ZAGROŻENIA TERRORYSTYCZNE I SABOTAŻOWE

infrastruktury krytycznej

Patronat polskiej prezydencji w Radzie UE
Patronage of the polish presidency of the Council of the EU
Patronage de la présidence polonaise du Conseil de l'UE

ABW

RCB

Zagrożenia terrorystyczne i sabotażowe infrastruktury krytycznej

Redakcja naukowa

dr Karolina Wojtasik i dr Damian Szlachter

Redakcja naukowa dr Karolina Wojtasik, dr Damian Szlachter

Recenzenci prof. dr hab. Waldemar Zubrzycki / Akademia Policji w Szczytnie
dr hab. Agata Tyburska / Akademia Policji w Szczytnie

Zespół redakcyjny dr Damian Szlachter (redaktor naczelny), Agnieszka Dębska (sekretarz redakcji, skład), Aleksandra Dąbała, Aneta Olkowska, Izabela Paczesna, Monika Sikora (redakcja, korekta), Izabela Laskus-Rock (korekta), Sylwia Kłobuszewska (tłumaczenie)

Projekt okładki Aleksandra Bednarczyk

ISSN 2720-4383
e-ISSN 2720-6351
ISBN 978-83-968287-7-4

Recenzji zostały poddane wszystkie teksty zamieszczone w numerze specjalnym

Teksty wyrażają poglądy autorów i nie reprezentują stanowiska Agencji Bezpieczeństwa Wewnętrznego i Rządowego Centrum Bezpieczeństwa

Deklaracja o wersji pierwotnej:
Wersja drukowana czasopisma jest jego wersją pierwotną
Numer specjalny ukazał się drukiem tylko w języku angielskim
Wersje elektroniczne są dostępne w dwóch językach: angielskim i polskim
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/

Zamknięto i oddano do druku w maju 2025 r.

Druk
Mazowieckie Centrum Poligrafii Sp. z o.o.
ul. Ciurlionisa 4, 05-270 Marki
tel. 505 727 782

SPIS TREŚCI

Bezpieczeństwo, Europo!

Polska po raz pierwszy przewodniczyła Radzie Unii Europejskiej w drugiej połowie 2011 r. Tuż po rozpoczęciu prezydencji, 22 lipca, doszło do zamachów terrorystycznych w Oslo i na norweskiej wyspie Utøya, stanowiących jedną z najbardziej tragicznych kart w historii terroryzmu w Europie. Sprawca zaatakował w otwartych przestrzeniach publicznych. Od tego momentu ochrona takich miejsc przed skutkami aktywności terrorystycznej to priorytet, zarówno w krajach członkowskich UE, jak i w instytucjach unijnych.

Druga prezydencja Rzeczpospolitej Polskiej w Radzie UE rozpoczęła się w styczniu 2025 r. Polska objęła przewodnictwo w czasach globalnego niepokoju, gdy najważniejszym zadaniem jest zapewnienie bezpieczeństwa unijnych granic zewnętrznych oraz ciągłości świadczenia usług kluczowych w krajach członkowskich UE. Wyrazem tego jest hasło tej prezydencji: „Bezpieczeństwo, Europo!". Dla Agencji Bezpieczeństwa Wewnętrznego oraz Rządowego Centrum Bezpieczeństwa w Polsce to czas podejmowania inicjatyw w kraju i za granicą, mających wspierać budowanie odporności na zagrożenia hybrydowe, ze szczególnych naciskiem na ochronę obiektów infrastruktury krytycznej (IK), krajowej i europejskiej (#OchronaIK).

W odniesieniu do IK temat przewodni polskiej prezydencji ukształtował się pod wpływem:

- wojny w Ukrainie i związanego z nią wzrostu liczby działań hybrydowych, w tym sabotaży podejmowanych przez rosyjskie podmioty wobec obiektów IK sektora energetycznego, transportowego, telekomunikacyjnego, wodociągowego, a także pod wpływem wsparcia udzielanego Ukrainie przez państwa UE i NATO;

- implementacji dyrektywy CER Parlamentu Europejskiego i Rady UE dotyczącej odporności podmiotów krytycznych, która zmienia koncepcję ich ochrony w krajach członkowskich i daje ich rządom nowy impuls do działań w tym strategicznym obszarze.

Numer specjalny czasopisma naukowego „Terroryzm – studia, analizy, prewencja" (T-SAP), przygotowany pod egidą Agencji Bezpieczeństwa Wewnętrznego i Rządowego Centrum Bezpieczeństwa, jest wydaniem tematycznym. Zebraliśmy w nim analizy i studia przypadków dotyczące aktualnych wyzwań związanych z ochroną IK na lądzie i morzu oraz w cyberprzestrzeni krajów UE. Autorami artykułów są eksperci reprezentujący cywilne i wojskowe środowiska akademickie, think tanki i specjalistyczne portale informacyjne, jak również pracownicy administracji państwowej i funkcjonariusze organów ścigania. Prezentują oni problematykę bezpieczeństwa IK z różnych perspektyw, uwzględniających ich kompetencje i doświadczenia.

Publikację otwiera artykuł, w którym omawiamy wykorzystanie IK w konfliktach hybrydowych oraz przedstawiamy analizę porównawczą rozwiązań dotyczących budowania odporności tej infrastruktury wynikających z dyrektyw CER i NIS 2 Parlamentu Europejskiego i Rady UE. Dyrektywa CER ma spowodować diametralne zmiany w budowaniu odporności IK na działania o charakterze terrorystycznym i sabotażowym. W Polsce podstawą projektowanego systemu ochrony IK będzie m.in. idea standaryzacji bezpieczeństwa fizycznego chronionych obiektów, co zostało szczegółowo omówione w jednej z analiz.

W lepszym zrozumieniu ewolucji zagrożeń oraz sposobów ich neutralizacji może pomóc artykuł poświęcony atakom terrorystycznym i sabotażowym na IK, do których doszło w przeszłości. Przyczynkiem do pokazania współczesnego krajobrazu zagrożeń terrorystycznych w UE są natomiast dane zawarte w dorocznych raportach Europolu TE-SAT (*EU Terrorism Situation & Trend Report*) z lat 2021–2024. Wiedzę na ten temat mogą poszerzyć również wyniki przeprowadzonych w 2025 r. badań ankietowych dotyczących percepcji zagrożeń terrorystycznych i sabotażowych. Respondentami byli doradcy

ds. budowania odporności na zagrożenia o charakterze terrorystycznym działający w ramach unijnej inicjatywy EU Protective Security Advisors. Europejscy eksperci ocenili aktualne wyzwania w tym obszarze oraz wskazali możliwości zwiększenia skuteczności działań prewencyjnych i ochronnych. Unijną perspektywę widzenia zagrożeń hybrydowych, zwłaszcza w Europie Środkowo-Wschodniej, przedstawia artykuł poświęcony analizie raportów opracowanych przez European Centre of Excellence for Countering Hybrid Threats w Helsinkach.

Jedną z domen, w których może się toczyć konflikt, jest obszar morski. W numerze specjalnym prezentujemy specyfikę, nasilających się od 2022 r., zagrożeń hybrydowych na Morzu Bałtyckim oraz możliwości przeciwdziałania im ze strony NATO. W artykule autor zwraca szczególną uwagę na zagrożenia, których źródłem są nowoczesne morskie systemy autonomiczne. Jako kraj sprawujący prezydencję w Radzie UE chcemy podzielić się naszymi doświadczeniami w budowaniu zdolności do ochrony obiektów strategicznych przed bezzałogowymi statkami powietrznymi. Prezentujemy to zagadnienie z uwzględnieniem aspektów prawnych i technicznych.

W wydaniu specjalnym podejmujemy również tematykę doświadczeń Ukrainy w przeciwdziałaniu rosyjskim atakom hybrydowym i konwencjonalnym na obiekty IK oraz w zwalczaniu tych działań. Z wojną rosyjsko-ukraińską wiąże się zagadnienie sankcji. W jednym z artykułów omawiamy krajowe indywidualne środki ograniczające wdrożone w Polsce w odniesieniu do podmiotów gospodarczych wspierających działania Federacji Rosyjskiej i Białorusi.

Najwięcej działań hybrydowych wobec obiektów IK krajów UE jest podejmowanych w cyberprzestrzeni. Prezentujemy konkretne incydenty cyberbezpieczeństwa w wybranych państwach europejskich, spowodowane przez grupy sponsorowane przez państwa, haktywistyczne i cyberprzestępcze. Opisujemy również różne strategie raportowania przyjęte przez służby i zespoły odpowiedzialne za cyberbezpieczeństwo krajów UE i NATO, dając zarys zagrożeń cybernetycznych, z którymi obecnie mierzy się Europa.

Ważnym wsparciem w kształtowaniu krajowych i unijnych inicjatyw zwiększających odporność IK na zagrożenia

hybrydowe, w tym terroryzm i sabotaż, są projekty badawcze realizowane z funduszy UE. W związku z tym zdecydowaliśmy, że warto omówić wybrane tematy realizowane w ramach programu Horyzont Europa, który jest jedną z flagowych unijnych inicjatyw w tym obszarze.

W czasie prezydencji Polska wspiera działania wzmacniające europejskie bezpieczeństwo w każdym jego wymiarze: zewnętrznym, wewnętrznym, informacyjnym, ekonomicznym, energetycznym, żywnościowym i zdrowotnym. Numer specjalny T-SAP wpisuje się w te cele, pokazując wieloaspektowość ochrony IK, która stanowi wspólny mianownik tych wszystkich wymiarów. Mamy nadzieję, że zaprezentowane w nim materiały przyczynią się do poszerzenia wiedzy na temat współczesnych zagrożeń dla obiektów IK oraz skutecznych sposobów przeciwdziałania tym niebezpieczeństwom, a także staną się inspiracją nie tylko do dalszych badań i analiz, lecz także do unijnych inicjatyw w obszarze bezpieczeństwa podejmowanych podczas prezydencji kolejnych państw w Radzie UE.

dr Karolina Wojtasik
Rządowe Centrum Bezpieczeństwa

dr Damian Szlachter
Agencja Bezpieczeństwa Wewnętrznego

ARTYKUŁY

Terroryzm – studia, analizy, prewencja, 2025, wydanie specjalne: 13–34

https://doi.org/10.4467/27204383TER.25.001.21504

Artykuł

Infrastruktura krytyczna jako cel działań hybrydowych. Studia przypadków ataków na obiekty i systemy IK

Critical infrastructure as a target for hybrid operations.
Case studies of attacks against the facilities and systems of CI

WITOLD SKOMRA https://orcid.org/0000-0002-2625-6683

Wydział Zarządzania, Politechnika Warszawska
Rządowe Centrum Bezpieczeństwa

KAROLINA WOJTASIK https://orcid.org/0000-0002-1215-5005

Stałe Przedstawicielstwo RP przy Unii Europejskiej
Rządowe Centrum Bezpieczeństwa

Abstrakt

Artykuł przedstawia analizę infrastruktury krytycznej (IK) jako celu ataku w operacjach hybrydowych, które łączą różne formy działań – od konwencjonalnych po terrorystyczne. Autorzy wskazują przyczyny atakowania IK. Podstawę rozważań stanowi teoria 5 pierścieni Wardena. W artykule omówiono operację Allied Force, kampanie dezinformacyjne poprzedzające synchronizację sieci energetycznych państw bałtyckich oraz atak na Colonial Pipeline. Autorzy przeprowadzają analizę porównawczą rozwiązań dotyczących budowania odporności IK wynikających z dyrektyw CER i NIS 2 Parlamentu Europejskiego i Rady Unii Europejskiej.

Słowa kluczowe

infrastruktura krytyczna, ochrona infrastruktury krytycznej, działania hybrydowe, zagrożenia hybrydowe, wojna hybrydowa, dyrektywa CER, dyrektywa NIS 2

Abstract

The article presents an analysis of critical infrastructure (CI) as a target for attack in hybrid operations, which combine various forms of action – from conventional to terrorist. The authors identify the reasons for attacking CI. The considerations are based on Warden's 5 rings theory. The article discusses Operation Allied Force, disinformation campaigns prior to the synchronisation of the Baltic states' energy networks, and the attack on the Colonial Pipeline. The authors conduct a comparative analysis of solutions for building CI resilience derived from the CER and NIS2 Directives of the European Parliament and the Council of the European Union.

Keywords

critical infrastructure, critical infrastructure protection, hybrid operations, hybrid threats, hybrid warfare, CER Directive, NIS 2 Directive

Wprowadzenie

Obecny poziom rozwoju cywilizacyjnego charakteryzuje się uzależnieniem społeczeństw od systemów i usług, które są związane z szeroko pojętą infrastrukturą krytyczną (IK). Prawodawstwo państw członkowskich Unii Europejskiej może różnić się w szczegółach dotyczących liczby systemów zaliczanych do IK, kryteriów uznawania podmiotu czy usługi za kluczowe czy progu zakłócenia takiej usługi, ale żadne nie kwestionuje znaczenia tej infrastruktury w funkcjonowaniu państwa i społeczeństwa. W artykule omówiono, w jaki sposób IK była i jest celem ataków hybrydowych. Ponadto autorzy pokazują, na ile zapisy *Dyrektywy 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* (dalej: dyrektywa CER) oraz *Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu*

cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dalej: dyrektywa NIS 2) wpływają na wzmocnienie odporności IK na te zagrożenia. Podstawę rozważań stanowi teoria 5 pierścieni Wardena[1] oraz pojęcie wojny hybrydowej rozumianej jako konflikt, w którym przeciwnik stosuje kombinację środków konwencjonalnych, nieregularnych, terrorystycznych i przestępczych w celu osiągnięcia swoich celów politycznych. Jednak najważniejszym elementem wojny hybrydowej jest – zdaniem Franka Hoffmana – wpływanie na społeczeństwo przeciwnika w taki sposób, aby wywarło presję na rząd i wymusiło określone działania lub ustępstwa[2].

Infrastruktura krytyczna jako cel ataku hybrydowego

Infrastruktura krytyczna stanowi podstawę funkcjonowania każdego państwa, a jej znaczenie sprawia, że jest szczególnie narażona na działania destabilizacyjne. Istnieje kilka powodów, dla których to właśnie IK jest priorytetowym celem ataków hybrydowych.

Ataki na IK mogą sparaliżować całe państwo. W przeciwieństwie do tradycyjnych operacji militarnych, które koncentrują się na siłach zbrojnych i infrastrukturze wojskowej, ataki hybrydowe na IK uderzają w systemy (np. sieci elektroenergetycznej), od których zależy życie codzienne obywateli i funkcjonowanie gospodarki. W przypadku skoordynowanego ataku na kilka sektorów, np. energetykę, transport i telekomunikację, przeprowadzonego bez użycia konwencjonalnej siły militarnej skutki mogą być porównywalne do działań wojennych.

Najlepiej obrazuje to blackout, do którego doszło w Nowym Jorku 13 lipca 1977 r. W ciągu kilku minut całe miasto zostało pozbawione prądu, co wywołało chaos i falę przestępczości, jakiej nie widziano tam od lat. Do stopniowego przeciążenia systemu elektroenergetycznego doprowadziły uderzenia piorunów w linie przesyłowe. Około godz. 21.27 pierwsze wyładowania atmosferyczne uszkodziły linię przesyłową w hrabstwie Westchester, co spowodowało automatyczne przeniesienie obciążenia na inne części sieci.

[1] G.M. Jackson, *Warden's five-ring system theory: legitimate wartime military targeting or an increased potential to violate the law and norms of expected behavior?,* Alabama 2000, https://apps.dtic.mil/sti/pdfs/ADA425331.pdf [dostęp: 20.02.2025].

[2] F.G. Hoffman, *Conflict in the 21'st Century: The Rise of Hybrid Wars*, Virginia 2007, https://www.comw.org/qdr/fulltext/0712hoffman.pdf, s. 14 [dostęp: 20.02.2025].

Kolejne uderzenie o 21.29 doprowadziło do dalszych zakłóceń, a trzecie o 21.34 unieruchomiło najważniejsze stacje przesyłowe i wywołało efekt domina.

W odróżnieniu od wcześniejszego blackoutu z 1965 r., który przebiegł stosunkowo spokojnie, ten incydent stał się katalizatorem masowych zamieszek, rabunków i aktów przemocy. W ciągu jednej nocy zgłoszono 1809 aktów grabieży i podpaleń, wybuchło 1037 pożarów, aresztowano 2931 osób[3]. Blackout pogłębił napięcia społeczne oraz kryzys gospodarczy, z jakim zmagał się ówczesny 12-milionowy Nowy Jork. Ta amerykańska metropolia w latach 70. XX w. przeżywała recesję związaną z deindustrializacją, rosnącym bezrobociem i wysokim poziomem przestępczości. Deficyt budżetowy miasta, który sięgał miliardów dolarów, doprowadził do cięć w administracji publicznej, w tym ograniczenia liczby policjantów i strażaków. Policja nie była w stanie powstrzymać zamieszek. W wielu miejscach funkcjonariusze unikali konfrontacji i pozwali ludziom na swobodne grabieże. Złodzieje wynosili towary ze sklepów, a nawet wyprowadzali samochody z salonów. Transport publiczny został sparaliżowany, a mieszkańcy, którzy byli poza domem, musieli wracać pieszo przez pogrążone w chaosie ulice. Prąd zaczęto przywracać stopniowo rankiem 14 lipca, a pełne zasilanie przywrócono w całym mieście ok. godz. 10.39. Skutki wydarzenia były odczuwane przez następne miesiące. Wiele małych biznesów nie podniosło się po rabunkach, co jeszcze bardziej pogłębiło kryzys gospodarczy. Wzrosły poczucie zagrożenia i nieufność wobec władz, które nie zdołały zapobiec eskalacji przemocy. Straty materialne oszacowano na ok. 300 mln dolarów[4], co w przeliczeniu na dzisiejsze pieniądze stanowi równowartość ok. 1,5 mld dolarów.

Infrastruktura niezbędna do utrzymania funkcjonowania współczesnego państwa i społeczeństwa składa się z powiązanych ze sobą elementów lub samodzielnych systemów. Stanowi to dodatkową trudność przy ich zabezpieczaniu, ponieważ zarówno w ramach ich elementów składowych, jak i połączeń między nimi wykorzystuje się różne technologie. Mogą to być technologie cyfrowe, oddziaływania i przepływy fizyczne, a także automatyzacja procesów. Wiele sektorów, takich jak sieci elektroenergetyczne czy systemy transportowe, opiera się na skomplikowanych zależnościach. Awaria jednego elementu może wywołać efekt domina, np. atak na system sterowania ruchem kolejowym czy lotniczym może sparaliżować transport krajowy.

[3] *Impact Assessment of the 1977 New York City Blackout*, lipiec 1978, https://www.ferc.gov/sites/default/files/2020-05/impact-77.pdf, s. 23 [dostęp: 23.03.2025].

[4] Tamże, s. 11.

Ponadto podstawą wielu systemów są technologie projektowane przed rozpowszechnieniem internetu, co czyni je podatnymi na ataki hakerskie.

Skala i charakter ataków hybrydowych nie pozwalają na uznanie zdarzenia za konflikt zbrojny, tzn. są to działania poniżej progu wojny. Takie ataki, zwłaszcza prowadzone w sferze cyfrowej, są trudne do atrybucji. Sprawcy często wykorzystują sieci pośredników, botnety lub fałszywe ślady, co niemal uniemożliwia wskazanie atakującego. W przypadku aktów fizycznego sabotażu, takich jak uszkodzenie kabli podmorskich czy rurociągów, sprawcy mogą upozorować niewyjaśnioną awarię czy działania grup terrorystycznych. To sprawia, że zaatakowane państwo ma ograniczone możliwości reakcji. Prześladowca prowadzi działania destabilizujące i unika oficjalnej konfrontacji zbrojnej.

Działania hybrydowe (np. atak ransomware lub sabotaż przemysłowy) charakteryzuje relatywnie niski koszt ataku przy wysokich kosztach odbudowy dla zaatakowanego podmiotu. Przeprowadzenie skutecznego cyberataku na sieć elektroenergetyczną, system bankowy czy transportowy wymaga znacznie mniejszych nakładów finansowych niż klasyczne operacje wojskowe. Przykładem jest atak na Colonial Pipeline w 2021 r., o czym szerzej w dalszej części artykułu.

Jednym z powodów dużej skuteczności ataków hybrydowych jest ich multiwektorowość, czyli możliwość łączenia różnych form ataku. Przykładowy scenariusz ataku na IK może obejmować jednocześnie:

- cyberatak na sieci przesyłowe, który wywołuje przerwy w dostawie prądu;
- sabotaż, np. podłożenie ładunku wybuchowego na ważnym węźle infrastrukturalnym;
- kampanię dezinformacyjną, w której sugeruje się, że awaria to wynik korupcji lub nieudolności rządu;
- spekulacje finansowe, które uderzają w wartość waluty krajowej i destabilizują gospodarkę.

Tego typu działania, jeśli są dobrze skoordynowane, mogą wywołać chaos o skali porównywalnej do konfliktu zbrojnego. Ataki na IK często mają na celu nie tylko fizyczne uszkodzenie infrastruktury, lecz także wywołanie efektu psychologicznego. W społeczeństwach, które tracą dostęp do podstawowych usług, rośnie niezadowolenie, pojawiają się teorie spiskowe i spada zaufanie do rządu oraz instytucji publicznych. W sytuacji kryzysowej mogą się pojawić zamieszki, masowe protesty, a w konsekwencji – destabilizacja polityczna.

Niezależnie od wspomnianej destabilizacji atak na IK może być elementem wojny gospodarczej i narzędziem politycznego szantażu. Współczesna rywalizacja między państwami coraz częściej przenosi się na poziom infrastrukturalny. Blokowanie głównych tras transportowych, niszczenie rurociągów czy zakłócanie pracy systemów bankowych to działania mogące wymusić ustępstwa polityczne. Przykładem jest sabotaż gazociągów Nord Stream w 2022 r., który miał wymiar zarówno ekonomiczny, jak i polityczny, a jednocześnie wpłynął na bezpieczeństwo energetyczne Europy.

Dodatkowym problemem związanym z ochroną IK jest fakt, że często obejmuje ona zarówno elementy publiczne, jak i prywatne. W wielu krajach sieci energetyczne są zarządzane przez firmy prywatne, które realizują cele przede wszystkim biznesowe, a zapewnienie społeczeństwu dostępu do usługi nie jest dla nich priorytetem.

Cyberataki to jeden z głównych wektorów ataków hybrydowych na IK. Narzędzia takie jak ransomware, malware czy ataki DDoS mogą być używane do destabilizacji sieci elektroenergetycznych, systemów finansowych czy łańcuchów logistycznych. Cyberprzestrzeń umożliwia przeprowadzenie ataku z dowolnego miejsca na świecie, co utrudnia identyfikację sprawców. Tak było w 2015 r. w przypadku cyberataku na ukraińską sieć elektroenergetyczną. Hakerzy wykorzystali wówczas złośliwe oprogramowanie Black Energy do przejęcia kontroli nad systemami sterowania i wyłączenia podstacji energetycznych, co spowodowało masowe przerwy w dostawie prądu. Podejrzewano, że ataku dokonały rosyjskie grupy hakerskie, ale nie znaleziono na to dowodów[5].

Ataki, takie jak sabotaż gazociągów, podmorskich kabli telekomunikacyjnych czy istotnych węzłów infrastruktury transportowej, mogą być przedstawiane jako wypadek lub awaria techniczna. Tak było w przypadku wspomnianego uszkodzenia gazociągów Nord Stream. Wiele państw uznało to zdarzenie za sabotaż, ale brakowało jednoznacznych dowodów pozwalających na wskazanie zleceniodawcy[6]. Podobnie było w 2019 r. w Arabii Saudyjskiej, gdzie przeprowadzono atak dronowy na instalacje naftowe

[5] K. Gapiński, *Blackout w zachodniej Ukrainie – cyberatak o wymiarze międzynarodowym*, Fundacja im. Kazimierza Pułaskiego, 20.01.2016, https://pulaski.pl/komentarz-blackout-w-zachodniej-ukrainie-cyber-atak-o-wymiarze-miedzynarodowym/ [dostęp: 23.03.2025].

[6] Zob. np. S. Kardaś, A. Łoskot-Strachota, *Dywersja na gazociągach Nord Stream 1 i Nord Stream 2*, Ośrodek Studiów Wschodnich, 29.09.2022, https://www.osw.waw.pl/pl/publikacje/analizy/2022-09-29/dywersja-na-gazociagach-nord-stream-1-i-nord-stream-2 [dostęp: 23.03.2025].

Aramco. Doprowadziło to do czasowego wstrzymania produkcji ropy naftowej, co wpłynęło na światowe ceny surowca[7]. Choć do ataku przyznała się grupa jemeńskich rebeliantów Huti, to w wielu analizach sugerowano, że operacja mogła być wspierana przez Iran[8].

Ataki na IK często są łączone z działaniami dezinformacyjnymi. Po cyberataku na systemy bankowe lub infrastrukturę energetyczną mogą się pojawiać w sieci zmanipulowane informacje, że władze nie radzą sobie z sytuacją lub że awaria była wynikiem wewnętrznych problemów, np. korupcji czy słabości rządu. Tego typu kampanie mają na celu osłabienie zaufania społeczeństwa do instytucji państwowych i wywołanie paniki.

Cybernetyczny atak na IK trudno jednoznacznie sklasyfikować jako akt wojny, co z perspektywy sprawcy jest największą zaletą. O ile bezpośredni atak militarny na IK mógłby spotkać się z reakcją zbrojną, o tyle atak przeprowadzony przez sieć internetową czy sabotaż mogą zostać uznane za działania o niejasnym charakterze. Jeśli nie można jednoznacznie wskazać sprawcy, trudno podjąć działania odwetowe i zaangażować w nie sojuszników. Nawet jeśli istnieją podejrzenia w kwestii odpowiedzialności określonego kraju, to wątpliwości co do dowodów mogą sprawić, że możliwości dyplomatycznej lub militarnej odpowiedzi będą ograniczone. Ataki na IK są skuteczne nie tylko dlatego, że powodują ogromne straty, lecz także dlatego, że sprawcy mogą działać anonimowo i bezkarnie.

Teoretyczne ramy odniesienia

Podstawy teorii 5 pierścieni Wardena można wywodzić z dzieła Carla von Clausewitza pt. *O wojnie*[9]. Clausewitz zauważa, że aby skutecznie pokonać przeciwnika, państwo powinno skierować wszystkie swoje wysiłki

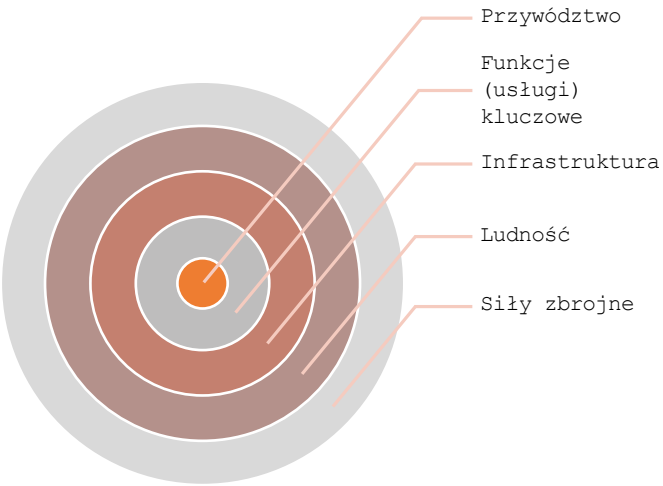
[7] A. Polus, *Atak na rafinerię w Arabii Saudyjskiej i jego konsekwencje dla Afryki*, Polskie Centrum Studiów Afrykanistycznych, 18.09.2019, https://pcsa.org.pl/atak-na-rafinerie-w-arabii-saudyjskiej-i-konsekwencje-dla-afryki/ [dostęp: 23.03.2025].

[8] Zob. np. G. Psujek, *Tajemnica ataku na saudyjską rafinerię*, Rzeczpospolita, 22.09.2019, https://radar.rp.pl/przemysl-obronny/art17499861-tajemnica-ataku-na-saudyjska-rafinerie [dostęp: 23.03.2025]; R. Muczyński, *Atak na saudyjskie rafinerie*, Milmag, 16.09.2019, https://milmag.pl/atak-na-saudyjskie-rafinerie/ [dostęp: 23.03.2025]; *CNN: Według ekspertów atak na Aramco nastąpił z Iranu*, Interia Wydarzenia, 18.09.2019, https://wydarzenia.interia.pl/zagranica/news-cnn-wedlug-ekspertow-atak-na-aramco-nastapil-z-iranu,nId,3209902 [dostęp: 23.03.2025].

[9] C. von Clausewitz, *O wojnie*, Warszawa 2022.

przeciwko tzw. punktom ciężkości, od których zależy istnienie wrogiego państwa. John Ashley Warden III[10] rozwinął tę zasadę, tworząc koncepcję ukierunkowaną na wybór celów w czasie wojny. Teoria 5 pierścieni Wardena służy do identyfikacji i hierarchizacji celów wojennych. Zakłada ona, że państwo można przedstawić jako system składający się z 5 koncentrycznych pierścieni (kręgów), z których każdy reprezentuje inny poziom strategicznego znaczenia. Są to przedstawione na rysunku 1:

1) przywództwo (władze państwowe i wojskowe),
2) zasoby systemowe niezbędne do funkcjonowania państwa i prowadzenia wojny,
3) infrastruktura, która łączy wszystkie elementy systemu,
4) ludność (cywile),
5) siły zbrojne (wojsko i sprzęt wojskowy).



Rysunek 1. Teoria 5 pierścieni Wardena.

Źródło: opracowanie własne na podstawie: G.M. Jackson, *Warden's five-ring system theory: legitimate wartime military targeting or an increased potential to violate the law and norms of expected behavior?*, Alabama 2000, https://apps.dtic.mil/sti/pdfs/ADA425331.pdf, s. 4 [dostęp: 20.02.2025].

[10] John Ashley Warden III – urodzony w 1943 r. amerykański strateg wojskowy z United States Air Force. Podczas wojny w Zatoce Perskiej (1990–1991) stworzył teorię 5 pierścieni, w której określił środki ciężkości (najbardziej wrażliwe elementy struktury państwa) i jednocześnie wskazał lotnictwo jako jedyną formację, która może zaatakować wnętrze każdego pierścienia bez przebijania się przez pozostałe.

Zaatakowanie wewnętrznych kręgów (przywództwo, niezbędne zasoby systemowe) wywołuje szybki paraliż i zakończenie konfliktu. Atakowanie zewnętrznych kręgów (ludność, siły zbrojne) jest mniej efektywne i może przedłużać wojnę.

Jeśli nie uda się skutecznie zaatakować przywództwa, Warden wskazuje następny cel, którym są zasoby systemowe (funkcje, usługi) niezbędne dla przeciwnika, m.in.: zaopatrzenie w energię elektryczną, ropę naftową, żywność i finanse. Ich zniszczenie może pozbawić państwo zdolności do prowadzenia działań wojennych, ale jednocześnie może zagrozić przetrwaniu ludności cywilnej. Według Wardena IK to elementy, takie jak drogi, lotniska, fabryki i inne, które umożliwiają funkcjonowanie państwa jako całości.

Teoria Wardena służyła ustalaniu priorytetów dla lotnictwa wykorzystywanego we współczesnej wojnie. Jednak płynące z niej wnioski mają szersze znaczenie. Kolejne poziomy (pierścienie) wskazują na ważność danego elementu dla funkcjonowania państwa. Warto zwrócić uwagę, że według tej teorii wojna XXI w. polega na tym, że siły zbrojne są atakowane na końcu lub wcale. Cele polityczne mają być osiągane przez eliminację przywództwa, blokadę najważniejszych funkcji państwa i zniszczenie infrastruktury, która tym funkcjom służy. Nadzwyczaj dobrze koresponduje to z rozważaniami o wojnie hybrydowej.

Wykorzystanie infrastruktury krytycznej w konfliktach hybrydowych

Realizacja celów politycznych bez udziału sił zbrojnych

Szczególnym przypadkiem osiągania celów politycznych przez oddziaływanie na IK była operacja Allied Force, czyli kampania bombardowań przeprowadzona przez wojska Sojuszu Północnoatlantyckiego przeciwko Jugosławii (Serbii i Czarnogórze) podczas wojny w Kosowie w 1999 r. W ten sposób chciano zmusić reżim Slobodana Miloševicia do zakończenia czystek etnicznych w Kosowie.

Bombardowania koncentrowały się początkowo na obiektach wojskowych, ale później rozszerzono je na ważną dla funkcjonowania państwa infrastrukturę, taką jak mosty (np. na Dunaju w Nowym Sadzie, którego zniszczenie miało sparaliżować transport), drogi i linie kolejowe (w tym atak na pociąg pasażerski na moście w Grdelicy), infrastrukturę lotniczą (lotnisko w Podgoricy), stacje telewizyjne i radiowe (np. atak na siedzibę

serbskiej telewizji RTS w Belgradzie, w wyniku którego zginęło 16 cywilów), zakłady przemysłowe (rafinerie, fabryki) oraz energetyczne (np. elektrownie, których bombardowanie doprowadziło do masowych przerw w dostawie prądu). Serbia poniosła ogromne straty gospodarcze, koszty odbudowy po nalotach szacowano na ok. 30–100 mld dolarów[11]. Zniszczenie obiektów cywilnych spotkało się z międzynarodową krytyką, ponieważ spowodowało ogromne problemy dla ludności. Operacja Allied Force wywołała także kontrowersje prawne, ponieważ zgodnie z prawem międzynarodowym (m.in. Protokołem I do Konwencji genewskich z 12 sierpnia 1949 r. dotyczącym ochrony ofiar międzynarodowych konfliktów zbrojnych[12]) atakowanie obiektów niezbędnych do przetrwania ludności cywilnej jest zabronione. Dowództwo NATO argumentowało jednak, że ta infrastruktura miała znaczenie również militarne, np. mosty wykorzystywano do transportu wojskowego. Allied Force była pierwszą w historii interwencją NATO bez mandatu Organizacji Narodów Zjednoczonych, co do dziś pozostaje przedmiotem debat prawnych i politycznych. Niezależnie od tych kontrowersji cele polityczne zostały osiągnięte bez wprowadzania żołnierzy na teren wrogiego państwa.

Oddziaływanie na społeczeństwo

Przytoczona na początku artykułu definicja wojny hybrydowej Hoffmana podkreśla oddziaływanie na społeczeństwo jako najważniejszy element strategii przeciwnika. Podobne podejście można znaleźć w koncepcji wojny nielinearnej Walerija Gierasimowa[13], gdzie głównymi narzędziami są manipulacja informacyjna, dezinformacja i działania psychologiczne,

[11] N. Stawarz, *„Nielegalne, ale moralne"? Operacja „Allied Force": przyczyny i konsekwencje*, Histmag.org, 24.03.2019, https://histmag.org/Nielegalne-ale-moralne-Operacja-Allied-Force-przyczyny-i-konsekwencje-18428? [dostęp: 23.03.2025]; R. Górski, *Specjalna operacja wojskowa NATO: bombardowanie Jugosławii*, Instytut Spraw Obywatelskich, 24.03.2023, https://instytutsprawobywatelskich.pl/specjalna-operacja-wojskowa-nato-bombardowanie-jugoslawii/ [dostęp: 23.03.2025].

[12] *Protokoły dodatkowe do Konwencji genewskich z 12 sierpnia 1949 r., dotyczący ochrony ofiar międzynarodowych konfliktów zbrojnych (Protokół I) oraz dotyczący ochrony ofiar niemiędzynarodowych konfliktów zbrojnych (Protokół II), sporządzone w Genewie dnia 8 czerwca 1977 r.*

[13] M.K. McKew, *The Gerasimov Doctrine. It's Russia's new chaos theory of political warfare. And it's probably being used on you*, Politico, wrzesień/październik 2017, https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538/ [dostęp: 23.03.2025].

które mają doprowadzić do destabilizacji społecznej i zmiany decyzji politycznych rządu pod presją własnych obywateli.

Szerzenie dezinformacji, propagandy oraz manipulowanie informacjami prowadzi do erozji zaufania publicznego, podważania autorytetu instytucji państwowych i międzynarodowych, a w konsekwencji – fundamentów demokracji. Osłabia to również pozycję państwa na arenie międzynarodowej. Aby wywołać niepokoje społeczne, protesty oraz podziały wewnętrzne, atakujący wykorzystują różne środki, takie jak media społecznościowe, fałszywe wiadomości czy cyberataki. Wysokie ceny energii elektrycznej, strach przed technologią 5G czy elektrownią jądrową to przykłady zagadnień, wokół których buduje się narrację dezinformacyjną. W tych działaniach szczególną rolę odgrywa IK.

Przed synchronizacją sieci energetycznych krajów bałtyckich z europejskim systemem elektroenergetycznym, do której doszło w lutym 2025 r., odnotowano nasilenie kampanii dezinformacyjnych na Litwie, Łotwie i w Estonii. Działania te były szczególnie intensywne w okresie poprzedzającym odłączenie od rosyjskiego systemu BRELL i przyłączenie do europejskiej sieci. Główne wątki dezinformacyjne koncentrowały się na kilku zagadnieniach. Po pierwsze – groźba przerw w dostawach prądu. Rozpowszechniano informacje sugerujące, że synchronizacja z europejskim systemem doprowadzi do długotrwałych blackoutów. W Estonii takie doniesienia spowodowały wzrost sprzedaży generatorów prądu, gdyż mieszkańcy obawiali się nawet trzydniowych przerw w dostawie energii[14]. Po drugie – wzrost cen energii. Pojawiały się pogłoski, że przyłączenie do europejskiej sieci wywoła znaczny wzrost cen prądu dla konsumentów, a co za tym idzie – wzrost cen podstawowych produktów i w efekcie ubożenie społeczeństwa. Litewski minister do spraw energii Žygimantas Vaičiūnas ostrzegał przed takimi dezinformacjami oraz zapewniał o stabilności systemu i braku podstaw do obaw o wzrost cen[15]. Po trzecie – niewydolność nowego systemu. Propagowano tezy o rzekomej zawodności europejskiego

[14] *Rosyjski atak dezinformacją ws. energetyki. Estończycy wykupują generatory, służby w stanie gotowości*, Polskie Radio 24, 6.02.2025, https://polskieradio24.pl/artykul/3480519,rosyjski-atak-dezinformacja-ws-energetyki-estonczycy-wykupuja-generatory-sluzby-w-stanie-gotowosci [dostęp: 20.02.2025].

[15] *Minister ostrzega mieszkańców przed możliwą dezinformacją*, Made in Vilnius, 4.02.2025, https://madeinvilnius.lt/pl/Aktualno%C5%9Bci/Lietuvos-naujienos/Minister-ostrzega-mieszka%C5%84c%C3%B3w-przed-mo%C5%BCliw%C4%85-dezinformacj%C4%85/ [dostęp: 20.02.2025].

systemu elektroenergetycznego i sugerowano, że kraje bałtyckie mogą doświadczyć problemów technicznych po odłączeniu od rosyjskiej sieci[16]. Ta kampania dezinformacyjna nasiliła się, zwłaszcza ze strony rosyjskich mediów, po synchronizacji sieci. Badania przeprowadzone przez litewską firmę Mediaskopas wykazały, że po odłączeniu się krajów bałtyckich od poradzieckiego systemu i przyłączeniu do europejskiego systemu przesyłowego CESA liczba artykułów na ten temat w rosyjskich mediach wzrosła z 3650 do ponad 8000. Przedstawiano w nich apokaliptyczne scenariusze, w których sugerowano, że kraje bałtyckie stoją w obliczu kryzysu energetycznego z powodu porzucenia współpracy z Rosją[17]. Władze oraz eksperci ds. energetyki tych krajów regularnie dementują te informacje. Zapewniają o stabilności i bezpieczeństwie nowego systemu. Aby podważyć te zapewnienia, przecięto jeden z podmorskich kabli elektroenergetycznych. Chodzi o kabel EstLink 2 łączący Finlandię z Estonią, o przepustowości 650 MW i długości 170 km, w tym 145 km pod dnem Zatoki Fińskiej. Dnia 25 grudnia 2024 r. ok. południa doszło do przerwania tego połączenia, będącego ważnym elementem infrastruktury energetycznej między krajami bałtyckimi. Operator sieci, firma Fingrid, poinformował o zakłóceniach w przesyle prądu i wszczął dochodzenie w celu ustalenia przyczyn awarii. Fińskie władze zatrzymały podejrzewany o spowodowanie uszkodzenia tankowiec Eagle S – statek pływający pod banderą Wysp Cooka, który przewoził benzynę bezołowiową z rosyjskich portów. Domniemano, że należał on do rosyjskiej tzw. floty cieni. Wstępne ustalenia sugerowały, że przecięcie kabla mogło być spowodowane przez kotwicę statku[18]. Skomplikowana i kosztowna naprawa EstLink 2 potrwa prawdopodobnie do 1 sierpnia 2025 r. i pochłonie dziesiątki milionów euro. Mimo awarii dostawy energii elektrycznej dla fińskich odbiorców pozostały niezakłócone. Jednak brak tego połączenia ograniczył eksport energii z Finlandii i w efekcie średnia cena energii w Estonii wzrosła od stycznia do lutego 2025 r. niemal

[16] *Przed synchronizacją z Europą służby ostrzegają przed dezinformacją*, TVP Wilno, 3.02.2025, https://wilno.tvp.pl/84820950/przed-synchronizacja-z-europa-sluzby-ostrzegaja-przed-dezinformacja [dostęp: 20.02.2025].

[17] *Po synchronizacji sieci energetycznych krajów bałtyckich z Europą zaktywizowała się propaganda Kremla*, Polska Agencja Prasowa, 20.02.2025, https://www.pap.pl/aktualnosci/po-synchronizacji-sieci-energetycznych-krajow-baltyckich-z-europa-zaktywizowala-sie [dostęp: 20.02.2025].

[18] *Awaria kabla EstLink 2. Rosyjski tankowiec podejrzany o akt sabotażu*, PolskieRadio.pl, 26.12.2024, https://www.polskieradio.pl/399/7977/artykul/3463666%2Cawaria-ka%20bla-estlink-2-rosyjski-tankowiec-podejrzany-o-akt-sabotazu? [dostęp: 20.02.2025].

dwukrotnie i wyniosła 184 EUR/MWh. Dla porównania, w lutym poprzedniego roku ta cena wynosiła 75,5 EUR/MWh[19]. Po uszkodzeniu kabla średnia hurtowa cena energii elektrycznej na Litwie wzrosła w ciągu tygodnia o 41% z 56 EUR/MWh do 79 EUR/MWh[20]. Incydent związany z uszkodzeniem EstLink 2 wywołał niepokój wśród mieszkańców krajów bałtyckich dotyczący stabilności dostaw energii oraz potencjalnych dalszych wzrostów cen. Cele atakującego zostały osiągnięte.

Warto zauważyć, że podobne kampanie dezinformacyjne były obserwowane w innych krajach UE. Próbowano w nich obarczać UE odpowiedzialnością za podwyżki cen energii.

Oddziaływanie na rząd

Dnia 7 maja 2021 r. doszło do jednego z najpoważniejszych cyberataków na IK w Stanach Zjednoczonych. Celem był Colonial Pipeline[21], największy system rurociągowy na Wschodnim Wybrzeżu USA, który transportuje ok. 45% dostaw paliwa w tym regionie. Hakerzy wykorzystali oprogramowanie ransomware, zaszyfrowali dane firmowe i zażądali okupu. W wyniku ataku rurociąg wstrzymał działalność, co doprowadziło do poważnych zakłóceń w dostawach paliwa. Władze zareagowały natychmiast. Administracja prezydenta USA Joe Bidena ogłosiła stan wyjątkowy, aby umożliwić transport paliwa alternatywnymi środkami. Właściciel Colonial Pipeline, który chciał jak najszybciej przywrócić funkcjonowanie systemu, zapłacił hakerom okup w wysokości 4,4 mln dolarów w bitcoinach[22]. Przywrócenie pełnej działalności rurociągu zajęło jednak kilka dni. W tym czasie na Wschodnim Wybrzeżu USA zaczęło brakować paliwa. To wywołało

[19] *Jak uszkodzenie Estlink 2 wpływa na ceny energii w Estonii*, Czas Wschodni, 14.02.2025, https://czaswschodni.pl/art/wiadomosci/jak-uszkodzenie-estlink-2-wplywa-na-ceny-energii-w-estonii_116f1090-c456-4bb7-abc1-c340f6da6cf5 [dostęp: 20.02.2025].

