe w tych służbach oraz żołnierzy pełniących służbę w oddziałach lub pododdziałach SZ RP (z uwagi na specyfikę zadań tych służb można rozważyć w tej sytuacji udział wyłącznie żołnierzy WS). Obowiązujące w tym zakresie przepisy art. 10 ustawy o ABW oraz AW[36] lub art. 4 oraz art. 19 ust. 1 ustawy o działaniach AT nie dają wystarczających podstaw do realnego współdziałania WS z ABW i AW, w tym do użycia broni lub środków przymusu bezpośredniego chociażby do ochrony infrastruktury krytycznej, bezpieczeństwa CBRN (ochrony przed proliferacją broni masowego rażenia) lub też działania poza granicami państwa. Podobnie zgodnie z art. 38 ustawy o SOP[37] nie przewiduje się możliwości wsparcia tej formacji przez SZ RP, w szczególności WS, a zwłaszcza JW GROM. W przypadku osób o szczególnym statusie ich ochrona na terenie w kraju, a przede wszystkim poza jego granicami, np. w rejonie konfliktu zbrojnego, wydaje się obszarem wymagającym rozważenia i skorygowania przez ustawodawcę. Tym bardziej że – jak była o tym mowa – art. 11 ustawy o obronie Ojczyzny przewiduje możliwość użycia JW GROM (jako elementu SZ RP) do działań antyterrorystycznych (właściwych przede wszystkim dla ABW, zgodnie z art. 3 ust. 1 w zw. z art. 2 pkt 1 ustawy o działaniach AT) oraz zarządzania

[36] *Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (t.j. DzU z 2024 r. poz. 812, ze zm.).

[37] *Ustawa z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa* (t.j. DzU z 2025 r. poz. 34, ze zm.).

kryzysowego, a więc m.in. ochrony infrastruktury krytycznej (art. 2 w zw. z art. 3 pkt 1 i 2 ustawy o zarządzaniu kryzysowym). Warto również rozważyć udział ekspertów z JW GROM w obradach grup roboczych oraz zespołów funkcjonujących w systemie zarządzania kryzysowego. Proponowane rozwiązanie niewątpliwie przyniesie korzyść także WS, co pokazały działania poza granicami państwa, m.in. w Islamskiej Republice Afganistanu. Po analizie tych operacji eksperci ocenili, że (...) *w późniejszym okresie doszło do zdobycia niezbędnych umiejętności pozwalających na korzystanie z własnych źródeł informacji, m.in. dzięki pozyskaniu odpowiedniego sprzętu i lepszej współpracy z właściwymi służbami*[38].

Elementem uzupełniającym powinno być dodanie WS do łańcucha organów, z którymi Szef ABW koordynuje czynności analityczno-informacyjne oraz wymienia informacje, zwłaszcza te dotyczące zdarzeń i zagrożeń o charakterze terrorystycznym (art. 5 ust. 1 ustawy o działaniach AT), a także uściślenie w dokumentach organizacyjnych, że WS są służbą rozpoznania SZ RP, o której mowa w art. 11 ustawy o ABW oraz AW.

Tak jak wspomniano, wsparcie „BOA" przez JW GROM może nastąpić zarówno w trybie ustawy o Policji (art. 18), jak i ustawy o działaniach AT (art. 22). W pierwszym przypadku współdziałanie (decyzja uprawnionego organu) może być rozpoczęte bez wprowadzonych stopni alarmowych, o których mowa w art. 15 ust. 1 ustawy o działaniach AT, ale z ograniczeniami co do użycia broni palnej[39]. W drugim przypadku natomiast użycie JW GROM do wsparcia działań kontrterrorystycznych prowadzonych przez „BOA" może nastąpić dopiero po wprowadzeniu trzeciego (CHARLIE) lub czwartego (DELTA) stopnia alarmowego (art. 22 ust. 1 ustawy o działaniach AT). Obie procedury są przeprowadzane na podstawie dwóch różnych podstaw prawnych. W związku z tym np. wsparcie Policji przez JW GROM podczas Święta Wojska Polskiego albo imprezy masowej związanej z wizytą osoby o szczególnym statusie z innego państwa (które bez trzeciego lub czwartego stopnia alarmowego może nastąpić tylko w trybie ustawy o Policji) nie może być kontynuowane jako działanie grupy kontrterrorystycznej w rozumieniu art. 23 ust. 4 ustawy o działaniach AT (dotyczy to również uprawnień do specjalnego użycia broni, o którym mowa w art. 23 ust. 1 tej ustawy) bezpośrednio po wprowadzeniu trzeciego lub czwartego stopnia

[38] T. Sapierzyński, *Operacje bojowe JW GROM w pierwszej dekadzie XXI wieku*, „Bezpieczeństwo. Teoria i Praktyka" 2020, nr 2, s. 164. https://doi.org/10.34697/2451-0718-btip-2020-2-009.

[39] Brak możliwości użycia broni w sposób specjalny, o którym mowa w art. 23 ustawy o działaniach AT.

alarmowego. Wynika to z tego, że wydawane na podstawie ustawy o Policji pierwotna decyzja Ministra Obrony Narodowej (art. 18 ust. 5) bądź postanowienie Prezydenta RP (art. 18 ust. 3), jak już wspomniano, są wydawane na innej podstawie prawnej.