[20] *Uszkodzenie kabla EstLink 2 podniosło ceny energii w krajach bałtyckich*, BalticWind.EU, 3.01.2025, https://balticwind.eu/pl/uszkodzenie-kabla-estlink-2-podnioslo-ceny-energii-w-krajach-baltyckich/ [dostęp: 20.02.2025].

[21] M. Perzyński, *Raport: O Colonial Pipline i zimnej wojnie w energetyce*, Biznesalert, 15.05.2021, https://biznesalert.pl/raport-colonial-pipeline-cyberatak-usa-rosja-energetyka/ [dostęp: 23.03.2025].

[22] *Prezes Colonial Pipeline potwierdza: zapłaciliśmy okup hakerom*, CyberDefence24, 20.05.2021, https://cyberdefence24.pl/biznes-i-finanse/prezes-colonial-pipeline-potwierdza-zaplacilismy-okup-hakerom [dostęp: 23.03.2025]; W. Urbanek, *Colonial Pipeline: niepożądana sława*, CRN, 24.06.2021, https://crn.pl/artykuly/colonial-pipeline-niepozadana-slawa/ [dostęp: 23.03.2025].

panikę wśród konsumentów, którzy masowo wykupywali benzynę i w ten sposób kryzys się pogłębiał. W niektórych stanach, np. w Karolinie Północnej, ponad 70% stacji benzynowych zgłaszało problemy z zaopatrzeniem. Za atak odpowiadała grupa hakerska DarkSide, działająca z Rosji. Atak na Colonial Pipeline ujawnił podatność amerykańskiej IK na cyberataki, co skłoniło administrację Bidena do zaostrzenia regulacji w zakresie cyberbezpieczeństwa dla sektora energetycznego[23]. Wprowadzono nowe wymogi dla operatorów IK, zobowiązujące ich do podjęcia dodatkowych środków ochrony przed atakami ransomware. Incydent nasilił napięcia między Waszyngtonem a Moskwą. Prezydent Biden zwrócił uwagę, że Kreml ponosi odpowiedzialność za egzekwowanie kontroli nad grupami cyberprzestępczymi działającymi w granicach Rosji, a DarkSide działało z terytorium tego kraju. Warto zauważyć, że wiosną 2021 r. USA i Niemcy prowadziły intensywne rozmowy dotyczące ukończenia gazociągu Nord Stream 2, który miał dostarczać rosyjski gaz bezpośrednio do Niemiec, z ominięciem Ukrainy i Polski. Administracja Bidena wyrażała obawy, że projekt zwiększy zależność Europy od rosyjskiego gazu i osłabi bezpieczeństwo energetyczne regionu. Mimo sprzeciwu wobec Nord Stream 2 amerykański rząd nie nałożył bezpośrednich sankcji na Nord Stream 2 AG – główną spółkę odpowiedzialną za budowę gazociągu – oraz jej prezesa Matthiasa Warniga[24]. Zamiast tego USA skupiły się na wypracowaniu porozumienia z Niemcami, które uwzględniałoby obawy dotyczące bezpieczeństwa energetycznego Europy Środkowo-Wschodniej. W lipcu 2021 r. USA i Niemcy zakończyły negocjacje. Berlin zobowiązał się do podjęcia działań w przypadku, gdyby Rosja próbowała użyć energii jako broni przeciwko Ukrainie lub innym krajom regionu, a także do wykorzystania wszelkich dostępnych środków nacisku w celu przedłużenia o 10 lat umowy tranzytowej między Rosją a Ukrainą, która wygasała w 2024 r. Ponadto Niemcy zgodziły się na utworzenie funduszu o wartości co najmniej 175 mln dolarów na wspieranie transformacji energetycznej i poprawę bezpieczeństwa energetycznego

[23] *Statement from CISA Acting Director Wales on Executive Order to Improve the Nation's Cybersecurity and Protect Federal Networks*, America's Cyber Defense Agency, 13.05.2021, https://www.cisa.gov/news-events/news/statement-cisa-acting-director-wales-executive-order-improve-nations-cybersecurity-and-protect [dostęp: 20.02.2025].

[24] W. Jakóbik, *USA mogą na dniach zadać nowy cios Nord Stream 2, ale unikają deklaracji*, Biznes Alert, 14.05.2021, https://biznesalert.pl/nord-stream-2-sankcje-usa-poszerzone-energetyka-gaz/ [dostęp: 20.02.2025].

Ukrainy[25]. Nie znaleziono bezpośrednich powiązań grupy hakerskiej z rosyjskimi służbami. Można zaryzykować jednak tezę, że cyberatak na ważne ogniwo amerykańskiego systemu energetycznego miał uzmysłowić administracji Joe Bidena, że działania na szkodę Federacji Rosyjskiej mogą się spotkać ze zdecydowaną, choć niebezpośrednią reakcją.

Postrzeganie działań hybrydowych w horyzoncie czasowym

Horyzont czasowy jest ważnym zagadnieniem, które należy brać pod uwagę przy rozważaniach na temat wykorzystywania IK w wojnie hybrydowej. Pierwszy jego wymiar to efekt zaskoczenia, czyli znalezienie takiej podatności lub wymyślenie takiego scenariusza ataku, który nie był dotąd rozpatrywany. Jest to atak, który nie spowoduje natychmiastowej reakcji, ponieważ nie istnieją odpowiednie ramy prawne, zarówno w kontekście procedury reagowania, wyznaczonego organu odpowiedzialnego za bezpieczeństwo IK, jak i sankcji karnej. Drugi wymiar dotyczy tego, że ograniczona możliwość przeprowadzenia analizy ryzyka pod kątem podatności na atak hybrydowy znacznie utrudnia zapewnienie ochrony IK. Trudno przewidzieć, czy dany obiekt będzie potencjalnym celem ataku hybrydowego. Jego typowe parametry (rodzaj produkcji, współzależności, potencjalne straty, liczba ludności, na którą oddziałuje itp.) i scenariusze ataku mogą mieć odmienne znaczenie dla użytkownika obiektu i dla atakującego. Na przykład dużym zainteresowaniem grup hakerskich cieszą się lokalne obiekty wodno-kanalizacyjne, które z punktu widzenia państwa mają niewielkie znaczenie[26]. Atak na tego rodzaju miejsce, nawet jeśli będzie dotkliwy dla społeczności lokalnej, nie wywoła kryzysu w kraju, chyba że agresor zdecyduje się na jednoczesny atak na więcej słabo zabezpieczonych instalacji. Efekt skali może wtedy spowodować reakcję mediów podobną do tej, jaka następuje po ataku na jedną dużą instalację. Trzeci wymiar horyzontu

[25] S. Lewis, A. Shalal, *U.S., Germany strike Nord Stream 2 pipeline deal to push back on Russian 'aggression'*, Reuters, 22.07.2021, https://www.reuters.com/business/energy/us-germany-deal-nord-stream-2-pipeline-draws-ire-lawmakers-both-countries-2021-07-21/ [dostęp: 20.02.2025].

[26] Zob. np. *Doniesienia o rosyjskim cyberataku. Pojawił się polski wątek*, Wirtualna Polska, 17.04.2024, https://wiadomosci.wp.pl/rosyjski-cyberatak-na-polska-infrastrukture-ofiara-oczyszczalnia-sciekow-7017937180834752a [dostęp: 20.02.2025]; *Atak hakerski na oczyszczalnię ścieków*, iSokolka.eu, 8.10.2024, https://isokolka.eu/kuznica/59444-atak-hakerski-na-oczyszczalnie-sciekow [dostęp: 20.02.2025].

czasowego to pozyskiwanie informacji, które mogą mieć militarne czy dezinformacyjne znaczenie w długiej perspektywie czasowej. Operacje hybrydowe niejednokrotnie są planowane na lata. Obiekt, który dziś nie ma strategicznego znaczenia, może w przyszłości pełnić ważną funkcję, np. jako część jakiegoś sytemu.

Budowanie odporności infrastruktury krytycznej na przykładzie dyrektyw: CER i NIS 2

Dyrektywa CER ma doprowadzić do osiągnięcia takiego poziomu odporności IK, aby zapobiegać skutkom zakłócenia usług kluczowych realizowanych za jej pomocą. Zgodnie z założeniami tej dyrektywy państwa członkowskie są zobowiązane do ustalenia listy tych usług oraz wskazania podmiotów krytycznych odpowiedzialnych za ich świadczenie. Każdy z tych podmiotów, aby przeciwdziałać skutkom zakłóceń, musi spełniać wymagania dotyczące odporności (art. 6 ust. 1 i 2 dyrektywy CER). Krajowe strategie odporności podmiotów krytycznych muszą obejmować identyfikację zagrożeń, ocenę ryzyka oraz wypracowanie środków zapobiegawczych, w tym ochronę przed zagrożeniami hybrydowymi (art. 5 ust. 1). Ponadto w dyrektywie CER zidentyfikowano wyzwania, które wynikają z coraz bardziej złożonych łańcuchów dostaw między podmiotami. Dlatego muszą one oceniać ryzyko związane z zależnościami w łańcuchu dostaw oraz stosować odpowiednie środki w celu zapewnienia ciągłości działania. W związku z tym w dyrektywie CER wskazano konieczność ustalenia alternatywnych dostawców i planów awaryjnych (art. 12 ust. 2). Podmioty są zobowiązane do utrzymywania zdolności operacyjnych w sytuacjach kryzysowych, z uwzględnieniem współzależności między różnymi podmiotami i sektorem krytycznym (art. 11 ust. 2). Dyrektywa wymaga analizy ryzyka i planów awaryjnych (art. 12 ust. 1), ale brakuje w niej wytycznych do przewidywania działań adwersarza oraz skutecznego zarządzania ryzykiem w złożonych strukturach organizacyjnych. Dyrektywa nakłada obowiązek ciągłego monitorowania i oceny zagrożeń, ale nie przewiduje mechanizmów, które mogłyby uwzględniać nieoczywiste cele ataków hybrydowych. Nie można, jak dowiedziono, przewidzieć, co będzie ważne dla przeciwnika. Tym samym podmioty, które nie zostały zidentyfikowane jako kluczowe, mogą z jakiegoś nieznanego obecnie powodu zostać zaatakowane, co będzie łatwiejsze ze względu na niższy – niż w przypadku

podmiotów realizujących usługi kluczowe – poziom ich ochrony. Należy przypomnieć, że operatorzy i instytucje zarządzające usługą kluczową nie są samowystarczalni, tzn. wykorzystują podwykonawców (często słabiej zabezpieczonych), realizują wspólne procesy, używają wspólnej infrastruktury (np. serwerowni), są zależni od globalnego łańcucha dostaw itp. Próba zarządzania ryzykiem w tak złożonej strukturze organizacyjnej powoduje lawinowy wzrost kosztów.

Inne podejście zastosowano w dyrektywie NIS 2, zgodnie z którą wszystkie podmioty objęte jej zakresem muszą stosować odpowiednie środki zarządzania ryzykiem w zakresie cyberbezpieczeństwa. Stosowanie tych środków nie jest warunkowane tym, czy potencjalna awaria może wywołać skutki nieakceptowalne z punktu widzenia bezpieczeństwa publicznego, czy też takiej skali skutków nie jesteśmy w stanie przewidzieć lub udowodnić w postępowaniu administracyjnym. Takie podejście wynika z powszechności zagrożenia oraz tego, że cyberpowiązania nie są możliwe do prześledzenia, a także z potrzeby zachowania równości podmiotów na wspólnym ryku. Taka regulacja powoduje, że koszty ochrony są porównywalne dla każdej organizacji i żadna nie jest szczególnie obciążana czy preferowana. Wprowadzenie jednolitego podejścia do cyberbezpieczeństwa podmiotów krytycznych ma na celu eliminację luk w ochronie wynikających ze złożoności powiązań między podmiotami (art. 20 ust. 1).

Po przeprowadzeniu analizy przypadków ataków hybrydowych pojawia się wątpliwość, czy metodyka przyjęta w dyrektywie CER jest kompletna, tzn. czy obejmuje wszystkie elementy systemu, także te, które mogą stać się (nieoczywistymi) celami ataków hybrydowych. Dyrektywa NIS 2 zapewnia bardziej wszechstronne podejście do zarządzania ryzykiem, które obejmuje wszystkie podmioty i gwarantuje większą odporność całego systemu cyfrowego. Zastosowanie w obu dyrektywach odmiennych strategii wyłaniania podmiotów o dużym znaczeniu dla bezpieczeństwa państwa i jego obywateli może doprowadzić do wielu niespójności w zakresie nakładania obowiązków na te podmioty. Już dziś można przewidywać, że za kilka lat pojawią się głosy, by obie te dyrektywy ujednolicić.

Bibliografia

Clausewitz C. von, *O wojnie*, Warszawa 2022.

Źródła internetowe

Atak hakerski na oczyszczalnię ścieków, iSokolka.eu, 8.10.2024, https://isokolka.eu/kuznica/59444-atak-hakerski-na-oczyszczalnie-sciekow [dostęp: 20.02.2025].

Awaria kabla EstLink 2. Rosyjski tankowiec podejrzany o akt sabotażu, PolskieRadio.pl, 26.12.2024, https://www.polskieradio.pl/399/7977/artykul/3463666%2Cawaria-ka%20bla-estlink-2-rosyjski-tankowiec-podejrzany-o-akt-sabotazu? [dostęp: 20.02.2025].

CNN: Według ekspertów atak na Aramco nastąpił z Iranu, Interia Wydarzenia, 18.09.2019, https://wydarzenia.interia.pl/zagranica/news-cnn-wedlug-ekspertow--atak-na-aramco-nastapil-z-iranu,nId,3209902 [dostęp: 23.03.2025].

Doniesienia o rosyjskim cyberataku. Pojawił się polski wątek, Wirtualna Polska, 17.04.2024, https://wiadomosci.wp.pl/rosyjski-cyberatak-na-polska-infrastrukture-ofiara-oczyszczalnia-sciekow-7017937180834752a [dostęp: 20.02.2025].

Gapiński K., *Blackout w zachodniej Ukrainie – cyberatak o wymiarze międzynarodowym*, Fundacja im. Kazimierza Pułaskiego, 20.01.2016, https://pulaski.pl/komentarz-blackout-w-zachodniej-ukrainie-cyber-atak-o-wymiarze-miedzynarodowym/ [dostęp: 23.03.2025].

Górski R., *Specjalna operacja wojskowa NATO: bombardowanie Jugosławii*, Instytut Spraw Obywatelskich, 24.03.2023, https://instytutsprawobywatelskich.pl/specjalna--operacja-wojskowa-nato-bombardowanie-jugoslawii/ [dostęp: 23.03.2025].

Hoffman F.G., *Conflict in the 21'st Century: The Rise of Hybrid Wars*, Virginia 2007, https://www.comw.org/qdr/fulltext/0712hoffman.pdf [dostęp: 20.02.2025].

Impact Assessment of the 1977 New York City Blackout, lipiec 1978, https://www.ferc.gov/sites/default/files/2020-05/impact-77.pdf [dostęp: 23.03.2025].

Jackson G.M., *Warden's five-ring system theory: legitimate wartime military targeting or an increased potential to violate the law and norms of expected behavior?*, Alabama 2000, https://apps.dtic.mil/sti/pdfs/ADA425331.pdf [dostęp: 20.02.2025].

Jak uszkodzenie Estlink 2 wpływa na ceny energii w Estonii, Czas Wschodni, 14.02.2025, https://czaswschodni.pl/art/wiadomosci/jak-uszkodzenie-estlink-2-wplywa-na-ceny-energii-w-estonii_116f1090-c456-4bb7-abc1-c340f6da6cf5 [dostęp: 20.02.2025].

Jakóbik W., *USA mogą na dniach zadać nowy cios Nord Stream 2, ale unikają deklaracji*, Biznes Alert, 14.05.2021, https://biznesalert.pl/nord-stream-2-sankcje-usa-poszerzone-energetyka-gaz/ [dostęp: 20.02.2025].

Kardaś S., Łoskot-Strachota A., *Dywersja na gazociągach Nord Stream 1 i Nord Stream 2*, Ośrodek Studiów Wschodnich, 29.09.2022, https://www.osw.waw.pl/pl/publikacje/analizy/2022-09-29/dywersja-na-gazociagach-nord-stream-1-i-nord-stream-2 [dostęp: 23.03.2025].

Lewis S., Shalal A., *U.S., Germany strike Nord Stream 2 pipeline deal to push back on Russian 'aggression'*, Reuters, 22.07.2021, https://www.reuters.com/business/energy/us-germany-deal-nord-stream-2-pipeline-draws-ire-lawmakers-both-countries-2021-07-21/ [dostęp: 20.02.2025].

McKew M.K., *The Gerasimov Doctrine. It's Russia's new chaos theory of political warfare. And it's probably being used on you*, Politico, wrzesień/październik 2017, https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538/ [dostęp: 23.03.2025].

Minister ostrzega mieszkańców przed możliwą dezinformacją, Made in Vilnius, 4.02.2025, https://madeinvilnius.lt/pl/Aktualno%C5%9Bci/Lietuvos-naujienos/Minister-ostrzega-mieszka%C5%84c%C3%B3w-przed-mo%C5%BCliw%C4%85-dezinformacj%C4%85/ [dostęp: 20.02.2025].

Muczyński R., *Atak na saudyjskie rafinerie*, Milmag, 16.09.2019, https://milmag.pl/atak-na-saudyjskie-rafinerie/ [dostęp: 23.03.2025].

Perzyński M., *Raport: O Colonial Pipline i zimnej wojnie w energetyce*, Biznesalert, 15.05.2021, https://biznesalert.pl/raport-colonial-pipeline-cyberatak-usa-rosja-energetyka/ [dostęp: 23.03.2025].

Polus A., *Atak na rafinerię w Arabii Saudyjskiej i jego konsekwencje dla Afryki*, Polskie Centrum Studiów Afrykanistycznych, 18.09.2019, https://pcsa.org.pl/atak-na-rafinerie-w-arabii-saudyjskiej-i-konsekwencje-dla-afryki/ [dostęp: 23.03.2025].

Po synchronizacji sieci energetycznych krajów bałtyckich z Europą zaktywizowała się propaganda Kremla, Polska Agencja Prasowa, 20.02.2025, https://www.pap.pl/aktualnosci/po-synchronizacji-sieci-energetycznych-krajow-baltyckich-z-europa-zaktywizowala-sie [dostęp: 20.02.2025].

Prezes Colonial Pipeline potwierdza: zapłaciliśmy okup hakerom, CyberDefence24, 20.05.2021, https://wilno.tvp.pl/84820950/przed-synchronizacja-z-europa-sluzby-ostrzegaja-przed-dezinformacja [dostęp: 23.03.2025].

Przed synchronizacją z Europą służby ostrzegają przed dezinformacją, TVP Wilno, 3.02.2025, https://wilno.tvp.pl/84820950/przed-synchronizacja-z-europa-sluzby-ostrzegaja-przed-dezinformacja [dostęp: 20.02.2025].

Psujek G., *Tajemnica ataku na saudyjską rafinerię*, Rzeczpospolita, 22.09.2019, https://radar.rp.pl/przemysl-obronny/art17499861-tajemnica-ataku-na-saudyjska-rafinerie [dostęp: 23.03.2025].

Rosyjski atak dezinformacją ws. energetyki. Estończycy wykupują generatory, służby w stanie gotowości, Polskie Radio 24, 6.02.2025, https://polskieradio24.pl/artykul/3480519,rosyjski-atak-dezinformacja-ws-energetyki-estonczycy-wykupuja-generatory-sluzby-w-stanie-gotowosci [dostęp: 20.02.2025].

Statement from CISA Acting Director Wales on Executive Order to Improve the Nation's Cybersecurity and Protect Federal Networks, America's Cyber Defense Agency, 13.05.2021, https://www.cisa.gov/news-events/news/statement-cisa-acting-director-wales-executive-order-improve-nations-cybersecurity-and-protect [dostęp: 20.02.2025].

Stawarz N., *„Nielegalne, ale moralne"? Operacja „Allied Force": przyczyny i konsekwencje*, Histmag.org, 24.03.2019, https://histmag.org/Nielegalne-ale-moralne-Operacja-Allied-Force-przyczyny-i-konsekwencje-18428? [dostęp: 23.03.2025].

Urbanek W., *Colonial Pipeline: niepożądana sława*, CRN, 24.06.2021, https://crn.pl/artykuly/colonial-pipeline-niepozadana-slawa/ [dostęp: 23.03.2025].

Uszkodzenie kabla EstLink 2 podniosło ceny energii w krajach bałtyckich, BalticWind.EU, 3.01.2025, https://balticwind.eu/pl/uszkodzenie-kabla-estlink-2-podnioslo-ceny-energii-w-krajach-baltyckich/ [dostęp: 20.02.2025].

Akty prawne

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. L 333/164 z 27.12.2022).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) – (Dz. Urz. L 333/80 z 27.12.2022).

Protokoły dodatkowe do Konwencji genewskich z 12 sierpnia 1949 r., dotyczący ochrony ofiar międzynarodowych konfliktów zbrojnych (Protokół I) oraz dotyczący ochrony ofiar niemiędzynarodowych konfliktów zbrojnych (Protokół II), sporządzone w Genewie dnia 8 czerwca 1977 r. (DzU z 1992 nr 41 poz. 175).

Dr Witold Skomra

Kierownik Wydziału Ochrony Infrastruktury Krytycznej w Rządowym Centrum Bezpieczeństwa. Ekspert w zakresie planowania cywilnego zarządzania kryzysowego oraz ochrony infrastruktury krytycznej. Krajowy delegat do grupy przygotowującej dyrektywę CER oraz do Wysokiego Forum ds. Ryzyka Organizacji Współpracy Gospodarczej i Rozwoju (OECD High Level Risk Forum). Wykładowca na Wydziale Zarządzania Politechniki Warszawskiej. Prowadzi zajęcia z zakresu ciągłości działania, zarządzania ryzykiem, zarządzania bezpieczeństwem publicznym oraz ochrony infrastruktury krytycznej. Były Komendant Główny Państwowej Straży Pożarnej, absolwent Szkoły Głównej Służby Pożarniczej oraz Akademii Obrony Narodowej.

Kontakt: witold.skomra@rcb.gov.pl

Dr Karolina Wojtasik, MBA

Specjalista ds. bezpieczeństwa, biegły sądowy, pracownik naukowy, wiceprezes ds. naukowych Polskiego Towarzystwa Bezpieczeństwa Narodowego, główny specjalista w Rządowym Centrum Bezpieczeństwa. Podczas polskiej prezydencji w Radzie Unii Europejskiej pełni funkcję przewodniczącej grupy roboczej PROCIV CER. Zajmuje się szeroko pojętym bezpieczeństwem infrastruktury krytycznej, szczególnie w kontekście zagrożeń bezpieczeństwa fizycznego i osobowego. Ponadto analizuje działalność salafickich organizacji terrorystycznych, modus operandi sprawców zamachów terrorystycznych w UE i USA, a także publikacje instruktażowe dotyczące metod przeprowadzania ataków na ludność cywilną i obiekty. Autorka książek: *Anatomia zamachu. O strategii i taktyce terrorystów*; *Ścieżki radykalizacji dżihadystycznej. Podręcznik dla studentów socjologii,*

politologii i bezpieczeństwa. Współautorka publikacji *Polski system antyterrorystyczny a realia zamachów drugiej dekady XXI wieku* oraz wielu innych publikacji związanych z terroryzmem, a także bezpieczeństwem i budowaniem odporności infrastruktury krytycznej. Twórca kanału popularnonaukowego Anatomia zamachu na YouTube.

Kontakt: karolina.wojtasik@rcb.gov.pl

Terroryzm – studia, analizy, prewencja, 2025, wydanie specjalne: 35–71

https://doi.org/10.4467/27204383TER.25.002.21505

Artykuł

Zagrożenia hybrydowe na Morzu Bałtyckim. Wyniki analizy możliwości przeciwdziałania

Hybrid threats in the Baltic Sea.
The results of analysis of countermeasure options

RAFAŁ MIĘTKIEWICZ

https://orcid.org/0000-0002-3129-7092

Akademia Marynarki Wojennej
im. Bohaterów Westerplatte w Gdyni

Abstrakt

Obszary morskie regionu bałtyckiego można uznać za przestrzeń, w której toczy się konflikt proxy, czyli o charakterze zastępczym, między Federacją Rosyjską a państwami Zachodu. Nasilające się od 2022 r. (początek pełnej rosyjskiej inwazji na Ukrainę) działania hybrydowe ze strony Rosji były skierowane w dużej mierze przeciwko obiektom infrastruktury krytycznej państw nadbrzeżnych. Na podstawie dostępnych informacji na temat zdarzeń, do których doszło w latach 2022–2024, w artykule zostały omówione różne formy działań podprogowych Rosji wymierzonych w tę infrastrukturę. Wskazano jej podatności na działania hybrydowe na Morzu Bałtyckim (możliwe sposoby oddziaływania na obiekty portowe i infrastrukturę morską, ze szczególnym uwzględnieniem podmorskich linii przesyłowych). W artykule zostały przedstawione również poglądy autora na temat możliwych odpowiedzi państw NATO, w postaci inicjatyw politycznych, wojskowych i technologicznych, na zagrożenia hybrydowe, których źródłem są nowoczesne morskie systemy autonomiczne.

Słowa kluczowe

zagrożenia hybrydowe na morzu, konflikt hybrydowy, morska infrastruktura krytyczna

Abstract

The maritime areas of the Baltic region, can be considered a space for the conduct of proxy conflict, i.e. of a substitute nature, between the Russian Federation and Western states. Intensifying since 2022 (the start of Russia's full-scale invasion of Ukraine) hybrid actions on the part of Russia have largely targeted the critical infrastructure facilities of coastal states. The article discusses the various forms of subliminal actions against this infrastructure undertaken by Russia, based on available information on events in the period from 2022 to the end of 2024. It also presents the vulnerabilities to hybrid actions that characterise critical infrastructure in the Baltic (possible ways of affecting port facilities and offshore infrastructure, with a particular focus on undersea transmission lines). The publication also presents the author's views on possible responses from NATO countries, in the form of political, military and technological initiatives, to hybrid threats posed by modern maritime autonomous systems.

Keywords

hybrid threats at sea, hybrid conflict, maritime critical infrastructure

Wprowadzenie

Na sytuację na Morzu Bałtyckim mają wpływ dynamiczne procesy kształtujące architekturę bezpieczeństwa w regionie. Można zaryzykować stwierdzenie, że basen tego morza jest przestrzenią konfliktu zastępczego między Federacją Rosyjską, dążącą do zmiany obecnego porządku w Europie, a państwami Zachodu (Unia Europejska i NATO), które wspierają Ukrainę. Morze Bałtyckie jest jednocześnie korytarzem umożliwiającym uniezależnienie się państw tego regionu (flanki NATO) od dostaw węglowodorów z rosyjskich źródeł (wykorzystywanych przez Kreml jako narzędzie przymusu lub nagradzania) oraz dywersyfikację dostaw surowców energetycznych (głównie gazu ziemnego i ropy naftowej). Odgrywa ono również coraz większą rolę w produkcji energii elektrycznej z wykorzystaniem odnawialnych

źródeł energii (morska energetyka wiatrowa o potencjale szacowanym przez Komisję Europejską na 93 GW do 2050 r.[1]). W przypadku Polski wskaźnik zależności energetycznej od Bałtyku, uwzględniający stosunek importu głównych surowców energetycznych i nośników energii do ich całkowitego zużycia, wyniósł w 2024 r. 48%. Oczekuje się, że do 2040 r. wzrośnie on do 60%[2]. Akwen ten pozostaje także ważnym obszarem realizacji celów strategicznych Federacji Rosyjskiej. Najważniejsze elementy składające się na bałtyckie aktywa Rosji to: silnie zmilitaryzowana eksklawa kaliningradzka, obwód petersburski (zdolności typu *anti-access-area denial*, A2/AD) z ważnymi portami (eksport ropy naftowej), infrastruktura przesyłu gazu (uszkodzone gazociągi Nord Stream 1 i Nord Stream 2) oraz operująca na Bałtyku Flota Bałtycka. Wprowadzona w 2022 r. rosyjska doktryna morska obniżyła rangę Morza Bałtyckiego (w dokumencie wyróżniono trzy poziomy ważności akwenów: żywotne, ważne i pozostałe) i pokazała konfrontacyjny kierunek polityki Rosji wobec państw zachodnich (totalna wojna hybrydowa), jak również chęć przemodelowania obecnego porządku światowego i architektury bezpieczeństwa międzynarodowego[3]. Wyzwania, z którymi państwa nadbałtyckie mierzą się od lat, a które wzrosły od wybuchu wojny w Ukrainie, wyraźnie potwierdzają, że Federacja Rosyjska nie zrezygnowała z wysiłków zmierzających do rozbicia jedności państw nadbałtyckich z wykorzystaniem instrumentarium znajdującego się w jej zasobach. Na długo przed atakiem Rosji na Ukrainę publikacje dotyczące strategii bezpieczeństwa dla Polski wskazywały, że istotnym sposobem realizacji celów Federacji Rosyjskiej poniżej progu wojny[4] oraz głównym zagrożeniem o charakterze militarnym i niemilitarnym w regionie bałtyckim będą działania hybrydowe[5].

Powodem zwiększenia zagrożeń hybrydowych w przyszłości może być nieskuteczność wielu działań podjętych przez Rosję w stosunku do

[1] *Study on Baltic offshore wind energy cooperation under BEMIP. Final report*, ENER/C1/2018-456, Luxembourg 2019, Publications Office of the European Union, s. 10.

[2] Z. Nowak, M. Maj, *Bałtyk jako przestrzeń strategicznej aktywności energetycznej*, w: *Czy morze pomoże? Bałtyk a bezpieczeństwo energetyczne Polski*, Z. Nowak (red.), Warszawa 2024, Institute for Foreign Affairs, s. 33–46.

[3] *Maritime Doctrine of the Russian Federation*, A. Davis, R. Vest (tłum.), Newport 2022, Russia Maritime Studies Institute, United States Naval War College.

[4] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2020.

[5] *Strategiczna Koncepcja Bezpieczeństwa Morskiego Rzeczypospolitej Polskiej*, Warszawa–Gdynia 2017, Biuro Bezpieczeństwa Narodowego, s. 11.

państw basenu Morza Bałtyckiego[6]. Przewiduje się, że w miarę pogarszania się sytuacji mogą zaistnieć zagrożenia o charakterze bezpośrednim w postaci użycia sił zbrojnych i gróźb ich użycia, jak również mogą zostać wykorzystane formy pośrednie (w przypadku obszarów morskich są to np. blokady morskie, pokazy siły z wykorzystaniem floty, niezapowiedziane ćwiczenia wojskowe na morzu, nękanie przeciwnika itp.)[7]. Typowym stanem rzeczy będą: zacieranie się granic między stanem pokoju i wojny, asymetria, wzrost znaczenia działań niekinetycznych (zwłaszcza operacji w cyberprzestrzeni) oraz wykorzystanie technologii autonomicznych[8]. Na intensyfikację konfliktu i wykorzystywanie przez Rosję nowych form działań wskazują zdarzenia, do których doszło na Morzu Bałtyckim w latach 2023–2024. W październiku 2023 r. pływający pod banderą Hongkongu statek Newnew Polar Bear, który obsługiwał rejs z Kaliningradu do Sankt Petersburga, uszkodził gazociąg Balticconnector. Ten fińsko-estoński rurociąg został uruchomiony ponownie w kwietniu 2024 r.[9] Po ponad 10 miesiącach śledztwa w tej sprawie, prowadzonego przez stronę fińską, nie potwierdzono wyjaśnień ze strony Chin, że uszkodzenie obiektu było przypadkowe[10]. W listopadzie 2024 r. zostały zerwane 2 światłowodowe połączenia telekomunikacyjne, łączące Litwę i Szwecję oraz Finlandię i Niemcy, a w grudniu 2024 r. uszkodzono podmorską linię energetyczną EstLink 2 łączącą Finlandię i Estonię. Jednym z działań Rosji jest korzystanie z tzw. szarej floty (ang. *grey fleet*) oraz tzw. ciemnej floty lub floty cieni (ang. *dark fleet*; *shadow fleet*). Pojęcie szarej floty oznacza flotę quasi-legalną

---

[6] P. Mickiewicz, *Bezpieczeństwo energetyczne czy bezpieczeństwo morskie? Dylemat oceny potencjalnych zagrożeń bezpieczeństwa Polski na akwenie Morza Bałtyckiego w trzeciej dekadzie XXI wieku*, „Nautologia" 2024, nr 161, s. 71.

[7] A. Nowakowska-Krystman, *Potencjał obronny Sił Zbrojnych RP w ujęciu relatywnym*, Warszawa 2018, Akademia Sztuki Wojennej, s. 73.

[8] R. Kasprzyk, *Sztuczna inteligencja i cyberprzestrzeń a proces złośliwego sterowania ludźmi i maszynami*, w: *GlobState*, t. 2: *Wyzwania dla Polski w kontekście zmian w środowisku bezpieczeństwa*, Ł. Jureńczyk, R. Reczkowski (red. nauk.), Bydgoszcz 2020, Centrum Doktryn i Szkolenia Sił Zbrojnych – Uniwersytet Kazimierza Wielkiego, s. 277–298.

[9] J. Hyndle-Hussein, *Uszkodzenie fińsko-estońskiego połączenia gazowego Balticconnector*, Ośrodek Studiów Wschodnich, 11.10.2023, https://www.osw.waw.pl/pl/publikacje/analizy/2023-10-11/uszkodzenie-finsko-estonskiego-polaczenia-gazowego-balticconnector [dostęp: 2.01.2025].

[10] *Finlandia: Władze nie potwierdzają informacji o „przypadkowym" uszkodzeniu Balticconnector*, Portal Morski, 13.08.2024, https://www.portalmorski.pl/offshore/56252-finlandia-wladze-nie-potwierdzaja-informacji-o-przypadkowym-uszkodzeniu-balticconnector [dostęp: 29.01.2025].

(niejasne pochodzenie i własność statku oraz bandera), działającą równolegle z flotą pozytywnie rozpatrzoną przez Międzynarodową Organizację Morską (International Maritime Organization). Ciemna flota to taka, która stosuje nielegalne praktyki (manipulowanie identyfikatorami i lokalizacją lub celowe wyłączanie systemów automatycznej identyfikacji), służące omijaniu sankcji nałożonych na Rosję w zakresie handlu ropą naftową[11].

Problem badawczy sprowadza się do odpowiedzi na pytanie, jak przeciwdziałać rosyjskim działaniom hybrydowym wymierzonym w obiekty infrastruktury krytycznej (IK) na morzu? Celem niniejszego artykułu jest po pierwsze przedstawienie możliwych form działań hybrydowych na Morzu Bałtyckim jako akwenie referencyjnym (częściowo na podstawie analizy minionych zdarzeń), które mogą zostać podjęte w ciągu najbliższych 2 lat wobec morskich obiektów IK. Po drugie, określenie podatności determinujących możliwość powstania zagrożeń hybrydowych w stosunku do obiektów IK na Morzu Bałtyckim. W kolejnym kroku zostaną przedstawione propozycje działań mających na celu przeciwdziałanie tego typu zagrożeniom i zwiększenie poziomu ochrony obiektów IK na Bałtyku.

W celu opracowania niniejszego artykułu przeprowadzono krytyczną analizę następujących źródeł[12]:

- dokumentów w postaci: doktryn (*Maritime Doctrine of the Russian Federation*, A. Davis, R. Vest, tłum.), strategii (*Plan REPowerEU, Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów*; *Council conclusions on the Revised EU Maritime Security Strategy (EUMSS) and its Action Plan*; *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020*; *Strategiczna Koncepcja Bezpieczeństwa Morskiego RP*; *Polityka Energetyczna Polski do 2040 r.*), oficjalnych informacji rządowych (*Joint Declaration on cooperation to secure critical subsea infrastructure*), raportu instytucji RP – Najwyższej Izby Kontroli (*Informacja o wynikach kontroli. Przygotowanie państwa na zagrożenia związane z działaniami hybrydowymi*; *Informacja o wynikach kontroli. Realizacja działań w zakresie poprawy bezpieczeństwa paliwowego w sektorze naftowym*) oraz publikacji organizacji międzynarodowych:

[11] *Russia's 'shadow fleet': Bringing the threat to light*, European Parliament, https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766242/EPRS_BRI(2024)766242_EN.pdf, s. 3 [dostęp: 23.01.2025].

[12] W tym miejscu wykorzystane materiały źródłowe zostały jedynie wymienione. Ich pełny opis bibliograficzny podano w bibliografii załącznikowej (przyp. red.).

Parlamentu Europejskiego (*P9_TA(2024)0079 – Russiagate: zarzuty dotyczące rosyjskiej ingerencji w procesy demokratyczne w Unii Europejskiej – Rezolucja Parlamentu Europejskiego z dnia 8 lutego 2024 r. w sprawie Russiagate: zarzuty dotyczące rosyjskiej ingerencji w procesy demokratyczne w Unii Europejskiej (2024/2548(RSP))*), Komisji Europejskiej (*Joint Statement by the European Commission and the High Representative on the Investigation into Damaged Electricity and Data Cables in the Baltic Sea*), Komisji Ochrony Środowiska Morskiego Bałtyku (*HELCOM, ensuring safe shipping in the Baltic*), NATO (N. Fridbertsson, *General Report – Protecting Critical Maritime Infrastructure – The Role of Technology*; A. Hagelstam, *Współpraca przeciwko zagrożeniom hybrydowym*), Rady Atlantyckiej (E. Braw, *Russia's growing dark fleet: Risks for the global maritime order*);

- dostępnych (jawnych) materiałów, w tym komunikatów prasowych (*Finland-Estonia power cable hit in latest Baltic Sea incident*, „The Guardian"; C. Chiappa, *6 countries move to protect the North Sea from Russians*, „Politico"), komunikatów ministerstw państw bałtyckich, opracowania pokonferencyjnego GlobState (K. Kasprzyk, *Sztuczna inteligencja i cyberprzestrzeń a proces złośliwego sterowania ludźmi i maszynami*);
- opracowań renomowanych ośrodków zajmujących się tematyką zagrożeń hybrydowych, takich jak: Hybrid Centre of Excellence (*Handbook on maritime hybrid threats: 15 scenarios and legal scans*), Maritime Security Centre of Excellence (D. Doğan, D. Çetikli, *Maritime Critical Infrastructure Protection (MCIP) in a Changing Security Environment*), oraz stosunkami międzynarodowymi, takich jak: International Centre for Defence and Security (N. Aliyev, *Does Russia want to revise its water border with the Nordic and Baltic states?*), U.S. Helsinki Commission (S. McGrath, *Spotlight on the Shadow War: Inside Russia's Attacks on NATO Territory*), Ośrodek Studiów Wschodnich (J. Hyndle-Hussein, *Uszkodzenie fińsko-estońskiego połączenia gazowego Balticconnector*), a także opracowania portalu branżowego Baltic Wind EU zajmującego się międzynarodowymi aspektami rozwoju morskiej energetyki wiatrowej na Morzu Bałtyckim (K. Bulski, *The Role of the New European Commission and Regional Cooperation in Accelerating Offshore Wind in the Baltic Sea*);
- publikacji think tanków o ugruntowanej pozycji, takich jak: Polski Instytut Spraw Międzynarodowych (K. Dudzińska, *Jądrowy zwrot*

w szwedzkiej polityce energetycznej), Center for International Maritime Security (O. Chiriac, *The 2022 Maritime Doctrine of the Russian Federation: Mobilization, Maritime Law, and Socio-Economic Warfare*), The Opportunity Institute for Foreign Affairs (R. Miętkiewicz, *Bałtyk jako obszar szczególnej ochrony*), Warsaw Institute (B. Fraszka, *Państwa bałtyckie a rosyjskie zagrożenia hybrydowe*), Polskie Towarzystwo Bezpieczeństwa Narodowego (K. Wojtasik, *Analiza wyników badań na temat percepcji zagrożeń o charakterze terrorystycznym wśród uczestników EU PSA*), Instytut Polityki Energetycznej im. I. Łukasiewicza (M. Ruszel, P. Ogarek, *Bezpieczeństwo paliwowe Polski w kontekście zmian właścicielskich na rynku logistyki produktów naftowych oraz remedies Komisji Europejskiej w sprawie fuzji PKN ORLEN i Grupy LOTOS. Polska u progu embargo na produkty naftowe z Rosji – analiza otwierająca 2023 rok*);

- analiz cyberzagrożeń opublikowanych przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (*ENISA Threat Landscape 2024*) i amerykańską Cybersecurity and Infrastructure Security Agency (*Russian Military Cyber Actors Target US and Global Critical Infrastructure*);
- wcześniejszych prac badawczych poświęconych współczesnym zagrożeniom na morzu (R. Miętkiewicz, *Dumped conventional warfare (munition) catalog of the Baltic Sea*; R. Miętkiewicz, *High explosive unexploded ordnance neutralization – Tallboy air bomb case study*), w tym dla obiektów morskiej infrastruktury energetycznej (R. Miętkiewicz, *Morskie farmy wiatrowe a bezpieczeństwo morskie państwa*; R. Miętkiewicz, *Bałtyk jako obszar szczególnej ochrony*), oraz prac dotyczących wykorzystania nowoczesnych technologii (R. Miętkiewicz, *Systemy autonomiczne w działaniach na morzu*; R. Miętkiewicz, *Obiekty morskiej infrastruktury energetycznej – próba określenia podatności na ataki platform bezzałogowych*). Uwzględniono także wyniki badania ankietowego wśród ekspertów EU Protective Security Advisors (K. Wojtasik, *Analiza wyników badań na temat percepcji zagrożeń o charakterze terrorystycznym wśród uczestników EU PSA*)[13].

[13] W lutym 2025 r. zostały przeprowadzone nowe badania ankietowe wśród uczestników EU PSA, których wyniki przedstawiono w artykule: K. Wojtasik, D. Szlachter, *Wyniki badania ankietowego dotyczącego percepcji zagrożeń terrorystycznych i sabotażowych wśród ekspertów EU Protective Security Advisors*, „Terroryzm - studia, analizy, prewencja", wydanie specjalne: *Zagrożenia terrorystyczne i sabotażowe infrastruktury krytycznej*, s. 263–287. https://doi.org/10.4467/27204383TER.25.010.21513 (przyp. red.).

Zagrożenia hybrydowe

Zagrożenia hybrydowe to szkodliwe i celowe działania, które są planowane i przeprowadzane przez państwa autorytarne i reżimy oraz przez podmioty niepaństwowe (działające wielokrotnie w charakterze proxy), aby osłabić cel (państwo lub instytucję) za pomocą różnych, często połączonych środków[14]. Wykorzystanie wielu podmiotów i działań sprzyja uzyskaniu efektu synergii potęgującego skuteczność ataku. Zagrożenia hybrydowe stale się zmieniają, a stosowane narzędzia obejmują szerokie spektrum środków, w tym: zaawansowane cyberataki[15], manipulację informacją (m.in. za pomocą fałszywych profili w mediach społecznościowych), wpływy ekonomiczne, a także zakulisowe manewry polityczne, dyplomację przymusu (operacje wpływu i ingerencji) czy groźby użycia siły militarnej. Cechą charakterystyczną konfliktów hybrydowych jest ciągła zmiana i problem ze zdefiniowaniem wszystkich ich aspektów. Łączą w sobie działania konwencjonalne i niekonwencjonalne, symetrię i asymetrię, aktorów państwowych i niepaństwowych (niekiedy trudnych do zidentyfikowania, działających poniżej progu wykrywalności i identyfikacji). Celem atakującego jest przeprowadzenie skoordynowanych uderzeń w kluczowe dla przeciwnika punkty (np. w słabości systemowe państw demokratycznych)[16].