Podobnie rewizji wymaga sprawa specjalnego użycia broni (art. 23 ust. 1 ustawy o działaniach AT), ponieważ dotyczy ono wyłącznie broni palnej. Dzisiaj już wiadomo, że można użyć także bezzałogowego statku powietrznego (ang. *unmanned aerial vehicle,* UAV) z podwieszonym ładunkiem wybuchowym, jeżeli jest to niezbędne do przeciwdziałania bezpośredniemu, bezprawnemu, gwałtownemu zamachowi na życie lub zdrowie człowieka bądź do uwolnienia zakładnika, a użycie broni palnej w sposób wyrządzający możliwie najmniejszą szkodę okazuje się niewystarczające i nie jest możliwe przeciwdziałanie takiemu zamachowi lub uwolnienie zakładnika w inny sposób. We wskazanych okolicznościach skutkiem tego specjalnego użycia broni może być śmierć lub bezpośrednie zagrożenie życia lub zdrowia osoby dokonującej zamachu.

W tym też zakresie – w związku z dynamicznym rozwojem techniki UAV – należy dostosować przepisy ustawy – Prawo lotnicze oraz przepisy resortowe tak, aby WS mogły użytkować UAV, w tym amunicję krążącą potocznie zwaną dronami kamikadze, jako broń[40], w trakcie zarówno realnej operacji, jak i ćwiczeń, bez konieczności traktowania ich uszkodzenia lub zniszczenia jako wypadku lub incydentu lotniczego albo szkody w mieniu. Ponadto należy odformalizować proces nabywania uprawnień do wykonywania lotów UAV przez pilotów wojskowych w celu przeciwdziałania zagrożeniom hybrydowym i wykonywania działań kontrterrorystycznych czy związanych z budowaniem odporności infrastruktury krytycznej.

W ostatnim czasie pojawił się także inny problem, a mianowicie prowadzenie operacji kontrterrorystycznej uwalniania zakładników w trakcie pełnoskalowego konfliktu zbrojnego. Co do zasady nie ma kontrowersji dotyczących jej podstaw prawnych, trudność pojawia się przy doborze służących temu narzędzi (środków). Jak wynika z art. 8 Rzymskiego Statutu Międzynarodowego Trybunału Karnego[41], zbrodnie wojenne oznaczają

[40] SOFCOM Doctrine and Lessons Learned 26.11.2024 r. – The New Frontiere of Warfare: Unmanned Systems and Countermeasures (dokument o klauzuli NATO UNCLASSIFIED, jednak nie został on przekazany do publikacji, z dokumentu mogą korzystać tylko wskazane w nim instytucje).

[41] *Rzymski Statut Międzynarodowego Trybunału Karnego sporządzony w Rzymie dnia 17 lipca 1998 r.* (DzU z 2003 r. poz. 708, ze zm.).

poważne naruszenia konwencji genewskich z 1949 r.[42] oraz inne poważne naruszenia praw i zwyczajów prawa międzynarodowego mających zastosowanie do konfliktów zbrojnych o międzynarodowym charakterze. Należy do nich m.in. stosowanie pocisków rozszerzających się lub spłaszczających w ciele człowieka, takich jak pociski z twardą łuską, która nie pokrywa w całości rdzenia lub jest ponacinana (art. 8 ust. 2 lit. a i b (xix) Rzymskiego Statutu Międzynarodowego Trybunału Karnego). W działaniach kontrterrorystycznych taka amunicja, czyli pociski *hollow-point*, jest wskazana z uwagi na jej właściwości antyrykoszetowe (bezpieczeństwo dla osób postronnych) oraz moc obalającą (zwiększenie prawdopodobieństwa eliminacji zagrożenia niewielką liczbą strzałów). Pociski te mają kilka zalet, które sprawiają, że są one doskonałe do samoobrony:

- są bezpieczniejsze dla osób postronnych niż pociski z pełną metalową osłoną,
- są mniej podatne na rykoszetowanie i trafienie osób postronnych, ponieważ rzadziej odbijają się od twardych powierzchni i trafiają w niezamierzone cele,
- jest mniej prawdopodobne, że zabiją osoby postronne, jeśli zostaną wystrzelone pod złym kątem,
- rozszerzają się przy uderzeniu, co tworzy większy kanał rany, a tym samym zwiększają szybkość obezwładniania[43].

Ten rodzaj amunicji jest wykorzystywany także w Polsce do działań kontrterrorystycznych na terenie kraju w czasie pokoju[44]. Jest to temat do dyskusji w zakresie prowadzenia skutecznych, a więc bezpiecznych dla zakładników operacji typu Hostage Rescue w analogicznych warunkach jak wyglądało to w Strefie Gazy[45], choć przy użyciu środków wątpliwych z punktu widzenia prawa międzynarodowego humanitarnego, tzn. amunicji typu *hollow-point*.

---

[42] *Konwencje o ochronie ofiar wojny podpisane w Genewie dnia 12 sierpnia 1949 r.* (DzU z 1956 r. poz. 171, ze zm.).

[43] *Amunicja typu Hollow Point a konwencja genewska*, Centrum Praw Człowieka, 9 VIII 2022 r., https://ofpc.pl/amunicja-typu-hollow-point-a-konwencja-genewska/ [dostęp: 23 I 2025].

[44] J. Sabak, *Milion pocisków antyrykoszetowych dla JW GROM*, Defence24, 15 V 2015 r., https://defence24.pl/geopolityka/milion-pociskow-antyrykoszetowych-dla-jw-grom [dostęp: 23 I 2025].

[45] P. Celej, *Elitarna izraelska jednostka Jamam w akcji: Kulisy uwolnienia zakładników przez Siły Obronne Izraela*, Gazeta Prawna, 8 VI 2024 r., https://www.gazetaprawna.pl/wiadomosci/swiat/artykuly/9522754,elitarna-izraelska-jednostka-jamam-w-akcji-kulisy-uwolnienia-zakladni.html [dostęp: 23 I 2025].

Podsumowanie

Przedstawione zagadnienia są wynikiem doświadczeń związanych z funkcjonowaniem WS i JW GROM zdobytych podczas realnych działań oraz ćwiczeń z różnymi formacjami krajowymi i zagranicznymi. Autor ma nadzieję, że zawarte w tekście przemyślenia pomogą zainicjować dyskusję ekspercką na temat roli jednostek WS we wsparciu tzw. układu pozamilitarnego. Należy przy tym podkreślić, że chodzi o zwiększenie możliwości ustawowego działania wchodzących w jego skład służb i formacji, a nie zastąpienie ich lub dublowanie zadań przez WS. Zdaniem autora zwiększenie tych możliwości jest niezbędne w przypadku prowadzenia działań w czasie pokoju i kryzysu niebędącego stanem wojny. Dotyczy to zwłaszcza zabezpieczenia infrastruktury krytycznej oraz zapewnienia bezpieczeństwa najważniejszych osób w państwie w sytuacji zagrożeń hybrydowych. Jednocześnie należy zwrócić uwagę na bezpieczeństwo prawne żołnierzy i funkcjonariuszy. Powinni oni mieć poczucie, że gdy wykonują zadania zlecone przez przełożonych, stoi za nimi państwo i jasne regulacje prawne oraz możliwość jak najszerszego doboru sił i środków adekwatnych do zagrożenia.

Łukasz Niemczyk

Radca prawny oraz żołnierz zawodowy. Zajmuje się tematyką Wojsk Specjalnych, a w szczególności rozwiązaniami prawnymi w zakresie wykorzystania tego rodzaju formacji do współdziałania w układzie pozamilitarnym, a także usprawnianiem procedur dotyczących użycia Sił Zbrojnych na terenie kraju i poza jego granicami. Wykładowca m.in. na Uczelni Techniczno-Handlowej w Warszawie oraz w Krajowej Szkole Sądownictwa i Prokuratury.

Kontakt: l.niemczyk@ron.mil.pl

Terroryzm – studia, analizy, prewencja, 2025, nr 7: 281–291

https://doi.org/10.4467/27204383TER.25.034.21811

Varia

35-lecie Jednostki Wojskowej GROM. Rola jednostek specjalnych w dobie zagrożeń hybrydowych

Duża dynamika zmian politycznych, ekonomicznych i technologicznych zachodzących we współczesnym świecie powoduje, że aby działać skutecznie, trzeba być proaktywnym i ustawicznie poszukiwać nowych rozwiązań. Nie jest pod tym względem wyjątkiem sfera wojskowa, w której wykorzystuje się nowoczesne narzędzia, np. w postaci rojów autonomicznych systemów bezzałogowych, druku 3D czy sztucznej inteligencji, a także ustawicznie aktualizuje taktyki, techniki i procedury. – W Jednostce Wojskowej GROM stale analizujemy zmiany dokonujące się w świecie i architekturze bezpieczeństwa, aby przewidywać zagrożenia i wyzwania, jakie może przynieść przyszłość, oraz wiedzieć, czy nasze obecne zdolności pozwolą im sprostać – podkreśla **płk Grzegorz Krawczyk**, zastępca dowódcy JW GROM. W lipcu 2025 r. ta elitarna jednostka Wojsk Specjalnych będzie obchodzić 35-lecie istnienia.

Damian Szlachter: Jednostka Wojskowa GROM została sformowana w 1990 r. i w tym roku będzie obchodzić 35-lecie istnienia. Proszę powiedzieć, jakie zmiany zaszły w niej przez ten czas i czy planowane są jakieś okolicznościowe przedsięwzięcia.

Płk Grzegorz Krawczyk: W ciągu 35 lat istnienia GROM był wielokrotnie reorganizowany. Z jednostki zdolnej do wykonywania zadań kontrterrorystycznych stał się jednostką mogącą samodzielnie prowadzić – w ramach systemu krajowego i sojuszniczego – złożone operacje specjalne, wymagające zaangażowania profesjonalistów z różnych dziedzin, takich jak np.: CBRNE, JTAC, K9, EOD[1], analityków i specjalistów w zakresie rozpoznania czy targetingu wspierających element bojowy. Zmieniły się także nasze zdolności przerzutu elementów zadaniowych i obecnie GROM może autonomicznie przerzucać operatorów drogą lądową, wodną i powietrzną. Największe przekształcenia dotyczyły jednak zdolności do dowodzenia. Wyszliśmy od modelu administrowania jednostką, a doszliśmy do modelu dowodzenia zadaniowymi zespołami bojowymi GROM-u i przydzielonymi, zarówno narodowymi, jak i koalicyjnymi, w trakcie operacji specjalnych prowadzonych w czasie kryzysu, poniżej progu wojny oraz kinetycznych operacji specjalnych podczas wojny. Zmiany są wynikiem doświadczeń zdobytych w różnych okolicznościach oraz obszarach, głównie przy wykonywaniu zadań poza granicami kraju, dzięki uczestnictwu w krajowych i zagranicznych ćwiczeniach wojskowych oraz tych z udziałem formacji pozamilitarnych. Szczególnie cenne są szkolenia z najlepszymi jednostkami wojsk specjalnych na świecie, tj. z brytyjskim 22 pułkiem SAS, amerykańskimi CAG, Navy SEAL czy 10th SFG. Stale analizujemy też zmiany, jakie zachodzą w świecie i architekturze bezpieczeństwa, aby przewidywać, jakie zagrożenia i wyzwania może przynieść przyszłość, i wiedzieć, czy nasze obecne zdolności pozwolą im sprostać.