Ze względu na obecną sytuację geopolityczną za najbardziej prawdopodobne źródło zagrożeń hybrydowych uważa się Federację Rosyjską. Główne cele jej działań hybrydowych to zdyskredytowanie na arenie międzynarodowej pozycji atakowanego państwa (m.in. przez wykazanie nieskuteczności wysiłków podejmowanych przez to państwo w odpowiedzi na sytuacje kryzysowe), osłabienie spójności zachodnich sojuszy i zmuszenie ich do spełnienia politycznych, gospodarczych i wojskowych żądań Rosji. Ekspert Polskiego Towarzystwa Bezpieczeństwa Narodowego zwraca

[14] *Hybrid threats as a concept, Frequently asked questions on hybrid threats*, The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ [dostęp: 2.12.2024].

[15] A. Hagelstam, *Współpraca przeciwko zagrożeniom hybrydowym*, NATO Review, 23.11.2018, https://www.nato.int/docu/review/pl/articles/2018/11/23/wspolpraca-przeciwko-zagrozeniom-hybrydowym/index.html [dostęp: 2.12.2024].

[16] B. Fraszka, *Państwa bałtyckie a rosyjskie zagrożenia hybrydowe*, Warsaw Institute, 26.10.2020, https://warsawinstitute.org/wp-content/uploads/2020/10/Pa%C5%84stwa-ba%C5%82tyckie-a-rosyjskie-zagro%C5%BCenia-hybrydowe-Bartosz-Fraszka.pdf, s. 4 [dostęp: 29.12.2024].

uwagę, że ze względu na braki w wyposażeniu regularnych jednostek rosyjskich sił zbrojnych oraz poziom strat poniesionych w Ukrainie nacisk w zakresie odziaływania zostanie przeniesiony na operacje hybrydowe. Szczególnie sprzyjający realizacji takich operacji wydaje się obszar morski, gdyż nie ma możliwości sprawowania nad nim pełnej kontroli[17].

Wyniki badania ankietowego dotyczącego percepcji zagrożeń o charakterze terrorystycznym przeprowadzonego na początku 2023 r. z udziałem ekspertów EU Protective Security Advisors (EU PSA) wskazały na najwyższą pozycję obiektów IK jako pierwszo-, drugo- i trzeciorzędnych potencjalnych celów ataków terrorystycznych w UE (63,63% wszystkich wskazań). Drugie miejsce zajęły systemy transportu publicznego (60% odpowiedzi). Spośród obiektów najbardziej narażonych na atak terrorystyczny (do wyboru były: bazy wojskowe wykorzystywane w ramach NATO, obiekty IK, system transportu publicznego, system transportu towarów handlowych, siedziby konstytucyjnych organów państwowych, infrastruktura turystyczna, obiekty sportowe i rozrywkowe, miejsca kultu religijnego, siedziby instytucji i agend UE) najwięcej respondentów (40%) wskazało obiekty infrastruktury energetycznej[18]. Z kolei spośród wielu środków wykorzystywanych do przeprowadzania ataków (bezzałogowe statki powietrzne, druk 3D, pojazdy służące do taranowania, improwizowane urządzenia wybuchowe, broń biała wykonana z kompozytów, środki CBRN, środki zapalające) terroryści najchętniej będą wybierać – według ekspertów EU PSA – systemy autonomiczne (49,09% wskazań). Zdecydowana większość respondentów (81,82%) uważa ponadto, że w ciągu najbliższych 3 lat w ramach działań hybrydowych podejmowanych na terytorium UE przez obce państwo zostanie wykorzystana aktywność terrorystyczna.

Europejskie Centrum Doskonalenia ds. Przeciwdziałania Zagrożeniom Hybrydowym (European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE) po przeprowadzeniu badań dotyczących współczesnych zagrożeń hybrydowych występujących na akwenach morskich wskazało, że zakres tego typu działań jest bardzo szeroki. Ich formy mogą obejmować: nielegalne połowy i użycie statków rybackich do prowadzenia

[17] M. Piekarski, *Ochrona infrastruktury krytycznej na polskich obszarach morskich w kontekście zagrożeń hybrydowych*, Ekspertyzy PTBN nr 1, Polskie Towarzystwo Bezpieczeństwa Narodowego 2023.

[18] K. Wojtasik, *Analiza wyników badań na temat percepcji zagrożeń o charakterze terrorystycznym wśród uczestników EU PSA*, Analizy PTBN nr 1, Polskie Towarzystwo Bezpieczeństwa Narodowego 2023, s. 5.

agresywnych działań, cyberataki, ataki szybkich łodzi motorowych czy też użycie złych warunków hydrometeorologicznych do uwiarygodnienia np. zarzucania kotwicy w bezpośrednim sąsiedztwie kabli podmorskich. W kilku scenariuszach przewidywano bezprawne ogłaszanie i zamykanie stref morskich pod pozorem ćwiczeń wojskowych oraz wprowadzanie stref kontroli przepływających statków[19]. Od rozpoczęcia rosyjskiej inwazji na Ukrainę w lutym 2022 r. do listopada 2024 r. pracownicy amerykańskiej Komisji Helsińskiej (U.S. Helsinki Commission) zidentyfikowali ok. 150 ataków hybrydowych przeprowadzonych na terytorium państw NATO przez Rosję lub podmioty z nią powiązane. Wśród 4 odrębnych kierunków operacji hybrydowych ataki na obiekty IK znalazły się na drugim miejscu (33%), za ingerowaniem w wybory i prowadzeniem kampanii informacyjnych (35%), a przed kampaniami przemocy (20%) i wykorzystaniem migrantów jako broni (12%)[20].

Znaczenie Morza Bałtyckiego dla Federacji Rosyjskiej

W 2022 r., po rozpoczęciu pełnoskalowej inwazji na Ukrainę, została opublikowana wspomniana już rosyjska doktryna morska, która zastąpiła poprzedni dokument obowiązujący od 2015 r. Morskie i energetyczne aktywa Rosji są przede wszystkim instrumentami władzy, wykorzystywanymi przez nią do osiągania celów strategicznych. Aspekty gospodarcze i społeczne pozostają na drugim planie[21]. Jednym z priorytetów sformułowanych w tym dokumencie w odniesieniu do Morza Bałtyckiego jest rozwój infrastruktury portowej i instalacji odpowiedzialnych za tranzyt węglowodorów (reorientacja eksportu), centrów logistycznych oraz systemu podmorskich rurociągów eksportowych. Istotne jest również dalsze wzmacnianie potencjału militarnego i sieci baz Floty Bałtyckiej (ochrona rosyjskich interesów

[19] *Hybrid CoE Paper 16*: *Handbook on maritime hybrid threats: 15 scenarios and legal scans*, The European Centre of Excellence for Countering Hybrid Threats 2023, s. 5.

[20] S. McGrath, *Spotlight on the Shadow War: Inside Russia's Attacks on NATO Territory. A Report by the U.S. Helsinki Commission Staff*, 2024, s. 2.

[21] O. Chiriac, *The 2022 Maritime Doctrine of the Russian Federation: Mobilization, Maritime Law, and Socio-Economic Warfare*, Center for International Maritime Security, 28.11.2022, https://cimsec.org/the-2022-maritime-doctrine-of-the-russian-federation-mobilization-maritime-law-and-socio-economic-warfare/ [dostęp: 7.12.2024].

na Morzu Bałtyckim)[22]. Bałtyk jest ważny dla Rosji ze względu na praktykę omijania zachodnich sankcji (embargo i limity cenowe) nałożonych na rosyjski eksport ropy naftowej w odpowiedzi na inwazję na Ukrainę. Tylko we wrześniu 2023 r. rosyjskie porty na Morzu Bałtyckim zapewniły 57% całkowitego eksportu ropy naftowej z Rosji[23]. Według danych z 2023 r. łączne obroty 3 rosyjskich portów stanowiły prawie połowę (46%) całkowitego wolumenu przeładunków 10 największych portów bałtyckich. Wartość ta utrzymuje się na podobnym poziomie od 2021 r.[24]

Rosyjskie statki z *grey fleet* oraz *shadow fleet* wykorzystują nieuporządkowane kwestie własnościowe i ubezpieczeniowe, aby łamać sankcje nałożone na rosyjską ropę. To samo w sobie jest źródłem zagrożenia dla państw nadbałtyckich, ze względu na wiek tych statków, stan techniczny, wykorzystywanie ich do operacji zwiadowczych, kwalifikacje załogi, przeładunki ropy na pełnym morzu[25]. *Grey fleet* oraz *shadow fleet*, jak pokazują wydarzenia z 2024 r., o których wspomniano we *Wprowadzeniu*, są również narzędziami do tworzenia zagrożeń hybrydowych i asymetrycznych.

W kontekście bezpieczeństwa na Morzu Bałtyckim istotne jest to, że Rosja ma wprowadzić pakiet mechanizmów nacisku obliczonych na maksymalizację zaangażowania sił i środków NATO w monitorowanie obiektów IK. Ma to służyć zwiększaniu kosztów związanych z zapewnieniem bezpieczeństwa Sojuszu[26]. Działania sabotażowe wymierzone w IK mogą mieć konsekwencje dla sieci przesyłowych, wpływać na dostępność surowców i nośników energii oraz powodować perturbacje na rynkach energetycznych. Należy zauważyć, że działania NATO, które doprowadzą do ograniczenia swobody Rosji w korzystaniu z *grey fleet* oraz *shadow fleet* (inspekcje rosyjskich statków zapowiedziane w grudniu 2024 r. przez Wielką Brytanię,

[22] *Maritime Doctrine of the Russian Federation*, A. Davis, R. Vest (tłum.)...

[23] K. Westgaard, *The Baltic Sea Region: A Laboratory for Overcoming European Security Challenges*, Carnegie Endowment for International Peace, 21.12.2023, https://carnegieendowment.org/research/2023/12/the-baltic-sea-region-a-laboratory-for-overcoming-european-security-challenges?lang=en [dostęp: 7.12.2024].

[24] P. Frankowski, *Bałtyckie TOP10*, Namiary na Morze i Handel, 9.05.2024, https://www.namiary.pl/2024/05/09/baltyckie-top10/ [dostęp: 3.01.2025].

[25] E. Braw, *Russia's growing dark fleet: Risks for the global maritime order*, Atlantic Council, 11.01.2024, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/russias-growing-dark-fleet-risks-for-the-global-mariti me-order/ [dostęp: 29.04.2024].

[26] Ł. Wyszyński, *Wyszyński: Wejście Szwecji do NATO rodzi korzyści, ale i wyzwania (rozmowa)*, Biznes Alert, 5.03.2024, https://biznesalert.pl/szwecja-nato-zalety-wady-rosja-morze-baltyckie-bezpieczenstwo/ [dostęp: 7.10.2024].

Danię, Szwecję, Finlandię, Polskę i Estonię), mogą spotkać się z reakcją z jej strony i spowodować wzrost zagrożeń bezpieczeństwa. Rosja może wykorzystać swój potencjał wojskowy (głównie okręty wojenne) do eskortowania statków podejrzewanych o to, że są przez nią wykorzystywane do łamania sankcji[27].

Bałtycka infrastruktura krytyczna

Zapewnienie państwom nadbałtyckim bezpieczeństwa energetycznego wymaga rozbudowy IK w postaci portów morskich, specjalistycznych terminali (naftowych, gazowych, pływających jednostek regazyfikujących – FSRU, z ang. *floating storage regasification unit*), podmorskich linii energetycznych (łączących systemy energetyczne poszczególnych państw), rurociągów (odpowiedzialnych głównie za przesył gazu ziemnego, a w przyszłości także wodoru), a także linii komunikacyjnych (światłowodowych), aż po platformy wiertnicze prowadzące wydobycie ropy naftowej i gazu ziemnego ze złóż podmorskich (jedynym krajem prowadzącym na Bałtyku poszukiwanie i wydobycie ropy naftowej i gazu jest Polska). Kraje bałtyckie mają duże ambicje w zakresie rozwoju zarówno morskiej energetyki wiatrowej, jak i energetyki jądrowej (jako elementu stabilizującego odnawialne źródła energii) oraz gospodarki wodorowej. Podmorskie połączenia elektroenergetyczne łączące Litwę, Łotwę i Estonię z systemami energetycznymi Szwecji (NordBalt), Finlandii (EstLink) i Polski (połączenie lądowe LitPol Link) umożliwiły desynchronizację tych krajów z postsowieckim systemem elektroenergetycznym BRELL (luty 2025 r.). Dzięki scentralizowanemu systemowi Rosja mogła zarządzać częstotliwością i stabilnością sieci, a państwa zależne nie miały możliwości działania w izolowanym trybie wyspowym[28].

Państwa nadbałtyckie przechodzą proces fundamentalnych zmian w produkcji energii elektrycznej. Zwrot Szwecji w kierunku energetyki jądrowej (do 2045 r. ma zostać uruchomionych 10 reaktorów) ma wpływ na bezpieczeństwo energetyczne krajów nadbałtyckich. Dla Norwegii

[27] *Russia's Shadow Fleet Tankers Could Get Naval Escorts*, The Maritime Executive, 18.12.2024, https://maritime-executive.com/article/russia-s-shadow-fleet-tankers-could-get-naval-escorts [dostęp: 9.01.2025].

[28] M. Paszkowski, *Litwa, Łotwa oraz Estonia planują stworzenie bałtyckiego hubu energetycznego*, „Komentarze IEŚ" 2024, nr 1259, s. 1.

oznacza to możliwość przejściowej stabilizacji własnego systemu (opartego na elektrowniach wodnych). Działania Szwecji są zachętą dla innych państw regionu do podjęcia podobnych kroków (Estonia i Finlandia planują wspólny projekt małych reaktorów modułowych – SMR, z ang. *small modular reactors*)[29]. Szwecja odgrywa również ważną rolę w budowie Bałtyckiego Pierścienia Energetycznego, dla którego członków jest gwarantem dostępu do energii elektrycznej w przypadku sytuacji kryzysowej. Moce wytwarzane przez szwedzki system mogą być w razie potrzeby dostarczane do systemów przesyłowych HVDC (ang. *high-voltage direct current,* pol. sieć wysokiego napięcia przesyłająca prąd stały) z Litwą (NordBalt), Finlandią (Fenno-Skan), Niemcami (Baltic Cable) i Polską (SwePol Link). W czasie eksploatacji podmorskiej linii z Polską doszło już do co najmniej kilkunastu incydentów, w tym do uszkodzeń fizycznych (działalność połowowa i kotwice statków)[30].

Kolejnym krajem realizującym program jądrowy jest Polska, która dzięki uruchomieniu 6 bloków (każdy o mocy od 1 GW do 1,6 GW) zamierza pozyskać stabilne źródło energii elektrycznej o łącznej mocy zainstalowanej od 6 GW do 9 GW. Pierwsza elektrownia jądrowa zostanie wybudowana na wybrzeżu Bałtyku. Taka lokalizacja umożliwi wykorzystanie wody morskiej do chłodzenia reaktorów, a także zapewni dostępność obszaru budowy dla transportu elementów wielkogabarytowych, co stworzy podstawę stabilnego i bezpiecznego łańcucha dostaw[31].

Region Skandynawii i Morza Bałtyckiego ma znaczny potencjał produkcji wodoru ze źródeł odnawialnych (zielonego wodoru), określony na ok. 27,1 mln t (łącznie z morskiej i lądowej energii wiatrowej i słonecznej) do 2040 r. Przewiduje się, że do 2040 r. Nordycko-Bałtycki Korytarz Wodorowy umożliwi transgraniczny przesył nawet 2,7 mln t wodoru odnawialnego z Finlandii przez Estonię, Łotwę, Litwę i Polskę do Niemiec, aby osiągnąć cele planu REPowerEU. Morska część korytarza, o łącznej długości ok. 2500 km, ma przebiegać wzdłuż dna Zatoki Fińskiej[32] – akwenu charakteryzującego się wysokim poziomem zagrożeń hybrydowych, o czym

[29] K. Dudzińska, *Jądrowy zwrot w szwedzkiej polityce energetycznej*, „Biuletyn PISM" 2024, nr 58, s. 1.

[30] R. Miętkiewicz, *Bałtyk jako obszar szczególnej ochrony*, w: *Czy morze pomoże? Bałtyk a bezpieczeństwo energetyczne Polski*, Z. Nowak (red.), Warszawa 2024, s. 33–46.

[31] Tamże.

[32] *Nordycko-Bałtycki Korytarz Wodorowy*, Gaz-System, 2024, https://www.gaz-system.pl/pl/rynek-wodoru/projekty/nordycko-baltycki-korytarz-wodorowy.html [dostęp: 3.01.2025].

świadczą wydarzenia z 2024 r., o których wcześniej wspomniano. Po uwzględnieniu realizacji europejskich planów rozwoju gospodarki wodorowej cele strategiczne nakreślone przez fiński rząd zakładają, że kraj ten stanie się europejskim liderem tej technologii w całym łańcuchu wartości. Oczekuje się, że do 2030 r. produkcja zielonego wodoru w Finlandii osiągnie poziom 10% w skali UE[33].

Podmorskie gazociągi mają strategiczne znaczenie dla bezpieczeństwa energetycznego państw nadbałtyckich. Pierwszym z nich jest Baltic Pipe, który umożliwia tranzyt 10 mld m^3 gazu rocznie z Norweskiego Szelfu Kontynentalnego do Polski (tranzyt przez Niemcy i Danię). Gazociąg Balticconnector odpowiada za dostawy gazu ziemnego do odbiorców na fińsko-estońsko-łotewskim rynku gazu. W polskiej wyłącznej strefie ekonomicznej znajduje się również gazociąg (dwie nitki) łączący polskie platformy wiertnicze (wydobycie i zrzut gazu związanego ze złożami ropy naftowej) z nadmorską elektrociepłownią. Finlandia ma możliwość pozyskiwania gazu przez swoje terminale LNG w Zatoce Fińskiej – Inkoo i Hamina (kraj ten posiada jeszcze 2 terminale, które obsługują obiekty przemysłowe), skąd surowiec jest przesyłany gazociągiem podmorskim do odbiorców po drugiej stronie Zatoki Fińskiej. W 2024 r. Niemcy uruchomiły w Mukran (wyspa Rugia) największy na Morzu Bałtyckim terminal FSRU, który umożliwia odbiór gazu z dwóch tankowców kriogenicznych jednocześnie (roczna przepustowość 13,5 mld m^3 gazu). Niemieckie plany obejmują budowę terminali stacjonarnych oraz jednostek FSRU o łącznej mocy regazyfikacji do 54 mld m^3 w 2027 r.[34]

Największym terminalem LNG na Morzu Bałtyckim (port specjalistyczny) pozostaje terminal w Świnoujściu, gdzie nadal trwają prace nad zwiększeniem mocy importowych (8,3 mld m^3 gazu rocznie) i zdolności magazynowych. W ciągu najbliższych kilku lat na polskim wybrzeżu Bałtyku ma zostać uruchomiony kolejny terminal (FSRU), umożliwiający eksport ok. 6 mld m^3 gazu (jeden statek), przy czym uwzględniono możliwość cumowania drugiego statku regazyfikującego[35]. Należy przypomnieć, że jeszcze w 2018 r. Polska niemal 80% ropy naftowej importowała z Rosji,

[33] *Government adopts resolution on hydrogen – Finland could produce 10% of EU's green hydrogen in 2030,* Ministry of Economic Affairs and Employment, 9.02.2023, https://valtioneuvosto.fi/en/-/1410877/government-adopts-resolution-on-hydrogen-finland-could-produce-10-of-eu-s-green-hydrogen-in-2030 [dostęp: 9.11.2024].

[34] M. Kędzierski, *Za wszelką cenę. Niemiecki zwrot ku LNG,* „Komentarze OSW" 2023, nr 510.

[35] R. Miętkiewicz, *Bałtyk jako obszar szczególnej ochrony…*, s. 47.

a w lutym 2023 r. całkowicie zaprzestała jej dostaw z tego kraju, w związku z atakiem Rosji na Ukrainę i wygaśnięciem kontraktów długoterminowych. Stało się to możliwe dzięki maksymalizacji obrotów Naftoportu (zaopatruje 4 rafinerie) – jednego z obiektów strategicznych tego typu na Morzu Bałtyckim (kolejne 2 znajdują się na Litwie). Ponadto od 2022 r. żaden z kierunków dostaw ropy nie przekroczył 50% importu[36]. Naftoport jest częścią łańcucha logistycznego dostaw ropy naftowej w Polsce i Niemczech. Ze względu na sytuację geopolityczną i ograniczenia terminalu w Rostocku Naftoport odgrywa istotną rolę w zaspokajaniu zapotrzebowania niemieckich rafinerii (Schwedt i Leuna). Warto wspomnieć, że polska infrastruktura naftowa wspiera dostawy paliw dla walczącej Ukrainy. Zachód pozostał jedynym kierunkiem importu produktów naftowych dla tego kraju (wcześniej szacowany na 5–10%). Od 2022 r. z tego kierunku pochodzi ponad 90% dostaw ropy naftowej i jej produktów, a głównymi dostarczycielami są Polska i Rumunia[37].

Morze Bałtyckie, po Morzu Północnym, jest akwenem o najkorzystniejszych warunkach (ze względu na wietrzność i głębokości morza) dla rozwoju morskiej energetyki wiatrowej w Europie. Reorientacja na odnawialne źródła energii pozyskiwane z mórz Bałtyckiego i Północnego spowoduje jednak znaczne uzależnienie od morza jako obszaru produkcji energii. Prognozy zakładają, że do 2050 r. będzie możliwe pozyskiwanie z energetyki wiatrowej na Morzu Bałtyckim 45 GW[38]. Projekty realizowane przez poszczególne kraje nadbałtyckie (tabela 1) często zmieniają, tak jak w przypadku Polski, obecny kształt systemu elektroenergetycznego w tym regionie.

[36] Najwyższa Izba Kontroli, *Informacja o wynikach kontroli. Realizacja działań w zakresie poprawy bezpieczeństwa paliwowego w sektorze naftowym*, KGP.430.7.2023, Warszawa 2023, s. 69.

[37] M. Ruszel, P. Ogarek, *Bezpieczeństwo paliwowe Polski w kontekście zmian właścicielskich na rynku logistyki produktów naftowych oraz remedies Komisji Europejskiej w sprawie fuzji PKN ORLEN i Grupy LOTOS. Polska u progu embargo na produkty naftowe z Rosji – analiza otwierająca 2023 rok*, Analiza IPE nr 1, Instytut Polityki Energetycznej 2023, s. 14.

[38] K. Bulski, *The Role of the New European Commission and Regional Cooperation in Accelerating Offshore Wind in the Baltic Sea*, BalticWind.EU, 11.09.2024, https://balticwind.eu/the-role-of-the-new-european-commission-and-regional-cooperation-in-accelerating-offshore-wind-in-the-baltic-sea/ [dostęp: 7.11.2024].

Tabela 1. Cele krajów regionu bałtyckiego w zakresie produkcji energii elektrycznej z morskich farm wiatrowych (w tym na Morzu Północnym).

Kraj regionu	Zadeklarowane cele wynikające z planów krajowych			Powierzchnia akwenów pod morską energetykę wiatrową [km^2]	Potencjalna moc [GW]
	2030 [GW]	2040 [GW]	2050 [GW]		
Dania	7,9	7,9	7,9	11 000	42,3
Niemcy	4,1	4,1	4,1	8400	70
Estonia	1	3,5	7	1850	9
Łotwa	0,4	0,4	0,4	300	4
Litwa	1,4	2,8	4,5	664	2,4 (może być zwiększona do 3,3)
Polska	5,9	10,9	10,9	3600	17,2
Finlandia	1	5	12	3500	15,7
Szwecja	0,7	-	-	1400 (może być zwiększona do 4400)	6–7 (może być zwiększona do 22)
Region łącznie	22,5	34,6	46,8	30 714 (może być zwiększona do 33 714) (cała UE – 52 000)	167,6 (może być zwiększona do 183,5)

Źródło: opracowanie własne. Dane zawarte w tabeli pochodzą z materiałów Baltic Energy Market Interconnection Plan (BEMIP) oraz raportu WindEurope Offshore pt. *Wind in EU Maritime Spatial Plans* opublikowanego 19.10.2022 r. Za: P. Wróbel, *Analiza: Inicjatywy UE wzmacniające współpracę regionalną na rzecz morskiej energetyki wiatrowej na Bałtyku*, BalticWind.EU, 4.06.2024, https://balticwind.eu/pl/analiza-inicjatywy-ue-wzmacniajace-wspolprace-regionalna-na-rzecz-morskiej-energetyki-wiatrowej-na-baltyku/ [dostęp: 9.11.2024].

Projekty takie jak Balticconnector między Estonią a Finlandią, rozbudowa połączenia międzysystemowego między Łotwą a Estonią, terminal LNG w Kłajpedzie i terminal LNG w Świnoujściu (długoterminowe kontrakty na dostawy gazu z USA i Kataru) wpłynęły na integrację rynku i zmniejszyły zależność od rosyjskiego gazu w regionie[39]. Co szczególnie istotne, wybrane wyspy bałtyckie (Gotlandia, Wyspy Alandzkie, Bornholm), oprócz strategicznego znaczenia dla NATO (możliwość sprawowania kontroli nad wodami Morza Bałtyckiego i jego przestrzenią powietrzną), mają

[39] *Plan REPowerEU. Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów*, COM(2022) 230 final, Bruksela 2022.

pełnić funkcję wysp energetycznych (miejsc produkcji i dystrybucji energii). Na przykład Bornholmska Wyspa Energetyczna ma w dużym stopniu przyczynić się do transformacji ekologicznej zarówno Danii, jak i pozostałej części Europy (budowa morskich farm wiatrowych o łącznej mocy co najmniej 3 GW i powierzchni ok. 650 km^2). Podmorskie linie energetyczne połączą morskie farmy wiatrowe z instalacjami na Bornholmie oraz z siecią przesyłową energii elektrycznej na Zelandii i w Niemczech[40]. Będzie to wymagać znacznej rozbudowy infrastruktury przesyłowej na dnie Morza Bałtyckiego, która będzie przecinała najważniejsze (o największym natężeniu ruchu) morskie szlaki komunikacyjne prowadzące z Cieśnin Bałtyckich m.in. do rosyjskich portów.

Porty morskie odgrywają ważną rolę w funkcjonowaniu gospodarek krajów regionu Morza Bałtyckiego. Według danych za 2023 r. największym portem pozostaje rosyjska Ust-Ługa (wielkość przeładunków: 112,5 mln t), tuż za nią plasuje się polski Gdańsk (81 mln t), który wyprzedza rosyjskie porty Primorsk (63,1 mln t) i Sankt Petersburg (49,6 mln t). Na dalszych miejscach znalazły się szwedzki Göteborg (36,3 mln t), polski kompleks portowy Szczecin-Świnoujście (35,3 mln t) i litewska Kłajpeda (32,7 mln t)[41]. W portach jest przeładowywany również sprzęt wojskowy w ramach wymiany sprzętu wojskowego jednostek NATO (stałych kontyngentów) czy ćwiczeń i manewrów. Porty morskie zabezpieczają ponadto obsługę zamówień na sprzęt wojskowy (w przypadku Polski jest to uzbrojenie w postaci czołgów i systemów artyleryjskich z USA i Korei Południowej).

Zagrożenia dla obiektów infrastruktury krytycznej na Morzu Bałtyckim

Wśród działań podjętych w ostatnich 10 latach przez Federację Rosyjską w stosunku do państw regionu bałtyckiego i noszących znamiona działań hybrydowych można wskazać następujące (wybrane):

- próby podważenia obowiązujących przepisów prawa międzynarodowego dotyczących delimitacji obszarów morskich (przebiegu granic państwowych), czego przykładem są wydarzenia z 21 maja

[40] *Plan Programu Wyspy Energetycznej Bornholm*, Danish Energy Agency 2023, ID: ENØ-FOR-115, s. 9.

[41] P. Frankowski, *Bałtyckie TOP10*...

2024 r. Rosja zaproponowała ustanowienie systemu prostych linii bazowych we wschodniej części Zatoki Fińskiej i części obwodu kaliningradzkiego, czym podważyła regulacje obowiązujące od 1985 r. (następnego dnia ta propozycja została odwołana przez źródło wojskowo-dyplomatyczne). Działania te obejmowały również fizyczne próby zakłócenia przebiegu granicy na rzece Narwa (Estonia), polegające na przesunięciu boi granicznych na stronę estońską[42]. Jednym z tego rodzaju działań było także prowadzenie ćwiczeń wojskowych na obszarach wyłącznej strefy ekonomicznej Litwy i Łotwy;

- zakłócanie działania systemów nawigacji satelitarnej (szczególnie w Zatoce Gdańskiej, Zatoce Fińskiej, Zatoce Ryskiej) oraz ataki hakerskie na strony internetowe dostarczające informacji o aktualnym położeniu jednostek na morzu[43], którą to aktywność od początku 2023 r. obserwują służby wywiadowcze Norwegii, Danii i Holandii;
- zwiększoną aktywność mającą na celu rozpoznanie portów morskich, rurociągów, kabli światłowodowych, platform wiertniczych i farm wiatrowych[44];
- przeloty rosyjskich samolotów wojskowych na niskich wysokościach w pobliżu obiektów IK (platform wiertniczych) oraz próby zakłócania ćwiczeń wojskowych (przelot nad USS Donald Cook w 2016 r.);
- prawdopodobne naruszenie szwedzkiej granicy przez rosyjskie miniaturowe okręty podwodne[45].

Działania podejmowane przeciwko infrastrukturze portów i terminali specjalistycznych mogą obejmować (uogólnione):

- wykorzystanie tzw. insiderów rekrutowanych spośród pracowników obiektów IK w celu rozpoznania systemów ochrony, wykrywania słabych punktów i wskazywania konkretnych celów działań (elementów kontroli itp.);

[42] N. Aliyev, *Does Russia want to revise its water border with the Nordic and Baltic states?*, International Centre for Defence and Security, 15.08.2024, https://icds.ee/en/does-russia-want-to-revise-its-water-border-with-the-nordic-and-baltic-states/ [dostęp: 16.12.2024].

[43] R. Miętkiewicz, *Systemy autonomiczne w działaniach na morzu*, Gdynia 2023, Wydawnictwo AMW, s. 228.

[44] F. Bryjka, T. Zając, *Wzmocnienie ochrony infrastruktury krytycznej państw UE i NATO*, „Biuletyn PISM" 2023, nr 79, s. 2.

[45] R. Miętkiewicz, *Systemy autonomiczne w działaniach na morzu*..., s. 230.

- bezpośrednie działania sabotażowe mające na celu wywołanie pożarów na dużą skalę (porty, rafinerie, terminale specjalistyczne) lub porażenie prądem wybranych elementów infrastruktury (istotnych z punktu widzenia utrzymania ciągłości działania);
- ataki terrorystyczne przybierające różne formy i przeprowadzane przy użyciu różnych środków;
- działania przestępcze przeciwko obiektom (wrażliwym elementom instalacji) w postaci kradzieży, dewastacji;
- celowe powodowanie katastrof ekologicznych skutkujących dużymi stratami w ekosystemie i powodujących konieczność przerwania lub ograniczenia pracy terminali portowych[46];
- działania mające na celu zablokowanie dostępu do infrastruktury z lądu (wymierzone w linie kolejowe, systemy kontroli ruchu itp.) oraz dostępu z morza (np. przez intencjonalne zatopienie lub uziemienie statku, aby zablokować głębokowodne tory wodne, stawianie min morskich);
- cyberataki mające na celu sparaliżowanie systemów odpowiedzialnych za działanie terminali, centrów operacyjnych i serwisowych (morskie farmy wiatrowe), systemów bezpieczeństwa itp. Ten rodzaj działalności obejmuje również zakłócanie działania systemów nawigacyjnych oraz generowanie awatarów jednostek i statków powietrznych. Według amerykańskich ocen cyberaktorzy powiązani z 161. Specjalistycznym Centrum Szkoleniowym Głównego Zarządu Wywiadowczego Sztabu Generalnego Rosji (jednostka 29155) i innymi jednostkami (26165 i 74455) od co najmniej 2020 r. są odpowiedzialni za operacje w cyberprzestrzeni przeciwko celom globalnym (szpiegostwo, sabotaż i działania dyskredytujące)[47]. Rosyjskie fundusze są wykorzystywane również do finansowania grup hakerskich, takich jak UNC1151/Ghostwriter i Digital Shadows/Conti, w państwach trzecich[48]. W drugiej połowie 2023 r. i pierwszej połowie 2024 r. nastąpiła eskalacja cyberataków. To pokazało, że skala

[46] D. Doğan, D. Çetikli, *Maritime Critical Infrastructure Protection (MCIP) in a Changing Security Environment*, Istanbul 2023, Maritime Security Centre of Excellence (MARSEC COE), s. 35.

[47] *Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure*, Cybersecurity and Infrastructure Security Agency 2024, ID: AA24-249A, s. 1.

[48] A.M. Dyner, *Działania hybrydowe Rosji przeciw państwom NATO i UE*, „Biuletyn PISM" 2022, nr 183, s. 1.

problemu zdecydowanie wzrosła, zarówno pod względem różnorodności i liczby tego rodzaju incydentów, jak i ich konsekwencji[49];
- ataki z wielu kierunków z wykorzystaniem systemów autonomicznych (możliwość wystąpienia we wszystkich domenach).

Działania podejmowane przeciwko infrastrukturze morskiej (morskie farmy wiatrowe, kable podmorskie, rurociągi podmorskie) mogą obejmować (uogólnione):
- zakłócanie prac związanych z budową obiektów na morzu polegające na wykonywaniu niebezpiecznych manewrów w pobliżu statków floty instalacyjnej (bez eskorty), zagrożenia te mogą być generowane przez platformy udające statki służb państwowych;
- naruszanie stref ochronnych ustanowionych wokół instalacji dokonywane pod różnymi pretekstami (awaria nawigacji, urządzeń napędowych itp.) oraz wykorzystywanie swobód prawnych i swobody prowadzenia działalności naukowej na morzu do penetracji podmorskich linii przesyłowych i otoczenia obiektów infrastruktury[50];
- próby przerwania podmorskich połączeń energetycznych i gazociągów polegające na przeciąganiu kotwic i celowym manewrowaniu statkami, działaniach sabotażowych prowadzonych przez wyspecjalizowane grupy sabotażowe;
- operacje z użyciem autonomicznych platform podwodnych (ang. *autonomous underwater vehicles*, AUV), nawodnych (ang. *unmanned surface vehicles*, USV), powietrznych (ang. *autonomous aerial vehicles*, AAV) oraz pochodnych, w tym wykorzystujących najnowsze osiągnięcia z zakresu sztucznej inteligencji, oraz z użyciem rojów (ławic podwodnych). Zagrożenia tego typu, na co wskazują faza morska wojny w Ukrainie oraz wcześniejsze działania terrorystów (np. bojowników Huti na Morzu Czerwonym), mogą być generowane również za pomocą doraźnie improwizowanych środków opartych na technologiach podwójnego zastosowania. Czynnikiem potęgującym tego typu zagrożenia jest postępujący proces proliferacji technologii bezzałogowych[51];

[49] *ENISA Threat Landscape 2024, July 2023 to June 2024*, European Union Agency For Cybersecurity 2024, s. 11. https://doi.org/10.2824/0710888.

[50] P. Mickiewicz, *Bezpieczeństwo energetyczne czy bezpieczeństwo morskie?...*, s. 73.

[51] R. Miętkiewicz, *Systemy autonomiczne (bezzałogowe) jako nowe narzędzie w rękach terrorystów*, w: *XX-lecie wojny z terroryzmem: bilans i konsekwencje*, t. 2: *Infrastruktura krytyczna – analizy – case study*, B. Wiśniewska-Paź, D. Szlachter (red.), Toruń 2022, Wydawnictwo Adam Marszałek, s. 69–98.

- wykorzystanie min morskich i morskich improwizowanych ładunków wybuchowych (ang. *water borne improvised explosive devices*, WBIED), zarówno w postaci nowoczesnych, quasi-inteligentnych min morskich (zapewniających selektywny wybór celów lub umożliwiających opóźnianie działań i wydłużanie czasu występowania zagrożeń), jak i w postaci min stanowiących pozostałości wojenne. Kamuflowaniu takich działań może sprzyjać fakt, że na Morzu Bałtyckim znajduje się ogromny depozyt amunicji chemicznej i konwencjonalnej, w tym od 16 000 do 61 000 min morskich[52].

Podatność obiektów infrastruktury krytycznej na Morzu Bałtyckim

Analiza obiektów IK, ze szczególnym uwzględnieniem tych odpowiedzialnych za produkcję, magazynowanie i przesył energii, wskazuje, że w przypadku wielu z nich (terminale specjalistyczne, morskie farmy wiatrowe) mamy do czynienia z obiektami działającymi na styku środowisk: lądowego, morskiego i powietrznego. Kolejną domeną, która ma bardzo duży wpływ na poziom bezpieczeństwa tego typu obiektów, jest cyberprzestrzeń. Tym samym w rozważaniach dotyczących utrzymania bezpieczeństwa obiektów morskiej IK należy wziąć pod uwagę wiele czynników determinujących możliwość wystąpienia zagrożeń stwarzanych celowo. W przypadku zamierzonego oddziaływania z wykorzystaniem metod typowych dla działań hybrydowych należy zauważyć, że[53]:

- zagrożenia będą miały charakter wielodomenowy, zsynchronizowany i będzie to połączone z silnym oddziaływaniem dezinformacyjnym w mediach;
- zagrożenia podprogowe przybiorą, ze względów politycznych, formę działań sabotażowych lub dywersyjnych, kreowanych przeciwko Polsce oraz innym państwom nadbałtyckim[54];

[52] R. Miętkiewicz, *Dumped conventional warfare (munition) catalog of the Baltic Sea*, „Marine Environmental Research" 2020, t. 161, s. 105057. https://doi.org/10.1016/j.marenvres.2020.105057.

[53] R. Miętkiewicz, *Obiekty morskiej infrastruktury energetycznej – próba określenia podatności na ataki platform bezzałogowych*, „Alcumena. Pismo Interdyscyplinarne" 2023, nr 3(15), s. 217. https://doi.org/10.34813/psc.3.2023.11.

[54] P. Mickiewicz, *Bezpieczeństwo energetyczne czy bezpieczeństwo morskie?*..., s. 72.

- zagrożenia na obszarach morskich (podwodnych i powietrznych) mogą dotyczyć zarówno obiektów infrastrukturalnych, jak i jednostek odpowiedzialnych za dostawy węglowodorów (zbiornikowce kriogeniczne i tankowce do transportu ropy naftowej i produktów ropopochodnych), a w przypadku obiektów *offshore* (morskich farm wiatrowych i platform wiertniczych, rurociągów i kabli podwodnych o różnym przeznaczeniu) – także floty instalacyjnej i serwisowej;
- obiekty o znaczeniu strategicznym dla bezpieczeństwa państw wschodniej flanki NATO są zlokalizowane w bezpośrednim sąsiedztwie granic z Rosją (eksklawa kaliningradzka w przypadku Polski i Litwy, okolice Sankt Petersburga w przypadku Finlandii i Estonii) oraz szlaków prowadzących z Zatoki Fińskiej do Kaliningradu. Obiekty rafinerii i Naftoportu oraz planowanego terminalu FSRU w Gdańsku (Polska) lub terminalu FSRU w Kłajpedzie (Litwa) znajdują się kilkadziesiąt kilometrów od granic z Rosją, co zwiększa ich podatność na zagrożenia hybrydowe;
- obiekty morskiej infrastruktury gazowej i energetycznej państw nadbałtyckich są zlokalizowane wzdłuż tzw. głębi i rynien podmorskich, których głębokości sprzyjają podejmowaniu działań sabotażowych. Do ich prowadzenia mogą być wykorzystywane zarówno okręty podwodne, jak i grupy specjalne operujące z pokładów jednostek nawodnych (np. ze statków badawczych przystosowanych do tego typu działań);
- obiekty w postaci morskich farm wiatrowych, platform wiertniczych, a także podmorskich rurociągów i połączeń kablowych o różnym przeznaczeniu są zlokalizowane poza morzem terytorialnym, na wodach wyłącznej strefy ekonomicznej państw nadbrzeżnych. Duża odległość od brzegu (wybrane inwestycje drugiej fazy rozwoju morskiej energetyki wiatrowej w Polsce sąsiadują z zewnętrznymi granicami tej strefy, a ich odległość od linii brzegowej wynosi blisko 80 km) oraz status prawny wód międzynarodowych (swoboda żeglugi) zwiększają ich podatność na zagrożenia hybrydowe[55];
- wiele obiektów infrastruktury ma charakter transgraniczny (gazociągi, kable energetyczne, łącza telekomunikacyjne) i jest eksploatowanych przez wielu operatorów z różnych krajów. Aby zapewnić

[55] R. Miętkiewicz, *Morskie farmy wiatrowe a bezpieczeństwo morskie państwa*, „Sprawy Międzynarodowe" 2019, t. 72, nr 1, s. 110. https://doi.org/10.35757/SM.2019.72.1.06.

ciągłość ich funkcjonowania, konieczne są współpraca i koordynacja działań (w przypadku gazociągu Baltic Pipe od miejsca wydobycia surowca na Norweskim Szelfie Kontynentalnym do końcowego punktu odbioru w Polsce);

- bardzo intensywny ruch żeglugowy (według raportów HELCOM Bałtyk jest jednym z najbardziej zatłoczonych akwenów na świecie)[56] w pobliżu gazociągów, linii elektroenergetycznych i telekomunikacyjnych ułatwia generowanie sytuacji niebezpiecznych (mapowanie dna, przeciąganie kotwic, stawianie min morskich i morskich improwizowanych ładunków wybuchowych). Takie działania mogą być maskowane np. przez wyłączanie transponderów AIS (ang. *automatic identification system*) lub manewry sugerujące problemy techniczne;
- w przypadku terminali specjalistycznych (Naftoport w Gdańsku, Terminal LNG w Świnoujściu, terminale FSRU) konieczne jest utrzymywanie torów głębokowodnych (sztucznie pogłębianych) w celu zapewnienia ciągłości dostaw. Działaniem umożliwiającym długotrwałe zablokowanie importu może być celowe zatopienie statku w osi toru wodnego (np. pod pozorem wypadku);
- zgodnie z zapisami dokumentów strategicznych wskazujących kierunki rozwoju systemu elektroenergetycznego w Polsce jednym z jego filarów ma być morska energetyka wiatrowa (obok energetyki jądrowej i gazu jako paliwa przejściowego)[57]. Tym samym przerwanie łańcucha produkcyjnego energii elektrycznej staje się głównym celem przeciwnika Polski i innych państw nadbałtyckich (spowodowanie poważnych zakłóceń w gospodarkach i funkcjonowaniu społeczeństw państw nadbrzeżnych);
- Federacja Rosyjska może podejmować próby przejmowania inwestycji związanych z IK lub blokowania ich na różnych etapach realizacji projektu. W rezolucji P9_TA(2024)0079 Parlament Europejski wskazał na rosyjskie działania i operacje mające na celu infiltrację europejskich demokracji i instytucji UE, obecność sieci agentów wpływu, którzy oddziałują na procesy wyborcze i politykę

[56] *HELCOM, ensuring safe shipping in the Baltic,* Helsinki Commission – Baltic Marine Environment Protection Commission 2009, s. 3.