W ramach obchodów święta JW GROM odbędzie się zamknięta konferencja na temat wyzwań stojących przed wojskami specjalnymi w związku z sytuacją geopolityczną na świecie – tą aktualną i tą, z którą możemy mieć do czynienia w przyszłości. W charakterze prelegentów wystąpią eksperci krajowi i zagraniczni. Naszym celem jest

[1] CBRNE (ang. *chemical, biological, radiological, nuclear, and explosives*) – akronim oznaczający zagrożenia chemiczne, biologiczne, radiologiczne, nuklearne i wybuchowe, JTAC (ang. *joint terminal attack controller*) – akronim oznaczający wysuniętego nawigatora naprowadzania lotnictwa, K9 – termin oznaczający psy bojowe, EOD (ang. *explosive ordnance disposal*) – akronim oznaczający pirotechników (przyp. red.).

pokazanie jak najszerszego spojrzenia na poruszaną tematykę i dlatego do udziału w spotkaniu zaprosiliśmy przedstawicieli sfery wojskowej i cywilnej. Swoje wystąpienia potwierdzili m.in. gen. rez. Austin S. Miller, były dowódca CAG oraz amerykańskiego dowództwa JSOC, i Peter W. Singer, specjalista ds. działań wojennych XXI w. Do lipca powinna ukazać się książka poświęcona historii GROM-u. Jej współautorami są zawodowi historycy związani z Muzeum Powstania Warszawskiego, a prace nad nią trwały ponad siedem lat. Zadbaliśmy o to, aby opracowanie miało formę przystępną dla czytelnika. Wierzę, że będzie to bardzo wartościowa pozycja w biblioteczce każdego sympatyka GROM-u i nie tylko.

W ostatnich kilkunastu latach GROM intensywnie wspierał rozwój polskiego systemu antyterrorystycznego, m.in. przez przekazywanie uwag do nowelizowanych aktów prawnych, organizowanie szkoleń, udział w ćwiczeniach kontrterrorystycznych, dzielenie się doświadczeniem bojowym z rejonów konfliktów zbrojnych, wsparcie w zabezpieczaniu VIP-ów oraz placówek dyplomatycznych czy budowaniu odporności obiektów infrastruktury krytycznej na działania sabotażowe. Obserwuję tę wielotorową aktywność od dawna i podziwiam za profesjonalizm i zaangażowanie. Jak udaje się łączyć w ramach jednej jednostki tak wiele różnych projektów i działań?

Tworzeniu w latach 90. JW GROM przyświecał jeden cel – dysponowanie profesjonalnym oddziałem mającym możliwości reagowania na zagrożenia terrorystyczne wynikające z ówczesnej sytuacji na świecie. Początkowo nie zakładano udziału GROM-u w działaniach wojskowych poza granicami kraju, mimo że takie zdarzało mu się prowadzić na Haiti czy na Bałkanach. Podporządkowanie jednostki Ministerstwu Spraw Wewnętrznych sprawiło, że można było ją szybko kierować do realizacji zadań kontrterrorystycznych w kraju, ale możliwości jej wykorzystania w misjach zagranicznych były ograniczone. W 1999 r. GROM został przeniesiony ze struktur MSW do Ministerstwa Obrony Narodowej. Miało to pozwolić na sprawniejsze wykorzystywanie jego potencjału poza granicami kraju oraz znacznie lepsze zabezpieczenie potrzeb logistycznych jednostki. Podporządkowanie MON nie zmieniło jednak podstawowych zadań GROM-u,

tj. gotowości do prowadzenia operacji uwalniania zakładników oraz zwalczania terroryzmu.

Jednostka była co prawda „wpięta" w krajowy system zarządzania kryzysowego, gotowa do wsparcia działań kontrterrorystycznych prowadzonych czy to przez Straż Graniczną, czy Policję, ale brakowało sprawnego systemu nadrzędnego, który w sytuacjach kryzysowych zarządzałby tymi siłami. Po 2014 r. stan bezpieczeństwa w naszym regionie diametralnie się zmienił. Analizując sytuację geopolityczną oraz mając na uwadze doświadczenia naszych brytyjskich partnerów, a także obowiązujące w Polsce prawodawstwo, stwierdziliśmy, że musimy być bardziej proaktywni na płaszczyźnie bezpieczeństwa wewnętrznego. W 2017 r. rozpoczęliśmy intensywne prace nad koncepcją służącą zwiększeniu naszej efektywności w tej sferze, przy czym uwzględniliśmy nie tylko zagrożenia terrorystyczne, lecz także hybrydowe, którym wówczas nie poświęcano tyle uwagi co obecnie. W tamtym czasie ten drugi obszar nie spotkał się jednak ze zrozumieniem w naszym środowisku wojskowym, nie przewidywano bowiem możliwości wystąpienia tego rodzaju zagrożeń. Opracowana przez nas koncepcja obejmowała wiele obszarów, m.in. wsparcie procesu szkolenia pododdziałów kontrterrorystycznych wywodzących się z układu pozamilitarnego, udział w ćwiczeniach i szkoleniach o tej tematyce, analizy prawne na potrzeby skutecznego wykorzystania jednostki w operacjach kontrterrorystycznych oraz rekomendacje w zakresie zmian prawnych. Dążyliśmy także do zwiększenia naszych zdolności do szybszego reagowania na kryzys. Znalazło to swoje odzwierciedlenie w skróceniu czasu, jaki upływał od momentu decyzji o podjęciu działania, co dodatkowo zwiększało możliwości zachowania odpowiedniego poziomu niejawności operacji specjalnych oraz zdolności do szybkiego przerzutu sił w każde miejsce w Polsce. Dzięki tej inicjatywie powstał w GROM-ie Zespół Lotniczy wyposażony w śmigłowce S-70i Black Hawk.

Obecnie w atakach terrorystycznych wykorzystuje się coraz bardziej zaawansowane technologie – roje pojazdów bezzałogowych, druk 3D, sztuczną inteligencję, internet satelitarny. Jak GROM doskonali swoje zasoby i taktyki, by sprostać nowym wyzwaniom i być skutecznym?

Tak to prawda, środowisko bezpieczeństwa bardzo się zmieniło, podobnie jak narzędzia ataku. Jest to jeden ze skutków konfliktu w Ukrainie. Wojny zawsze przyspieszały proces adaptacji różnego rodzaju technologii do celów wojskowych. Tak było np. z dynamitem, który pierwotnie był przeznaczony do cywilnych prac górniczych, a chwilę później znalazł zastosowanie w działaniach wojskowych. Drukarki 3D, które początkowo służyły do zabawy czy wytwarzania różnych rzeczy na potrzeby cywilne, teraz stały się narzędziem do produkcji broni i jej komponentów. W tej materii mamy do czynienia ze wzrostem wykładniczym i praktycznie co dwa tygodnie, może co miesiąc, pojawiają się ulepszone lub zupełnie nowe rozwiązania. Kultura organizacyjna GROM-u od początku kładła nacisk na kreatywność oraz nieustanne poszukiwanie najlepszych narzędzi, technik, taktyk i procedur do wykonania zadania. Mamy wbudowane mechanizmy, które to wspierają. Dużo wnosi pod tym względem nasza wielonarodowa kooperacja oraz wymiana doświadczeń z zagranicznymi partnerami. To proces ciągłego zbierania i analizowania informacji. Następny poziom to inicjatywa własna – szukamy rozwiązań problemów, przy czym staramy się myśleć poza schematami. Mamy też własną pracownię druku 3D i dział innowacji, gdzie nasze pomysły są ucieleśniane, a następnie testowane przez użytkowników końcowych. Jest to proces 360°, co oznacza, że jesteśmy w permanentnym cyklu obserwacji, analizy, wdrażania i dostosowywania się do świata VUCA[2]. Warto byłoby jeszcze pomyśleć o możliwości współdziałania lub wykorzystania GROM-u do wsparcia wszystkich polskich służb specjalnych, aby wypracowywać optymalne rozwiązania, uwzględniające doświadczenia różnych organizacji zagranicznych.

[2] VUCA (ang. *volality, uncertainly, complexity, ambiguity*) – akronim oznaczający świat zmienny, niepewny, złożony i niejednoznaczny (przyp. red.).

Czego na temat roli jednostek specjalnych we współczesnym konflikcie zbrojnym uczy wojna w Ukrainie? Jakie zmiany w związku z nią wprowadzają wasi partnerzy z krajów NATO?

Wojna w Ukrainie jest ogromnym źródłem informacji o wielu aspektach współczesnego konfliktu. Jest to pierwsza wojna w XXI w., w przypadku której można przyjąć, że walczą ze sobą dwa nazwijmy to równorzędne militarnie państwa, a działania są prowadzone w prawie wszystkich domenach, tj. lądowej, morskiej, powietrznej i w cyberprzestrzeni. Analiza trzech lat tej wojny pozwala na wyciągnięcie wielu pozytywnych, ale też negatywnych wniosków co do użycia jednostek wojsk specjalnych. Od 2014 r. NATO dokładało wielu starań, aby zorganizować ukraińskie wojska specjalne na wzór zachodni. Po prawie ośmiu latach wytężonych szkoleń udało się stworzyć dowództwo wojsk specjalnych oraz certyfikować ukraińskie jednostki specjalne według standardów Sojuszu. Początek wojny ujawnił jednak problem polegający na zupełnym niezrozumieniu przez dowódców ogólnowojskowych roli i zadań wojsk specjalnych. Błędne decyzje dotyczące użycia tego rodzaju wojsk spowodowały, że w ciągu kilku miesięcy utracono prawie cały ich potencjał. I to jest pierwsza lekcja, dla nas najważniejsza. Po przeanalizowaniu polskiego środowiska wojskowego jako dowództwo jednostki specjalnej nie mamy pewności, czy w czasie wojny nie podzielilibyśmy podobnego losu. To jest nasza bolączka, gdyż jesteśmy świadomi, ile wysiłku i czasu kosztuje wyselekcjonowanie, a następnie wyszkolenie operatora jednostki wojsk specjalnych (szkolenie podstawowe to minimum 12 miesięcy) i jak wymagający jest proces odbudowywania takich zdolności. Dlatego traktowanie wojsk specjalnych jako lepiej wyszkolonej piechoty i wyznaczanie do takich zadań jak „czyszczenie" okopów jest prostą drogą do utraty tych zdolności i pojawienia się poważnego problemu z ich odtworzeniem na odpowiednim poziomie w krótkim czasie. Podczas analizy przebiegu konfliktu zarówno my, jak i nasi partnerzy z NATO projektujemy potencjalne zadania dla nas podczas operacji specjalnych. Możemy wyróżnić trzy fazy przyszłego konfliktu. Pierwsza prawdopodobnie będzie miała charakter działań hybrydowych, może terrorystycznych, w celu zdezorganizowania funkcjonowania infrastruktury krytycznej i państwa. Tutaj rola operacji specjalnych jako elementu wspierającego układ pozamilitarny w zapobieganiu takim zagrożeniom i zwalczaniu ich jest dość oczywista. Czas tej fazy może być zarówno krótki, ale intensywny, jak i długi w celu wyczerpania sił.