[57] *Polityka Energetyczna Polski do 2040 r.* (PEP2040), Warszawa 2022, Ministerstwo Klimatu i Środowiska, s. 7.

w kluczowych kwestiach strategicznych, takich jak infrastruktura energetyczna[58];

- można się spodziewać, że odpowiedź na eskalację sytuacji i odwetowy charakter działań zantagonizowanych stron coraz częściej będzie obejmować wykorzystanie potencjału militarnego, co stanowiłoby przypomnienie scenariuszy „zimnowojennych" (próby fizycznego wypychania okrętów w celu wyegzekwowania własnej interpretacji przepisów, zawisy helikopterów nad okrętami przeciwnika, blokowanie szlaków komunikacyjnych pod pozorem ćwiczeń);
- w działania mogą być zaangażowane podmioty niepaństwowe (organizacje i ruchy aktywistów o różnej genezie), mniejszości narodowe, grupy przestępcze, wykorzystywane zarówno do działań bezpośrednich, jak i prób testowania procedur bezpieczeństwa, współpracy służb itp.;
- podejmowanym działaniom będą towarzyszyć ataki w mediach prowadzone na dużą skalę i kształtowanie własnej wersji wydarzeń (w przypadku Federacji Rosyjskiej skierowane do rosyjskiego społeczeństwa, w celu utrzymania wizerunku Rosji jako „oblężonej twierdzy" i kraju, który jest demonizowany przez Zachód);
- zagrożenia hybrydowe w regionie bałtyckim mogą się cechować wykorzystaniem nowoczesnych technologii (systemy autonomiczne), a także systemów podwójnego zastosowania, aż po środki całkowicie improwizowane[59];
- w odniesieniu do obiektów morskiej IK zagrożenia mogą być kreowane również z wykorzystaniem obiektów pochodzących z przeszłości. Zdaniem autora do planowania tego typu działań mogą posłużyć dane dotyczące lokalizacji niebezpiecznych depozytów broni chemicznej i konwencjonalnej. Szacunki wskazują na obecność na Bałtyku od 300 000 do 385 000 t amunicji konwencjonalnej i chemicznej, celowo zatopionej po II wojnie

[58] *P9_TA(2024)0079 – Russiagate: zarzuty dotyczące rosyjskiej ingerencji w procesy demokratyczne w Unii Europejskiej – Rezolucja Parlamentu Europejskiego z dnia 8 lutego 2024 r. w sprawie Russiagate: zarzuty dotyczące rosyjskiej ingerencji w procesy demokratyczne w Unii Europejskiej (2024/2548(RSP))*.

[59] R. Miętkiewicz, *Systemy autonomiczne (bezzałogowe) jako nowe narzędzie w rękach terrorystów*..., s. 69–98.

światowej. Do tego należy dodać dużą liczbę wraków z niebezpieczną zawartością[60];
- zagrożenia mogą być kreowane w okresach świątecznych, tak jak w przypadku przecięcia linii energetycznej EstLink 2 (Boże Narodzenie 2024 r.), o co początkowo podejrzewano chiński statek Yi Peng 3[61].

Środki przeciwdziałania zagrożeniom hybrydowym na Morzu Bałtyckim

Charakter zagrożeń hybrydowych występujących i mogących wystąpić na Morzu Bałtyckim wymaga po pierwsze daleko idącej konsolidacji działań i współpracy transgranicznej między instytucjami (głównie siłami zbrojnymi, strażami przybrzeżnymi i wywiadami) państw nadbrzeżnych. Po drugie, konieczne wydaje się wykorzystanie osiągnięć nowoczesnych technologii, ze szczególnym uwzględnieniem morskich systemów autonomicznych i metod sztucznej inteligencji. W celu skutecznego przeciwdziałania incydentom niezbędne jest podjęcie działań o charakterze politycznym (strategie, doktryny, wspólne mapy drogowe członków NATO), prawnym (narzędzia i regulacje prawne umożliwiające tworzenie rozwiązań i egzekwowanie prawa), wojskowym (obecność sił, ćwiczenia, wielonarodowe operacje i inicjatywy), technologicznym (ukierunkowanie badań naukowych, wykorzystanie dostępnych rozwiązań w celu podniesienia poziomu ochrony) oraz budowa wspólnych systemów przetwarzania i wymiany danych (wspólna świadomość sytuacyjna, sprawne dowodzenie). Projekty mające na celu minimalizację zagrożeń hybrydowych dla obiektów IK na morzu powinny obejmować:
- prowadzenie bieżących analiz poziomu bezpieczeństwa, uwzględniających identyfikację zagrożeń, szacowanie prawdopodobieństw i skutków (matryce ryzyka) oraz opracowywanie metod ograniczania tych skutków. Wymaga to ścisłej współpracy pomiędzy sektorami

[60] R. Miętkiewicz, *High explosive unexploded ordnance neutralization – Tallboy air bomb case study*, „Defence Technology" 2022, t. 18, nr 3, s. 524–535. https://doi.org/10.1016/j.dt.2021.03.011.

[61] *Finland-Estonia power cable hit in latest Baltic Sea incident*, The Guardian, 25.12.2024, https://www.theguardian.com/world/2024/dec/25/finland-estonia-power-cable-hit-in-latest-baltic-sea-incident [dostęp: 27.12.2024].

(inwestorzy prywatni) i służbami państwowymi, a także wymiany informacji między sojusznikami;

- prowadzenie monitoringu szlaków komunikacyjnych na Morzu Bałtyckim, który umożliwi wykrywanie i śledzenie statków pomimo wyłączonych transponderów AIS, a także jednostek (głównie o długości do 20 m lub wyporności do 150 t) nieobjętych systemami meldunkowymi VTS (ang. *vessel traffic service*). Ze względu na duże przestrzenie wymagające nadzoru zaleca się korzystanie z komponentu kosmicznego (zdjęcia satelitarne). Aby minimalizować koszty i zwiększać efektywność działań, należy używać autonomicznych systemów monitoringu (w przypadku infrastruktury podwodnej – również ukrytych). Wymagana jest współpraca w tym zakresie na poziomie systemów bezpieczeństwa morskiego państw nadbałtyckich;
- wdrażanie unijnych standardów ochrony IK (mimo że zarządzanie IK leży głównie w gestii państw członkowskich UE). Do najważniejszych dokumentów w tym zakresie należy zaliczyć zmienioną strategię bezpieczeństwa morskiego UE (*Revised EU Maritime Security Strategy*), której wybrane najważniejsze cele to: poprawa odporności podmiotów krytycznych oraz bezpieczeństwa sieci i systemów informatycznych i zapewnienie odporności i ochrony morskiej IK[62], oraz dyrektywę w sprawie odporności podmiotów krytycznych (*The Critical Entities Resilience Directive*), dotyczącą zmniejszenia podatności podmiotów krytycznych na zagrożenia i wzmocnienia ich fizycznej odporności[63];
- wykorzystanie metod sztucznej inteligencji umożliwiające wytypowanie jednostek (na podstawie danych wywiadowczych, danych z monitoringu o podejrzanym zachowaniu w postaci zmniejszenia prędkości, manewrowania nad IK itp.), co ograniczy potencjalnym sprawcom możliwości wykorzystywania dużego natężenia ruchu do maskowania swoich działań. Tego rodzaju aktywność NATO podjęło w styczniu 2025 r., kiedy to Połączone Siły Ekspedycyjne (Joint Expeditionary Force), tworzone przez 10 krajów z Wielką Brytanią na czele, uruchomiły system reagowania (o kryptonimie Nordic

[62] *Council conclusions on the Revised EU Maritime Security Strategy (EUMSS) and its Action Plan*, Brussels 2023, Council of the European Union.

[63] *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.*

Warden) w celu śledzenia potencjalnych zagrożeń dla infrastruktury podmorskiej i monitorowania rosyjskiej floty cieni. System obejmuje 22 obszary zainteresowania, w tym Morze Bałtyckie i Cieśniny Bałtyckie. Wygenerowane przez niego ostrzeżenia będą przekazywane członkom NATO[64];

- utrzymanie zdolności państw nadbrzeżnych do natychmiastowego (w ciągu kilku godzin) reagowania na sabotaż i inne niebezpieczne zdarzenia. Wymaga to posiadania wykwalifikowanych pododdziałów utrzymywanych w odpowiednim reżimie gotowości, zdolnych do szybkiego zajmowania statków i odzyskiwania obiektów IK na morzu i na styku środowisk (porty morskie);
- wsparcie na poziomie międzynarodowym w obliczu pojawiających się zagrożeń, pokazujące akceptację UE i jednakowy sposób postrzegania incydentów i reagowania na nie, jak to miało miejsce w przypadku wydarzeń z grudnia 2024 r. i działań fińskich władz związanych z przejęciem statku Eagle S[65];
- zacieśnienie współpracy pomiędzy siłami zbrojnymi i innymi podmiotami odpowiedzialnymi za utrzymanie bezpieczeństwa na akwenach morskich a interesariuszami branży energetycznej (zwłaszcza naftowo-gazowej i wiatrowej na morzu) w celu budowania świadomości branży w zakresie zagrożeń, podatności i zwiększania odporności, a także zrozumienia potrzeb z tym związanych (np. wydatków na systemy bezpieczeństwa). Dzielenie się wiedzą wrażliwą może budzić niechęć sektora prywatnego;
- przyjęcie przez kraje nadbałtyckie NATO inicjatywy podobnej do deklaracji podpisanej w 2024 r. przez Belgię, Holandię, Niemcy, Norwegię, Wielką Brytanię i Danię w sprawie ochrony podwodnej IK przed atakami i aktami sabotażu[66]. Takie inicjatywy służą wspólnemu

[64] *Joint Expeditionary Force activates UK-led reaction system to track threats to undersea infrastructure and monitor Russian shadow fleet*, 6.01.2025, https://www.gov.uk/government/news/joint-expeditionary-force-activates-uk-led-reaction-system-to-track-threats-to-undersea-infrastructure-and-monitor-russian-shadow-fleet [dostęp: 7.01.2025].

[65] *Joint Statement by the European Commission and the High Representative on the Investigation into Damaged Electricity and Data Cables in the Baltic Sea*, Brussels 2024, European Commission – Statement.

[66] C. Chiappa, *6 countries move to protect the North Sea from Russians*, Politico, 9.04.2024, https://www.politico.eu/article/6-european-countries-sign-pact-protect-critical-energy-infrastructure-north-sea-from-russia/ [dostęp: 27.12.2024].

wdrażaniu odpowiednich rozwiązań, wymianie informacji i najlepszych praktyk w celu zwiększenia poziomu ochrony i prewencji[67];

- kompleksowe podejście do zagrożeń dla IK na morzu, obejmujące zarówno działania zapobiegawcze, jak i ochronne oraz rozwój zdolności do szybkiego odzyskiwania (przywracania) infrastruktury (zdolności do naprawy na poziomie transgranicznym). Takie podejście powinno uwzględniać również łagodzenie skutków ataków na IK przez planowanie z wyprzedzeniem alternatywnych łańcuchów dostaw (przywrócenie sprawności operacyjnej Balticconnector zajęło prawie pół roku). Oznacza to, że ciężar nadal będzie się przesuwał z ochrony na budowanie odporności, przy czym ważne jest nie tylko zapobieganie wystąpieniu niekorzystnego zdarzenia, lecz także gotowość do szybkiego minimalizowania jego skutków (również z wykorzystaniem potencjału partnerów zagranicznych). Przy realizacji takich działań powinny być stosowane międzynarodowe (UE, NATO) ujednolicone standardy oceny odporności IK;
- rozwój inicjatywy *maritime policing* zaproponowanej przez premiera RP, która ma zwiększyć obecność sił morskich NATO i grup działających w ramach bilateralnych i wielonarodowych inicjatyw państw nadbałtyckich (np. na zasadzie rotacyjnego dowodzenia i deklarowania sił do wspólnych operacji). Takie rozwiązanie pozwoli zminimalizować koszty i jednocześnie zwiększyć poziom interoperacyjności sił, a także zbudować właściwe relacje (zaufanie);
- stałe mapowanie i analizowanie podatności i słabych punktów IK przez jej właścicieli (często podmioty prywatne) oraz zacieśnianie współpracy między UE a NATO. Niektóre kraje, takie jak Norwegia czy Wielka Brytania, są członkami tylko jednej z tych organizacji;
- podjęcie szybkich i skutecznych działań w celu zminimalizowania wyzwań związanych z flotą cieni, która ma ogromny potencjał do tworzenia zagrożeń hybrydowych dla morskiej IK (niszczenie linii podmorskich przez przeciąganie kotwic, szpiegostwo, powodowanie celowych kolizji, zagrożenie katastrofą ekologiczną na dużą skalę i inne). W tym celu konieczna jest wielostronna współpraca między krajami UE a Międzynarodową Organizacją Morską, armatorami i ubezpieczycielami, aby promować przepisy prawa

[67] *Joint Declaration on cooperation to secure critical subsea infrastructure*, Regjeringen, 9.04.2024, https://www.regjeringen.no/en/aktuelt/joint-declaration-on-cooperation-to-secure-critical-subsea-infrastructure/id3033122/ [dostęp: 27.12.2024].

międzynarodowego. Przepisy te są skuteczne tylko wtedy, gdy stosuje się do nich większość użytkowników morza.

Wnioski

Zagrożenia hybrydowe to konwergencja działań poniżej progu wojny prowadzonych w wielu domenach, w sposób niejawny bądź bezpośredni (rzadziej), jednak zaplanowany i skoordynowany, przy użyciu różnych środków (politycznych, militarnych, ekonomicznych, prawnych, społecznych i innych). Działania hybrydowe zagrażają bezpieczeństwu funkcjonowania państwa i jego obywateli, a do ich kreowania jest wykorzystywany szeroki wachlarz środków, w tym zarówno narzędzia klasyczne (dezinformacja), jak i nowoczesne (cyberataki). Cechą szczególną jest pełzający, rozłożony w czasie i trudny do natychmiastowego zdiagnozowania charakter zagrożeń, które przybierają różne formy i w których wykorzystuje się efekt synergii[68]. Biorąc pod uwagę powyższe rozważania, należy wskazać, że zagrożenia, które może stwarzać Federacja Rosyjska i podmioty z nią powiązane w odniesieniu do obiektów morskiej IK na Morzu Bałtyckim, są bardzo różnorodne. Po uwzględnieniu podejścia domenowego oraz faktu, że w najbliższych latach zostaną uruchomione liczne obiekty *offshore* (głównie morskie farmy wiatrowe, które w przypadku najbardziej zaawansowanych projektów w 2025 r. wejdą w fazę fizycznej budowy na konkretnych lokalizacjach inwestycyjnych), na pierwszy plan wysuwają się zagrożenia cybernetyczne (oprócz cyberataków jest to także generowanie awatarów jednostek i statków powietrznych naruszających strefy wokół IK oraz zakłócanie systemów nawigacji satelitarnej) i podwodne (skutkujące problemami w funkcjonowaniu IK na dnie morskim), a w dalszej kolejności zagrożenia nawodne. Celem takich działań będzie zakłócenie harmonogramów prac budowlanych lub przerwanie łańcuchów logistycznych przez wywoływanie incydentów z użyciem elementów walki minowej (skrytego stawiania min morskich, morskich improwizowanych ładunków wybuchowych) czy naruszanie stref zakazanych przez autonomiczne jednostki podwodne, okręty podwodne i grupy sabotażowe (w celu prowadzenia aktywności rozpoznawczej, stawiania min morskich, mapowania dna, identyfikacji słabych punktów itp.). Wśród zagrożeń nawodnych

[68] Najwyższa Izba Kontroli, *Informacja o wynikach kontroli. Przygotowanie państwa na zagrożenia związane z działaniami hybrydowymi*, KPB.430.002.2023, Warszawa 2023, s. 7.

do prawdopodobnych form działania można zaliczyć niebezpieczne manewry w stosunku do okrętów instalacyjnych i flot serwisowych prowadzących skomplikowane operacje oraz działania okrętów symulujących problemy techniczne (wleczenie kotwic, dryfowanie w kierunku obiektów IK, celowe kolizje, aż po intencjonalne zatapianie okrętów np. floty cieni). Statki cywilne realizujące działania na zlecenie Rosji mogą przewozić grupy dywersyjne, prowadzić aktywność zwiadowczą oraz powodować zakłócenia w systemach nawigacyjnych i łączności w bezpośrednim sąsiedztwie inwestycji w celu utrudnienia prac. Jeśli dojdzie do dalszego eskalowania sytuacji, zagrożenia będą generowane również przez jednostki zakamuflowane jako okręty służb państwowych krajów nadbałtyckich. Możliwe jest ponadto wykorzystanie autonomicznych platform powietrznych (zdaniem autora artykułu operujących również z pokładów statków cywilnych) do kreowania zagrożeń dla platform wiertniczych i stacji transformatorowych (element morskich farm wiatrowych). Należy przypuszczać, że platformy autonomiczne w niedalekiej przyszłości będą obejmować zarówno systemy hybrydowe (zdolne do zmiany środowiska działania), jak i platformy biomimetyczne przypominające organizmy morskie. Rozwój metod sztucznej inteligencji umożliwia obecnie tworzenie rojów (w przypadku pojazdów podwodnych celowe wydaje się użycie określenia: ławic) platform bezzałogowych, których wykorzystanie pozwala uzyskać efekt synergii.

Analiza zagrożeń hybrydowych wskazuje na rosnące znaczenie nowoczesnych technologii w kreowaniu tych zagrożeń (coraz doskonalsze platformy o stale rosnących możliwościach), zwłaszcza w domenie podwodnej. W związku ze wzrostem możliwości w tej domenie, pod względem zarówno ataku, jak i ochrony i obrony, mówi się nawet o wojnie podwodnej (ang. *seabed warfare*)[69].

Bibliografia

Bryjka F., Zając T., *Wzmocnienie ochrony infrastruktury krytycznej państw UE i NATO*, „Biuletyn PISM" 2023, nr 79.

[69] N. Fridbertsson, *Protecting Critical Maritime Infrastructure – The Role of Technology. General Report,* NATO Parliamentary Assembly, Science and Technology Committee (STC) 2023, s. 1.

Doğan D., Çetikli D., *Maritime Critical Infrastructure Protection (MCIP) in a Changing Security Environment*, Istanbul 2023, Maritime Security Centre of Excellence (MARSEC COE).

Dudzińska K., *Jądrowy zwrot w szwedzkiej polityce energetycznej*, „Biuletyn PISM" 2024, nr 58.

Dyner A.M., *Działania hybrydowe Rosji przeciw państwom NATO i UE*, „Biuletyn PISM" 2022, nr 183.

ENISA Threat Landscape 2024, July 2023 to June 2024, European Union Agency For Cybersecurity 2024. https://doi.org/10.2824/0710888.

HELCOM, ensuring safe shipping in the Baltic, Helsinki Commission – Baltic Marine Environment Protection Commission 2009.

Hybrid CoE Paper 16: *Handbook on maritime hybrid threats: 15 scenarios and legal scans*, The European Centre of Excellence for Countering Hybrid Threats 2023.

Kasprzyk R., *Sztuczna inteligencja i cyberprzestrzeń a proces złośliwego sterowania ludźmi i maszynami*, w: *GlobState*, t. 2: *Wyzwania dla Polski w kontekście zmian w środowisku bezpieczeństwa*, Ł. Jureńczyk, R. Reczkowski (red. nauk.), Bydgoszcz 2020, Centrum Doktryn i Szkolenia Sił Zbrojnych – Uniwersytet Kazimierza Wielkiego, s. 277–298.

Kędzierski M., *Za wszelką cenę. Niemiecki zwrot ku LNG*, „Komentarze OSW" 2023, nr 510.

Mickiewicz P., *Bezpieczeństwo energetyczne czy bezpieczeństwo morskie? Dylemat oceny potencjalnych zagrożeń bezpieczeństwa Polski na akwenie Morza Bałtyckiego w trzeciej dekadzie XXI wieku*, „Nautologia" 2024, nr 161, s. 71–76.

Miętkiewicz R., *Bałtyk jako obszar szczególnej ochrony*, w: *Czy morze pomoże? Bałtyk a bezpieczeństwo energetyczne Polski*, Z. Nowak (red.), Warszawa 2024, Institute for Foreign Affairs, s. 33–46.

Miętkiewicz R., *Dumped conventional warfare (munition) catalog of the Baltic Sea*, „Marine Environmental Research" 2020, t. 161, s. 105057. https://doi.org/10.1016/j.marenvres.2020.105057.

Miętkiewicz R., *High explosive unexploded ordnance neutralization – Tallboy air bomb case study*, „Defence Technology" 2022, t. 18, nr 3, s. 524–535. https://doi.org/10.1016/j.dt.2021.03.011.

Miętkiewicz R., *Morskie farmy wiatrowe a bezpieczeństwo morskie państwa*, „Sprawy Międzynarodowe" 2019, t. 72, nr 1, s. 97–112. https://doi.org/10.35757/SM.2019.72.1.06.

Miętkiewicz R., *Obiekty morskiej infrastruktury energetycznej – próba określenia podatności na ataki platform bezzałogowych*, „Alcumena. Pismo Interdyscyplinarne" 2023, nr 3(15), s. 205–225. https://doi.org/10.34813/psc.3.2023.11.

Miętkiewicz R., *Systemy autonomiczne (bezzałogowe) jako nowe narzędzie w rękach terrorystów*, w: *XX-lecie wojny z terroryzmem: bilans i konsekwencje*, t. 2: *Infrastruktura krytyczna – analizy – case study*, B. Wiśniewska-Paź, D. Szlachter (red.), Toruń 2022, Wydawnictwo Adam Marszałek, s. 69–98.

Miętkiewicz R., *Systemy autonomiczne w działaniach na morzu*, Gdynia 2023, Wydawnictwo AMW.

Nowak Z., Maj M., *Bałtyk jako przestrzeń strategicznej aktywności energetycznej*, w: *Czy morze pomoże? Bałtyk a bezpieczeństwo energetyczne Polski*, Z. Nowak (red.), Warszawa 2024, Institute for Foreign Affairs, s. 33–46.

Nowakowska-Krystman A., *Potencjał obronny Sił Zbrojnych RP w ujęciu relatywnym*, Warszawa 2018, Akademia Sztuki Wojennej.

Paszkowski M., *Litwa, Łotwa oraz Estonia planują stworzenie bałtyckiego hubu energetycznego*, „Komentarze IEŚ" 2024, nr 1259.

Piekarski M., *Ochrona infrastruktury krytycznej na polskich obszarach morskich w kontekście zagrożeń hybrydowych*, Ekspertyzy PTBN nr 1, Polskie Towarzystwo Bezpieczeństwa Narodowego 2023.

Plan Programu Wyspy Energetycznej Bornholm, Danish Energy Agency, 2023, ID: ENØ-FOR-115.

Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure, Cybersecurity and Infrastructure Security Agency 2024, ID: AA24-249A.

Ruszel M., Ogarek P., *Bezpieczeństwo paliwowe Polski w kontekście zmian właścicielskich na rynku logistyki produktów naftowych oraz remedies Komisji Europejskiej w sprawie fuzji PKN ORLEN i Grupy LOTOS. Polska u progu embargo na produkty naftowe z Rosji – analiza otwierająca 2023 rok*, Analiza IPE nr 1, Instytut Polityki Energetycznej 2023.

Wojtasik K., *Analiza wyników badań na temat percepcji zagrożeń o charakterze terrorystycznym wśród uczestników EU PSA*, Analizy PTBN nr 1, Polskie Towarzystwo Bezpieczeństwa Narodowego 2023.

Źródła internetowe

Aliyev N., *Does Russia want to revise its water border with the Nordic and Baltic states?*, International Centre for Defence and Security, 15.08.2024, https://icds.ee/en/does-russia-want-to-revise-its-water-border-with-the-nordic-and-baltic-states/ [dostęp: 16.12.2024].

Braw E., *Russia's growing dark fleet: Risks for the global maritime order*, Atlantic Council, 11.01.2024, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/russias-growing-dark-fleet-risks-for-the-global-maritime-order/ [dostęp: 29.04.2024].

Bulski K., *The Role of the New European Commission and Regional Cooperation in Accelerating Offshore Wind in the Baltic Sea*, BalticWind.EU, 11.09.2024, https://balticwind.eu/the-role-of-the-new-european-commission-and-regional-cooperation-in-accelerating-offshore-wind-in-the-baltic-sea/ [dostęp: 7.11.2024].

Chiappa C., *6 countries move to protect the North Sea from Russians*, Politico, 9.04.2024, https://www.politico.eu/article/6-european-countries-sign-pact-protect-critical-energy-infrastructure-north-sea-from-russia/ [dostęp: 27.12.2024].

Chiriac O., *The 2022 Maritime Doctrine of the Russian Federation: Mobilization, Maritime Law, and Socio-Economic Warfare*, Center for International Maritime Security, 28.11.2022, https://cimsec.org/the-2022-maritime-doctrine-of-the-russian-federation-mobilization-maritime-law-and-socio-economic-warfare/ [dostęp: 7.12.2024].

Finland-Estonia power cable hit in latest Baltic Sea incident, The Guardian, 25.12.2024, https://www.theguardian.com/world/2024/dec/25/finland-estonia-power-cable-hit-in-latest-baltic-sea-incident [dostęp: 27.12.2024].

Finlandia: Władze nie potwierdzają informacji o „przypadkowym" uszkodzeniu Balticconnector, Portal Morski, 13.08.2024, https://www.portalmorski.pl/offshore/56252-finlandia-wladze-nie-potwierdzaja-informacji-o-przypadkowym-uszkodzeniu-balticconnector [dostęp: 29.01.2025].

Frankowski P., *Bałtyckie TOP10*, Namiary na Morze i Handel, 9.05.2024, https://www.namiary.pl/2024/05/09/baltyckie-top10/ [dostęp: 3.01.2025].

Fraszka B., *Państwa bałtyckie a rosyjskie zagrożenia hybrydowe*, Warsaw Institute, 26.10.2020, https://warsawinstitute.org/wp-content/uploads/2020/10/Pa%C5%84stwa-ba%C5%82tyckie-a-rosyjskie-zagro%C5%BCenia-hybrydowe-Bartosz-Fraszka.pdf [dostęp: 29.12.2024].

Government adopts resolution on hydrogen – Finland could produce 10% of EU's green hydrogen in 2030, Ministry of Economic Affairs and Employment, 9.02.2023, https://valtioneuvosto.fi/en/-/1410877/government-adopts-resolution-on-hydrogen-finland-could-produce-10-of-eu-s-green-hydrogen-in-2030 [dostęp: 9.11.2024].

Hagelstam A., *Współpraca przeciwko zagrożeniom hybrydowym*, NATO Review, 23.11.2018, https://www.nato.int/docu/review/pl/articles/2018/11/23/wspolpraca-przeciwko-zagrozeniom-hybrydowym/index.html [dostęp: 2.12.2024].

Hybrid threats as a concept, Frequently asked questions on hybrid threats, The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ [dostęp: 2.12.2024].

Hyndle-Hussein J., *Uszkodzenie fińsko-estońskiego połączenia gazowego Balticconnector*, Ośrodek Studiów Wschodnich, 11.10.2023, https://www.osw.waw.pl/pl/publikacje/analizy/2023-10-11/uszkodzenie-finsko-estonskiego-polaczenia-gazowego-balticconnector [dostęp: 2.01.2025].

Joint Expeditionary Force activates UK-led reaction system to track threats to undersea infrastructure and monitor Russian shadow fleet, 6.01.2025, https://www.gov.uk/government/news/joint-expeditionary-force-activates-uk-led-reaction-system-to-track-threats-to-undersea-infrastructure-and-monitor-russian-shadow-fleet [dostęp: 7.01.2025].

Nordycko-Bałtycki Korytarz Wodorowy, Gaz-system, 2024, https://www.gaz-system.pl/pl/rynek-wodoru/projekty/nordycko-baltycki-korytarz-wodorowy.html [dostęp: 3.01.2025].

Russia's 'shadow fleet': Bringing the threat to light, European Parliament, https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766242/EPRS_BRI(2024)766242_EN.pdf [dostęp: 23.01.2025].

Russia's Shadow Fleet Tankers Could Get Naval Escorts, The Maritime Executive, 18.12.2024, https://maritime-executive.com/article/russia-s-shadow-fleet-tankers-could-get-naval-escorts [dostęp: 9.01.2025].

Westgaard W., *The Baltic Sea Region: A Laboratory for Overcoming European Security Challenges*, Carnegie Endowment for International Peace, 21.12.2023, https://carnegieendowment.org/research/2023/12/the-baltic-sea-region-a-laboratory-for-overcoming-european-security-challenges?lang=en [dostęp: 7.12.2024].

Wróbel P., *Analiza: Inicjatywy UE wzmacniające współpracę regionalną na rzecz morskiej energetyki wiatrowej na Bałtyku*, BalticWind.EU, 4.06.2024, https://balticwind.eu/pl/analiza-inicjatywy-ue-wzmacniajace-wspolprace-regionalna-na-rzecz-morskiej-energetyki-wiatrowej-na-baltyku/ [dostęp: 9.11.2024].

Wyszyński Ł., *Wyszyński: Wejście Szwecji do NATO rodzi korzyści, ale i wyzwania (rozmowa)*, Biznes Alert, 5.03.2024, https://biznesalert.pl/szwecja-nato-zalety-wady-rosja-morze-baltyckie-bezpieczenstwo/ [dostęp: 7.10.2024].

Akty prawne

P9_TA(2024)0079 – Russiagate: zarzuty dotyczące rosyjskiej ingerencji w procesy demokratyczne w Unii Europejskiej – Rezolucja Parlamentu Europejskiego z dnia 8 lutego 2024 r. w sprawie Russiagate: zarzuty dotyczące rosyjskiej ingerencji w procesy demokratyczne w Unii Europejskiej (2024/2548(RSP)) – (Dz. Urz. UE C/2024/6343 z 7.11.2024).

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 27.12.2022).

Inne dokumenty

Council conclusions on the Revised EU Maritime Security Strategy (EUMSS) and its Action Plan, Brussels 2023, Council of the European Union.

Fridbertsson N., *General Report – Protecting Critical Maritime Infrastructure – The Role of Technology*, NATO Parliamentary Assembly 2023, Science and Technology Committee (STC).

Joint Declaration on cooperation to secure critical subsea infrastructure, Regjeringen, 9.04.2024, https://www.regjeringen.no/en/aktuelt/joint-declaration-on-cooperation-to-secure-critical-subsea-infrastructure/id3033122/ [dostęp: 27.12.2024].

Joint Statement by the European Commission and the High Representative on the Investigation into Damaged Electricity and Data Cables in the Baltic Sea, Brussels 2024, European Commission – Statement.

Maritime Doctrine of the Russian Federation, A. Davis, R. Vest (tłum.), Newport 2022, Russia Maritime Studies Institute, United States Naval War College.

McGrath S., *Spotlight on the Shadow War: Inside Russia's Attacks on NATO Territory. A Report by the U.S. Helsinki Commission Staff*, 2024.

Najwyższa Izba Kontroli, *Informacja o wynikach kontroli. Przygotowanie państwa na zagrożenia związane z działaniami hybrydowymi*, KPB.430.002.2023, Warszawa 2023.

Najwyższa Izba Kontroli, *Informacja o wynikach kontroli. Realizacja działań w zakresie poprawy bezpieczeństwa paliwowego w sektorze naftowym*, KGP.430.7.2023, Warszawa 2023.

Plan REPowerEU. Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, COM(2022) 230 final, Bruksela 2022.

Polityka Energetyczna Polski do 2040 r. (PEP2040), Warszawa 2022, Ministerstwo Klimatu i Środowiska.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2020.

Strategiczna Koncepcja Bezpieczeństwa Morskiego Rzeczypospolitej Polskiej, Warszawa–Gdynia 2017, Biuro Bezpieczeństwa Narodowego.

Study on Baltic offshore wind energy cooperation under BEMIP. Final report, ENER/C1/2018-456, Luxembourg 2019, Publications Office of the European Union.

Kmdr dr hab. Rafał Miętkiewicz, prof. AMW

Profesor Akademii Marynarki Wojennej im. Bohaterów Westerplatte w Gdyni (AMW). Doktor habilitowany nauk społecznych w dziedzinie nauk o bezpieczeństwie. Absolwent AMW oraz Akademii Morskiej w Gdyni (studia podyplomowe z zakresu zarządzania kryzysowego). Ekspert Instytutu Polityki Energetycznej im. Ignacego Łukasiewicza w Rzeszowie, członek Polskiego Towarzystwa Bezpieczeństwa Narodowego i Polskiego Towarzystwa Nautologicznego. Oficer liniowy z kilkunastoletnim doświadczeniem na pokładach okrętów morskiej walki minowej, były dowódca ORP „Śniardwy" (645). Wykładowca akademicki na studiach wojskowych, kursach

oraz studiach podyplomowych (Politechnika Gdańska, Uniwersytet Gdański) i MBA (Collegium Civitas w Warszawie). Autor i współautor kilku monografii, podręczników akademickich i kilkudziesięciu artykułów, raportów i analiz. Komentator publikujący na portalach branżowych (Portal Stoczniowy, Biznes Alert, Baltic Wind EU, Polon). Uczestnik programu Erasmus+ oraz europejskich i narodowych programów badawczych (DAIMON, EU Interreg South Baltic, SABUVIS, SWAT-SHOAL). Jego zainteresowania naukowe obejmują wykorzystanie nowoczesnych technologii autonomicznych (bezzałogowych) w działaniach na morzu. W badaniach zajmuje się m.in. kwestiami bezpieczeństwa morskiego państwa, bezpieczeństwa energetycznego, ze szczególnym uwzględnieniem dostaw surowców strategicznych, oraz bezpieczeństwa infrastruktury krytycznej na polskich obszarach morskich.

Kontakt: r.mietkiewicz@amw.gdynia.pl

Terroryzm – studia, analizy, prewencja, 2025, wydanie specjalne: 73–114

https://doi.org/10.4467/27204383TER.25.003.21506

Artykuł

Ataki terrorystyczne i sabotażowe na wybrane systemy infrastruktury krytycznej – perspektywa historyczna

Terrorist and sabotage attacks on selected critical infrastructure systems – a historical perspective

KRZYSZTOF IZAK

https://orcid.org/0000-0001-9815-6035

Autor niezależny

Abstrakt

W artykule zostały opisane ataki terrorystyczne i sabotażowe przeprowadzone na świecie na dwa główne systemy infrastruktury krytycznej (IK): zaopatrzenia w energię oraz transport publiczny. Wybór zdarzeń opisanych w artykule miał charakter subiektywny. W części dotyczącej ataków na sektor energetyczny autor przyjął podział geograficzny – na Bliski Wschód, Afrykę i Amerykę Południową. W części poświęconej atakom na transport publiczny podział obejmuje transport lądowy i transport powietrzny. W przypadku ataków terrorystycznych na infrastrukturę kolejową autor posiłkował się głównie opracowaniem Anneli Bothy obejmującym dane z lat 2000–2017 oraz pracami Briana M. Jenkinsa i Bruce'a R. Butterwortha, a w odniesieniu do transportu lotniczego – pracą Jacques'a Duchesneau. Nie wszystkie dane dotyczące ataków na systemy IK zostały zaktualizowane z uwagi na to, że informacje zawarte w źródłach są cząstkowe. Autor wysuwa wniosek, że wraz z rozwojem nowoczesnych technologii i nasilaniem się napięć w stosunkach międzynarodowych poziom zagrożenia dla IK będzie rósł.

Słowa kluczowe

ataki terrorystyczne, energia, infrastruktura krytyczna, transport, sabotaż

Abstract

The article describes terrorist and sabotage attacks carried out worldwide against two major critical infrastructure (CI) systems: energy supply and public transport. The selection of the events described in the article was subjective. In the section on attacks on the energy sector, the author adopted a geographical division – Middle East, Africa and South America. In the section on attacks on public transport, the division includes land transport and air transport. In the case of terrorist attacks on rail infrastructure, the author mainly used Anneli Botha's study covering data from 2000 to 2017 and the work of Brian M. Jenkins and Bruce R. Butterworth, and for air transport, the work of Jacques Duchesneau. Not all data on attacks on CI systems has been updated due to the fact that the information contained in the sources is partial. The author draws the conclusion that with the development of modern technology and the escalation of tensions in international relations, the level of threat to CI will increase.

Keywords

terrorist attacks, energy, critical infrastructure, transport, sabotage

Wprowadzenie

Ataki terrorystyczne i sabotażowe na obiekty infrastruktury krytycznej (IK) są jednym z poważniejszych zagrożeń bezpieczeństwa państwa. Mają one często daleko idące skutki, ponieważ zniszczenie czy uszkodzenie jednego obiektu IK może negatywnie rzutować na funkcjonowanie innych. Rozbudowa IK jest istotną składową nowoczesnej gospodarki. Siłą napędową tej gospodarki jest m.in. dynamiczny rozwój nowoczesnych technologii informacyjno-komunikacyjnych (ang. *information and communications technology*). Wyzwanie stanowi zapewnienie bezpieczeństwa systemów opartych na tych technologiach, w tym systemów IK.

Częste ataki na rurociągi naftowe, linie energetyczne, sieci telekomunikacyjne i inne obiekty IK skłoniły Radę Bezpieczeństwa ONZ do przyjęcia w 2017 r. rezolucji nr 2341 o ochronie IK przed atakami

terrorystycznymi[1]. W następnym roku Biuro ds. Zwalczania Terroryzmu ONZ (ang. United Nations Office of Counter-Terrorism, UNOCT) oraz Dyrekcja Wykonawcza Komitetu ds. Zwalczania Terroryzmu ONZ (ang. United Nations Counter-Terrorism Committee Executive Directorate, UNCTED) opracowały pierwsze kompendium dobrych praktyk w zakresie ochrony IK przez atakami terrorystycznymi[2]. W 2008 r. Unia Europejska przyjęła dyrektywę 2008/114/WE, która ustanowiła ogólnounijną procedurę identyfikacji i wyznaczania europejskich infrastruktur krytycznych oraz wskazała działania służące poprawie poziomu ich ochrony[3]. Dokument ten został uchylony dyrektywą Parlamentu Europejskiego i Rady UE 2022/2557 przyjętą w grudniu 2022 r., wprowadzającą dodatkowe środki ochrony IK[4]. Dyrektywa ta weszła w życie 16 stycznia 2023 r. Dnia 25 lipca 2023 r. Komisja Europejska zaakceptowała listę 11 sektorów objętych dyrektywą CER dotyczącą odporności podmiotów krytycznych (*The Critical Entities Resilience Directive*). Są to sektory IK świadczące podstawowe usługi w zakresie utrzymywania ważnych elementów systemu społecznego, wspierania gospodarki, zapewniania zdrowia publicznego i bezpieczeństwa oraz ochrony środowiska[5]. Takie działania legislacyjne mają szanse przynieść realne korzyści związane z obniżeniem poziomu zagrożenia terrorystycznego i sabotażowego dopiero w ciągu kilku lat po wdrożeniu ich zapisów przez operatorów IK.

Obecnie niewiele dziedzin życia człowieka i zaawansowanej technicznie cywilizacji pozostaje poza systemami IK. Są to przede wszystkim: turystyka, kultura, duchowość, handel wewnętrzny i powiązana z nimi infrastruktura (dużych centrów handlowych nie zalicza się do IK). Bazary, świątynie, turyści w hotelach, na plażach i w muzeach nadal stanowią

---

1 United Nations, *Security Council resolution 2341 (2017) [on protection of critical infrastructure against terrorist acts]*.

2 UNOCT, UNCTED, Interpol, *The protection of critical infrastructure against terrorist attacks. Compendium of good practices*, https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf [dostęp: 12.12.2024].

3 *Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony*.

4 *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*.

5 European Commission, *Enhancing EU resilience: A step forward to identify critical entities for key sectors*, https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_23_3992/IP_23_3992_EN.pdf [dostęp: 12.12.2024].

doskonały cel dla terrorystów, głównie w Afryce i Azji. Dokonywane przez nich ataki powodowały niekiedy wiele ofiar śmiertelnych, lecz poza nielicznymi wyjątkami nie miały wpływu na gospodarkę kraju. W Egipcie tymi wyjątkami były kampania terrorystyczna ekstremistów muzułmańskich w latach 90. XX w. oraz ataki ISIS w XXI w. W ich wyniku znacznie zmniejszyła się liczba turystów odwiedzających ten kraj, co przełożyło się na spadek dochodu narodowego i konieczność zwiększenia liczby funkcjonariuszy policji potrzebnych do ochrony turystów. Z tych względów w Egipcie infrastruktura turystyczna jest traktowana jak IK.

Celem artykułu była analiza danych statystycznych dotyczących ataków terrorystycznych i sabotażowych na świecie skierowanych na 2 systemy IK – sektor energetyczny i transport publiczny, wraz z krótkim opisem wybranych zdarzeń. Wybór ten miał charakter subiektywny. Autor zrezygnował z przytaczania definicji IK ze względu na ograniczenia związane z objętością tekstu i analizowanie tego zagadnienia w wielu innych publikacjach. W przypadku ataków terrorystycznych na infrastrukturę kolejową w artykule zostały wykorzystane głównie dane pochodzące z pracy Anneli Botha[6] oraz publikacji Briana M. Jenkinsa i Bruce'a R. Butterwortha[7], a w odniesieniu do transportu lotniczego – z pracy Jacques'a Duchesneau[8]. W związku z tym, że w pierwszej i drugiej publikacji prezentowane statystyki kończą się na roku 2017, a w trzeciej – na 2011, autor podjął próbę ich aktualizacji na podstawie innych źródeł. Zawarte w nich informacje były jednak cząstkowe. W części dotyczącej ataków na sektor energetyczny autor przyjął podział geograficzny – Bliski Wschód, Afryka i Ameryka Południowa, a w części poświęconej transportowi publicznemu – podział na transport lądowy i powietrzny. W przypadku transportu powietrznego zdarzenia zostały pogrupowane następująco: porwania,

[6] A. Botha, *Prevention of Terrorist Attacks on Critical Infrastructure*, w: *Handbook of Terrorism Prevention and Preparedness*, A.P. Schmid (red.), https://icct.nl/sites/default/files/2023-01/Handbook_Schmid_2020.pdf, s. 841–870 [dostęp: 20.11.2024].

[7] B.M. Jenkins, B.R. Butterworth, *Train Wrecks and Track Attacks: An Analysis of Attempts by Terrorists and Other Extremists to Derail Trains or Disrupt Rail Transportation*, https://transweb.sjsu.edu/sites/default/files/1794_Jenkins_Train-Wrecks-Train-Attacks.pdf [dostęp: 3.12.2024].

[8] J. Duchesneau, *Aviation Terrorism. Thwarting High-Impact Low-Probability Attacks*, Royal Military College of Canada 2015, https://espace.rmc.ca/jspui/bitstream/11264/741/1/Duchesneau%20PhD%20Thesis%2020150726%20Final%20e-Space%20RMC.pdf [dostęp: 6.12.2024].

zamachy bombowe, terroryzm samobójczy, ataki na porty lotnicze i samoloty uziemione oraz ataki z ziemi na samoloty w powietrzu.

Sektor energetyczny

W każdym państwie sektor energii stanowi główne ogniwo IK, gdyż bez energii pozostałe sektory nie mogą sprawnie funkcjonować. W latach 2000––2009 zanotowano na świecie 565 ataków terrorystycznych na obiekty zaopatrzenia w energię, surowce energetyczne i paliwa, a w latach 2010–2017 aż 1745, co oznacza trzykrotny wzrost liczby takich zdarzeń. W 88% przypadków wykorzystano materiały wybuchowe, w 9% były to podpalenia. Najwięcej ataków odnotowano w dwóch latach: w 2014 r. – 347 i w 2015 r. – 390[9]. W 2003 r. ataki na elektrownie, obiekty sieci gazowych i naftowych stanowiły 25% wszystkich ataków terrorystycznych na świecie. W 2005 r. odsetek ten wzrósł do 35%. W 2016 r. liczba ataków terrorystycznych wymierzonych w przemysł naftowy i gazowniczy wzrosła o 14% w stosunku do roku poprzedniego i stanowiły one prawie 42% z ogólnej liczby tego rodzaju zdarzeń. Dane te obejmują również inne działania przestępcze, m.in. kradzieże ropy lub gazu z rurociągów, wymuszenia lub sprzedaż surowców, m.in. w celu finansowania ugrupowań terrorystycznych[10].

Sektor energetyczny jest zagrożony zwłaszcza w rejonach, w których dochodzi do rebelii bądź działań wojennych. Przykładem jest Ukraina, której infrastruktura energetyczna jest nieustannie atakowana. Skutkiem wojny toczącej się w tym kraju była akcja sabotażowa polegająca na wysadzeniu 26 września 2022 r. gazociągów Nord Stream 1 i Nord Stream 2, którymi przesyłano gaz z północnej Rosji do Niemiec[11]. To wydarzenie było symbolicznym końcem dostępu Europy do taniej energii. Dotychczasowa strategia jej pozyskiwania ze złóż ropy, węgla i gazu w Rosji i innych krajach

[9] A. Botha, *Prevention of Terrorist Attacks...*, s. 855–856.

[10] A. Olech, *Terrorist Threats to the Energy Sector in Africa and the Middle East*, w: S.J. Lohman i in., *Countering Terrorism on Tomorrow's Battlefield: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 2)*, https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1953&context=monographs, s. 166 [dostęp: 15.12.2024].

[11] P. Oltermann, P. Beaumont, D. Sabbagh, *European leaders blame sabotage as gas pours into Baltic from Nord Stream pipelines*, The Guardian, 28.09.2022, https://www.theguardian.com/business/2022/sep/27/nord-stream-1-2-pipelines-leak-baltic-sabotage-fears [dostęp: 28.12.2024].

regionu nie może być kontynuowana z powodów politycznych i ekonomicznych. Z kolei ciągłości dostaw z krajów znad Zatoki Perskiej przez Morze Czerwone i Kanał Sueski zagraża szyicka rebelia jemeńskiego ruchu Huti, zwanego również Zwolennikami Boga (arab. Ansar Allah), a wcześniej akty piractwa w Zatoce Adeńskiej i na Oceanie Indyjskim dokonywane przez somalijskich bandytów, wspieranych przez Ruch Młodych Mudżahedinów (arab. Harakat asz-Szabab al-Mudżahidin).

Sektor energetyczny, podobnie jak inne systemy IK, jest również zagrożony cyberatakami. Jeden z najbardziej niszczycielskich przeprowadzono w sierpniu 2012 r. za pomocą wirusa Shamoon. Celem był saudyjski koncern paliwowo-chemiczny Saudi Aramco. Wirus zainfekował 10 000 komputerów w firmie i spowodował wyłączenie na prawie miesiąc wszystkich ważnych sieci wewnętrznych. Uznano, że atakującym nie chodziło o przejęcie danych, lecz o wyeliminowanie jak największej liczby systemów. Po tym zdarzeniu koncern odizolował swoje systemy elektroniczne od świata zewnętrznego. Pięć lat później Aramco zostało zaatakowane ponownie, tym razem za pomocą nowej wersji złośliwego oprogramowania – Shamoon 2.0. Celem było usunięcie danych oraz spowodowanie eksplozji i ofiar śmiertelnych. Cyberataki te, pokazujące, jak poważne skutki mogą mieć działania hakerów, nasiliły obawy o bezpieczeństwo obiektów energetycznych na świecie[12]. Dotkliwe konsekwencje miał atak hakerski w maju 2021 r. na system komputerowy sterujący pracą rurociągu naftowego Colonial Pipeline w Stanach Zjednoczonych. Doszło do sześciodniowej przerwy w dostawach ropy, co wywołało panikę społeczną i masowy wykup materiałów pędnych[13]. W listopadzie 2023 r. została zaatakowana wewnętrzna sieć komputerowa kanadyjskiej firmy Trans-Northern Pipelines Inc., której sieć rurociągów łączy m.in. rafinerie z lotniskami. Spowodowało to opóźnienia w wymianie plików i generowaniu raportów na temat oceny inżynieryjnej rurociągów i związanych z nimi obiektów, ale bez strat materialnych[14].

[12] A. Olech, *Terrorist Threats…*, s. 168.

[13] Ł. Kielban, *Zagrożenia Infrastruktury Krytycznej – podstawy dla urzędników i przedsiębiorców*, Polska Platforma Bezpieczeństwa Wewnętrznego, 13.06.2024, https://ppbw.pl/zagrozenia-infrastruktury-krytycznej-podstawy/ [dostęp: 13.12.2024].

[14] A. Ribeiro, *Cyber attacks continue to hit critical infrastructure, exposing vulnerabilities in oil, water, healthcare sectors*, Industrial Cyber, 14.02.2024, https://industrialcyber.co/critical-infrastructure/cyber-attacks-continue-to-hit-critical-infrastructure-exposing-vulnerabilities-in-oil-water-healthcare-sectors/ [dostęp: 14.12.2024].

Celem ataków dywersyjno-terrorystycznych są również elektrownie i linie je zasilające. Na Kaukazie Północnym to zjawisko pojawiło się stosunkowo niedawno. W 2009 r. jeden z dżamaatów Emiratu Kaukaskiego wziął na siebie odpowiedzialność za awarię w Sajańsko-Suszeńskiej Elektrowni Wodnej na Syberii (oficjalne dochodzenie wykluczyło zamach terrorystyczny). Wcześniej przywódca Emiratu Kaukaskiego, Doku Umarow, groził wojną dywersyjną skierowaną przeciw infrastrukturze energetycznej w głębi Rosji. W republice Kabardo-Bałkarii 22 października 2008 r. terroryści wysadzili konstrukcje wspierające linie elektroenergetyczne. W Inguszetii we wrześniu 2009 r. trzykrotnie zostały zaatakowane linie wysokiego napięcia. Pierwszy atak, polegający na wysadzeniu słupa wysokiego napięcia, spowodował straty w wysokości ponad 5 mln rubli[15]. Do pierwszego udanego ataku na cel o znaczeniu strategicznym doszło na Kaukazie Północnym 21 lipca 2010 r. Grupa bojowników dokonała sabotażu w Baksańskiej Elektrowni Wodnej w Kabardo-Bałkarii. Zabito strażników, poddano torturom pracowników cywilnych i podłożono ładunki wybuchowe. Eksplozje zniszczyły 2 z 3 generatorów i wywołały pożar. Straty wyceniono na 800 mln rubli. Dnia 7 września 2010 r. wybuchł pożar w Irganajskiej Elektrowni Wodnej w Dagestanie. W trakcie jego gaszenia odkryto ładunki wybuchowe i minę pułapkę. Do sabotażu przyznał się dagestański Dżamaat Guraba i poinformował, że na terenie elektrowni podłożono łącznie 9 ładunków. Podczas remontu w lutym 2011 r. odnaleziono 2 bomby składające się z kostek trotylu, plastiku i pyłu aluminiowego. Nie ma informacji o zlokalizowaniu pozostałych ładunków[16].

W drugiej dekadzie XXI w. doszło do wielu naruszeń przestrzeni powietrznej nad obiektami jądrowymi we Francji, ale nie potwierdzono związku tych zdarzeń z działalnością terrorystyczną. Francuskie prawo zakazuje lotów w odległości 5 km od terenu elektrowni atomowej i na wysokości poniżej 1000 m. Złamanie tego zakazu jest zagrożone grzywną w wysokości 75 000 euro i karą 1 roku pozbawienia wolności. W październiku i listopadzie 2014 r. odnotowano prawie 30 przelotów bezzałogowych statków powietrznych (ang. *unmanned aerial vehicles*, UAV) nad 15 elektrowniami jądrowymi we Francji. Celem prowokacji było zakłócenie kontroli i systemu ochrony tych obiektów. Początkowo podejrzewano, że sprawcami

[15] T.W. Grabowski, *Terroryzm północnokaukaski. Źródła, przejawy i przeciwdziałanie zjawisku*, Kraków 2017, s. 272.

[16] Tamże, s. 272–273.

są przeciwnicy energetyki jądrowej, którzy starają się w ten sposób zwrócić uwagę na niedostateczny – według nich – poziom bezpieczeństwa tego rodzaju elektrowni. Greenpeace zaprzeczył, że ma związek z tymi wydarzeniami, i nazwał je bardzo niepokojącymi. Na początku stycznia 2015 r. 2 drony pojawiły się nad elektrownią atomową w Nogent-sur-Seine w północnej Francji[17]. Mimo wprowadzenia systemów wykrywających UAV doszło do kolejnych incydentów z ich udziałem. W listopadzie 2021 r. członkowie Greenpeace rozbili o betonową osłonę reaktora elektrowni jądrowej Bugey we Francji dron w kształcie Supermana. Zdarzenie to nie zagroziło bezpieczeństwu reaktora, ale pokazało, że UAV mogą mieć bardzo nietypowe kształty, utrudniające ich wykrycie[18]. W październiku 2023 r. drony przeleciały nad 7 elektrowniami jądrowymi we Francji, a 1 sierpnia 2024 r. – nad 6 takimi obiektami[19].

Bliski Wschód

W latach 1918–1939 odnotowywano pierwsze przypadki atakowania rurociągów naftowych na Bliskim Wschodzie. Podczas antyżydowskiego i antybrytyjskiego powstania w Palestynie w latach 1936–1939 celem akcji sabotażowych stał się rurociąg, którym przesyłano ropę naftową z Iraku do Hajfy[20]. W 1970 r. palestyńskie organizacje mające bazy w Jordanii domagały się od króla Husajna zdemontowania jordańskiej części tego rurociągu. Gdy odmówił, Palestyńczycy próbowali wysadzić obiekt[21].

---

[17] *Au total, 17 sites nucléaires ont été survolés par des drones depuis octobre*, Le Monde, 29.01.2015, https://www.lemonde.fr/planete/article/2015/01/29/dix-sept-sites-nucleaires-ont-ete-survoles-par-des-drones-depuis-octobre_4565967_3244.html [dostęp: 29.01.2025]; AFP, *Deux drones ont survolé la centrale nucléaire de Nogent-sur-Seine*, BFMTV, 4.01.2015, https://www.bfmtv.com/police-justice/deux-drones-ont-survole-la-centrale-nucleaire-de-nogent-sur-seine_AN-201501040009.html [dostęp: 4.01.2025].

[18] J. Łukasiewicz, *Bezzałogowe statki powietrzne jako źródło zagrożeń infrastruktury zaopatrzenia państw w energię elektryczną oraz proponowane metody ochrony tej infrastruktury*, „Terroryzm – studia, analizy, prewencja" 2022, nr 1, s. 103. https://doi.org/10.4467/27204383TER.22.004.15420.

[19] *De nouvelles centrales nucléaires survolées par de présumés drones*, TF1Info, 2.08.2024, https://www.tf1info.fr/societe/de-nouvelles-centrales-nucleaires-survolees-par-de-presumes-drones-1562592.html [dostęp: 2.08.2024].

[20] K. Gebert, *Pokój z widokiem na wojnę. Historia Izraela*, Warszawa 2023, s. 122.

[21] A. Chiczkin, *Jordania: zamach stanu w odwrotnej kolejności*, TopWar, 12.04.2021, https://pl.topwar.ru/181817-iordanija-perevorot-naoborot.html [dostęp: 12.12.2024].

Po wkroczeniu sił USA do Iraku w 2003 r. ropociągi wielokrotnie były celami rebeliantów, a później ISIS. W 2014 r. w Syrii ISIS zdobyło kontrolę nad rurociągiem i przejmowaną ropę sprzedawało Turcji[22]. W tym samym roku ISIS przejęło kontrolę nad irackim miastem Bajdżi, gdzie znajduje się największa w kraju rafineria ropy naftowej. To spowodowało najpotężniejszy kryzys w Iraku od czasu opuszczenia go przez Amerykanów w grudniu 2011 r. i przejęcia władzy przez lokalne elity. Rafineria w Bajdżi, do której prowadzą ropociągi ze wszystkich irackich pól naftowych, zaopatrywała w produkty rafineryjne 11 z 18 irackich prowincji. Dżihadystom nie udało się jej uruchomić. W listopadzie 2014 r. obiekt został odbity przez irackie wojsko przy wsparciu amerykańskiego lotnictwa. W dniu 13 czerwca 2015 r. dżihadyści przeprowadzili w nim zamach samobójczy. Sprawcy wjechali na teren rafinerii samochodem wypełnionym ładunkami wybuchowymi. Zginęło 11 osób, a 27 zostało rannych[23].

Gazociągi i ropociągi są również celem arabskich separatystów w południowo-zachodniej części Iranu. W lutym 2024 r. celem działań sabotażowych stały się dwie nitki gazociągu. Teheran pośrednio oskarżył o to Izrael[24]. Wiele ataków terrorystycznych było skierowanych na biegnący przez północną część półwyspu Synaj gazociąg, którym Egipt dostarcza gaz do Izraela. W lipcu 2010 r. usiłowali go wysadzić Beduini w ramach protestu przeciwko rządowi w Kairze. Do kolejnego ataku doszło w lutym 2011 r. W wyniku Arabskiej Wiosny w Egipcie powstała organizacja Obrońcy Jerozolimy (arab. Ansar Bajt al-Makdis). Do końca 2013 r. zaatakowała ona ten gazociąg 13 razy[25]. W listopadzie 2014 r. Obrońcy Jerozolimy przyjęli zwierzchnictwo ISIS i kontynuowali ataki jako Prowincja Synaj (Wilajet Sinai). Od 2011 r. do końca 2015 r. stał się on celem kilkadziesiąt razy.

[22] D. Butter, *Does Turkey really get its oil from Islamic State?*, BBC, 1.12.2015, https://www.bbc.com/news/world-europe-34973181 [dostęp: 1.12.2025].

[23] O. Wasiuta, S. Wasiuta, P. Mazur, *Państwo Islamskie ISIS. Nowa twarz ekstremizmu*, Warszawa 2018, s. 205.

[24] *Iran condemns 'terrorist' attack on gas pipelines*, Al Jazeera, 14.02.2024, https://www.aljazeera.com/news/2024/2/14/iranian-gas-pipeline-blasts-due-to-terrorism-and-sabotage-official-says [dostęp: 14.12.2024].

[25] D. Barnett, *Ansar Jerusalem claims responsibility for recent Sinai gas pipeline attack*, FDD's Long War Journal, 19.01.2014, https://www.longwarjournal.org/archives/2014/01/ansar_jerusalem_claims_respons.php [dostęp: 19.01.2025].

Terroryści wysadzali jego niewielkie odcinki, co skutkowało przerwami w dostawie gazu do Izraela i znacznymi stratami materialnymi[26].

Po raz pierwszy ośrodek przemysłu naftowego w Arabii Saudyjskiej został zaatakowany 1 maja 2004 r. Atak na rafinerię w Janbu nad Morzem Czerwonym przeprowadziło 4 napastników. Zginęło w nim 6 osób – 5 pracowników koncernu z Zachodu oraz funkcjonariusz saudyjskiej ochrony[27]. Dnia 29 maja 2004 r. Al-Kaida zaatakowała instalacje naftowe i osiedle dla pracujących przy nich cudzoziemców w Al-Khobar, we wschodniej części Arabii Saudyjskiej. Zginęły 22 osoby, w tym 19 obcokrajowców[28].

Od kilku lat instalacje przemysłu petrochemicznego w Arabii Saudyjskiej są celem ataków wspomnianego już ruchu Huti. W lipcu 2017 r. rebelianci po raz pierwszy zaatakowali za pomocą pocisku rakietowego instalacje naftowe w porcie Janbu. Pocisk nie dosięgnął celu[29]. W następnych latach Huti kontynuowali ostrzał saudyjskich lotnisk i obiektów przemysłu petrochemicznego przy użyciu rakiet i dronów. Precyzyjny atak ponad 20 dronów i pocisków manewrujących uszkodził 14 września 2019 r. instalacje naftowe w Bukajk i Churajs należące do koncernu Aramco. W wyniku zniszczeń wydobycie ropy w Arabii Saudyjskiej zmniejszyło się o połowę, co spowodowało krótkotrwały skok cen tego surowca o 20%. Odpowiedzialność za ten atak wziął ruch Huti, a jako przyczynę podał interwencję krajów arabskich w Jemenie. Natomiast Arabia Saudyjska oskarżyła o ten atak Iran. Teheran odrzucił zarzuty, wsparł wersję Huti i zagroził siłom USA w Zatoce Perskiej. Stany Zjednoczone były uważane za gwaranta niezakłóconego eksportu ropy z Zatoki Perskiej. Amerykańska marynarka wojenna strzegła szlaków żeglugowych nie tylko na tym akwenie, lecz także na pozostałych obszarach Morza Arabskiego. Udział ropy z tego regionu w imporcie USA zmalał jednak do 16%. Większość

[26] AFP, *Des djihadistes revendiquent l'attaque d'un gazoduc*, 20 Minutes, 8.01.2016, https://www.20min.ch/fr/story/des-djihadistes-revendiquent-l-attaque-d-un-gazoduc-826827705429 [dostęp: 9.01.2025].

[27] M. Scheuer, S. Ulph, J.C.K. Daly, *Saudi Arabian Oil Facilities: The Achilles Heel of the Western Economy*, The Jamestown Foundation 2006, https://jamestown.org/wp-content/uploads/2006/05/Jamestown-SaudiOil.pdf, s. 43 [dostęp: 24.02.2025].

[28] K. Izak, *Leksykon organizacji i ruchów islamistycznych*, Warszawa 2014, s. 322.

[29] *Atak rakietowy na Rijad*, Defence24, 5.11.2017, https://defence24.pl/atak-rakietowy-na-rijad [dostęp: 5.11.2024].

wydobytej ropy (80%) płynęła do Azji (dane z 2019 r.)[30]. W okresie od stycznia 2018 r. do końca 2021 r. Huti wystrzelili w kierunku Arabii Saudyjskiej 430 pocisków balistycznych i 850 dronów. W 2021 r. przeprowadzali w ciągu miesiąca średnio 78 ataków wymierzonych w to państwo, podczas gdy w 2020 r. średnia ta wynosiła 38[31]. W 2023 r. Huti zaczęli intensywnie atakować przy użyciu rakiet i dronów statki przepływające u wybrzeży Jemenu. W styczniu 2024 r. najwięksi armatorzy wstrzymali żeglugę przez Morze Czerwone. Zrobiły to także koncerny naftowe BP i Shell. Sytuacja stała się na tyle poważna, że Chiny zaczęły wywierać presję na Iran, aby powstrzymał ataki Huti[32].

Afryka

Ponad 30 uzbrojonych terrorystów należących do organizacji Podpisani Krwią (arab. Muwakaum bi ad-Dima), zwanej również Zamaskowaną Brygadą (arab. Katibat al-Mulassamin), zaatakowało 16 stycznia 2013 r. algierską bazę skraplania gazu w Tiguentourine, w pobliżu miasta In Amenas na Saharze. Ośrodek należał do konsorcjum, w którego skład wchodziły: brytyjski BP, norweski Statoil i algierska państwowa firma Sonatrach. W zakładzie przebywało ponad 800 pracowników, w tym 137 obcokrajowców. Po 4 dniach oblężenia i szturmie algierskiej jednostki specjalnej zakładnicy zostali uwolnieni. W wyniku ataku śmierć poniosło 38 osób, zginęło również 29 terrorystów[33].

W latach 90. XX w. w południowo-wschodniej Nigerii uzbrojone bandy przeprowadzały nieskoordynowane ataki na pracowników i własność koncernów naftowych oraz funkcjonariuszy sił bezpieczeństwa ochraniających infrastrukturę naftową. Część tych grup zjednoczyła się w Ruch

[30] M.A. Piotrowski, *Taktyka oraz konsekwencje strategiczne ataku na instalacje naftowe Arabii Saudyjskiej*, „Biuletyn PISM" 2019, nr 137, https://pism.pl/publikacje/Taktyka_oraz_konsekwencje_strategiczne_ataku_na_instalacje_naftowe_Arabii_Saudyjskiej [dostęp: 4.12.2024].

[31] *Atak rakietowy na Arabię Saudyjską i naloty w Jemenie*, Defence24, 27.12.2024, https://defence24.pl/geopolityka/arabia-saudyjska-przeprowadza-naloty-huti-w-jemenie-za-atak-na-miasto-jazan [dostęp: 27.12.2024].

[32] J. Losik, *Wiadomo, co przewoził zaatakowany statek. Powód do niepokoju dla Moskwy*, Money.pl, 27.01.2024, https://www.money.pl/gospodarka/nieoczekiwany-cios-w-handel-rosyjskim-paliwem-zaplonal-tankowiec-6989192670440384a.html [dostęp: 27.01.2025].

[33] T. Kijewski, *Atak terrorystyczny na kompleks gazowy Tiguentourine w In Amenas w Algierii w styczniu 2013 r. jako przykład nowych zagrożeń dla energetycznej infrastruktury krytycznej i bezpieczeństwa wewnętrznego państwa*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9, s. 202–224.

na rzecz Emancypacji Delty Nigru (ang. Movement for the Emancipation of the Niger Delta, MEND). MEND wymuszał haracze na koncernach naftowych, dokonywał kradzieży i przemytu ropy. Koncerny oszacowały, że straty wyniosły 9 mln baryłek ropy naftowej rocznie. W styczniu 2006 r. kilkudziesięciu uzbrojonych członków organizacji opanowało jeden z obiektów Shella i uprowadziło 4 specjalistów z zagranicy zatrudnionych przez brytyjsko-holenderski koncern. Rzecznik MEND, Jomo Gbomo, zapowiedział wtedy, że to dopiero początek działań jego organizacji. *Naszym celem jest całkowite zniszczenie zdolności nigeryjskiego rządu do eksportu ropy*[34].

W marcu 2016 r. grupa zbrojna Mściciele z Delty Nigru (ang. Niger Delta Avengers, NDA) ogłosiła oficjalnie swoje istnienie. Dwa miesiące później zaatakowała platformę wiertniczą koncernu Chevron, a następnie instalacje naftowe i gazownicze w delcie Nigru. Podczas trzymiesięcznej operacji przeprowadzono ponad 30 ataków. Dochodziło do nich również w kolejnych miesiącach 2016 r., ale znacznie zmniejszyła się ich intensywność. Spowodowały one 36-procentowy spadek produkcji ropy naftowej, co przełożyło się na zmniejszenie się dochodów państwa o połowę. Organizacja wydała oświadczenie, w którym domagała się większego udziału w sprzedaży ropy naftowej i zagroziła zakłóceniem funkcjonowania gospodarki Nigerii, jeśli jej żądania nie zostaną spełnione. NDA dążą do utworzenia suwerennego państwa w delcie Nigru[35]. W tym regionie kraju nadal jest niespokojnie. Na wodach Nigerii zagrożenie stanowią piraci, a mieszkańcy delty Nigru dokonują kradzieży ropy wprost z rurociągów[36].

We wrześniu 2022 r. władze Nigerii ogłosiły, że import ropy z tego kraju był najniższy od 25 lat, a jej produkcja spadła poniżej 1,18 mln baryłek dziennie, co według OPEC (ang. Organization of the Petroleum Exporting Countries) uplasowało ten kraj na drugim miejscu, po Angoli. Zdaniem ówczesnego prezydenta Muhammadu Buhariego była to wina masowych kradzieży tego surowca w południowo-wschodniej części kraju. Sytuacja ta mocno wpłynęła na stan finansów państwa. W sierpniu 2022 r. skalę kradzieży ropy naftowej w Nigerii oszacowano na 700 000 baryłek dziennie.

[34] D. Howden, *Shell may pull out of Niger Delta after 17 die in boat raid*, The Independent, 17.01.2006, https://web.archive.org/web/20170527010950/http://www.corpwatch.org/article.php?id=13121 [dostęp: 17.01.2025]. Tłumaczenie pochodzi od autora (dop. red.).

[35] A. Olech, *Terrorist Threats…*, s. 173–174.

[36] F. Mbah, *In Nigeria's crude capital, a plan to win the war against oil theft*, Al Jazeera, 19.12.2024, https://www.aljazeera.com/news/2024/12/19/in-nigerias-crude-capital-a-plan-to-win-the-war-against-oil-theft [dostęp: 19.12.2024].

Niektóre firmy twierdziły, że nawet ponad 80% ropy, która wpływa do rurociągów, jest kradzione w trakcie jej przepływu[37]. W innej części Afryki, w Mozambiku, olbrzymie straty spowodował atak terrorystyczny przeprowadzony przez organizację Zwolennicy Tradycji (arab. Ansar as-Sunna). Jej bojownicy zajęli 24 marca 2021 r. portowe miasto Palma w północno-wschodniej części kraju i okupowali je do 8 kwietnia. W tym czasie dokonali poważnych zniszczeń, zabili wielu mieszkańców oraz 12 inżynierów z krajów zachodnich, pracujących przy realizacji projektu gazowego wartego 60 mld dolarów[38].

Ameryka Południowa

Kolumbia jest krajem, w którym przeprowadzono najwięcej na świecie ataków terrorystycznych i akcji sabotażowych na rurociągi i linie energetyczne zasilające urządzenia do eksploatacji ropy naftowej. Władze tego kraju od połowy lat 60. XX w. walczą z ugrupowaniami, które są pozostałością po marksistowskich partyzantkach. Są to m.in. Armia Wyzwolenia Narodowego (hiszp. Ejército de Liberación Nacional, ELN) i Rewolucyjne Siły Zbrojne Kolumbii (hiszp. Fuerzas Armadas Revolucionarias de Colombia, FARC). Obecnie rozłamowe grupy FARC walczą zarówno między sobą (nie zgodziły się na porozumienie pokojowe zawarte w 2016 r.), jak i z ELN i różnymi grupami paramilitarnymi o kontrolę nad lukratywnymi uprawami koki, nielegalnym wydobyciem złota i szlakami przemytniczymi oraz atakują rurociągi naftowe. Dla Kolumbii ropa naftowa stanowi ok. 1/3 dochodów z eksportu, co oznacza, że nawet niewielkie zakłócenia w wydobyciu i transporcie tego surowca mają wpływ na dochody państwa[39]. Ataki na infrastrukturę naftową, należącą do krajowych i zagranicznych spółek naftowych, pozostają jedną z podstawowych metod walki z rządem. W latach 1987–1991 ELN dokonała 141 aktów sabotażu na najważniejszych odcinkach ropociągów biegnących w środkowej części Kolumbii. Straty finansowe poniesione w ciągu

[37] *Nigerian oil exports at lowest level in 25 years due to oil theft*, Al Jazeera, 9.09.2022, https://www.aljazeera.com/news/2022/9/9/nigerian-oil-exports-at-lowest-level-in-25-years-due-to-oil-theft [dostęp: 9.01.2025].

[38] T. Mandrup, *The attack on Palma in Mozambique: An insurgency getting out of hand?*, Risk Intelligence, 8.04.2021, https://www.riskintelligence.eu/analyst-briefings/the-attack-on-palma-in-mozambique-an-insurgency-getting-out-of-hand [dostęp: 8.01.2025].

[39] D. Czyżewski, *Ropa pod uprawami koki, czyli problemy Kolumbii*, Energetyka24, 2.10.2021, https://energetyka24.com/ropa/ropa-pod-uprawami-koki-czyli-problemy-kolumbii-komentarz [dostęp: 2.12.2024].

tych 4 lat oszacowano na 634 mln dolarów[40]. Od 1986 r. do 2002 r. ELN przeprowadziła również 950 ataków bombowych (średnio od 40 do 50 ataków rocznie) na 800-kilometrowy odcinek rurociągu, którym płynie ropa ze złoża Caño Limón w zachodniej części Kolumbii. Jego udziałowcem była spółka Occidental Petroleum Corp. z Los Angeles. Straty oszacowano na 2,5 mld dolarów[41]. Skutkiem tych działań było również zanieczyszczenie środowiska naturalnego na ogromną skalę. Na przykład ropa naftowa wydobywająca się z rurociągu wysadzonego w czerwcu 1990 r. zanieczyściła znaczny odcinek rzeki Catatumbo, wzdłuż której zamieszkiwało kilkanaście tysięcy ludzi. Inne ataki spowodowały m.in. zniszczenie ponad 3000 ha ziemi uprawnej[42]. Akcje sabotażowe zmusiły zagraniczne koncerny naftowe do tworzenia prywatnych armii oraz finansowania szkolenia sił rządowych do ochrony rurociągów. W latach 90. XX w. British Petroleum poniosło z tego tytułu koszty sięgające kilkudziesięciu milionów dolarów[43]. Z kolei Stany Zjednoczone wysłały grupę doradców wojskowych, aby przeprowadzili szkolenia dla żołnierzy kolumbijskich związane z ochroną rurociągu, którego udziałowcem była wspomniana spółka z Los Angeles[44]. Mimo to akcje sabotażowe nie ustawały, a terroryści kazali sobie płacić za ich zaprzestanie. W 2001 r. odnotowano 170 ataków bombowych na rurociąg Caño Limón–Coveñas. Przeprowadzony w lutym 2005 r. atak, w którym użyto materiałów wybuchowych, spowodował zamknięcie rurociągu na kilka tygodni, ponieważ zniszczono również sieć dostarczającą energię niezbędną do eksploatacji złoża Caño Limón[45].

FARC zintensyfikowały ataki na rurociągi po śmierci swojego przywódcy Raula Reyesa, który zginął 1 marca 2008 r. w wyniku operacji sił rządowych. Kilka dni później wysadzono w powietrze odcinek rurociągu naftowego, przesyłającego 100 000 baryłek ropy naftowej dziennie. Jego naprawa

[40] *Encyklopedia terroryzmu*, M. Crenshaw, J. Pimlott (red.), Warszawa 2004, s. 428.

[41] G. Marx, *Oleoducto en peligro recibe tropas estadounidenses en Colombia*, Amazon Watch, 12.11.2002, https://amazonwatch.org/es/news/2002/1112-imperiled-pipeline-gets-us-troops-in-colombia [dostęp: 12.11.2024].

[42] *Encyklopedia terroryzmu…*, s. 428.

[43] J. McEvoy, *La Financión de BP a los militares asesinos de Colombia*, Declassified UK, 18.07.2023, https://www.declassifieduk.org/es/la-financiacion-de-bp-a-los-militares-asesinos-de-colombia/ [dostęp: 18.12.2024].

[44] K. Wang, D. Kashi, *Major U.S. military operations/actions to protect oil*, https://nationalsecurityzone.medill.northwestern.edu/archives/oilchangeproject/how-do-we-protect-the-flow-of-oil/index.html [dostęp: 12.12.2024].

[45] Library of Congress, Federal Research Division, *Country Profile: Colombia*, 2007, https://maint.loc.gov/rr/frd/cs/profiles/Colombia.pdf, s. 19 [dostęp: 15.12.2024].

trwała kilka dni[46]. W pierwszej połowie 2012 r. grupy zbrojne FARC dokonały ponad 40 ataków na ropociągi. Częste były porwania i morderstwa inżynierów zatrudnionych w przemyśle naftowym. Atakowano również żołnierzy ochraniających rurociągi. W lipcu 2013 r. oddział żołnierzy wpadł w zasadzkę zorganizowaną przez FARC. Piętnastu z nich zginęło. Do zdarzenia doszło na słabo zaludnionych obszarach prowincji Arauca[47]. W sierpniu 2014 r. nieopodal granicy z Wenezuelą został zaatakowany rurociąg Bicentenario. Wywołało to ogromny pożar w regionie. W maju 2019 r. po kolejnym ataku rurociąg na pewien czas zamknięto. Ataki z mniejszą lub większą intensywnością zdarzały się do połowy 2023 r., następnie na ponad rok ustały. Dnia 26 sierpnia 2024 r. władze spółki naftowej Ecopetrol poinformowały o serii ataków na najważniejsze rurociągi w kraju – Bicentenario zaatakowano dwukrotnie, Caño Limón–Coveñas – trzykrotnie. Od 26 sierpnia do 9 września 2024 r. doszło do 9 ataków na inne rurociągi. Nastąpiły one po załamaniu się rozmów między partyzancką grupą ELN a kolumbijskim rządem. ELN uważa, że zagraniczne koncerny naftowe uzyskały kontrakty, które są bardzo korzystne dla nich samych, ale niekorzystne dla kraju. Według przywódców ELN Kolumbia powinna mieć pełną kontrolę nad swoimi zasobami naturalnymi, tak jak Wenezuela. Dopóki to nie nastąpi, infrastruktura energetyczna nadal ma być celem ataków tej grupy[48].

Sektor transportu publicznego – transport lądowy

Z analizy danych statystycznych wynika, że transport publiczny jest systemem IK najbardziej narażonym na terroryzm i sabotaż[49]. Liczba ataków na ten sektor wzrosła z 1165 w latach 2000–2009 do 1966 w latach 2010––2017. Największy wzrost dotyczył liczby ataków na pociągi: z 366 do 647.

[46] Reuters, *Terroryści z FARC biorą na cel rurociągi*, „Dziennik", 7.03.2008.

[47] PAP, *Kolumbia: 15 żołnierzy zginęło w zasadzce FARC*, Wirtualna Polska Wiadomości, 21.07.2013, https://wiadomosci.wp.pl/kolumbia-15-zolnierzy-zginelo-w-zasadzce-farc-6079340922-217089a [dostęp: 21.12.2024].

[48] K. Byzdra, *Partyzanci mieli zaatakować rurociągi w Kolumbii. Na miejsce wysłano wojsko*, Energetyka24, 27.08.2024, https://energetyka24.com/ropa/wiadomosci/partyzanci-mieli-zaatakowac-rurociagi-w-kolumbii-na-miejsce-wyslano-wojsko [dostęp: 27.12.2024]; Ch. Kennedy, *Guerilla Attacks on Pipelines Threaten Colombia's Oil Production*, Oil Price, 10.09.2024, https://oilprice.com/Energy/Crude-Oil/Guerilla-Attacks-on-Pipelines-Threaten-Colombias-Oil-Production.html [dostęp: 10.09.2024].

[49] A. Botha, *Prevention of Terrorist Attacks...*, s. 849.

W latach 1970–2009 infrastruktura transportu autobusowego na świecie stanowiła cel 1497 ataków. Najwięcej przeprowadzono ich w Izraelu i Okupowanym Terytorium Palestyny (142), Indiach (88), Filipinach (72), Pakistanie (70), Kolumbii (38), Federacji Rosyjskiej (37) i Sri Lance (36). Prawie 60% celów zaatakowano przy użyciu materiałów wybuchowych. Sprawcami ataków w tych państwach były organizacje separatystyczne, skrajnie lewicowe i muzułmańskie[50]. W latach 2010–2017 liczba ataków, których celem były autobusy, wzrosła z 476 do 740. Odnotowano także wzrost liczby ataków i akcji sabotażu w przypadku innych obiektów, w tym dworców i przystanków autobusowych – ze 138 do 179, mostów i tuneli – ze 116 do 249 oraz dróg – z 38 do 52[51]. Najczęściej wykorzystywano w nich broń palną (1450 zdarzeń) i podpalenia (216 zdarzeń)[52].

Siłą napędową rewolucji przemysłowej w Europie, europejskiej ekspansji kolonialnej i skutecznym narzędziem prowadzenia wojny była kolej parowa. Jest to jeden z pierwszych elementów IK będących celem ataków terrorystycznych. W Wielkiej Brytanii w latach 1881–1885 Fenianie, prekursorzy IRA (ang. Irish Republican Army), toczyli tzw. wojnę dynamitową. W Londynie przeprowadzono wówczas 13 ataków, w tym kilka na stacje kolejowe[53]. Pierwszego ataku na londyńskie metro dokonano 30 października 1883 r. Wieczorem ładunek wybuchowy eksplodował w tunelu między stacjami Charing Cross i Westminster, kolejny – przed stacją Praed Street. Rannych zostało 72 pasażerów, w tym wielu ciężko. Poważnie uszkodzono 6 wagonów[54]. W styczniu 1885 r. eksplodowały 2 bomby: jedna na stacji Gower Street, druga w pociągu Metropolitan Line. Skład został uszkodzony, a kilku pasażerów odniosło rany[55].

---

[50] B.M. Jenkins, B.R. Butterworth, K.S. Shrum, *Terrorist Attacks on Public Bus Transportation: A Preliminary Empirical Analysis*, Mineta Transportation Institute 2010, https://transweb.sjsu.edu/sites/default/files/2982-Terrorist-Attacks-On-Public-Bus-Transportation.pdf, s. 3, 23, 27 [dostęp: 3.12.2024].

[51] A. Botha, *Prevention of Terrorist Attacks…*, s. 855.

[52] Tamże, s. 850.

[53] R. Kirkland, *'A secret, melodramatic sort of conspiracy': The disreputable legacies of Fenian violence in nineteenth-century London*, King's Research Portal, https://kclpure.kcl.ac.uk/ws/portalfiles/portal/114850253/A_secret_melodramatic_sort_KIRKLAND_Accepted25July2017Published12August2019_GREEN_AAM.pdf, s. 6–7 [dostęp: 3.12.2024].

[54] I. Mansfield, *The first terrorist attack on the London Underground*, IanVisits, 30.10.2013, https://www.ianvisits.co.uk/articles/130th-anniversary-of-the-first-terrorist-attack-on-the-london-underground-9335/ [dostęp: 30.10.2024].

[55] *List of terrorist incidents in London*, Wikipedia, https://en.wikipedia.org/wiki/List_of_terrorist_incidents_in_London [dostęp: 19.12.2024].

Gęsta sieć kolejowa w Europie miała kluczowe znaczenie dla operacji militarnych podczas I wojny światowej. Kolej umożliwiała wielkim mocarstwom zmobilizowanie armii na bezprecedensową skalę i utrzymanie jej w terenie, pomimo rosnących i coraz bardziej złożonych potrzeb logistycznych. Infrastruktura kolejowa była więc celem ataków i akcji sabotażowych prowadzonych przez wojska strony przeciwnej. Do historii przeszły ataki organizowane przez Arabów dowodzonych przez Thomasa E. Lawrence'a na wiodącą z Damaszku do Medyny kolej hidżaską, będącą dla sił tureckich linią o znaczeniu strategicznym. Podczas kampanii palestyńskiej w latach 1917–1918 był to jeden z głównych celów natarcia Brytyjczyków oraz ataków arabskich rebeliantów. Część linii została wysadzona w powietrze, a liczne stacje – zniszczone[56]. Celem niemieckich ataków była z kolei brytyjska kolej ugandyjska, prowadząca z Port Florence (obecnie Kisumu) nad jeziorem Wiktorii do Mombasy w ówczesnej Brytyjskiej Afryce Wschodniej (obecnie Kenia). Niemieckie grupy dywersyjne wyruszały z Tanganiki (obecnie Tanzania), by wysadzać tory i atakować brytyjskie pociągi[57].

W okresie międzywojennym wykorzystano kolej oraz jej infrastrukturę do zorganizowania masowego mordu. Dnia 13 września 1931 r. Szilvester Matuszka podłożył bombę pod tory kolejowe na wiadukcie w Biatorbágy na przedmieściach Budapesztu. Potężna eksplozja doprowadziła do wykolejenia Ekspresu Wiedeńskiego. Zginęły 24 osoby, a 120 zostało rannych, w tym 14 ciężko. Matuszka podjął również dwie nieudane próby wykolejenia pociągów w Austrii i zdetonował bombę niedaleko Berlina. Jego głośny proces wskazał kierunek rozwoju działalności terrorystycznej. W następnych latach terroryści atakowali całą infrastrukturę kolejową, w tym stacje, hale biletowe, poczekalnie, restauracje dworcowe, mosty, tory, sygnalizacje, pociągi, bocznice, parowozownie. Ich celem było spowodowanie jak największych ofiar w ludziach i strat materialnych, dzięki czemu zyskiwali rozgłos medialny[58].

Dnia 28 sierpnia 1939 r. niemiecki agent Antoni Guzy pozostawił dwie walizki wypełnione materiałem wybuchowym w przechowalni bagażu na dworcu kolejowym w jednym z polskich miast. Eksplozja spowodowała

[56] T.E. Lawrence, *Siedem filarów mądrości*, Warszawa 1971, s. 198–203.

[57] R. Farnworth, *The Uganda Railway during the First World War*, https://rogerfarnworth.com/2020/12/28/the-uganda-railway-during-the-first-world-war/ [dostęp: 28.12.2024].

[58] *Tragically Explosive – Szilvestre Matuschka: A Fetish For Disaster (Part Three)*, Europe Between East And West, 7.03.2020, https://europebetweeneastandwest.wordpress.com/tag/hungarian-serial-killers/ [dostęp: 7.12.2024].

śmierć 20 osób, a 35 zostało rannych. Zamach w Tarnowie był jedną z akcji sabotażowych niemieckiej piątej kolumny, która paraliżowała działania obronne państwa polskiego przed wybuchem II wojny światowej[59]. Podczas tego konfliktu sabotaż kolejowy był jednym z najczęstszych działań partyzanckich we wszystkich teatrach wojny. Jego skala była tak duża, że działania partyzanckie w okupowanej Europie wymierzone w kontrolowaną przez Niemców infrastrukturę kolejową zostały nazwane bitwą o szyny lub wojną o szyny. Najwięcej akcji sabotażowych na kolei partyzanci przeprowadzali na terenie ZSRR[60]. Polska była drugim krajem pod względem liczby ataków na infrastrukturę kolejową. Od 1 stycznia 1941 r. do 30 czerwca 1944 r. Związek Walki Zbrojnej i Armia Krajowa przeprowadziły ok. 29 000 akcji sabotażu kolejowego. Wskutek tych działań uszkodzono 6930 lokomotyw i 19 058 wagonów, wykolejono 732 transporty, a 443 podpalono, zniszczono 1167 cystern oraz wysadzono w powietrze 38 mostów[61].

Na temat ataków terrorystycznych przeprowadzonych na świecie w latach 1950–1970, których celem była infrastruktura transportowa, informacje są sprzeczne, a statystyki – niekompletne. Problemem jest ocena zdarzeń, do których doszło podczas procesów dekolonizacyjnych w Azji i Afryce. Ugrupowania narodowowyzwoleńcze i nacjonalistyczne nazywały ataki operacjami bojowymi wymierzonymi w kolonialistów, administracja w koloniach natomiast, jej siły bezpieczeństwa i władze w metropoliach uznawały je za akty terroryzmu, a przeprowadzające je organizacje za terrorystyczne. Ataki takie były organizowane w Palestynie w latach 40., we francuskich Indochinach w latach 40. i 50., w Algierii w latach 50. oraz w Angoli i Mozambiku w latach 70. Wątpliwości budzą zdarzenia, które kwalifikowano jako „zwykłą" katastrofę kolejową, a nie akt sabotażu. Tak się działo, gdy sprawcy zachowywali milczenie na temat danego incydentu[62].

W miarę dokładne dane statystyczne dotyczące ataków na świecie, których celem była infrastruktura transportu publicznego, są dostępne

[59] M. Biedroń, *Zamach bombowy na tarnowskim dworcu kolejowym*, Tarnowskie Centrum Informacji, https://www.it.tarnow.pl/atrakcje/tarnow/ciekawostki/taka-jest-historia/zamach-bombowy-na-tarnowskim-dworcu-kolejowym/ [dostęp: 3.12.2024].

[60] P.W. Blood, *Hitler's Bandit Hunters: The SS and the Nazi Occupation of Europe*, Washington 2006, https://books.google.pl/books?id=jR49G7eyxBUC&pg=PA101&redir_esc=y#v=onepage&q&f=false, s. 101 [dostęp: 3.12.2024].

[61] M. Ney-Krwawicz, *Armia Krajowa: siła zbrojna Polskiego Państwa Podziemnego*, Warszawa 1993, s. 214.

[62] M. Tomczak, *Ewolucja terroryzmu, sprawcy – metody – finanse*, Poznań 2010, s. 40–47.

od początku lat 70. dzięki utworzonemu w 1991 r. amerykańskiemu Instytutowi Transportu im. Minety (Mineta Transportation Institute, MTI). Publikuje on okresowe raporty na ten temat. Obiekty transportu publicznego są celem organizacji o charakterze separatystycznym, skrajnie lewicowym, skrajnie prawicowym i religijnym, przede wszystkim ekstremistów muzułmańskich (dżihadystów), oraz grup bandyckich. Według danych MTI w latach 1970–2019 doszło do ok. 5800 ataków na infrastrukturę kolejową, przy czym w 346 przypadkach celem były pociągi pasażerskie. W wyniku tych działań zginęło 676 osób, a ponad 9720 zostało rannych. Pozostałe zdarzenia dotyczyły pociągów towarowych oraz innych elementów infrastruktury kolejowej. Dane te pochodzą z krajów należących do OECD, z wyłączeniem Turcji. W tym kraju w latach 1970–2010 doszło do 33 zamachów na infrastrukturę kolejową, które spowodowały 17 ofiar śmiertelnych[63].