Druga faza to dynamiczne starcie kinetyczne, w którym manewr taktyczny będzie kluczowym czynnikiem. Operacje specjalne mogą mieć w tej fazie inny charakter – poczynając od klasycznego zadania polegającego na wyszukiwaniu i niszczeniu wartościowych i wysokoopłacalnych celów, np. systemów obrony przeciwlotniczej, rakiet balistycznych, zaopatrzenia logistycznego, operacyjnych systemów dowodzenia i łączności, przez działania przeciwdywersyjne, a na wsparciu militarnym wojsk konwencjonalnych kończąc. To ostatnie polegałoby nie na walce w szeregach pododdziałów ogólnowojskowych, lecz bardziej na doradzaniu dowódcom szczebla batalionu, aby zgrać całość wielodomenowego potencjału pola walki, ale z takim pierwiastkiem charakterystycznym dla wojsk specjalnych. Ten pogląd rozważa wiele NATO-wskich jednostek wojsk specjalnych. Trzecia faza to stabilizacja frontu, gdzie będą się toczyć walki statyczne, czyli to, co teraz obserwujemy w Ukrainie. Środek ciężkości zadań wojsk specjalnych może zostać w tym przypadku przesunięty na tworzenie i kierowanie ruchem oporu na terenach zajętych przez przeciwnika oraz na uderzenia w interesy polityczno-gospodarcze państwa agresora, zarówno w głębi jego kraju, jak i w państwach trzecich, w których takie interesy ono ma. To są wnioski z poziomu operacyjnego, bardzo ważne dla nas, aby stworzyć u decydentów wojskowych i politycznych obraz prawidłowego prowadzenia operacji specjalnych w czasie kryzysu i wojny.

W obszarze taktyk, technik i procedur wniosków jest jeszcze więcej. Ktoś dość trafnie określił toczącą się wojnę Rosji z Ukrainą jako połączenie gwiezdnych wojen z I wojną światową. Powszechne użycie różnego rodzaju dronów spowodowało, że nie da się już walczyć tak jak kiedyś. Dron pełni teraz funkcję lornetki, karabinka i granatu, ale ma dużo większy zasięg niż te atrybuty walki. Użycie dronów latających, pływających czy lądowych jest analizowane pod kątem zarówno teoretycznym, jak i praktycznym. Pewne zdolności są już wdrażane, nad innymi nadal się pracuje. Drony nie są game changerem tylko dlatego, że można nimi niszczyć sprzęt wojskowy i neutralizować przeciwnika. Bardziej istotna jest zależność koszt – efekt. Drony są relatywnie tanie, a w porównaniu z klasyczną bronią precyzyjną, tj. HIMARS czy JASSM, równie skuteczne. Ich produkcja jest mniej wymagająca i może być prowadzona na masową skalę w przygodnym terenie lub w przysłowiowym garażu.

Kolejnym ważnym elementem w tej układance jest łączenie świata służb specjalnych i wojsk specjalnych. Można to obserwować w Ukrainie, gdzie zarówno wywiad wojskowy HUR, jak i kontrwywiad SBU mają swoje elementy bojowe i skutecznie prowadzą wojskowe operacje specjalne. Dlatego też istotny jest m.in. nasz udział w operacjach specjalnych prowadzonych przez instytucje centralne najwyższego szczebla, aby zmniejszyć potencjał i zdolności operacyjno-strategiczne adwersarza w skali całej wojny, a nie tylko wzdłuż linii frontu. I takie działanie na rzecz tych instytucji należałoby traktować jako główne zadanie dla GROM-u. W polskim obszarze prawnym Wojska Specjalne mogą tworzyć zespoły zadaniowe ze Służbą Kontrwywiadu Wojskowego i Służbą Wywiadu Wojskowego, utrudnione są natomiast możliwości bezpośredniego współdziałania z Agencją Wywiadu, Agencją Bezpieczeństwa Wewnętrznego i Służbą Ochrony Państwa.