W krajach rozwiniętych (raport MTI wymienia 27 państw) ataki terrorystyczne na koleje pasażerskie są statystycznie rzadkim zjawiskiem. W okresie półwiecza (lata 1970–2019) było to średnio 7 incydentów rocznie, przy czym zamachy przeprowadzane na terenie Wielkiej Brytanii, Hiszpanii, Francji, Niemiec i Włoch stanowiły 67% ogólnej liczby ataków. Wielka Brytania znalazła się na pierwszym miejscu z powodu długiej kampanii terrorystycznej IRA. Druga w kolejności była Hiszpania ze względu na aktywność ETA (bask. Euskadi Ta Askatasuna). W Stanach Zjednoczonych spółki będące właścicielami kolei pasażerskich odnotowały 27 ataków w latach 1970–2019. Ponadto wykryto 7 przypadków przygotowań do zamachów. Pod względem liczby ofiar na czele statystyki znajduje się Korea Południowa, gdzie 18 lutego 2003 r. w mieście Daegu w pożarze wznieconym w pociągu metra zginęło 198 osób. Na drugim miejscu jest Hiszpania. W skoordynowanych zamachach na pociągi podmiejskie przeprowadzonych 11 marca 2004 r. w Madrycie zginęły 192 osoby. Trzecie miejsce zajmują Włochy. W zamachu bombowym, do którego doszło 2 sierpnia 1980 r. na dworcu kolejowym w Bolonii, śmierć poniosło 85 osób[64].

Analiza dostępnych danych pozwala stwierdzić, że najczęstszym sposobem działania sprawców były zamachy bombowe. Wśród wspomnianych 346 ataków na pociągi pasażerskie aż 216 (62%) przeprowadzono przy użyciu materiałów wybuchowych umieszczonych w pociągach, na torach

[63] B.M. Jenkins, B.R. Butterworth, *How Sophisticated are Terrorist Attacks on Passenger Rail Transportation*, San José 2020, https://transweb.sjsu.edu/sites/default/files/SP0520-Jenkins-Terrorist-Attacks-Passenger-Rail-Transportation.pdf, s. 8 [dostęp: 3.12.2024].

[64] Tamże, s. 11.

kolejowych i w samochodach. W 33 zamachach (10%) działania sprawców polegały na mechanicznym uszkodzeniu lub zniszczeniu urządzeń kolejowych, w 32 (9%) – na wznieceniu pożaru przy użyciu materiałów łatwopalnych, w 29 (8%) – na użyciu noża, a w 19 (6%) – broni palnej. W 17 przypadkach (5%) zastosowano inne metody ataku. Jednego ataku dokonano przy użyciu broni masowego rażenia – broni chemicznej. W marcu 1995 r. w tokijskim metrze posłużono się sarinem. Spowodował on śmierć 12 osób, a ponad 5000 miało objawy zatrucia[65].

W innym raporcie MTI uwzględniono ataki na koleje pasażerskie przeprowadzone na świecie w latach 1970–2017. Wyszczególniono w nich wykolejenia pociągów: mechaniczne (64%) i przy użyciu materiałów wybuchowych (31%). W 39 państwach te metody zostały wykorzystane w 282 atakach. Najwięcej było ich w: Indiach – 82, Pakistanie – 66, Rosji – 22, Turcji – 11, Bangladeszu – 10, Tajlandii – 10, Algierii – 7, Włoszech – 7, Wielkiej Brytanii – 7, Niemczech – 6 i Francji – 5. W wyniku tych zdarzeń śmierć poniosło 1068 osób, a ponad 3040 zostało rannych. Najwięcej ofiar było w Indiach – 485, Angoli, gdzie w dwóch zamachach zginęło 278 osób, Pakistanie – 67 i w Mozambiku, w którym w jednym ataku zginęło 58 osób[66]. Najwięcej wykolejeń pociągów (37 zdarzeń) spowodowali indyjscy maoiści (naksalici). W wyniku tych działań zginęło 199 osób. Największą liczbą ofiar skutkowały jednak zamachy zorganizowane przez różne ugrupowania dżihadystyczne. W 10 dokonanych przez nich atakach śmierć poniosło 208 osób[67].

Osobną kategorię zdarzeń stanowią ataki na infrastrukturę kolejową, których głównym celem jest zakłócenie funkcjonowania komunikacji kolejowej, a nie śmierć ludzi. W latach 1970–2017 odnotowano 817 takich zdarzeń. W 721 przypadkach (88%) celem były tory kolejowe, mosty i tunele, w 59 (7%) – sygnalizacja kolejowa, łączność i systemy elektroenergetyczne, w 29 (4%) – personel i przeznaczone dla niego obiekty. Środkami ataku były najczęściej urządzenia wybuchowe, dynamit, miny i granaty – 702 zdarzenia (86%). W pozostałych przypadkach był to sabotaż polegający na uszkodzeniach mechanicznych oraz podpaleniach. Najwięcej takich zdarzeń

[65] Tamże, s. 13–14.

[66] B.M. Jenkins, B.R. Butterworth, *Train Wrecks and Track Attacks*..., s. 8–9.

[67] Tamże, s. 26.

odnotowano w Azji Południowej – 482 (59%) i Europie Zachodniej – 126 (15%), zginęło w nich 48 osób, a 268 zostało rannych[68].

Do tej kategorii zdarzeń należy zaliczyć również cyberataki na sieć kolejową. Pierwszy znany przypadek, w którym dokonano udanego fizycznego sabotażu przez Internet, został odnotowany w Polsce. W styczniu 2008 r. 14-letni chłopiec, utalentowany elektronik, przy użyciu samodzielnie zbudowanego nadajnika włamał się do miejskiego systemu tramwajowego w Łodzi, przejął kontrolę nad ruchem tramwajów i doprowadził do wykolejenia 4 z nich. Rannych zostało 12 osób[69]. W latach 2014–2024 cyberincydenty wpływające na systemy kolejowe odnotowano w takich krajach, jak: Belgia, Białoruś, Czechy, Dania, Francja, Indie, Niemcy, Stany Zjednoczone, Ukraina i Polska. Bardzo duży wzrost liczby cyberataków w kolejnictwie (o 220%) nastąpił w latach 2020–2024. Stało się to problemem na skalę światową[70]. W 2023 r. nieuprawnione włączanie sygnału „radio-stop" wielokrotnie unieruchomiło pociągi w Polsce. Powtarzające się zdarzenia miały charakter dobrze zorganizowanych akcji sabotażu[71].

Uprowadzenia pociągów wraz z pasażerami w celu wymuszenia na władzach określonych działań są rzadkie. W 1975 r. i 1977 r. w Holandii bojownicy Frontu na rzecz Republiki Południowych Moluków (hol. Front Republik Maluku Selatan) porwali pociąg i domagali się od Holandii utworzenia państwa niezależnego od Indonezji, dawnej kolonii holenderskiej. W latach 2006, 2009, 2012 naksalici porywali pociągi pasażerskie we wschodnich Indiach[72]. W Nigerii w 2022 r. bandyci zdetonowali ładunek wybuchowy umieszczony na torach tuż przed nadjeżdżającym pociągiem relacji Abudża–Kaduna, ostrzelali skład z broni maszynowej i uprowadzili

[68] Tamże, s. 16–17.

[69] *14-latek przestawiał zwrotnice*, Policja.pl, 9.01.2008, https://www.policja.pl/pol/aktualnosci/13278,14-latek-przestawial-zwrotnice.html [dostęp: 9.01.2025].

[70] C. Sivesind, *Cyber Attacks on Railway Systems Increase by 220%*, SecureWorld, 20.08.2024, https://www.secureworld.io/industry-news/railway-cyber-attacks [dostęp: 20.08.2024].

[71] M. Olanicki, *Tajemnicze awarie polskich pociągów. O sabotaż podejrzewany producent*, Biznes Info, 6.12.2023, https://www.biznesinfo.pl/tajemnicze-awarie-polskich-pociagow-o-sabotaz-podejrzewany-producent-mo-wak-061223 [dostęp: 6.12.2024].

[72] N. Shukla, *Maoists briefly hijack Indian train*, Reuters, 22.04.2009, https://www.reuters.com/article/world/maoists-briefly-hijack-indian-train-idUSTRE53L102/ [dostęp: 22.12.2024]; M. Saqib, *Recent Trends of Naxal Violence in India: Need for Comprehensive Approach from the Government*, „International Journal of Research in Social Sciences" 2018, t. 8, https://www.ijmra.us/project%20doc/2018/IJRSS_NOVEMBER2018/IJMRA-14770.pdf, s. 878 [dostęp: 3.12.2024].

ponad 150 z ok. 1000 pasażerów. Zginęło 8 osób, a wiele innych zostało rannych. Incydent skłonił władze Nigerii do traktowania wszystkich ugrupowań bandyckich jako organizacji terrorystycznych[73].

Sektor transportu publicznego – transport lotniczy

Przez wiele dekad transport lotniczy był celem chętnie wybieranym zarówno przez różne organizacje terrorystyczne, jak i sprawców indywidualnych. W 1967 r. porwano 15 samolotów, w 1968 r. – 30, a w 1969 r. – 80. Dokonano też 5 sabotaży w samolotach należących do 37 państw. W wyniku tych incydentów zginęło 6 osób, a 34 odniosło rany. Od 1 stycznia do 16 czerwca 1970 r. porwano 32 samoloty i przeprowadzono 8 sabotaży w maszynach należących do 23 krajów. Zginęło 90 pasażerów, a 23 zostało rannych[74]. Duża liczba uprowadzeń samolotów cywilnych na przełomie lat 60. i 70. XX w. przyczyniła się do podjęcia prób klasyfikacji takich zdarzeń. Do zdarzeń o charakterze terrorystycznym nie należą porwania samolotów dokonane w celu ucieczki, osiągnięcia rozgłosu medialnego czy uzyskania korzyści materialnych. Należy je uznać za bandytyzm powietrzny, znany również pod pojęciem piractwa powietrznego. Są to działania przestępcze podejmowane w celu zawładnięcia statkiem powietrznym, bez względu na pobudki, motywy i cele, jakimi kieruje się sprawca lub sprawcy[75]. Aby oddzielnie gromadzić dane dotyczące przypadków terroryzmu w lotnictwie i te dotyczące incydentów, których nie można tak zakwalifikować, powstały dwie bazy: Aviation Terrorism Sub-Database (ATSD) i Global Aviation Criminal Incidents Database (GACID)[76].

[73] *Nigeria train resumes operations eight months after major attack*, Al Jazeera, 5.12.2022, https://www.aljazeera.com/news/2022/12/5/nigeria-train-resumes-eight-months-after-deadly-attack [dostęp: 5.12.2024].

[74] J. Laskowski, *Terroryzm lotniczy – charakterystyka zjawiska*, „Studia Humanistyczno-Społeczne" 2013, t. 7, s. 146.

[75] K. Jałoszyński, *Współczesne zagrożenie terroryzmem powietrznym, kierunki przedsięwzięć w zakresie przeciwdziałania mu oraz walka z tym zjawiskiem*, w: *„Bezpieczne niebo". Materiały z konferencji naukowej AON*, J. Gotowała (red.), Warszawa 2002, s. 116.

[76] J. Duchesneau, *Aviation Terrorism…*, s. 5.

Porwania

Porwania samolotów powszechnie określa się jako *hijacking*. Pierwszą próbę porwania samolotu odnotowano w 1931 r. Peruwiańscy rewolucjoniści schwytali amerykańskiego pilota wykonującego lot z Limy do Arequipy. Chcieli wykorzystać jego samolot do rozrzucenia ulotek. Pilot stanowczo odmówił i plan porywaczy się nie powiódł. Po 10 dniach Amerykanina uwolniono i bezpiecznie wrócił do Limy. Do pierwszego uprowadzenia samolotu po zakończeniu II wojny światowej doszło – według Organizacji Międzynarodowego Lotnictwa Cywilnego (ang. International Civil Aviation Organization, ICAO) – w 1948 r. Samolot linii Cathay Pacific, lecący z Macao do Hongkongu, został porwany dla okupu. Maszyna spadła do Oceanu Spokojnego, zginęło 25 osób. W 1958 r. odnotowano pierwszy przypadek hijackingu w USA. Czterech Kubańczyków porwało samolot lecący z Miami do Hawany. Rozbił się on podczas próby lądowania na terytorium kontrolowanym przez rebeliantów Fidela Castro. Na początku lat 60. na Kubie samoloty były porywane przez dysydentów. Chcieli oni w ten sposób uciec od reżimu Castro do USA. Potem sytuacja się odwróciła. Członkowie różnych skrajnie lewicowych organizacji oraz przestępcy uciekający przed wymiarem sprawiedliwości porywali samoloty ze Stanów Zjednoczonych, aby dotrzeć na Kubę. W 1969 r. uprowadzenia samolotów pomiędzy USA a Kubą stały się na tyle częste i uciążliwe, że rządy obu państw podpisały umowę bilateralną dotyczącą zwalczania tego procederu, co w zasadzie rozwiązało problem[77].

Terroryzm lotniczy był sposobem działania palestyńskich organizacji, w większości o charakterze lewicowym, marksistowskim, które konflikt palestyńsko-izraelski przekształciły w terroryzm międzynarodowy. Serię uprowadzeń samolotów przez Palestyńczyków zapoczątkowało 22 lipca 1968 r. trzech członków Ludowego Frontu Wyzwolenia Palestyny (LFWP, arab. Al-Dżabha asz-Szaabijja li-Tahrir Filastin). Opanowali oni izraelski samolot linii El Al lecący z Rzymu do Tel Awiwu i zmusili załogę do lądowania w Algierze. W wyniku trwających ok. 40 dni negocjacji terroryści zgodzili się uwolnić zakładników w zamian za zwolnienie z izraelskich więzień grupy Palestyńczyków[78]. Zdarzenie to stało się precedensem, ponieważ pokazało, że porwania samolotów bardzo skutecznie pozwalają osiągnąć terrorystom główne cele, tj. wywrzeć polityczną presję na władze oraz skupić uwagę światowej opinii publicznej. George Habasz, jeden z przywódców LFWP,

[77] J. Laskowski, *Terroryzm lotniczy...*, s. 145–146.

[78] *Encyklopedia terroryzmu...*, s. 295.

zwrócił uwagę, że przed rozpoczęciem w 1968 r. działań terrorystycznych sprawa palestyńska nie była znana światu: *Prawdopodobnie mniej niż połowa Amerykanów w ogóle wiedziała, że coś takiego istnieje. Chcieliśmy zrobić coś, co by zmusiło ludzi do zapytania: Dlaczego oni to robią?* (...) *Osiągnęliśmy nasz cel. Sprawa palestyńska stała się natychmiast znana w całym świecie.* (...) *Uprowadzenie dużego samolotu odnosi propagandowo, medialnie większy skutek, niż zabicie w bitwie stu Izraelczyków. Przez dziesięciolecia opinia światowa nie była ani za Palestyńczykami, ani przeciwko nim. Teraz przynajmniej świat o nas mówi*[79].

W latach 1968–1970 porwano 151 samolotów[80]. Bezprecedensowe było porwanie 6 września 1970 r. przez członków LFWP 3 samolotów pasażerskich startujących z europejskich lotnisk. Jeden z nich wylądował w Kairze i po opuszczeniu pokładu przez pasażerów został zniszczony. Dwa skierowano na lotnisko Dawson's Field niedaleko Zarki w Jordanii. Trzy dni później terroryści porwali kolejny samolot i skierowali na to lotnisko. Wszystkie 3 samoloty zostały wysadzone 12 września. Większość pasażerów wypuszczono, w niewoli pozostali jedynie amerykańscy Żydzi i obywatele Izraela. Uwolniono ich w zamian za zwolnienie Palestyńczyków z europejskich więzień[81]. W następnych latach palestyńscy bojownicy przeprowadzili dziesiątki zamachów terrorystycznych na Bliskim Wschodzie i w Europie, w tym 52 ataki na samoloty izraelskich linii lotniczych El Al[82].

Do porwań samolotów często dochodziło w krajach bloku wschodniego, jednak ówczesna propaganda starała się pominąć te zdarzenia milczeniem. Motywy sprawców najczęściej miały charakter osobisty. W latach 1960–1980 odnotowano ok. 100 przypadków uprowadzenia samolotów, m.in. w celu ucieczki z państw bloku wschodniego do RFN, Berlina Zachodniego i Danii[83]. W latach 70. i 80. zwiększyła się liczba porwań samolotów w Polsce. Kierowano je głównie do Berlina Zachodniego. Takich zdarzeń było ponad 20. Najwięcej samolotów, aż 10, porwano z lotniska Katowice-Pyrzowice. Uprowadzano maszyny wykonujące loty krajowe ze

[79] T.R. Aleksandrowicz, K. Liedel, *Zwalczanie terroryzmu lotniczego. Wybrane zagadnienia i źródła prawa międzynarodowego*, Szczytno 2010, s. 13.

[80] B.M. Jenkins, *The Terrorist Threat to Commercial Aviation*, Santa Monica 1989, https://www.rand.org/content/dam/rand/pubs/papers/2008/P7540.pdf, s. 4 [dostęp: 25.02.2025].

[81] *Encyklopedia terroryzmu...*, s. 300.

[82] Ł. Szymankiewicz, *Terroryzm lotniczy wobec Izraela*, Warszawa 2019, s. 7.

[83] E. Ciborowska, *Wybrane przypadki piractwa powietrznego w Polsce w latach 80.*, „Terroryzm" 2008, nr 1, s. 6.

względu na to, że łatwiej było wejść na ich pokład. Wynikało to z braku kontroli paszportowej i odprawy granicznej oraz z uproszczonej procedury bezpieczeństwa w przypadku takich lotów[84]. W 1990 r. dziennik „Izwiestia" poinformował, że w ZSRR w latach 1958–1990 uprowadzono 69 maszyn. Sprawcy zabili 120 zakładników, kolejnych 200 ranili[85]. Ogółem w latach 1931–2011 doszło na świecie do 218 przypadków hijackingu o charakterze terrorystycznym (279 ofiar) oraz 1067 incydentów hijackingu kryminalnego (530 ofiar)[86]. Według innych danych w latach 1980–2022 zanotowano 553 porwania samolotów. Najmniej (18) było ich w dekadzie 2011–2022[87].

Zamachy bombowe

Według ICAO polegają one na umieszczaniu na pokładach samolotów ładunków wybuchowych i ich zdetonowaniu, gdy samolot znajduje się na ziemi lub w powietrzu. Ładunek może znajdować się w bagażu rejestrowanym lub może go podrzucić pasażer[88]. Od 1931 r. do 2024 r. na świecie przeprowadzono w samolotach 73 zamachy bombowe o charakterze terrorystycznym (zginęły w nich 1644 osoby) oraz 119 ataków o charakterze kryminalnym (1184 ofiary)[89]. Do 48 ataków doszło w latach 2000–2009, w 27 przypadkach był to hijacking, w 14 wykorzystano materiały wybuchowe. W latach 2010–2017 doszło do 26 ataków, z czego 5 to były porwania, a 10 – ataki z użyciem materiałów wybuchowych[90]. Według innych danych w latach 1970–2022 dokonano w samolotach 64 zamachów bombowych, w których zginęło 2097 osób. Najmniej (2 zamachy) tego rodzaju zdarzeń było w dekadzie 2011–2022. Zginęło 225 osób[91].

---

[84] M. Desler, *Seven five – man with knife, lotnictwo, a terroryzm*, dlapilota.pl, 9.04.2014, https://dlapilota.pl/wiadomosci/monika-desler/seven-five-man-knife-lotnictwo-terroryzm [dostęp: 9.12.2024].

[85] Tamże.

[86] J. Duchesneau, *Aviation Terrorism...*, s. 139.

[87] O. Čokorilo, S. Čokorilo, L. Tomic, *A framework for aviation security*, AIIT 4th International Conference on Transport Infrastructure and Systems (TIS ROMA 2024), https://www.researchgate.net/publication/381768379_A_framework_for_aviation_security, s. 5 [dostęp: 28.02.2025].

[88] J. Duchesneau, *Aviation Terrorism...*, s. 118.

[89] Tamże, s. 139; A. Botha, *Prevention of Terrorist Attacks...*, s. 851; *Timeline of airliner bombing attacks*, Wikipedia, https://en.wikipedia.org/wiki/Timeline_of_airliner_bombing_attacks [dostęp: 26.02.2025].

[90] A. Botha, *Prevention of Terrorist Attacks...*, s. 851.

[91] O. Čokorilo, S. Čokorilo, L. Tomic, *A framework for aviation security...*, s. 3.

Pierwszy zamach bombowy w samolocie został przeprowadzony 21 lutego 1970 r. Sprawcą był LFWP, a celem maszyna Convair linii Swissair lecąca z Zurichu do Tel Awiwu. Bomba umieszczona w luku bagażowym eksplodowała 9 minut po starcie. Piloci podjęli próbę powrotu na lotnisko w Zurichu, ale z powodu utraty sterowności samolot runął na ziemię. Zginęło 47 osób[92]. Tego samego dnia eksplodował ładunek wybuchowy w samolocie Caravelle linii Austrian Airlines lecącym z Frankfurtu nad Menem do Tel Awiwu. Bomba została umieszczona pomiędzy grubymi plikami gazet, które znacznie osłabiły siłę wybuchu. Pilot bezpiecznie wylądował. Na początku lat 70. zamachy bombowe przeprowadzane przez palestyńskie ugrupowania terrorystyczne były skierowane głównie przeciwko samolotom linii lotniczych El Al. Ze względu na wspieranie przez rząd USA antypalestyńskiej polityki Izraela celem stały się również maszyny amerykańskich przewoźników. We wrześniu 1974 r. eksplozja bomby w samolocie Boeing linii TWA, lecącym z Tel Awiwu przez Ateny do Nowego Jorku, spowodowała rozerwanie samolotu nad Morzem Jońskim i śmierć 88 osób. Do zamachu przyznał się LFWP. W latach 70. odnotowano ogółem 42 zamachy bombowe, w wyniku których zginęło ponad 650 osób. W kolejnej dekadzie liczba zamachów spadła do 24, wzrosła jednak liczba ofiar – do ok. 1000 osób[93]. Najbardziej tragiczne pod względem liczby ofiar były 2 ataki terrorystyczne. Członkowie separatystycznej organizacji sikhijskiej Babbar Khalsa umieścili bombę na pokładzie samolotu Boeing 747 linii Air India lecącego 22 czerwca 1985 r. z Montrealu do Nowego Delhi. Ładunek eksplodował, gdy maszyna była nad Oceanem Atlantyckim u wybrzeży Irlandii. Zginęło 329 osób, najwięcej w historii tego rodzaju zamachów. Do drugiego ataku doszło 21 grudnia 1988 r. za sprawą agentów libijskiego wywiadu, którym udało się umieścić ładunek wybuchowy w bagażu nadanym na lot nr 103 samolotu Boeing 727 linii Pan Am lecącego z Londynu do Nowego Jorku. Samolot eksplodował nad Lockerbie. Zginęło 259 osób na pokładzie i 11 mieszkańców szkockiej miejscowości[94]. Do jednego z ostatnich zamachów, w którym wykorzystano ten sam schemat działania, doszło 31 października 2015 r. Terroryści należący do ugrupowania Prowincja Synaj związanego z ISIS podłożyli ładunek wybuchowy w samolocie Airbus A321 rosyjskich linii lotniczych Metrojet, lecącym z Szarm el-Szejk

[92] J. Laskowski, *Terroryzm lotniczy*..., s. 149.

[93] Tamże, s. 149–150.

[94] *Encyklopedia terroryzmu*..., s. 369.

do Petersburga. Eksplozja nastąpiła ok. 23 minuty po starcie. Samolot rozbił się na półwyspie Synaj. Zginęły 224 osoby[95].

Terroryzm samobójczy

Inną metodą atakowania statków powietrznych są akty terroryzmu samobójczego, w których statek powietrzny jest wykorzystywany jako narzędzie ataku. Od 1989 r. do 2011 r. zanotowano łącznie 17 takich zamachów oraz nieudanych i udaremnionych prób ich przeprowadzenia. Zginęły w nich 3143 osoby[96]. Pierwszy incydent samobójczy odnotowano w listopadzie 1989 r. Saudyjczycy usiłowali zdetonować bombę na pokładzie samolotu Saudi Arabian Airlines. Do eksplozji nie doszło z powodu wady konstrukcyjnej zapalnika. Na temat tego zdarzenia niewiele wiadomo, poza tym że aresztowano 10 osób[97]. Do tej kategorii aktów terroryzmu należą zamachy z 11 września 2001 r. na World Trade Center i Pentagon w USA. To zdarzenie jest uznawane za apogeum terroryzmu lotniczego i największą udaną operację terrorystyczną w historii. Zginęło w niej 2996 osób. Liczba ofiar tego ataku przewyższyła liczbę zabitych w wyniku hijackingu o charakterze terrorystycznym (279 osób) i terrorystycznych zamachów bombowych (1418 osób)[98]. Zamachy z 11 września wyrządziły również ogromne straty materialne. Bardzo duże koszty poniosły towarzystwa ubezpieczeniowe i reasekuracyjne, linie lotnicze oraz producenci samolotów, a także branża turystyczna. Szwajcarskie towarzystwo reasekuracyjne Swiss Re oceniło, że straty sektora ubezpieczeniowego związane z wrześniowym atakiem wyniosły 90 mld dolarów, z czego 19 mld to były koszty bezpośrednie. Łączne straty linii lotniczych szacowano na 12–13 mld dolarów[99]. Wydarzenia te pogrążyły komunikację lotniczą w kryzysie najgłębszym od czasów II wojny światowej. W kolejnych latach doszło do kilku zdarzeń pokazujących możliwości wykorzystania samolotów jako narzędzia terroru. Między innymi 5 stycznia 2002 r. uczeń szkoły latania porwał niewielki samolot typu

[95] PAP, *Egipt: katastrofa samolotu Airbus A321 na Półwyspie Synaj (aktualizacja)*, dlapilota.pl, 17.11.2015, https://dlapilota.pl/wiadomosci/pap/egipt-katastrofa-samolotu-airbus-a321-na-polwyspie-synaj [dostęp: 17.12.2024].

[96] J. Duchesneau, *Aviation Terrorism...*, s. 139.

[97] Tamże, s. 123.

[98] Tamże, s. 126.

[99] K. Izak, *Dwadzieścia lat od ataku 11 września 2001 roku. Przygotowania do ataku terrorystycznego na USA oraz jego przebieg i skutki*, „Przegląd Bezpieczeństwa Wewnętrznego" 2021, nr 25, s. 21. https://doi.org/10.4467/20801335PBW.21.027.14304.

Cessna i rozbił go na wieżowcu w Tampie na Florydzie. Pilot zginął na miejscu, a konstrukcja budynku została lekko uszkodzona[100].

W latach 1989–2011 przeprowadzono 32 ataki samobójcze, które zakwalifikowano jako kryminalne. Śmierć poniosło w nich 691 osób[101]. Tego rodzaju zdarzeniem mogło być – według niektórych opinii – zaginięcie w marcu 2014 r. samolotu linii Malaysia Airlines. Boeing 777 lecący z Kuala Lumpur do Pekinu zmienił trasę lotu i zniknął z radarów. Zginął kapitan samolotu Zaharia Ahmad Szah wraz z 238 pasażerami i członkami załogi. Pojawiły się doniesienia, że kapitan mógł celowo doprowadzić do uderzenia samolotu w wody Oceanu Indyjskiego. Jako motywy wskazywano jego radykalizm religijny i trudne przeżycia osobiste[102]. W lutym 2025 r. rozpoczęto ponowne poszukiwania szczątków tego samolotu[103]. Ostatnie zdarzenie miało miejsce 24 marca 2015 r. Samolot Airbus A320 linii Germanwings lecący z Barcelony do Düsseldorfu rozbił się we francuskich Alpach. Zginęli wszyscy pasażerowie i członkowie załogi – w sumie 150 osób. Katastrofę spowodował celowo drugi pilot, Andreas Lubitz[104].

W sektorze transportu lotniczego misje samobójcze są najrzadziej wykorzystywanym sposobem działania (3% zdarzeń). Ze względu jednak na liczbę ofiar ataku z 11 września 2001 r. okazały się najbardziej śmiercionośne (51% ofiar)[105]. Tylko 8 spośród przygotowywanych 17 ataków samobójczych doszło do skutku i spowodowało ofiary śmiertelne. Dwa z nich stanowiły zamachy Czeczenek, tzw. czarnych wdów, na rosyjskie

[100] M.L. Wald, *Student Pilot, 15, Crashes Plane Into Tower in Florida*, New York Times, 6.01.2002, https://www.nytimes.com/2002/01/06/us/student-pilot-15-crashes-plane-into-tower-in-florida.html [dostęp: 6.01.2025].

[101] J. Duchesneau, *Aviation Terrorism…*, s. 139.

[102] Daily Mail, *New report explores the pilot of MH370 troubled personal life, likely scenario of what happened on flight*, New Zealand Herald, 18.06.2019, https://www.nzherald.co.nz/world/new-report-explores-the-pilot-of-mh370-troubled-personal-life-likely-scenario-of-what-happened-on-flight/TOQ557EGUHWQDXG5DU47E7JOVE/ [dostęp: 18.12.2024].

[103] T. Jones, *MH370: Search resumes to find missing plane 11 years on*, Deutsche Welle, 25.02.2025, https://www.dw.com/en/mh370-search-resumes-to-find-missing-plane-11-years-on/a-71739469 [dostęp: 25.02.2025].

[104] M. Zafimehy, G. Chieze, *Crash de la Germanwings: à quoi ont ressemblé les dernières minutes avant la catastrophe?*, RTL, 26.03.2023, https://www.rtl.fr/actu/justice-faits-divers/crash-de-la-germanwings-a-quoi-ont-ressemble-les-dernieres-minutes-avant-la-catastrophe-7900246615 [dostęp: 26.01.2025].

[105] J. Duchesneau, *Aviation Terrorism…*, s. 123.

samoloty[106]. Trzy ataki były nieudane, w tym atak Brytyjczyka Richarda Reida, znanego jako *shoe bomber*. Z ładunkiem wybuchowym umieszczonym w butach usiłował on wejść na pokład samolotu lecącego z Paryża do Miami[107]. Sześć ataków udaremniono, m.in. operację „Bojinka", wykrytą w styczniu 1995 r. w Manili, w ramach której terroryści zamierzali uprowadzić 11 samolotów i posłużyć się nimi do ataków samobójczych na obiekty w USA (na wzór ataku z 11 września)[108]. Inną operację terrorystyczną udaremniono w Londynie w sierpniu 2006 r. Celem terrorystów samobójców było wywołanie eksplozji w samolotach lecących ze stolicy Wielkiej Brytanii do Nowego Jorku, Waszyngtonu, Chicago, San Francisco, Toronto i Montrealu[109]. Nigeryjczyk Umar Farouk Abdulmutallab zamierzał wysadzić samolot amerykańskich linii lotniczych NorthWest Airlines z 289 osobami na pokładzie, lecący 25 grudnia 2009 r. z Amsterdamu do Detroit. Został jednak obezwładniony przez pasażerów i załogę podczas próby zdetonowania ładunku pentrytu ukrytego w bieliźnie[110].

Ataki na porty lotnicze i samoloty uziemione oraz ataki z ziemi na samoloty w powietrzu

Ostatnią kategorię zdarzeń stanowią zamachy w portach lotniczych oraz ataki przeprowadzane na samoloty znajdujące się na ziemi i znajdujące się w powietrzu. Jest to najliczniejsza kategoria incydentów. Do 2017 r. odnotowano ogółem 624 tego typu zdarzenia o charakterze terrorystycznym[111]. W latach 2010–2017 liczba incydentów terrorystycznych w portach lotniczych wzrosła z 83 do 164[112]. Z kolei w 2019 r. zanotowano 31 ataków terrorystycznych w portach i samolotach, o 10 więcej niż w roku poprzednim[113]. Pierwszy odnotowany atak terrorystyczny na lotnisku pasażerskim przeprowadzono 10 lutego 1970 r. Trzej terroryści z LFWP na lotnisku w Monachium obrzucili granatami i ostrzelali pasażerów udających się

[106] Tamże, s. 205.

[107] Tamże.

[108] K. Izak, *Leksykon organizacji i ruchów...*, s. 164–165.

[109] Tamże, s. 411.

[110] Tamże, s. 478.

[111] J. Duchesneau, *Aviation Terrorism...*, s. 139.

[112] A. Botha, *Prevention of Terrorist Attacks...*, s. 854.

[113] START, *Global Terrorism Overview: Terrorism in 2019*, https://www.start.umd.edu/pubs/START_GTD_GlobalTerrorismOverview2019_July2020.pdf, s. 11 [dostęp: 30.07.2024].

do samolotu izraelskich linii El Al. Jedna osoba zginęła, a 11 zostało rannych[114]. W latach 70. i 80. palestyńscy terroryści kilkakrotnie atakowali włoskie lotniska Rzym-Fiumicino i Leonardo da Vinci[115]. W grudniu 1999 r. na przejściu granicznym między Kanadą i USA został aresztowany Algierczyk Ahmed Ressam podczas próby wjazdu do Stanów Zjednoczonych. W jego samochodzie znaleziono materiały wybuchowe i broń. Celem Ressama było przeprowadzenie ataku bombowego na lotnisku w Los Angeles w noc sylwestrową 1999 r.[116] W ostatnich latach także lotniska cywilne w Arabii Saudyjskiej były celem ataków wspomnianego już ruchu Huti. Bojownicy tej organizacji wystrzelili 4 listopada 2017 r. rakietę Burkan H-2 w kierunku Międzynarodowego Portu Lotniczego Króla Chalida w Rijadzie. Pocisk został zestrzelony przez system antyrakietowy Patriot[117]. W latach 2000–2009 odnotowano 83 ataki na porty lotnicze przeprowadzone przy użyciu broni palnej, materiałów wybuchowych i zapalających. W latach 2010–2017 takich ataków było 169[118]. Do ostatniego doszło 5 sierpnia 2024 r. Wykorzystano w nim rakietę Katiusza, a celem była baza lotnicza Ain al-Asad w Iraku. Rannych zostało 5 amerykańskich żołnierzy[119].

W ostatnich latach coraz częstszym zagrożeniem dla portów lotniczych oraz startujących i lądujących samolotów są UAV. Rok 2013 był ostatnim, w którym nie zanotowano tego typu zdarzeń. W grudniu 2018 r. z powodu licznych przelotów dronów wstrzymano ruch na londyńskim lotnisku Gatwick. W lipcu poprzedniego roku doszło tam niemal do zderzenia UAV z samolotem pasażerskim. Według British Airline Pilots Association liczba incydentów z udziałem dronów bardzo wzrosła. W 2017 r. było ich 93, a od stycznia do listopada 2018 r. – 117[120]. Podobne przypadki notowano również w Polsce. W marcu 2014 r. dron zrzucił niewielki ładunek wybuchowy na pas startowy w wojskowej części lotniska w Balicach.

---

[114] J. Laskowski, *Terroryzm lotniczy*..., s. 151.

[115] M. Zimmerman, *„Cud, że tyle osób przeżyło". Mija 50 lat od zamachu na lotnisku Fiumicino*, Onet, 17.12.2023, https://wiadomosci.onet.pl/swiat/50-lat-od-ataku-na-lotnisku-fiumicino-najbardziej-krwawy-z-tamtych-zamachow/mpd5nm4 [dostęp: 17.12.2024].

[116] K. Izak, *Leksykon organizacji i ruchów*..., s. 186.

[117] *Atak rakietowy na Rijad*...

[118] A. Botha, *Prevention of Terrorist Attacks*..., s. 854.

[119] *At least five US personnel injured in rocket attack on Iraq military base*, Al Jazeera, 6.08.2024, https://www.aljazeera.com/news/2024/8/6/at-least-five-us-personnel-injured-in-attack-on-iraq-military-base [dostęp: 6.08.2024].

[120] A. Botha, *Prevention of Terrorist Attacks*..., s. 853.

W lipcu 2015 r. UAV stworzył poważne zagrożenie dla podchodzącego do lądowania samolotu Lufthansy, lecącego z Monachium do Warszawy. Podobny incydent odnotowano w Balicach w czerwcu 2022 r. oraz na Okęciu i w Pyrzowicach w maju 2023 r.[121] Wszystkie te zdarzenia miały charakter kryminalny.

W ostatnich latach obserwuje się znaczny wzrost liczby cyberataków na porty i linie lotnicze. Mają one głównie charakter kryminalny. W 2020 r. w Europie zanotowano 178 cyberataków na porty lotnicze i 775 cyberataków na linie lotnicze, co oznacza 530-procentowy wzrost w porównaniu z 2019 r. Cyberataki na linie lotnicze stanowiły aż 61% wszystkich cyberataków przeprowadzonych w Europie w 2020 r. Większość z nich (735) miała podłoże finansowe[122]. Należy zwrócić uwagę, że w 2023 r. globalna IK była celem ponad 420 mln cyberataków, co oznacza ok. 13 ataków na sekundę. Najwięcej było ich w USA. Ataki te często przypisuje się hakerom powiązanym z Chinami, Rosją i Iranem[123].

Do pierwszego aktu terroryzmu polegającego na zestrzeleniu samolotu pasażerskiego doszło 21 grudnia 1948 r. Greccy powstańcy zestrzelili czechosłowacki samolot lecący z Rzymu do Aten, w wyniku czego zginęły 2 osoby. W latach 70. tego typu ataki upowszechniły się wraz z dostępem do przenośnych rakietowych zestawów przeciwlotniczych (ang. *man portable air defence system*, MANPADS). Po raz pierwszy terroryści użyli MANPADS 5 września 1973 r. na lotnisku Rzym-Fiumicino. Palestyńczycy usiłowali wystrzelić pocisk rakietowy SA-7 w stronę kołującego samolotu linii lotniczych El Al, ale próba się nie powiodła. Pierwszy udany zamach tego typu został przeprowadzony 12 lutego 1979 r. w okolicy miasta Kariba w Zimbabwe. Tuż po starcie samolot linii Air Rhodesia został trafiony pociskiem SA-7. Śmierć poniosło 59 osób[124]. MANPADS były powszechnie używane przez afgańskich mudżahedinów przeciwko radzieckim

[121] M. Walków, *Coraz więcej incydentów z dronami. Lotnisko Chopina przetestuje rozwiązanie*, Money.pl, 30.05.2023, https://www.money.pl/gospodarka/lotnisko-chopina-sie-zbroi-drony-to-coraz-powazniejsze-zagrozenie-dla-samolotow-6903403450051296a.html [dostęp: 30.12.2024].

[122] EUROCONTROL, *Aviation under attack from a wave of cybercrime*, https://www.eurocontrol.int/sites/default/files/2021-07/eurocontrol-think-paper-12-aviation-under-cyber-attack.pdf [dostęp: 5.07.2024].

[123] B. Candan, *Top 5 critical infrastructure cyberattacks*, Anapaya, 17.10.2024, https://www.anapaya.net/blog/top-5-critical-infrastructure-cyberattacks [dostęp: 17.10.2024].

[124] J. Laskowski, *Terroryzm lotniczy*..., s. 151–152.

samolotom wojskowym i helikopterom, a później przez talibów. Korzystały z nich również ugrupowania rebelianckie w Somalii, Iraku, Syrii, bojownicy czeczeńscy, bojownicy tamilscy z organizacji Tygrysy Wyzwoliciele Tamilskiego Ilamu (ang. Liberation Tigers of Tamil Eelam, LTTE) i kolumbijscy z FARC[125]. Z taktyki atakowania samolotów cywilnych przy użyciu systemów rakietowych regularnie korzystają różnego rodzaju ugrupowania terrorystyczne, zwalczające się ugrupowania zbrojne (Sudan), a w ostatnich latach także państwa. Na przykład 17 lipca 2014 r. Boeing 777 linii Malaysia Airlines, lecący z Amsterdamu do Kuala Lumpur, został zestrzelony w obwodzie donieckim na wschodzie Ukrainy przy użyciu pocisku kierowanego ziemia-powietrze Buk. Sprawcami byli separatyści z Rosji. Zginęło 283 pasażerów i 15 członków załogi[126]. W dniu 8 stycznia 2020 r. siły zbrojne Iranu zestrzeliły lecący z Teheranu do Kijowa samolot Boeing 737 linii Ukraine International Airlines ze 176 osobami na pokładzie[127]. Do jednego z ostatnich ataków na samolot doszło 11 listopada 2024 r. Dwa pasażerskie airbusy, należące do amerykańskich linii lotniczych, zostały ostrzelane przez gangi w Port-au-Prince, stolicy Haiti. Lekko ranna została stewardessa jednego z samolotów. Po tym zdarzeniu linie lotnicze z USA zawiesiły loty do tego kraju. Z kolei w październiku 2024 r. został ostrzelany lecący nad Port-au-Prince śmigłowiec ONZ, który musiał zawrócić na lotnisko[128].

[125] A. Radomyski, D. Michalski, *Managing the Threat of Manpads Use Against Civil Aviation*, „Rocznik Bezpieczeństwa Morskiego" 2023, t. 17, s. 569–571. https://doi.org/10.5604/01.3001.0054.1602.

[126] A. Pawluszek, *Malezyjski Boeing 777 zestrzelony przez Rosjan w 2014 r. Sąd w Hadze przedstawił stanowisko*, Gazeta Prawna, 17.11.2022, https://www.gazetaprawna.pl/wiadomosci/swiat/artykuly/8590126,holandia-sad-zestrzelenie-2014-malezyjski-boeing-777-ukraina.html [dostęp: 17.11.2024].

[127] Reuters, *Teheran proponuje odszkodowania rodzinom ofiar zestrzelonego boeinga. Kijów krytykuje*, TVN24, 30.12.2020, https://tvn24.pl/swiat/ukrainski-samolot-zestrzelony-nad-teheranem-wladze-iranu-oferuja-odszkodowania-dla-rodzin-ofiar-st4851794 [dostęp: 30.12.2024].

[128] *Horror w przestworzach, gangi ostrzelały dwa samoloty. Ranna stewardessa*, Polskie Radio 24, 12.11.2024, https://polskieradio24.pl/artykul/3445609,horror-w-przestworzach-gangi-ostrzelaly-dwa-samoloty-ranna-stewardessa [dostęp: 21.12.2024].

Wnioski

Infrastruktura krytyczna z uwagi na swoją wielosektorowość, rozproszenie i wynikającą z tego trudność w zapewnieniu jej dostatecznego bezpieczeństwa od wielu lat jest głównym celem zarówno organizacji terrorystycznych, jak i sprawców indywidualnych. Przeprowadzane na nią ataki, zwłaszcza w sektorze transportu, powodują masowe ofiary i stają się pożywką dla mediów. W wielu przypadkach dzięki współpracy międzynarodowej, wzmacnianiu kontroli antyterrorystycznej, środków bezpieczeństwa i działaniom wywiadowczym udało się skutecznie zapobiec zamachom na obiekty IK. Nie zapewnia to jednak dostatecznego poziomu bezpieczeństwa całej IK. Dynamicznemu postępowi naukowo-technicznemu i rozwojowi cywilizacyjnemu towarzyszą nowe ogniska napięć i konfliktów zbrojnych na świecie, w których wykorzystuje się najnowsze osiągnięcia techniki. Z tych osiągnięć korzystali i będą korzystać również terroryści oraz rebelianci i „partyzanci", aby przeprowadzać ataki i akty sabotażu w ramach działań hybrydowych. Można więc założyć, że poziom zagrożenia dla IK na świecie będzie wzrastał.

Bibliografia

Aleksandrowicz T.R., Liedel K., *Zwalczanie terroryzmu lotniczego. Wybrane zagadnienia i źródła prawa międzynarodowego*, Szczytno 2010.

Ciborowska E., *Wybrane przypadki piractwa powietrznego w Polsce w latach 80.*, „Terroryzm" 2008, nr 1, s. 6–9.

Encyklopedia terroryzmu, M. Crenshaw, J. Pimlott (red.), Warszawa 2004.

Gebert K., *Pokój z widokiem na wojnę. Historia Izraela*, Warszawa 2023.

Grabowski T.W., *Terroryzm północnokaukaski. Źródła, przejawy i przeciwdziałanie zjawisku*, Kraków 2017.

Izak K., *Dwadzieścia lat od ataku 11 września 2001 roku. Przygotowania do ataku terrorystycznego na USA oraz jego przebieg i skutki*, „Przegląd Bezpieczeństwa Wewnętrznego" 2021, nr 25, s. 219–250. https://doi.org/10.4467/20801335PBW.21.027.14304.

Izak K., *Leksykon organizacji i ruchów islamistycznych*, Warszawa 2014.

Jałoszyński K., *Współczesne zagrożenie terroryzmem powietrznym, kierunki przedsięwzięć w zakresie przeciwdziałania mu oraz walka z tym zjawiskiem*, w: *„Bezpieczne niebo". Materiały z konferencji naukowej AON*, J. Gotowała (red.), Warszawa 2002, s. 114–132.

Kijewski T., *Atak terrorystyczny na kompleks gazowy Tiguentourine w In Amenas w Algierii w styczniu 2013 r. jako przykład nowych zagrożeń dla energetycznej infrastruktury krytycznej i bezpieczeństwa wewnętrznego państwa*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9, s. 202–224.

Laskowski J., *Terroryzm lotniczy – charakterystyka zjawiska*, „Studia Humanistyczno-Społeczne" 2013, t. 7, s. 133–163.

Lawrence T.E., *Siedem filarów mądrości*, Warszawa 1971.

Łukasiewicz J., *Bezzałogowe statki powietrzne jako źródło zagrożeń infrastruktury zaopatrzenia państw w energię elektryczną oraz proponowane metody ochrony tej infrastruktury*, „Terroryzm – studia, analizy, prewencja" 2022, nr 1, s. 90–122. https://doi.org/10.4467/27204383TER.22.004.15420.

Ney-Krwawicz M., *Armia Krajowa: siła zbrojna Polskiego Państwa Podziemnego*, Warszawa 1993.

Radomyski A., Michalski D., *Managing the Threat of Manpads Use Against Civil Aviation*, „Rocznik Bezpieczeństwa Morskiego" 2023, t. 17, s. 559–579. https://doi.org/10.5604/01.3001.0054.1602.

Reuters, *Terroryści z FARC biorą na cel rurociągi*, „Dziennik", 7.03.2008.

Szymankiewicz Ł., *Terroryzm lotniczy wobec Izraela*, Warszawa 2019.

Tomczak M., *Ewolucja terroryzmu, sprawcy – metody – finanse*, Poznań 2010.

Wasiuta O., Wasiuta S., Mazur P., *Państwo Islamskie ISIS. Nowa twarz ekstremizmu*, Warszawa 2018.

Źródła internetowe

AFP, *Des djihadistes revendiquent l'attaque d'un gazoduc*, 20 Minutes, 8.01.2016, https://www.20min.ch/fr/story/des-djihadistes-revendiquent-l-attaque-d-un-gazoduc-826827705429 [dostęp: 9.01.2025].

AFP, *Deux drones ont survolé la centrale nucléaire de Nogent-sur-Seine*, BFMTV, 4.01.2015, https://www.bfmtv.com/police-justice/deux-drones-ont-survole-la-centrale-nucleaire-de-nogent-sur-seine_AN-201501040009.html [dostęp: 4.01.2025].

Atak rakietowy na Arabię Saudyjską i naloty w Jemenie, Defence24, 27.12.2024, https://defence24.pl/geopolityka/arabia-saudyjska-przeprowadza-naloty-huti-w-jemenie--za-atak-na-miasto-jazan [dostęp: 27.12.2024].

Atak rakietowy na Rijad, Defence24, 5.11.2017, https://defence24.pl/atak-rakietowy--na-rijad [dostęp: 5.11.2024].

At least five US personnel injured in rocket attack on Iraq military base, Al Jazeera, 6.08.2024, https://www.aljazeera.com/news/2024/8/6/at-least-five-us-personnel-injured-in-attack-on-iraq-military-base [dostęp: 6.08.2024].

Au total, 17 sites nucléaires ont été survolés par des drones depuis octobre, Le Monde, 29.01.2015, https://www.lemonde.fr/planete/article/2015/01/29/dix-sept-sites--nucleaires-ont-ete-survoles-par-des-drones-depuis-octobre_4565967_3244.html [dostęp: 29.01.2025].

Barnett D., *Ansar Jerusalem claims responsibility for recent Sinai gas pipeline attack*, FDD's Long War Journal, 19.01.2014, https://www.longwarjournal.org/ar-chives/-2014/01/ansar_jerusalem_claims_respons.php [dostęp: 19.01.2025].

Biedroń M., *Zamach bombowy na tarnowskim dworcu kolejo*wym, Tarnowskie Centrum Informacji, https://www.it.tarnow.pl/atrakcje/tarnow/ciekawostki/taka-jest-historia/zamach-bombowy-na-tarnowskim-dworcu-kolejowym/ [dostęp: 3.12.2024].

Blood P.W., *Hitler's Bandit Hunters: The SS and the Nazi Occupation of Europe*, Washington 2006, https://books.google.pl/books?id=jR49G7eyxBUC&pg=PA101&redir_esc=y#v=onepage&q&f=false [dostęp: 3.12.2024].

Botha A., *Prevention of Terrorist Attacks on Critical Infrastructure*, w: *Handbook of Terrorism Prevention and Preparedness*, A.P. Schmid (red.), https://icct.nl/sites/default/files/2023-01/Handbook_Schmid_2020.pdf, s. 841–870 [dostęp: 20.11.2024].

Butter D., *Does Turkey really get its oil from Islamic State?*, BBC, 1.12.2015, https://www.bbc.com/news/world-europe-34973181 [dostęp: 1.12.2025].

Byzdra K., *Partyzanci mieli zaatakować rurociągi w Kolumbii. Na miejsce wysłano wojsko*, Energetyka24, 27.08.2024, https://energetyka24.com/ropa/wiadomosci/partyzanci-mieli-zaatakowac-rurociagi-w-kolumbii-na-miejsce-wyslano-wojsko [dostęp: 27.12.2024].

Candan B., *Top 5 critical infrastructure cyberattacks*, Anapaya, 17.10.2024, https://www.anapaya.net/blog/top-5-critical-infrastructure-cyberattacks [dostęp: 17.10.2024].

Chiczkin A., *Jordania: zamach stanu w odwrotnej kolejności*, TopWar, 12.04.2021, https://pl.topwar.ru/181817-iordanija-perevorot-naoborot.html [dostęp: 12.12.2024].

14-latek przestawiał zwrotnice, Policja.pl, 9.01.2008, https://www.policja.pl/pol/aktualnosci/13278,14-latek-przestawial-zwrotnice.html [dostęp: 9.01.2025].

Czyżewski D., *Ropa pod uprawami koki, czyli problemy Kolumbii*, Energetyka24, 2.10.2021, https://energetyka24.com/ropa/ropa-pod-uprawami-koki-czyli-problemy-kolumbii-komentarz [dostęp: 2.12.2024].

Čokorilo O., Čokorilo S., Tomic L., *A framework for aviation security*, AIIT 4th International Conference on Transport Infrastructure and Systems (TIS ROMA 2024), https://www.researchgate.net/publication/381768379_A_framework_for_aviation_security [dostęp: 28.02.2025].

Daily Mail, *New report explores the pilot of MH370 troubled personal life, likely scenario of what happened on flight*, New Zealand Herald, 18.06.2019, https://www.nzherald.co.nz/world/new-report-explores-the-pilot-of-mh370-troubled-personal-life-likely-scenario-of-what-happened-on-flight/TOQ557EGUHWQDXG5DU47E7JOVE/ [dostęp: 18.12.2024].

De nouvelles centrales nucléaires survolées par de présumés drones, TF1Info, 2.08.2024, https://www.tf1info.fr/societe/de-nouvelles-centrales-nucleaires-survolees-par-de-presumes-drones-1562592.html [dostęp: 2.08.2024].

Desler M., *Seven five – man with knife, lotnictwo, a terroryzm*, dlapilota.pl, 9.04.2014, https://dlapilota.pl/wiadomosci/monika-desler/seven-five-man-knife-lotnictwo-terroryzm [dostęp: 9.12.2024].

Duchesneau J., *Aviation Terrorism. Thwarting High-Impact Low-Probability Attacks*, Royal Military College of Canada, Kingston 2015, https://espace.rmc.ca/jspui/bitstream/11264/741/1/Duchesneau%20PhD%20Thesis%2020150726%20Final%20e-Space%20RMC.pdf [dostęp: 6.12.2024].

EUROCONTROL, *Aviation under attack from a wave of cybercrime*, https://www.eurocontrol.int/sites/default/files/2021-07/eurocontrol-think-paper-12-aviation-under-cyber-attack.pdf [dostęp: 5.07.2024].

European Commission, *Enhancing EU resilience: A step forward to identify critical entities for key sectors*, https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_23_3992/IP_23_3992_EN.pdf [dostęp: 12.12.2024].

Farnworth R., *The Uganda Railway during the First World War*, https://rogerfarnworth.com/2020/12/28/the-uganda-railway-during-the-first-world-war/ [dostęp: 28.12.2024].

Horror w przestworzach, gangi ostrzelały dwa samoloty. Ranna stewardessa, Polskie Radio 24, 12.11.2024, https://polskieradio24.pl/artykul/3445609,horror-w-przestworzach-gangi-ostrzelaly-dwa-samoloty-ranna-stewardessa [dostęp: 21.12.2024].

Howden D., *Shell may pull out of Niger Delta after 17 die in boat raid*, The Independent, 17.01.2006, https://web.archive.org/web/20170527010950/http://www.corpwatch.org/article.php?id=13121 [dostęp: 17.01.2025].

Iran condemns 'terrorist' attack on gas pipelines, Al Jazeera, 14.02.2024, https://www.aljazeera.com/news/2024/2/14/iranian-gas-pipeline-blasts-due-to-terrorism-and-sabotage-official-says [dostęp: 14.12.2024].

Jenkins B.M., *The Terrorist Threat to Commercial Aviation*, Santa Monica 1989, https://www.rand.org/content/dam/rand/pubs/papers/2008/P7540.pdf [dostęp: 25.02.2025].

Jenkins B.M., Butterworth B.R., *How Sophisticated are Terrorist Attacks on Passenger Rail Transportation*, San José 2020, https://transweb.sjsu.edu/sites/default/files/SP0520-Jenkins-Terrorist-Attacks-Passenger-Rail-Transportation.pdf [dostęp: 3.12.2024].

Jenkins B.M., Butterworth B.R., *Train Wrecks and Track Attacks: An Analysis of Attempts by Terrorists and Other Extremists to Derail Trains or Disrupt Rail Transportation*, https://transweb.sjsu.edu/sites/default/files/1794_Jenkins_Train-Wrecks-Train-Attacks.pdf [dostęp: 3.12.2024].

Jenkins B.M., Butterworth B.R., Shrum K.S., *Terrorist Attacks on Public Bus Transportation: A Preliminary Empirical Analysis*, Mineta Transportation Institute 2010, https://transweb.sjsu.edu/sites/default/files/2982-Terrorist-Attacks-On-Public-Bus-Transportation.pdf [dostęp: 3.12.2025].

Jones T., *MH370: Search resumes to find missing plane 11 years on*, Deutsche Welle, 25.02.2025, https://www.dw.com/en/mh370-search-resumes-to-find-missing-plane-11-years-on/a-71739469 [dostęp: 25.02.2025].

Kennedy C., *Guerilla Attacks on Pipelines Threaten Colombia's Oil Production*, Oil Price, 10.09.2024, https://oilprice.com/Energy/Crude-Oil/Guerilla-Attacks-on-Pipelines-Threaten-Colombias-Oil-Production.html [dostęp: 10.09.2024].

Kielban Ł., *Zagrożenia dla Infrastruktury Krytycznej – podstawy dla urzędników i przedsiębiorców,* Polska Platforma Bezpieczeństwa Wewnętrznego, 13.06.2024, https://ppbw.pl/zagrozenia-infrastruktury-krytycznej-podstawy/ [dostęp: 13.12.2024].

Kirkland R., *„A secret, melodramatic sort of conspiracy": The disreputable legacies of Fenian violence in nineteenth-century London,* King's Research Portal, https://kcl-pure.kcl.ac.uk/ws/portalfiles/portal/114850253/A_secret_melodramatic_sort_KIRKLAND_Accepted25July2017Published12August2019_GREEN_AAM.pdf [dostęp: 3.12.2024].

Library of Congress, Federal Research Division, *Country Profile: Colombia,* 2007, https://maint.loc.gov/rr/frd/cs/profiles/Colombia.pdf [dostęp: 15.12.2024].

List of terrorist incidents in London, Wikipedia, https://en.wikipedia.org/wiki/List_of_terrorist_incidents_in_London [dostęp: 19.12.2024].

Losik J., *Wiadomo, co przewoził zaatakowany statek. Powód do niepokoju dla Moskwy,* Money.pl, 27.01.2024, https://www.money.pl/gospodarka/nieoczekiwany-cios-w-handel-rosyjskim-paliwem-zaplonal-tankowiec-6989192670440384a.html [dostęp: 27.01.2025].

Mandrup T., *The attack on Palma in Mozambique: An insurgency getting out of hand?,* Risk Intelligence, 8.04.2021, https://www.riskintelligence.eu/analyst-briefings/the-attack-on-palma-in-mozambique-an-insurgency-getting-out-of-hand [dostęp: 8.01.2025].

Mansfield I., *The first terrorist attack on the London Underground,* IanVisits, 30.10.2013, https://www.ianvisits.co.uk/articles/130th-anniversary-of-the-first-terrorist-attack-on-the-london-underground-9335/ [dostęp: 30.10.2024].

Marx G., *Oleoducto en peligro recibe tropas estadounidenses en Colombia,* Amazon Watch, 12.11.2002, https://amazonwatch.org/es/news/2002/1112-imperiled-pipeline-gets-us-troops-in-colombia [dostęp: 12.11.2024].

Mbah F., *In Nigeria's crude capital, a plan to win the war against oil theft,* Al Jazeera, 19.12.2024, https://www.aljazeera.com/news/2024/12/19/in-nigerias-crude-capital-a-plan-to-win-the-war-against-oil-theft [dostęp: 19.12.2024].

McEvoy J., *La Financión de BP a los militares asesinos de Colombia,* Declassified UK, 18.07.2023, https://www.declassifieduk.org/es/la-financiacion-de-bp-a-los-militares-asesinos-de-colombia/ [dostęp: 18.12.2024].

Nigeria train resumes operations eight months after major attack, Al Jazeera, 5.12.2022, https://www.aljazeera.com/news/2022/12/5/nigeria-train-resumes-eight-months--after-deadly-attack [dostęp: 5.12.2024].

Nigerian oil exports at lowest level in 25 years due to oil theft, Al Jazeera, 9.09.2022, https://www.aljazeera.com/news/2022/9/9/nigerian-oil-exports-at-lowest-level-in--25-years-due-to-oil-theft [dostęp: 9.01.2025].

Olanicki M., *Tajemnicze awarie polskich pociągów. O sabotaż podejrzewany producent*, Biznes Info, 6.12.2023, https://www.biznesinfo.pl/tajemnicze-awarie-polskich-pociagow-o-sabotaz-podejrzewany-producent-mo-wak-061223 [dostęp: 6.12.2024].

Olech A., *Terrorist Threats to the Energy Sector in Africa and the Middle East*, w: S.J. Lohman i in., *Countering Terrorism on Tomorrow's Battlefield: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 2)*, https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1953&context=monographs [dostęp: 15.12.2024].

Oltermann P., Beaumont P., Sabbagh D., *European leaders blame sabotage as gas pours into Baltic from Nord Stream pipelines*, The Guardian, 28.09.2022, https://www.theguardian.com/business/2022/sep/27/nord-stream-1-2-pipelines-leak-baltic-sabotage-fears [dostęp: 28.12.2024].

PAP, *Egipt: katastrofa samolotu Airbus A321 na Półwyspie Synaj (aktualizacja)*, dlapilota.pl, 17.11.2015, https://dlapilota.pl/wiadomosci/pap/egipt-katastrofa-samolotu--airbus-a321-na-polwyspie-synaj [dostęp: 17.12.2024].

PAP, *Kolumbia: 15 żołnierzy zginęło w zasadzce FARC*, Wirtualna Polska Wiadomości, 21.07.2013, https://wiadomosci.wp.pl/kolumbia-15-zolnierzy-zginelo-w-zasadzce--farc-6079340922217089a [dostęp: 21.12.2024].

Pawluszek A., *Malezyjski Boeing 777 zestrzelony przez Rosjan w 2014 r. Sąd w Hadze przedstawił stanowisko*, Gazeta Prawna, 17.11.2022, https://www.gazetaprawna.pl/wiadomosci/swiat/artykuly/8590126,holandia-sad-zestrzelenie-2014-malezyjski--boeing-777-ukraina.html [dostęp: 17.11.2024].

Piotrowski M.A., *Taktyka oraz konsekwencje strategiczne ataku na instalacje naftowe Arabii Saudyjskiej*, „Biuletyn PISM" 2019, nr 137, https://pism.pl/publikacje/Taktyka_oraz_konsekwencje_strategiczne_ataku_na_instalacje_naftowe_Arabii_Saudyjskiej [dostęp: 4.12.2024].

Reuters, *One killed, dozens injured in truck ramming at Israeli bus stop*, https://www.reuters.com/world/middle-east/multiple-injuries-truck-strikes-bus-stop-central-israel-police-say-2024-10-27/ [dostęp: 27.02.2024].

Reuters, *Teheran proponuje odszkodowania rodzinom ofiar zestrzelonego boeinga. Kijów krytykuje*, TVN24, 30.12.2020, https://tvn24.pl/swiat/ukrainski-samolot-zestrzelony-nad-teheranem-wladze-iranu-oferuja-odszkodowania-dla-rodzin-ofiar-st4851794 [dostęp: 30.12.2024].

Ribeiro A., *Cyber attacks continue to hit critical infrastructure, exposing vulnerabilities in oil, water, healthcare sectors*, Industrial Cyber, 14.02.2024, https://industrialcyber.co/critical-infrastructure/cyber-attacks-continue-to-hit-critical-infrastructure-exposing-vulnerabilities-in-oil-water-healthcare-sectors/ [dostęp: 14.12.2024].

Saqib M., *Recent Trends of Naxal Violence in India: Need for Comprehensive Approach from the Government*, „International Journal of Research in Social Sciences" 2018, t. 8, https://www.ijmra.us/project%20doc/2018/IJRSS_NOVEMBER2018/IJMRA-14770.pdf [dostęp: 3.12.2024].

Scheuer M., Ulph S., Daly J.C.K., *Saudi Arabian Oil Facilities: The Achilles Heel of the Western Economy*, The Jamestown Foundation 2006, https://jamestown.org/wp-content/uploads/2006/05/Jamestown-SaudiOil.pdf [dostęp: 24.02.2025].

Shukla N., *Maoists briefly hijack Indian train*, Reuters, 22.04.2009, https://www.reuters.com/article/world/maoists-briefly-hijack-indian-train-idUSTRE53L102/ [dostęp: 22.12.2024].

Sivesind C., *Cyber Attacks on Railway Systems Increase by 220%*, SecureWorld, 20.08.2024, https://www.secureworld.io/industry-news/railway-cyber-attacks [dostęp: 20.08.2024].

START, *Global Terrorism Overview: Terrorism in 2019*, https://www.start.umd.edu/pubs/START_GTD_GlobalTerrorismOverview2019_July2020.pdf [dostęp: 30.07.2024].

Timeline of airliner bombing attacks, Wikipedia, https://en.wikipedia.org/wiki/Timeline_of_airliner_bombing_attacks [dostęp: 26.02.2025].

Tragically Explosive – Szilvestre Matuschka: A Fetish For Disaster (Part Three), Europe Between East And West, 7.03.2020, https://europebetweeneastandwest.wordpress.com/tag/hungarian-serial-killers/ [dostęp: 7.12.2024].

UNOCT, CTED, Interpol, *The protection of critical infrastructure against terrorist attacks: Compendium of good practices*, https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf [dostęp: 12.12.2024].

Wald M.L., *Student Pilot, 15, Crashes Plane Into Tower in Florida*, New York Times, 6.01.2002, https://www.nytimes.com/2002/01/06/us/student-pilot-15-crashes-plane-into-tower-in-florida.html [dostęp: 6.01.2025].

Walków M., *Coraz więcej incydentów z dronami. Lotnisko Chopina przetestuje rozwiązanie*, Money.pl, 30.05.2023, https://www.money.pl/gospodarka/lotnisko-chopina-sie-zbroi-drony-to-coraz-powazniejsze-zagrozenie-dla-samolotow-6903403450051296a.html [dostęp: 30.12.2024].

Wang K., Kashi D., *Major U.S. military operations/actions to protect oil*, https://nationalsecurityzone.medill.northwestern.edu/archives/oilchangeproject/how-do-we-protect-the-flow-of-oil/index.html [dostęp: 12.12.2024].

Zafimehy M., Chieze G., *Crash de la Germanwings: à quoi ont ressemblé les dernières minutes avant la catastrophe?*, RTL, 26.03.2023, https://www.rtl.fr/actu/justice-faits-divers/crash-de-la-germanwings-a-quoi-ont-ressemble-les-dernieres-minutes-avant-la-catastrophe-7900246615 [dostęp: 26.01.2025].

Zimmerman M., *„Cud, że tyle osób przeżyło". Mija 50 lat od zamachu na lotnisku Fiumicino*, Onet, 17.12.2023, https://wiadomosci.onet.pl/swiat/50-lat-od-ataku-na-lotnisku-fiumicino-najbardziej-krwawy-z-tamtych-zamachow/mpd5nm4 [dostęp: 17.12.2024].

Akty prawne

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 27.12.2022).

Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (Dz. Urz. UE L 345/75 z 23.12.2008).

Inne dokumenty

United Nations, *Security Council resolution 2341 (2017) [on protection of critical infrastructure against terrorist acts]*.

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, wydanie specjalne: 115–135

https://doi.org/10.4467/27204383TER.25.004.21507

Artykuł

Infrastruktura krytyczna jako cel ataków hybrydowych i konwencjonalnych. Wnioski z ukraińskich doświadczeń

Critical infrastructure as a target of hybrid and conventional attacks. Lessons from the Ukrainian experience

MICHAŁ PIEKARSKI

https://orcid.org/0000-0003-1514-7657

Wydział Nauk Społecznych,
Uniwersytet Wrocławski

Abstrakt

Autor omawia problematykę ataków na infrastrukturę krytyczną Ukrainy, podejmowanych zarówno podczas działań hybrydowych (od 2014 r.), jak i w czasie pełnoskalowej rosyjskiej inwazji (od 2022 r.). Na podstawie dostępnych informacji analizuje operacje przeciwko infrastrukturze energetycznej Ukrainy. Zwraca uwagę na to, że ataki prowadzone przez rosyjskie siły mogą sięgać również na terytorium Unii Europejskiej. Przedstawia także wstępne wnioski dotyczące zarówno odporności, jak i obrony infrastruktury krytycznej.

Słowa kluczowe

Ukraina, infrastruktura krytyczna, ochrona infrastruktury krytycznej, wojna hybrydowa, strategiczna kampania powietrzna

Abstract

The author discusses the issue of attacks on Ukraine's critical infrastructure, undertaken both during hybrid operations (since 2014) and during a full-scale Russian invasion (since 2022). Based on the available information, he analyses the operations against Ukraine's energy infrastructure. He points out that attacks conducted by Russian forces may also reach the territory of the European Union. He also presents preliminary conclusions on both the resilience and defence of critical infrastructure.

Keywords

Ukraine, critical infrastructure, critical infrastructure protection, hybrid warfare, strategic air campaign

Wprowadzenie

Rosnące napięcia międzynarodowe, rosyjskie działania hybrydowe i zagrożenie możliwym konfliktem konwencjonalnym wpływają na infrastrukturę krytyczną (IK). Aby lepiej przygotować IK w Unii Europejskiej na potencjalny atak, konieczne jest skorzystanie z doświadczeń płynących z konfliktów toczących się w innych regionach.

Ukraina od 2014 r. była celem rosyjskich działań hybrydowych, a od 2022 r. – konwencjonalnych. Ataki prowadzone w ramach tych działań były wymierzone również w IK. Autor artykułu przedstawia wstępne wnioski wyciągnięte z dotychczasowych ukraińskich doświadczeń. Zaznacza, że bieżące wiadomości na temat rosyjskiej agresji na Ukrainę, zwłaszcza w mediach społecznościowych, są często powierzchowne i mogą być niezgodne z faktami lub zawierać treści propagandowe albo dezinformacyjne. Dogłębną analizę tej wojny będzie można przeprowadzić dopiero po jej zakończeniu. Przykładowo w jednym z cytowanych w artykule tomów, opublikowanym w 2025 r., opisano tylko pierwszy rok pełnoskalowej wojny. Dlatego autor zdecydował się korzystać z wielu źródeł, w tym raportów think tanków, książek i innych publikacji, opisujących różne aspekty ataków na ukraińską IK.

Ataki na infrastrukturę krytyczną w kontekście zagrożenia hybrydowego

Zgodnie z publikacją *The Landscape of Hybrid Threats*[1] wszelkie wrogie działania wymierzone w IK (aktywa lub systemy albo części tych systemów) mogą:

(a) pogorszyć jakość oferowanych towarów i usług (np. zmniejszyć dostępność, niezawodność),
(b) zniszczyć kluczowe części infrastruktury,
(c) zwiększyć koszty ich eksploatacji,
(d) wpłynąć na popyt, wywierać presję na infrastrukturę,
(e) ograniczyć lub usunąć możliwość dywersyfikacji dostaw dóbr i usług oraz powodować jednostronną zależność od wrogiego podmiotu,
(f) uzyskać lub ograniczyć dostęp do kluczowych zasobów dla jej funkcjonalności (surowce, technologia, wiedza specjalistyczna itp.) i nie tylko[2].

Ponadto (...) *każde narzędzie, które może stworzyć bądź wykorzystać lukę w infrastrukturze (luki wewnętrzne lub luki iniekcyjne) i osiągnąć jeden z powyższych efektów, może być potencjalnie wykorzystane jako część zestawu narzędzi hybrydowych*[3]. Ponieważ działania te są określane jako hybrydowe, atak na infrastrukturę może być przeprowadzony przy użyciu narzędzi cybernetycznych i wpływać na gospodarkę, społeczeństwo i administrację publiczną.

Ciekawe wydaje się także spojrzenie na wojnę hybrydową jako część szerszej strategii. Raport *Countering Gray-Zone Hybrid Threats*[4] (pol. Przeciwdziałanie zagrożeniom hybrydowym w szarej strefie), opublikowany w 2016 r. przez Akademię Wojskową Stanów Zjednoczonych, opisuje zagrożenia hybrydowe jako spektrum składające się z 2 głównych części: szarej strefy i otwartej wojny.

---

1 G. Giannopoulos, H. Smith, M. Theocharidou, *The Landscape of Hybrid Threats: A Conceptual Model Public Version*, Publications Office of the European Union, Luxembourg 2021, https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf [dostęp: 15.01.2025].

2 Tamże, s. 28. Tłumaczenia w artykule pochodzą od redakcji (dop. red.).

3 Tamże.

4 J. Chambers, *Countering Gray-Zone Hybrid Threats. An Analysis of Russia's 'New Generation Warfare' and Implications for the US Army*, 2016, https://mwi.westpoint.edu/wp-content/uploads/2016/10/Countering-Gray-Zone-Hybrid-Threats.pdf [dostęp: 15.01.2025].

Szara strefa jest opisywana jako znajdująca się poniżej progu konfliktu konwencjonalnego, mająca niejednoznaczny charakter. Zagrożenia hybrydowe w tej strefie mogą obejmować wykorzystywanie cywilów, agentów wywiadu, sił nieregularnych, działanie w różnych domenach (lądowej, powietrznej, morskiej, cybernetycznej, informacyjnej), z zastosowaniem instrumentów władzy, w tym dyplomacji, polityki gospodarczej, polityki informacyjnej i wojska.

Zagrożenia hybrydowe w otwartej wojnie z kolei bardziej przypominają konflikt konwencjonalny. Agresorzy nie ukrywają swojego zaangażowania, używają zarówno konwencjonalnych, jak i niekonwencjonalnych narzędzi (np. działań wojsk specjalnych, działań nieregularnych). Te ramy koncepcyjne mogą być bardzo ciekawe w szczegółowej analizie ataków na ukraińską IK, ponieważ ten kraj najpierw stanął w obliczu ograniczonej (szarej strefy) agresji, która rozpoczęła się w 2014 r., a następnie w 2022 r. – otwartej wojny.

Ukraińska infrastruktura krytyczna jako cel wojny hybrydowej

Ukraina, wraz z jej IK, była celem szerokiego zakresu rosyjskich działań hybrydowych, w tym wojny politycznej, prób zamachów, użycia siły wojskowej, łącznie z tzw. zielonymi ludzikami na Krymie, oraz buntów inspirowanych przez Rosję na wschodzie Ukrainy. Na przykład celem cyberataku na sieć energetyczną z 2015 r. było 3 operatorów systemu dystrybucji energii elektrycznej w Iwano-Frankiwsku, Czerniowcach i Kijowie. Ten zdalny atak spowodował przerwę w dostawie prądu dla 225 000 odbiorców[5]. Rok później kolejne cyberataki były wymierzone w pojedynczy element systemu dystrybucyjnego – podstację w pobliżu Kijowa[6]. Do następnego ataku doszło w 2017 r., był on jednak bardziej rozległy, ponieważ za pomocą ransmowaree'u Petya zaatakowano systemy nie tylko w Ukrainie[7].

[5] *Cyber-Attack Against Ukrainian Critical Infrastructure*, CISA, 20.07.2021, https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 [dostęp: 15.01.2025].

[6] *Ukraine power cut 'was cyber-attack'*, BBC News, 11.01.2017, https://www.bbc.co.uk/news/technology-38573074 [dostęp: 15.01.2025].

[7] N. Perlroth, M. Scott, S. Frenkel, *Cyberattack Hits Ukraine Then Spreads Internationally*, The New York Times, 27.06.2017, https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html [dostęp: 16.01.2025]; A. Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, Wired, 22.08.2018,

W tym samym czasie odnotowano także inne ataki. Na przykład w maju 2015 r. most kolejowy w Odessie został uszkodzony przez eksplozję improwizowanego ładunku wybuchowego (ang. *improvised explosive device*), która nastąpiła na krótko przed tym, jak pociąg miał przejechać przez miejsce ataku. Eksplozja była częścią szerszej serii zamachów bombowych w tym mieście portowym[8].

Celem agresji były również innego rodzaju infrastruktury. W maju 2014 r. eksplozja uszkodziła gazociąg Urengoj-Pomary-Użhorod w pobliżu Połtawy[9]. Kolejne eksplozje odnotowano w magazynach amunicji w Winnicy[10] w 2017 r. i rok później w Iczni[11]. Rosyjskie operacje hybrydowe od 2014 r. do początku 2022 r. były prowadzone, aby osłabić państwo ukraińskie, podważyć zaufanie obywateli do rządu i służb publicznych. Ponieważ celem politycznym Rosji pozostaje przejęcie kontroli nad Ukrainą i zmiana rządu na prorosyjski, operacje hybrydowe mogły stworzyć ku temu sprzyjające warunki.

Wzrost napięcia był widoczny szczególnie w ostatnich miesiącach przed rozpoczęciem pełnoskalowej inwazji Rosji na Ukrainę. Rosja, według raportu Royal United Services Institute (RUSI), przygotowywała się do przeprowadzenia kampanii niekonwencjonalnych działań wspierających jawną, konwencjonalną agresję, a celem miała być również IK: *Oczekuje się również, że krajowa infrastruktura krytyczna, w tym telekomunikacja, usługi rządowe, energia elektryczna i usługi użyteczności publicznej zostaną zaatakowane zarówno poprzez fizyczny sabotaż, jak i cyberatak. Ukraińskie służby bezpieczeństwa spodziewają się, że nie będą w stanie przerwać wszystkich tych ataków*[12].

https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [dostęp: 16.01.2025].

[8] *Explosion in Ukraine's Odessa Destroys Railroad Bridge but Misses Train*, The Moscow Times, 13.05.2015, https://www.themoscowtimes.com/2015/05/13/explosion-in-ukraines-odessa-destroys-railroad-bridge-but-misses-train-a46507 [dostęp: 16.01.2025].

[9] *Major Ukraine gas pipeline hit by blast*, 17.06.2014, BBC, https://www.bbc.com/news/world-europe-27891018 [dostęp: 16.01.2025].

[10] J. Mendel, *In Ukraine a Huge Ammunition Depot Catches Fire*, The New York Times, 27.09.2017, https://www.nytimes.com/2017/09/27/world/europe/ukraine-ammunition-depot-explosion.html?mcubz=0 [dostęp: 16.01.2025].

[11] *Ukraine ammo dump blasts blamed on 'possible sabotage'*, BBC, 9.10.2018, https://www.bbc.co.uk/news/world-europe-45794963 [dostęp: 16.01.2025].

[12] J. Watling, N. Reynolds, *The Plot to Destroy Ukraine*, 15.02.2022, https://static.rusi.org/special-report-202202-ukraine-web.pdf [dostęp: 17.01.2025].

Ataki na infrastrukturę, choć zróżnicowane pod względem skali i metod, były wstępem do znacznie szerszej operacji konwencjonalnej. Ataki hybrydowe nie zakończyły się sukcesem. W sektorze IK podjęto działania mające na celu zwiększenie jej odporności. Na przykład w 2015 r. opublikowano tzw. zieloną księgę ochrony infrastruktury krytycznej[13] w Ukrainie, a w 2022 r. przyjęto specjalną ustawę parlamentu o IK[14].

Warto zauważyć, że ataki na Ukrainę, szczególnie cyberataki, zostały opisane także jako poligon doświadczalny do prowadzenia cyberwojny przeciwko innym krajom, w tym państwom członkowskim UE i Stanom Zjednoczonym[15].

Ukraińska infrastruktura krytyczna jako cel wojny konwencjonalnej

Celem pełnoskalowej inwazji Rosji na Ukrainę, rozpoczętej 24 lutego 2022 r., było przejęcie kontroli nad Ukrainą przez zajęcie Kijowa. Kiedy nie został on osiągnięty, operacja wojskowa skupiła się na innych obszarach, w tym na Donbasie[16]. Rosjanie byli w stanie przejąć znaczne tereny Ukrainy, w tym południową część kraju. W ten sposób powstało połączenie lądowe między Krymem a Rosją kontynentalną. Istniało wiele elementów IK, w tym 2 elektrownie jądrowe, linie kolejowe i inne, które znalazły się pod rosyjską kontrolą, jednak zostały one przejęte głównie dlatego, że znajdowały się na ziemiach zajętych przez rosyjskie siły, nie były zaś oddzielnymi celami. Takim przykładem jest Czarnobylska Elektrownia Jądrowa, którą przejęto, ponieważ znajdowała się na trasie rosyjskich wojsk wkraczających na Ukrainę z Białorusi. Następnie została odzyskana przez Ukrainę, gdy rosyjskie wojska wycofały się po nieudanej

[13] D. Biriukov, S. Kondratov, O. Nasvit, O. Sukhodolia, *Green Paper on Critical Infrastructure Protection in Ukraine. Analytical Report*, Kiev 2015.

[14] *Закон України про критичну інфраструктуру* (Відомості Верховної Ради України (ВВР), 2023, № 5, ст. 13) – [*Zakon Ukrajiny pro krytycznu infrastrukturu* (Widomosti Werchownoji Rady Ukrajiny (WWR), 2023, № 5, st. 13)], https://zakon.rada.gov.ua/laws/show/1882-20#Text [dostęp: 17.01.2025].

[15] A. Greenberg, *How an Entire Nation Became Russia's Test Lab for Cyberwar*, Wired, 20.06.2017, https://www.wired.com/story/russian-hackers-attack-ukraine/ [dostęp: 18.01.2025].

[16] J. Watling, N. Reynolds, *Operation Z. The Death Throes of an Imperial Delusion*, 22.04.2022, https://static.rusi.org/special-report-202204-operation-z-web.pdf [dostęp: 18.01.2025].

bitwie o Kijów. Zniszczenie tamy w Nowej Kachowce także było częścią rosyjskiej operacji wojskowej, przeprowadzonej w celu zakłócenia ukraińskich operacji ofensywnych, ponieważ wyłączyło z użytkowania 1 ważny most i uniemożliwiło dalsze operacje przekraczania rzeki poniżej tamy z powodu katastrofalnej powodzi[17]. Podobny incydent odnotowano w 2023 r.[18] Wiele innych obiektów IK również zostało zaatakowanych lub przejętych podczas walk.

Nowe wyzwania pojawiły się później, gdy stało się jasne, że rosyjskie siły nie są w stanie zająć Kijowa, a ukraińskie siły zbrojne przeprowadzają udane operacje zarówno obronne, jak i ofensywne. Jesienią 2022 r. Rosjanie rozpoczęli pierwszą strategiczną kampanię wymierzoną w ukraiński sektor energetyczny. Ataki nie były tylko kolejnym elementem kampanii na froncie, lecz także – podobnie jak w przypadku innych konfliktów, w tym II wojny światowej – próbą kształtowania sytuacji strategicznej i osłabienia ukraińskiej odporności społecznej. Tego typu ataki mają pogarszać warunki życia ludności cywilnej, zakłócać kluczowe sektory gospodarki. Mogą zmusić rząd do zaakceptowania żądań agresora, w obliczu groźby buntu społeczeństwa wyczerpanego strategiczną kampanią powietrzną. Koncepcja ta nie jest niczym nowym w historii działań wojennych, począwszy od teorii wojny powietrznej Giulio Douheta[19], przez strategiczne ataki w czasie II wojny światowej, aż po teorię 5 pierścieni Johna Ashleya Wardena III. Teoria Wardena, jako najnowocześniejsza, jest szczególnie pomocna w wyjaśnianiu rosyjskich ataków na ukraińską IK, ponieważ umieszcza je w 2 pierścieniach: infrastrukturze (opisywanej głównie jako transportowa) i tzw. krytycznych podstawach (z ang. *critical essentials*) – obejmujących zasilanie[20]. Ponadto w rosyjskiej strategii wojskowej istnieje koncepcja Strategicznej Operacji Zniszczenia Krytycznie Ważnych Celów (ang. Strategic Operation

[17] H. Altman, *Dam Destroyed, Accusations Fly, Waters Rise, War Plans Could Change*, The War Zone, 6.06.2023, https://www.twz.com/dam-destroyed-accusations-fly-waters-rise-war-plans-could-change [dostęp: 18.01.2025].

[18] T. Newdick, *Ukraine Accuses Russia Of Blowing Up Another Dam*, The War Zone, 12.06.2023, https://www.twz.com/ukraine-accuses-russia-of-blowing-up-another-dam [dostęp: 18.01.2025].

[19] G. Douhet, *Panowanie w powietrzu. Przypuszczalne formy przyszłej wojny oraz ostatnie artykuły*, Warszawa 2013.

[20] J.A. Warden III, *The Enemy as System*, „Airpower Journal" 1995, t. 9, nr 1, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-09_Issue-1-Se/1995_Vol9_No1.pdf, s. 44–50 [dostęp: 1.02.2025].

for the Destruction of Critically Important Targets, SODCIT)[21]. Ten rodzaj operacji ma na celu zniszczenie obiektów (systemów), które mogą mieć charakter wojskowy lub niewojskowy, aby zmusić wroga do zaprzestania działań na warunkach korzystnych dla Rosji[22]. Według Michaela Kofmana operacja ta nie została przeprowadzona na początku otwartej inwazji, ale uderzenia na ukraińską sieć energetyczną były w rzeczywistości SODCIT[23]. Zostaną one opisane szczegółowo w dalszej części tekstu.

Rosyjskie ataki powietrzne i rakietowe na ukraińską sieć energetyczną

Pierwsze uderzenia wymierzone w ukraińską infrastrukturę energetyczną, które można interpretować jako część SODCIT, zostały przeprowadzone 10 października 2022 r. Wystrzelono wówczas 84 pociski rakietowe i 24 drony. Celem były elektrownie i podstacje w Kijowie i 11 regionach, co spowodowało przerwy w dostawie prądu[24]. Dodatkowe, ale ograniczone uderzenie (28 pocisków wspieranych przez drony) nastąpiło dzień później. Zmasowane ataki odnotowano 31 października[25] i 15 listopada[26], a także w grudniu. Pod koniec 2022 r. przeprowadzono dziesiąty atak na dużą skalę[27]. Do następnych uderzeń doszło w pierwszych miesiącach 2023 r.,

[21] M. Kofman i in., *Russian Military Strategy: Core Tenets and Operational Concepts*, sierpień 2021, https://www.cna.org/archive/CNA_Files/pdf/russian-military-strategy-core-tenets-and-operational-concepts.pdf [dostęp: 3.02.2025].

[22] M. Depczyński, L. Elak, *Rosyjska sztuka operacyjna w zarysie*, Warszawa 2020, s. 369–376.

[23] M. Kofman, *Russian airpower in context: The first year of war*, w: *The Air War in Ukraine – The First Year of Conflict*, D. Henriksen, J. Bronk (red.), New York 2025.

[24] S. Matuszak, *Rosja destabilizuje system energetyczny Ukrainy*, Ośrodek Studiów Wschodnich, 11.10.2022, https://www.osw.waw.pl/pl/publikacje/analizy/2022-10-11/rosja-destabilizuje-system-energetyczny-ukrainy [dostęp: 5.02.2025].

[25] L. Harding, D. Sabbagh, I. Koshiw, *Russia targets Ukraine energy and water infrastructure in missile attacks*, The Guardian, 31.10.2022, https://www.theguardian.com/world/2022/oct/31/russian-missiles-kyiv-ukraine-cities [dostęp: 5.02.2025].

[26] A. Wilk, P. Żochowski, *Ukraina bez prądu. 265. dzień wojny*, Ośrodek Studiów Wschodnich, 16.11.2022, https://www.osw.waw.pl/pl/publikacje/analizy/2022-11-16/ukraina-bez-pradu-265-dzien-wojny [dostęp: 5.02.2025].

[27] A. Wilk, P. Żochowski, *Dziesiąty zmasowany ostrzał Ukrainy. 309. dzień wojny*, Ośrodek Studiów Wschodnich, 30.12.2022, https://www.osw.waw.pl/pl/publikacje/analizy/2022-12-30/dziesiaty-zmasowany-ostrzal-ukrainy-309-dzien-wojny [dostęp: 5.02.2025].

a w maju odnotowano kolejną falę ataków. Większość z nich koncentrowała się na systemie przesyłowym (podstacjach).

Pod koniec 2023 r. odnotowano wiele mniejszych ataków przy użyciu dronów (z niewielką liczbą różnego rodzaju pocisków) i tylko jeden duży atak (29 grudnia). Zmienił się przebieg kampanii powietrznej, ponieważ celowała ona nie tylko w sieć energetyczną, lecz także w przemysł zbrojeniowy[28]. Do kolejnych ataków doszło w 2024 r. – w styczniu do 5 dużych[29], w lutym nie odnotowano żadnego[30], co może świadczyć o wyczerpaniu zapasu środków rażenia, pod koniec marca przeprowadzono duży atak (łącznie 151 pocisków rakietowych i dronów), w następnych dniach były realizowane dalsze ataki[31].

W maju odnotowano 3 ataki na dużą skalę[32], a w czerwcu – 4, w tym największy z użyciem łącznie 100 rakiet i dronów[33]. Dnia 26 sierpnia 2024 r. siły rosyjskie rozpoczęły atak, określany jako najpotężniejszy od początku otwartej inwazji. Wykryto 236 dronów i pocisków rakietowych, w tym 109 dronów, 77 pocisków manewrujących Ch-101 oraz łącznie 50 pocisków Ch-59, Ch-22 i pocisków balistycznych. Celem były elementy sieci energetycznej w 15 regionach Ukrainy[34]. Jedną z zauważalnych zmian w porównaniu z poprzednimi atakami było skupienie się na elektrowniach, zwłaszcza wodnych i węglowych, w celu destabilizacji sieci elektrycznej[35].