Chciałbym zwrócić uwagę na pewien aspekt. Nie należy się łudzić, że przyszły konflikt będzie taki sam jak ten za wschodnią granicą UE, i próbować kopiować pewne rozwiązania w stu procentach. Z rozmów prowadzonych z naszymi ukraińskimi partnerami wynika, że działania wojenne są dynamiczne, a techniki, taktyki i procedury bardzo szybko się dezaktualizują. Powoduje to niekiedy, że do zmian dotyczących narzędzi i procedur dochodzi nawet w cyklu dwutygodniowym, jak już wspomniałem wcześniej. Dlatego tak ważne jest zbieranie informacji z pola walki, ich analiza i wyciąganie poprawnych wniosków, a następnie szybkie podejmowanie decyzji, co i w jakim zakresie należy wdrożyć.

Co w kontekście działań antyterrorystycznych i kontrterrorystycznych powinniśmy przemyśleć i zmienić na poziomie systemowym w Polsce, aby organy ścigania i wojskowe jednostki specjalne mogły współdziałać bez przeszkód i wykorzystywać swój potencjał w przypadku rozpoznania zagrożeń o charakterze terrorystycznym oraz wprowadzenia III lub IV stopnia alarmowego?

Można by powiedzieć, że na pierwszy rzut oka wszystko działa i nie ma o czym dyskutować. Mamy przecież ustawę o działaniach antyterrorystycznych, w której zostały ujęte różne zdarzenia o charakterze terrorystycznym i sposoby reagowania na nie. Gdy wniknie się jednak w szczegóły, weźmie pod uwagę doświadczenia wynikające z ćwiczeń

międzyresortowych, choćby z corocznych ćwiczeń taktyczno-specjalnych Kaper, to sprawa nie przedstawia się już tak optymistycznie. Do przemyślenia są przede wszystkim podstawy prawne. We wspomnianej ustawie jest co prawda zapis o użyciu Wojsk Specjalnych, ale uregulowania dotyczące III lub IV stopnia alarmowego mogą znacznie opóźnić wsparcie pododdziałów układu pozamilitarnego (głównie pododdziałów kontrterrorystycznych Policji) przez Wojska Specjalne. Należy pamiętać, że ataki terrorystyczne charakteryzują się dużą dynamiką i czas ma kluczowe znaczenie w odpowiedzi na nie, a zapisy ustawowe powodują, że nie można działać prewencyjnie, a jedynie reaktywnie. Kolejnym problemem jest to, że ustawa nie przewiduje zarządzania na poziomie rządowym kryzysem związanym z działaniem terrorystycznym (jak w modelu brytyjskim). Jest to cedowane na poziom ministerialny (za granicą odpowiada za to MSZ) lub nawet na poziom służby (działania kontrterrorystyczne będące odpowiedzialnością Policji). To utrudnia użycie wszystkich środków potrzebnych do rozwiązania kryzysu, gdyż często niezbędne jest zaangażowanie sił podległych różnym ministerstwom. Działanie na morzu może przykładowo wymagać udziału jednostek podporządkowanych MSWiA, MON, MSZ (w przypadku wód terytorialnych państwa trzeciego), Ministerstwu Infrastruktury czy też ministrowi koordynatorowi służb specjalnych. Kolejnym problemem jest niespójne prawo. Istnieją ustawy, których zapisy nie korespondują z tymi zawartymi w ustawie antyterrorystycznej. Przykładem może być ustawa o ochronie żeglugi i portów morskich, w której wiodącą rolę przypisano MON. Powstaje dylemat prawny, który akt jest w takich sytuacjach nadrzędny. Organ rządowy zarządzający kryzysem mógłby mieć w tym przypadku głos rozstrzygający, gdyż premier byłby na czele takiej grupy. Takie rozwiązanie przyjęto w Wielkiej Brytanii. Kolejnym elementem wartym przemyślenia jest przećwiczenie w formie gier wojennych różnych potencjalnych scenariuszy zdarzeń. Trzeba sprawdzić, czy przyjęty system podejmowania decyzji i generowania sił jest skuteczny i umożliwia odpowiednio szybką reakcję, adekwatną do dynamiki takiego kryzysu. Kto powinien być zaangażowany w takie gry wojenne? Moim zdaniem na początek ci, którzy zgodnie z obowiązującymi przepisami prawa są zobowiązani do rozwiązania kryzysu terrorystycznego. Dobrze poprowadzone gry wojenne, oparte na różnych scenariuszach, dałyby według mnie odpowiedzi na wiele pytań i dylematów oraz podsunęłyby argumenty

na rzecz zmian prawnych i organizacyjnych. Zanim prawo zostałoby zmienione, gra mogłaby zostać zrealizowana również w modelowej grupie docelowej, aby upewnić się, czy proponowane zmiany są skuteczne, oraz zapoznać rządową grupę zarządzania kryzysowego z procedurami działania.

Ważnym elementem polskiego systemu antyterrorystycznego, który ukształtował się po 11 września 2001 r., była współpraca nieformalna. Jego architekci kładli nacisk na integrowanie działań instytucji i organów państwowych, na budowanie wzajemnego szacunku i zaufania. Dziś u sterów poszczególnych ogniw wspólnoty antyterrorystycznej w RP jest inne pokolenie i obserwujemy rywalizację między różnymi służbami i jednostkami. Podziały były, są i będą, ale chodzi o to, by budować bezpieczeństwo ponad nimi. Jak utrzymać jedność blisko 30 podmiotów poziomu operacyjnego i taktycznego?

Bardzo ciekawe i trudne pytanie. Nie ma co ukrywać – w instytucjach siłowych, które zajmują się szeroko rozumianym bezpieczeństwem państwa, służą osoby z silnymi charakterami, osobowości alfa i z pewnością stanowi to wyzwanie w kontekście budowania bezpieczeństwa ponad podziałami. W dowództwie JW GROM zawsze podkreślamy, że nie chodzi o to, kto jest najlepszy i kto będzie wykonywał zadanie. Najważniejsze jest to, że wszyscy mamy wspólny cel, którym jest zapewnienie bezpiecznego środowiska do rozwoju państwa i poczucia bezpieczeństwa polskim obywatelom, zarówno tym przebywającym w kraju, jak i poza jego granicami. Jeżeli wszyscy to zrozumiemy, to będzie dobrze, a jeśli będziemy się tym kierować w działaniu, to będzie bardzo dobrze. Musimy także pamiętać, że nasze zdolności do odpowiedzi są z jednej strony rozproszone, a z drugiej wystarczające. Mam na myśli to, że np. Siły Zbrojne RP mają większy potencjał w obszarze statków powietrznych czy zdolności do działania na morzu, a Policja i Straż Graniczna mogą szybciej aktywować swoje formacje w razie natychmiastowej potrzeby takiego wygenerowania sił. Z kolei służby specjalne, tj. ABW, AW, SKW i SWW, mają wiedzę i zdolności do przeprowadzenia operacji. Rozwijanie i utrzymywanie zdolności, które zostały już rozwinięte w innym resorcie, jest ekonomicznie nieuzasadnione, ale konieczne są ścisła i wielopłaszczyznowa współpraca oraz kompleksowe i dobrze skoordynowane podejście

do pojawiających się zagrożeń, z określeniem kompetencji i zależności. Następnym ważnym elementem budowania bezpieczeństwa jest stała, wzajemna edukacja międzyresortowa – czy to w postaci konferencji i spotkań roboczych, czy ćwiczeń. Po pierwsze, pozwoli to na nawiązywanie i podtrzymywanie kontaktów, czyli *networking*, a po drugie – na aktualizowanie wiedzy, kto i czym dysponuje. Zawsze pojawia się przy tym pytanie, kto powinien to organizować. Ministerstwa, dowództwa czy jednostki? Odpowiem prosto – każdy, komu zależy na bezpieczeństwie. W GROM-ie uczymy, aby nie być biernym i nie czekać, aż ktoś coś dla nas zrobi, tylko brać na siebie odpowiedzialność i szukać rozwiązań, jeśli widzimy, że system jeszcze nie rozpoznaje problemu. Stąd nacisk na kreatywność, o której wcześniej wspomniałem.

Ostatnia i chyba najbardziej kontrowersyjna propozycja to organizowanie ćwiczeń w postaci tzw. stress testingu, czyli testów przeciążających. Ich scenariusz jest tak projektowany, aby nieprzerwanie poddawać ćwiczących sytuacjom ekstremalnym. Doprowadza to do przeciążenia systemu i poniesienia porażki. Z doświadczenia wiemy, że takie porażki są jak kubeł zimnej wody. Przynosi to pozytywne skutki i sprzyja tworzeniu kreatywnych rozwiązań, gdy ćwiczący spotkają się z podobną sytuacją w przyszłości.

Rozmawiał: Damian Szlachter

studia
analizy
prewencja

TERRORYZM

wydanie specjalne

Zagrożenia terrorystyczne i sabotażowe infrastruktury krytycznej

W numerze m.in.:

- **Wykorzystanie infrastruktury krytycznej w konfliktach hybrydowych**
Studia przypadków ataków na IK. Budowanie odporności IK na przykładzie dyrektyw: CER i NIS 2.

- **Zagrożenia hybrydowe w Europie**
Rosyjskie operacje w państwach UE w świetle analiz Europejskiego Centrum Doskonalenia ds. Przeciwdziałania Zagrożeniom Hybrydowym – Hybrid CoE.

- **Znaczenie Morza Bałtyckiego dla bezpieczeństwa energetycznego państw nadbałtyckich**
Zagrożenia dla obiektów IK na Morzu Bałtyckim i infrastruktury portowej. Możliwości przeciwdziałania.

- **Ukraińska infrastruktura jako cel w wojnie hybrydowej i konwencjonalnej**
Rosyjskie operacje przeciwko IK Ukrainy. Taktyki, broń, odporność i obrona – wnioski z ukraińskich doświadczeń.

- **Cyberprzestrzeń UE jako domena działań hybrydowych**
Aktualne zagrożenia w europejskiej cyberprzestrzeni ze strony grup sponsorowanych przez państwa, grup haktywistycznych i cyberprzestępczych.

- **Ochrona infrastruktury krytycznej przed bezzałogowymi statkami powietrznymi**
Ocena systemów detekcji i neutralizacji bezzałogowych statków powietrznych. Zmiany prawne w Polsce zwiększające ochronę IK przed dronami.

Więcej na:
https://abw.gov.pl/wyd/terroryzm-studia-analizy-prewe/1974,Wstep.html

Numer przygotowany pod egidą Agencji Bezpieczeństwa Wewnętrznego i Rządowego Centrum Bezpieczeństwa w ramach polskiej prezydencji w Radzie UE.

RCB