Częstotliwość ataków i zastosowana w nich broń różniły się w późniejszym okresie. Na przykład każdego dnia od maja do września 2024 r.

---

[28] M. Strembski, *Wojna powietrzna nad Ukrainą – grudzień 2023 r.*, „Lotnictwo" 2024, nr 1, s. 38.

[29] M. Strembski, *Wojna powietrzna nad Ukrainą – styczeń 2024 r.*, „Lotnictwo" 2024, nr 2, s. 14, 16, 18–19.

[30] Według publikacji Ośrodka Studiów Wschodnich.

[31] S. Matuszak, *Ukraina: poważny cios w energetykę*, Ośrodek Studiów Wschodnich, 28.03.2024, https://www.osw.waw.pl/pl/publikacje/analizy/2024-03-28/ukraina-powazny-cios-w-energetyke [dostęp: 5.02.2025].

[32] M. Strembski, *Wojna powietrzna nad Ukrainą. Maj 2024 r.*, „Lotnictwo" 2024, nr 6, s. 43, 48–49.

[33] M. Strembski, *Wojna powietrzna nad Ukrainą. Czerwiec 2024 r.*, „Lotnictwo" 2024, nr 7–8, s. 30, 32, 34, 36.

[34] M. Strembski, *Wojna powietrzna nad Ukrainą. Sierpień 2024 r.*, „Lotnictwo" 2024, nr 10, s. 46.

[35] M. Zaniewicz, *Ukraine in Darkness: Preventing the Worst-Case Scenario for Its Energy System*, Forum Energii, 1.07.2024, https://www.forum-energii.eu/en/ukraine-destroyed-system [dostęp: 7.02.2025].

przeprowadzano mniejsze uderzenia z wykorzystaniem dronów, ale 30 września użyto łącznie 76 pocisków i dronów[36].

W listopadzie 2024 r. doszło do poważnego natarcia, np. 17 listopada ok. 210 pocisków i dronów zostało użytych do ataku na sieć energetyczną, w tym elektrownie i podstacje, co spowodowało przerwy w dostawie prądu w całym regionie. Zostały również uszkodzone systemy ciepłownicze i sieci wodociągowe. W dniu 21 listopada celem kolejnego ataku na dużą skalę był obszar Dniepru. Z kolei 28 listopada co najmniej 188 rakiet i dronów użyto do ataku na infrastrukturę energetyczną i cele przemysłowe[37].

Były to przemyślane, nieprzypadkowe uderzenia na sieć energetyczną powodujące wieloaspektowe konsekwencje. Naprawienie lub wymiana uszkodzonych elementów wymaga czasu, dostępu do części lub nowych komponentów, np. transformatorów, dostępności wykwalifikowanej siły roboczej. W przypadku braku części zamiennych możliwości generowania i przesyłania energii są ograniczone[38]. Ponadto system energetyczny wymaga zarówno podsystemów wytwarzania (elektrowni), jak i podsystemów przesyłowych, a wczesne rosyjskie ataki (w latach 2022–2023) były ukierunkowane na część przesyłową – podstacje, co blokowało możliwości dostarczania wytworzonej energii[39].

W wyniku ukraińskich prób złagodzenia skutków ataków i poprawienia odporności, późniejsze rosyjskie ataki były skoncentrowane na systemie wytwarzania energii. Według Macieja Zaniewicza miały one na celu destabilizację systemu przez uniemożliwienie jego zbilansowania i dostarczania energii w godzinach szczytowego zapotrzebowania. Rosja była w stanie zmniejszyć ukraińskie moce wytwórcze o 3/4 – z 40 GW przed wojną do 10 GW w maju 2024 r.[40] Według Międzynarodowej Agencji Energetycznej ok. 70% ukraińskich mocy wytwórczych energii cieplnej, a także połowa podstacji wysokiego

[36] M. Strembski, *Wojna powietrzna nad Ukrainą. Wrzesień 2024 r.*, „Lotnictwo" 2024, nr 11, s. 34.

[37] M. Strembski, *Wojna powietrzna nad Ukrainą – listopad 2024 r.*, „Lotnictwo" 2025, nr 1, s. 33, 36, 38.

[38] B.E. Humpreys, *Attacks on Ukraine's Electric Grid: Insights for U.S. Infrastructure Security and Resilience*, Congressional Research Service, 17.05.2024, https://crsreports.congress.gov/product/pdf/R/R48067 [dostęp: 8.02.2025].

[39] Tamże.

[40] M. Zaniewicz, *Ukraine in Darkness*...

napięcia zostało zajętych lub uszkodzonych. Uszkodzenia zmusiły operatora systemu energetycznego do ograniczenia dostaw energii[41].

Terminy i częstotliwość działań, zwłaszcza w latach 2022–2023, zostały dostosowane do warunków środowiskowych i społecznych. Ataki na sieć energetyczną, w tym elektrownie i elektrociepłownie, mogłyby mieć katastrofalny wpływ na społeczeństwo, gdyby nie było ogrzewania, nawet uzupełniającego z urządzeń zasilanych energią elektryczną. Również inne systemy potrzebujące energii elektrycznej, w tym system wodny, zostałyby zakłócone. Brak elektryczności oznacza także ograniczony dostęp do informacji i zakupów (płatności można dokonywać tylko gotówką).

Taktyka i broń zastosowane podczas ataku rosyjskich sił na ukraińską sieć energetyczną

Zastosowaną broń można podzielić na kilka kategorii, od konwencjonalnych samolotów, przez pociski kierowane różnych typów, do rakiet balistycznych i jednokierunkowych dronów atakujących. Samoloty pilotowane, zwłaszcza wielozadaniowe samoloty bojowe Su-30, Su-34 i bombowce, takie jak Tu-22M, Tu-95 i Tu-160[42], są wykorzystywane wyłącznie jako nośniki pocisków manewrujących, w atakach typu *stand-off* z dala od ukraińskich systemów obrony powietrznej. Nie odnotowano bezpośrednich bombardowań przy użyciu bomb niekierowanych lub kierowanych, ponieważ ten tryb ataku zwiększyłby ryzyko strat.

Większość pocisków manewrujących wystrzeliwanych z powietrza to pociski Ch-59, Ch-69, Ch-22, Ch-32, Ch-101 i Ch-555, uzupełnione przez pociski balistyczne Ch-47. Poddźwiękowe pociski Ch-59 (i ich zmodernizowany wariant Ch-69) mają zasięg do 258 km. Zostały zaprojektowane do atakowania małych celów stacjonarnych lub okrętów wojennych i – w zależności od wariantu[43] – przenoszą głowice o masie 140–258 kg.

Pociski Ch-22 i Ch-32, przenoszone przez bombowce Tu-22M, pełnią podwójną funkcję. Choć zostały zaprojektowane jako broń przeciw okrętom, to są zdolne do rażenia również stacjonarnych celów lądowych.

[41] *Ukraine's Energy Security and the Coming Winter*, IEA, wrzesień 2024, https://iea.blob.core.windows.net/assets/cec49dc2-7d04-442f-92aa-54c18e6f51d6/UkrainesEnergySecurityandtheComing-Winter.pdf, s. 12 [dostęp: 9.02.2025].

[42] P. Butowski, *Russian Air Power*, 2023, s. 7–30, 70–87.

[43] T. Kwasek, *Lotnicze pociski skrzydlate rodziny Ch-59*, „Lotnictwo" 2024, nr 3, s. 42.

Maksymalny zasięg tych pocisków wynosi 500 km (Ch-22) lub 1000 km (Ch-32), a waga ich głowic bojowych to 600 kg. Pociski te po wystrzeleniu osiągają wysokość do 44 km i prędkość naddźwiękową do 3200 km/h. Zarówno Ch-101, jak i Ch-555 to nisko latające pociski manewrujące, wystrzeliwane przez samoloty bombowe. Mają duży zasięg: Ch-555 do 3500 km[44], Ch-101 do 2800 km[45]. Dodatkowo czasami są używane pociski Ch-47. Są one wystrzeliwane z powietrza wariantem pocisku Iskander o zasięgu do 2000 km[46].

Lądowe pociski rakietowe używane przeciwko ukraińskiej sieci energetycznej należą głównie do systemu Iskander, zaprojektowanego do atakowania celów lądowych. Ten zestaw uderzeniowy wykorzystuje pociski balistyczne 9M723, a także 2 warianty pocisków manewrujących: 9M728 i 9M729, które mają maksymalny zasięg 480 km[47]. W przypadku pocisków lądowych czasami zgłaszano użycie zestawów przeciwokrętowych Bastion i Bał lub pocisków ziemia-powietrze S-300, ponieważ wszystkie te pociski są zdolne do uderzania w stacjonarne cele lądowe. Innym rodzajem pocisków, które zostały użyte w atakach, są okrętowe pociski manewrujące 3M14 Kalibr. Mają one zasięg do 2000 km i mogą być wystrzeliwane przez okręty nawodne i podwodne[48].

Oprócz tej rosyjskiej broni konwencjonalnej powszechnie są stosowane irańskie samoloty bezzałogowe Szahed-136 i Szahed-131 (znane również jako Geran-2 i Geran-1). Drony te przenoszą małe głowice bojowe (od 15 do 50 kg), są napędzane silnikami tłokowymi i mają zasięg do 2500 km[49].

To połączenie różnych typów rakiet i dronów pozwala rosyjskim siłom na atakowanie z wielu kierunków, z różną prędkością i wysokością. Z tego powodu nie ma jednego środka obronnego, np. systemu obrony powietrznej umieszczonego tylko na jednym, najbardziej prawdopodobnym

[44] *Kh-55 (AS-15)*, Missile Threat, 23.04.2024, https://missilethreat.csis.org/missile/kh-55/ [dostęp: 12.02.2025].

[45] *Kh-101 / Kh-102*, Missile Threat, 23.04.2024, https://missilethreat.csis.org/missile/kh-101-kh-102/ [dostęp: 12.02.2025].

[46] *Kh-47M2 Kinzhal*, Missile Threat, 23.04.2024, https://missilethreat.csis.org/missile/kinzhal/ [dostęp: 12.02.2025].

[47] T. Kwasek, *Rakiety Putina. Rosyjskie lądowe, lotnicze i morskie systemy rakietowe oraz pociski manewrujące*, „Nowa Technika Wojskowa" 2023, numer specjalny: *Wojna rosyjsko-ukraińska*, s. 44.

[48] *3M-14 Kalibr (SS-N-30A)*, Missile Threat, 23.04.2024, https://missilethreat.csis.org/missile/ss-n-30a/ [dostęp: 12.02.2025].

[49] M. Glajzer, *Irański oręż w rosyjskiej służbie*, „Nowa Technika Wojskowa" 2022, nr 11, s. 13–14.

kierunku. Wystrzelenie wielu rodzajów broni – nazywane atakiem nasycającym – utrudnia ich przechwytywanie, ponieważ liczba systemów obrony powietrznej i ich możliwości są ograniczone. Ponadto użycie różnych rodzajów broni zwiększa szanse powodzenia ataku – nawet jeśli jedna grupa lub typ pocisków zostaną zestrzelone, inne mogą dotrzeć do celów. Użycie różnych rodzajów broni pozwala także odwrócić uwagę obrońców przez skierowanie ognia w stronę ataku dywersyjnego, co również zwiększa szansę na sukces. Zastosowanie zaawansowanej broni, takiej jak nowoczesne pociski kierowane do obrony przed atakiem z użyciem taniej broni, zwłaszcza dronów, wywiera presję na żołnierzy, a ponadto może prowadzić do wyczerpania zapasów wysokiej klasy uzbrojenia. Uzupełnienie tych strat może być trudne i kosztowne.

Problemem dla Rosji są kwestie ekonomiczne. Ataki wymagające użycia dużej liczby broni mogą być przeprowadzone po zgromadzeniu niezbędnych zapasów, a dostępność środków transportu, zwłaszcza samolotów, prawdopodobnie ogranicza rosyjskie możliwości. Z tego powodu ataków nie przeprowadza się w sposób ciągły, lecz raczej falami, co zmusza Rosję do uderzenia tylko wtedy, gdy atak może przynieść największe zniszczenia.

Jeśli chodzi o środki obrony i ochrony, Ukrainie udało się jak dotąd zapobiec najgorszemu. Pomimo uszkodzeń infrastruktury i spowodowanych nimi przerw w dostawie prądu nie ma bezpośredniego, strategicznego wpływu kampanii na ukraińską sieć energetyczną. Ataki z przełomu 2022 i 2023 r. nie zmusiły Ukrainy do zaakceptowania rosyjskich żądań, wręcz przeciwnie, była ona w stanie prowadzić operacje ofensywne. Możliwe, że długoterminowe skutki, zwłaszcza rosnące zmęczenie Ukraińców wojną, mogą stać się ważnym czynnikiem demobilizacji społecznej i spadku poparcia dla kontynuowania wojny, szczególnie jeśli potrwa ona przez następny rok lub dłużej, a dalsze ataki spowodują kolejne uszkodzenia ukraińskiej sieci energetycznej. Inną kwestią jest jednak wytrwałość społeczeństwa, wytrzymałość sieci energetycznej i zdolność do obrony infrastruktury.

Jednym z czynników wzmacniających odporność jest to, że ukraińska sieć energetyczna, produkcji radzieckiej, zaprojektowana do zasilania przemysłu ciężkiego, była w stanie zapewnić dodatkową moc, której zwykle nie wykorzystywano. Ponadto istotna jest również zdolność do naprawy uszkodzeń, zwłaszcza linii przesyłowych i podstacji (może to być jedna ze zmian w wybieraniu celów: od podstacji do elektrowni, które są trudniejsze do naprawy).

Podjęto także inne środki w celu zapewnienia energii elektrycznej, w tym import z europejskiej sieci energetycznej. Tymczasowym rozwiązaniem dla ludności mieszkającej na obszarach dotkniętych awarią było rozmieszczenie generatorów zasilanych olejem napędowym w wyznaczonych punktach pomocy, tzw. punktach niezwyciężoności (ang. *points of invincibility*), które zapewniają dostęp do energii elektrycznej, ciepła i wody. Według doniesień medialnych utworzono ok. 13 000 takich punktów[50].

Obronę zapewniały różnego rodzaju systemy przeciwlotnicze i samoloty. Rozwój ukraińskiej obrony przeciwlotniczej był pozornie szybki i często wymagał improwizacji ze względu na skalę ataków i malejące zasoby systemów obrony przeciwlotniczej. Ukraina w 2022 r. dysponowała systemami produkcji radzieckiej, takimi jak S-300, Buk, Osa, uzupełnionymi przez artylerię i systemy przenośne (np. Strieła)[51]. W późniejszych latach dostarczono więcej systemów z krajów NATO, w tym polskie przenośne przeciwlotnicze zestawy rakietowe Grom i Piorun, systemy krótkiego i średniego zasięgu, takie jak IRIS-T, Hawk, NASAMS, Aspide oraz dalekiego zasięgu Patriot i SAMP/T[52]. Aby zwalczać zagrożenie ze strony nisko latających dronów, dodatkowe tanie systemy – wykorzystujące karabiny maszynowe montowane na ciężarówkach – zostały opracowane na wczesnym etapie rosyjskich ataków w 2022 r.[53] Ponadto przekształcono starsze systemy, co umożliwiło korzystanie z zachodnich pocisków rakietowych lub pozwoliło na użycie dostępnych pocisków powietrze-powietrze w wyrzutniach lądowych. Znane rodzaje tych systemów – tzw. FrankenSAM – to pociski Buk wystrzeliwujące pociski RIM-7[54], wyrzutnie OSA wykorzystujące

[50] *There are almost 13 thousand Invincibility Points in Ukraine*, UNN, 3.04.2024, https://unn.ua/en/news/there-are-almost-13-thousand-invincibility-points-in-ukraine [dostęp: 13.02.2025].

[51] *Russia and Eurasia*, „The Military Balance" 2022, t. 122, nr 1, s. 164–217. https://doi.org/10.1080/04597222.2022.2022930.

[52] Tamże.

[53] M.E. Miller, A. Galouchka, *Ukraine's drone hunters scramble to destroy Russia's Iranian–built fleet*, The Washington Post, 28.11.2022, https://www.washingtonpost.com/world/2022/11/28/ukraine-drone-hunters-mykolaiv-russia/ [dostęp: 13.02.2025].

[54] J. Trevithick, *'FrankenSAM' Systems Are Now Shooting Down Drones In Ukraine*, The War Zone, 17.01.2024, https://www.twz.com/frankensam-systems-are-now-shooting-down-drones-in-ukraine [dostęp: 14.02.2025].

pociski R-73[55] i inne, w tym kontenerowe wyrzutnie R-73[56]. Istnieją również samoloty służące do zestrzeliwania pocisków rakietowych i dronów. Oprócz konwencjonalnych myśliwców (MiG-29, Su-27, F-16) są dostępne także niedrogie rozwiązania. Podano, że śmigłowce były wykorzystywane do zwalczania dronów[57]. Ten szeroki zestaw broni obronnej zmniejszył liczbę pocisków i dronów docierających do celów.

Wnioski

Ukraińska IK od 2014 r. była celem rosyjskich ataków, zarówno w formie hybrydowej, jak i konwencjonalnej. Wojna hybrydowa musi być traktowana jako wstęp do możliwej konwencjonalnej agresji i rozumiana również w kontekście ochrony IK – zagrożenia hybrydowe i konwencjonalne są częścią tego samego kontinuum. Oznacza to również, że nie ma możliwości zastąpienia jednego rodzaju działań wojennych innym lub jednego rodzaju ataków innym. Fakt, że ukraińska sieć energetyczna była celem cyberataków, nie wykluczył ataków konwencjonalnych.

Państwa członkowskie UE mierzą się z podobnym zagrożeniem. Agresywna postawa Rosji oznacza ciągłe, wyraźne i obecne zagrożenie zarówno atakami hybrydowymi, jak i konwencjonalnymi. Należą do nich ataki rakietowe i dronowe, które mogą sięgać głęboko na terytorium UE, zwłaszcza jeśli weźmie się pod uwagę platformy morskie (okręty nawodne i podwodne). Wynik ataku na IK może być druzgocący w wymiarze fizycznym, społecznym i politycznym. Zagrożenie zwiększa się w związku z tym, że rosyjskie siły morskie – z wyjątkiem tych na Morzu Czarnym – nie są dotknięte wojną, a we Flocie Północnej (ros. Северный флот) i Flocie Bałtyckiej Marynarki Wojennej Federacji Rosyjskiej (ros. Балтийский флот

[55] T. Newdick, *Ukraine's SA-8 Gecko 'FrankenSAM' Adapted To Fire Air-To-Air Missiles Seen In New Detail*, The War Zone, 12.12.2024, https://www.twz.com/land/ukraines-sa-8-gecko-frankensam-adapted-to-fire-air-to-air-missiles-seen-in-new-detail [dostęp: 14.02.2025].

[56] J. Trevithick, *Containerized SAM System That Fires Soviet Air-To-Air Missiles For Ukraine Breaks Cover*, The War Zone, 12.02.2025, https://www.twz.com/land/containerized-sam-system-that-fires-soviet-air-to-air-missiles-for-ukraine-breaks-cover [dostęp: 14.02.2025].

[57] D. Axe, *Ukrainian Helicopter Crews Are Shooting Down Russian Drones – Like World War II Turret Gunners*, Forbes, 22.08.2024, https://www.forbes.com/sites/davidaxe/2024/08/22/ukrainian-helicopter-crews-are-shooting-down-russian-drones-like-world-war-ii-turret-gunners/ [dostęp: 14.02.2025].

ВМФ Российской Федерации) znajduje się wiele okrętów zdolnych do wystrzelenia pocisków manewrujących przeciwko celom lądowym.

Kolejne wnioski dotyczą odporności i obrony. Odporność infrastruktury ma kluczowe znaczenie, ponieważ obejmuje ona zdolność do zapewnienia zapasowych źródeł zasilania – w przypadku sieci energetycznej dotyczy to wytwarzania i przesyłu energii. Im więcej źródeł zasilania i dróg przesyłu energii jest dostępnych, tym lepiej, ponieważ nawet jeśli niektóre z nich zostaną uszkodzone, pozostałe mogą przejąć ich rolę. Można to zastosować również do innych rodzajów infrastruktury, takich jak koleje. Podobną formą rezerw jest zapewnienie nadwyżki mocy do wykorzystania w sytuacji kryzysowej, co mogłoby ograniczyć skutki uszkodzeń. Ponadto wysoce zalecane jest posiadanie odpowiedniej liczby części zamiennych lub urządzeń. Jeśli to możliwe, należałoby wziąć pod uwagę rozproszenie infrastruktury, np. w przypadku elementów sieci energetycznej możliwa jest decentralizacja wytwarzania, a małe instalacje, nawet przydomowe, wykorzystujące energię odnawialną mogą być uzupełnieniem dla istniejących elektrowni konwencjonalnych.

Innym wymiarem odporności jest zdolność do zapewnienia odpowiedniej liczby wykwalifikowanego personelu w celu utrzymania, naprawy bądź odbudowy infrastruktury. Zapotrzebowanie na wykwalifikowanych pracowników będzie wyższe niż na co dzień w przypadku ataków na IK, a zazwyczaj właściciele lub operatorzy IK zatrudniają odpowiednią liczbę osób do pracy w normalnych warunkach. W związku z tym zaleca się uwzględnienie w ochronie IK przygotowań do zwiększenia liczby pracowników w sytuacjach kryzysowych. Można to osiągnąć przez włączenie rezerwy personelu do realizacji planów obrony cywilnej.

Odporność społeczna ma również wymiar osobisty. Jeśli obywatele są w stanie wytrzymać okresy ograniczonej dostępności pewnych towarów lub usług, zarządzanie kryzysowe jest łatwiejsze, nawet jeśli wiąże się z drastycznymi decyzjami, takimi jak tymczasowe zawieszenie dostaw energii elektrycznej na pewnym obszarze w celu zasilania najważniejszych miejsc i stref lub innych form reglamentowania. Rozmieszczenie ponad 13 000 punktów pomocy w Ukrainie jest przykładem wspierania odporności społecznej. Dlatego też zaleca się uwzględnienie jej w ochronie IK.

Z uwagi na liczbę ataków konwencjonalnych na ukraińską sieć energetyczną i zastosowaną broń konieczne jest rozważenie ochrony IK w wymiarze militarnym. Ryzyko rosyjskich ataków konwencjonalnych oznacza, że niektóre środki łagodzące są poza zasięgiem operatorów IK. Należy

opracować zintegrowany, wielowarstwowy system obrony powietrznej, zdolny do zapobiegania atakom rakietowym i dronom. Jest to odpowiedzialność państwa i jego sił zbrojnych. Taki system musi być w stanie wykorzystywać broń niskiej i wysokiej klasy, zdolną do przechwytywania małych dronów, a także pocisków manewrujących i balistycznych. Planowanie wojskowe musi obejmować również kwestie ochrony IK, takie jak liczba i lokalizacja elektrowni oraz innych elementów sieci energetycznej, a także systemów uznanych za krytyczne (np. porty, kluczowe węzły systemu kolejowego lub inne obiekty).

Bibliografia

Biriukov D., Kondratov S., Nasvit O., Sukhodolia O., *Green Paper on Critical Infrastructure Protection in Ukraine. Analytical Report*, Kiev 2015.

Butowski P., *Russian Air Power*, 2023.

Depczyński M., Elak L., *Rosyjska sztuka operacyjna w zarysie*, Warszawa 2020.

Douhet G., *Panowanie w powietrzu. Przypuszczalne formy przyszłej wojny oraz ostatnie artykuły*, Warszawa 2013.

Glajzer M., *Irański oręż w rosyjskiej służbie*, „Nowa Technika Wojskowa" 2022, nr 11, s. 12–15.

Kofman M., *Russian airpower in context: The first year of war*, w: *The Air War in Ukraine – The First Year of Conflict*, D. Henriksen, J. Bronk (red.), New York 2025.

Kwasek T., *Lotnicze pociski skrzydlate rodziny Ch-59*, „Lotnictwo" 2024, nr 3.

Kwasek T., *Rakiety Putina. Rosyjskie lądowe, lotnicze i morskie systemy rakietowe oraz pociski manewrujące*, „Nowa Technika Wojskowa" 2023, numer specjalny: *Wojna rosyjsko-ukraińska*, s. 40–55.

Russia and Eurasia, „The Military Balance" 2022, t. 122, nr 1, s. 164–217. https://doi.org/10.1080/04597222.2022.2022930.

Strembski M., *Wojna powietrzna nad Ukrainą – grudzień 2023 r.*, „Lotnictwo" 2024, nr 1, s. 32–39.

Strembski M., *Wojna powietrzna nad Ukrainą – listopad 2024 r.*, „Lotnictwo" 2025, nr 1, s. 28–40.

Strembski M., *Wojna powietrzna nad Ukrainą – styczeń 2024 r.*, „Lotnictwo" 2024, nr 2, s. 14–20.

Strembski M., *Wojna powietrzna nad Ukrainą. Czerwiec 2024 r.*, „Lotnictwo" 2024, nr 7–8, s. 30–42.

Strembski M., *Wojna powietrzna nad Ukrainą. Maj 2024 r.*, „Lotnictwo" 2024, nr 6, s. 42–51.

Strembski M., *Wojna powietrzna nad Ukrainą. Sierpień 2024 r.*, „Lotnictwo" 2024, nr 10, s. 40–49.

Strembski M., *Wojna powietrzna nad Ukrainą. Wrzesień 2024 r.*, „Lotnictwo" 2024, nr 11, s. 21–35.

Źródła internetowe

Altman H., *Dam Destroyed, Accusations Fly, Waters Rise, War Plans Could Change*, The War Zone, 6.06.2023, https://www.twz.com/dam-destroyed-accusations-fly-waters-rise-war-plans-could-change [dostęp: 18.01.2025].

Axe D., *Ukrainian Helicopter Crews Are Shooting Down Russian Drones – Like World War II Turret Gunners*, Forbes, 22.08.2024, https://www.forbes.com/sites/davidaxe/2024/08/22/ukrainian-helicopter-crews-are-shooting-down-russian-drones-like-world-war-ii-turret-gunners/ [dostęp: 14.02.2025].

Chambers J., *Countering Gray-Zone Hybrid Threats. An Analysis of Russia's 'New Generation Warfare' and Implications for the US Army*, 2016, https://mwi.westpoint.edu/wp-content/uploads/2016/10/Countering-Gray-Zone-Hybrid-Threats.pdf [dostęp: 15.01.2025].

Cyber-Attack Against Ukrainian Critical Infrastructure, CISA, 20.07.2021, https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 [dostęp: 15.01.2025].

Explosion in Ukraine's Odessa Destroys Railroad Bridge but Misses Train, The Moscow Times, 13.05.2015, https://www.themoscowtimes.com/2015/05/13/explosion-in-ukraines-odessa-destroys-railroad-bridge-but-misses-train-a46507 [dostęp: 16.01.2025].

Giannopoulos G., Smith H., Theocharidou M., *The Landscape of Hybrid Threats: A Conceptual Model Public Version*, Publications Office of the European Union, Luxembourg 2021, https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf [dostęp: 15.01.2025].

Greenberg A., *How an Entire Nation Became Russia's Test Lab for Cyberwar*, Wired, 20.06.2017, https://www.wired.com/story/russian-hackers-attack-ukraine/ [dostęp: 18.01.2025].

Greenberg A., *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, Wired, 22.08.2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [dostęp: 16.01.2025].

Harding L., Sabbagh D., Koshiw I., *Russia targets Ukraine energy and water infrastructure in missile attacks*, The Guardian, 31.10.2022, https://www.theguardian.com/world/2022/oct/31/russian-missiles-kyiv-ukraine-cities [dostęp: 5.02.2025].

Humpreys B.E., *Attacks on Ukraine's Electric Grid: Insights for U.S. Infrastructure Security and Resilience*, Congressional Research Service, 17.05.2024, https://crsreports.congress.gov/product/pdf/R/R48067 [dostęp: 8.02.2025].

Kh-55 (AS-15), Missile Threat, 23.04.2024, https://missilethreat.csis.org/missile/kh-55/ [dostęp: 12.02.2025].

Kh-47M2 Kinzhal, Missile Threat, 23.04.2024, https://missilethreat.csis.org/missile/kinzhal/ [dostęp: 12.02.2025].

Kh-101 / Kh-102, Missile Threat, 23.04.2024, https://missilethreat.csis.org/missile/kh-101-kh-102/ [dostęp: 12.02.2025].

Kofman M., Fink A., Gorenburg D., Chesnut M., Edmonds J., Waller J., *Russian Military Strategy: Core Tenets and Operational Concepts*, sierpień 2021, https://www.cna.org/reports/2021/08/Russian-Military-Strategy-Core-Tenets-and-Operational-Concepts.pdf [dostęp: 3.02.2025].

Major Ukraine gas pipeline hit by blast, BBC, 17.06.2014, https://www.bbc.com/news/world-europe-27891018 [dostęp: 16.01.2025].

Matuszak S., *Rosja destabilizuje system energetyczny Ukrainy*, Ośrodek Studiów Wschodnich, 11.10.2022, https://www.osw.waw.pl/pl/publikacje/analizy/2022-10-11/rosja-destabilizuje-system-energetyczny-ukrainy [dostęp: 5.02.2025].

Matuszak S., *Ukraina: poważny cios w energetykę*, Ośrodek Studiów Wschodnich, 28.03.2024, https://www.osw.waw.pl/pl/publikacje/analizy/2024-03-28/ukraina-powazny-cios-w-energetyke [dostęp: 5.02.2025].

Mendel J., *In Ukraine a Huge Ammunition Depot Catches Fire*, The New York Times, 27.09.2017, https://www.nytimes.com/2017/09/27/world/europe/ukraine-ammunition-depot-explosion.html?mcubz=0 [dostęp: 16.01.2025].

Miller M.E., Galouchka A., *Ukraine's drone hunters scramble to destroy Russia's Iranian–built fleet*, The Washington Post, 28.11.2022, https://www.washingtonpost.com/world/2022/11/28/ukraine-drone-hunters-mykolaiv-russia/ [dostęp: 13.02.2025].

Newdick T., *Ukraine Accuses Russia Of Blowing Up Another Dam*, The War Zone, 12.06.2023, https://www.twz.com/ukraine-accuses-russia-of-blowing-up-another-dam [dostęp: 18.01.2025].

Newdick T., *Ukraine's SA-8 Gecko 'FrankenSAM' Adapted To Fire Air-To-Air Missiles Seen In New Detail*, The War Zone, 12.12.2024, https://www.twz.com/land/ukraines-sa-8-gecko-frankensam-adapted-to-fire-air-to-air-missiles-seen-in-new-detail [dostęp: 14.02.2025].

Perlroth N., Scott M., Frenkel S., *Cyberattack Hits Ukraine Then Spreads Internationally*, The New York Times, 27.06.2017, https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html [dostęp: 16.01.2025].

There are almost 13 thousand Invincibility Points in Ukraine, UNN, 3.04.2024, https://unn.ua/en/news/there-are-almost-13-thousand-invincibility-points-in-ukraine [dostęp: 13.02.2025].

3M-14 Kalibr (SS-N-30A), Missile Threat, 23.04.2024, https://missilethreat.csis.org/missile/ss-n-30a/ [dostęp: 12.02.2025].

Trevithick J., *'FrankenSAM' Systems Are Now Shooting Down Drones In Ukraine*, The War Zone, 17.01.2024, https://www.twz.com/frankensam-systems-are-now-shooting-down-drones-in-ukraine [dostęp: 14.02.2025].

Trevithick J., *Containerized SAM System That Fires Soviet Air-To-Air Missiles For Ukraine Breaks Cover*, The War Zone, 12.02.2025, https://www.twz.com/land/containerized-sam-system-that-fires-soviet-air-to-air-missiles-for-ukraine-breaks-cover [dostęp: 14.02.2025].

Ukraine ammo dump blasts blamed on 'possible sabotage', BBC, 9.10.2018, https://www.bbc.co.uk/news/world-europe-45794963 [dostęp: 16.01.2025].

Ukraine power cut 'was cyber-attack', BBC News, 11.01.2017, https://www.bbc.co.uk/news/technology-38573074 [dostęp: 15.01.2025].

Ukraine's Energy Security and the Coming Winter, IEA, wrzesień 2024, https://iea.blob.core.windows.net/assets/cec49dc2-7d04-442f-92aa-54c18e6f51d6/UkrainesEnergySecurityandtheComingWinter.pdf [dostęp: 9.02.2025].

Warden III J.A., *The Enemy as System*, „Airpower Journal" 1995, t. 9, nr 1, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-09_Issue-1-Se/1995_Vol9_No1.pdf, s. 41–55 [dostęp: 1.02.2025].

Watling J., Reynolds N., *Operation Z. The Death Throes of an Imperial Delusion*, 22.04.2022, https://static.rusi.org/special-report-202204-operation-z-web.pdf [dostęp: 18.01.2025].

Watling J., Reynolds N., *The Plot to Destroy Ukraine*, 15.02.2022, https://static.rusi.org/special-report-202202-ukraine-web.pdf [dostęp: 17.01.2025].

Wilk A., Żochowski P., *Dziesiąty zmasowany ostrzał Ukrainy. 309. dzień wojny*, Ośrodek Studiów Wschodnich, 30.12.2022, https://www.osw.waw.pl/pl/publikacje/analizy/2022-12-30/dziesiaty-zmasowany-ostrzal-ukrainy-309-dzien-wojny [dostęp: 5.02.2025].

Wilk A., Żochowski P., *Ukraina bez prądu. 265. dzień wojny*, Ośrodek Studiów Wschodnich, 16.11.2022, https://www.osw.waw.pl/pl/publikacje/analizy/2022-11-16/ukraina-bez-pradu-265-dzien-wojny [dostęp: 5.02.2025].

Zaniewicz M., *Ukraine in Darkness: Preventing the Worst-Case Scenario for Its Energy System*, Forum Energii, 1.07.2024, https://www.forum-energii.eu/en/ukraine-destroyed-system [dostęp: 7.02.2025].

Akty prawne

Закон України про критичну інфраструктуру (Відомості Верховної Ради України (ВВР), 2023, № 5, ст. 13) – [*Zakon Ukrajiny pro krytycznu infrastrukturu* (Widomosti Werchownoji Rady Ukrajiny (WWR), 2023, № 5, st. 13)], https://zakon.rada.gov.ua/laws/show/1882-20#Text [dostęp: 17.01.2025].

Dr Michał Piekarski

Adiunkt w Zakładzie Studiów nad Bezpieczeństwem Instytutu Studiów Międzynarodowych i Bezpieczeństwa Uniwersytetu Wrocławskiego. Zajmuje się analizą zjawiska wojny hybrydowej w Europie, współczesnego terroryzmu, problematyką bezpieczeństwa morskiego państwa oraz zagadnieniami z zakresu kultury strategicznej Polski. Uczestnik prac zespołów międzyresortowych oraz grup roboczych administracji państwowej, których zadaniem było budowanie odporności na zagrożenia terrorystyczne oraz hybrydowe obiektów strategicznych dla bezpieczeństwa państwa oraz infrastruktury krytycznej.

Kontakt: michal.piekarski@uwr.edu.pl

Terroryzm – studia, analizy, prewencja, 2025, wydanie specjalne: 137–165

https://doi.org/10.4467/27204383TER.25.005.21508

Artykuł

Zagrożenia hybrydowe infrastruktury krytycznej w Unii Europejskiej. Wybrane analizy Hybrid CoE

Hybrid threats to critical infrastructure in the European Union. Selected Hybrid CoE analyses

ALEKSANDER OLECH

https://orcid.org/0000-0002-3793-5913

Defence24

Abstrakt

Autor artykułu opisuje rozwój zagrożeń hybrydowych, zwłaszcza w Europie Środkowo-Wschodniej. Koncentruje się na operacjach wpływu prowadzonych przez Rosję. Na podstawie analizy 6 najważniejszych publikacji Europejskiego Centrum Doskonalenia ds. Przeciwdziałania Zagrożeniom Hybrydowym (European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE) autor identyfikuje taktyki hybrydowe – od dezinformacji i cyberataków po zagrożenia morskie i kinetyczne. Analizowane badania obejmują kwestie strategicznej rywalizacji, budowania odporności oraz ram prawnych niezbędnych do przeciwdziałania wyzwaniom związanym z tymi taktykami. Wyniki tych badań podkreślają konieczność ciągłej adaptacji do pojawiających się wyzwań, intensyfikacji współpracy międzynarodowej oraz proaktywnych działań mających na celu ograniczenie wpływu operacji hybrydowych na państwa Zachodu. Zrozumienie ewolucji zagrożeń hybrydowych jest ważne dla wzmocnienia bezpieczeństwa narodowego, zwiększenia odporności oraz opracowania skutecznych strategii przeciwdziałania im.

Słowa kluczowe

Rosja, infrastruktura krytyczna, zagrożenia hybrydowe, terroryzm, Finlandia, Morze Bałtyckie

Abstract

The author of the article describes the progression of hybrid threats, particularly in Central and Eastern Europe, with a focus on Russian influence operations. By examining 6 key publications from the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), the author identifies hybrid tactics, from disinformation and cyberattacks to maritime and kinetic threats. The research explores strategic competition, resilience-building, and legal frameworks necessary to counter challenges of these tactics. The findings highlight the need for continuous adaptation to emerging challenges, increased international cooperation, and proactive measures to mitigate the impact of hybrid operations on Western states. Understanding the evolution of these threats is important for strengthening national security, improving resilience, and developing effective counterstrategies.

Keywords

Russia, critical infrastructure, hybrid threats, terrorism, Finland, Baltic Sea

Wprowadzenie

Zagrożenia hybrydowe i ich ewolucja nabierają coraz większego znaczenia dla globalnego bezpieczeństwa. Nie są to już tylko negatywne działania, które można sklasyfikować jako rywalizację w Europie między państwami członkowskimi Unii Europejskiej i NATO a Federacją Rosyjską (FR). Dziś zagrożenia hybrydowe są widoczne w skali globalnej, a imperialna polityka Kremla zwiększa ich zasięg i udoskonala narzędzia wykorzystywane do wywierania wpływu, a także uwzględnia szkodliwe działania innych podmiotów, takich jak Korea Północna i Iran.

Europejskie Centrum Doskonalenia ds. Przeciwdziałania Zagrożeniom Hybrydowym (European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE) definiuje zagrożenia hybrydowe jako działania prowadzone przez podmioty państwowe lub niepaństwowe, które przez

połączenie jawnych i niejawnych środków wojskowych i niewojskowych mają osłabić cel lub zaszkodzić mu. W tych działaniach są wykorzystywane progi wykrywalności i atrybucji, a także granica między wojną a pokojem, aby wpływać na procesy decyzyjne na różnych poziomach – lokalnym, regionalnym, państwowym lub instytucjonalnym – w celu osiągnięcia strategicznych celów podmiotu atakującego i jednoczesnego zaszkodzenia podmiotowi zaatakowanemu.

Celem działań hybrydowych jest wpływanie na różne procesy decyzyjne na poziomie regionalnym, krajowym lub instytucjonalnym, aby promować i/lub osiągać własne cele strategiczne, przy jednoczesnym zdyskredytowaniu przeciwnika, którym dla Rosji obecnie są głównie państwa zachodnie.

Pozornie łagodne działania mogą być częścią operacji hybrydowej, która zgodnie z planem sprawcy powinna pozostać ukryta lub zmniejszyć zdolność ofiary do powiązania tej operacji z jej inicjatorem. Utrudnia to reakcję, ponieważ takie aktywności – widoczne w przypadku krajów wzdłuż wschodniej granicy NATO i UE – odbywają się poniżej progu wojny lub są w nie zaangażowane podmioty, które trudno zweryfikować. Pomimo przypisywania niektórych działań Rosji, Iranowi lub Chinom reakcje państw zachodnich pozostają ograniczone.

Niektóre podmioty państwowe i niepaństwowe chętnie wykorzystują luki w prawie międzynarodowym, aby skomplikować zbiorową obronę państw zachodnich przed zagrożeniami hybrydowymi. Stanowi to ich największą przewagę. Istotną przeszkodą dla narodów przestrzegających prawa międzynarodowego jest wydłużony proces konsultacji i podejmowania decyzji o właściwej odpowiedzi, który wymaga zaangażowania podmiotów takich jak ONZ, UE, NATO. W tym okresie antagonista może prowadzić działania hybrydowe. Jest to również widoczne w tworzeniu narzędzi do minimalizowania zagrożeń, ponieważ dla państw przestrzegających prawa proces ten jest znacznie wydłużony.

Wszystkie kraje Europy Środkowo-Wschodniej są narażone na zagrożenia hybrydowe, które – o ile pozostają poniżej progu wojny – mogą przybrać dowolną formę ataku. Wciąż płynna pozostaje jednak granica określająca, kiedy konflikt faktycznie się rozpoczyna czy też kiedy zaatakowane państwo (lub podmiot) może zareagować.

Od 2014 r. stale rośnie częstotliwość ataków hybrydowych przeprowadzanych przez FR. Są one realizowane przez personel wojskowy, agencje wywiadowcze, dziennikarzy i polityków, a także osoby, które są albo

nieświadome swojego wsparcia dla rosyjskiej aktywności, albo są zwerbowanymi agentami działającymi w interesie Rosji dla korzyści finansowych, zawodowych lub politycznych czy też z powodu przekonań osobistych. W rezultacie zagrożenia hybrydowe można zaobserwować nie tylko w sferze wojny, perspektywie przestrzegania prawa międzynarodowego, lecz także w cyberbezpieczeństwie, informacji (dezinformacja), polityce, ekonomii, kulturze, religii i społeczeństwie. Dodatkowo takie zagrożenia obejmują działania kinetyczne, takie jak incydenty morskie i powietrzne (np. naruszenie przestrzeni powietrznej). Rosja szuka wszelkich sposobów, aby negatywnie wpłynąć na wybranych przeciwników.

Niniejsza analiza opiera się na 6 publikacjach naukowych Hybrid CoE:

1. *The Landscape of Hybrid Threats: A Conceptual Model*[1] – przedstawia ewolucję zagrożeń hybrydowych, działania Rosji, Chin i podmiotów niepaństwowych, a także obszary, w których są przeprowadzane ataki hybrydowe.
2. *The concept of hybrid war in Russia: A national security threat and means of strategic coercion*[2] – koncentruje się przede wszystkim na zagrożeniach dla samej Rosji, co z kolei służy jej jako uzasadnienie dla opracowywania strategii ochrony własnych interesów i tworzenia strategicznej rywalizacji z państwami zachodnimi w określonych obszarach.
3. *Handbook on maritime hybrid threats: 15 scenarios and legal scans*[3] – analizuje szeroki wachlarz zagrożeń hybrydowych, zwłaszcza tych związanych z działaniami w sferze morskiej. Jest to szczególnie istotne w kontekście obecnych wyzwań w regionie Morza Bałtyckiego.

[1] G. Giannopoulos, H. Smith, M. Theocharidou, *The Landscape of Hybrid Threats: A Conceptual Model Public Version*, Publications Office of the European Union, Luxembourg 2021, https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf [dostęp: 2.01.2025].

[2] K. Pynnöniemi, *The concept of hybrid war in Russia: A national security threat and means of strategic coercion*, Hybrid CoE Strategic Analysis / 27, maj 2021, https://www.hybridcoe.fi/wp-content/uploads/2021/05/20210518_Hybrid_CoE_Strategic_Analysis_27_The_concept_of_hybrid_war_in_Russia_WEB.pdf [dostęp: 10.01.2025].

[3] *Hybrid CoE Paper 16: Handbook on maritime hybrid threats: 15 scenarios and legal scans*, marzec 2023, https://www.hybridcoe.fi/wp-content/uploads/2023/03/NEW_web_Hybrid_CoE_Paper-16_rgb.pdf [dostęp: 17.01.2025].

4. *A comprehensive resilience ecosystem*[4] – uwzględnia rosnącą złożoność ataków, w tym zagrożeń hybrydowych, zdolność do odbudowy i regeneracji infrastruktury; jest istotna dla zrozumienia odporności – filaru bezpieczeństwa narodowego i międzynarodowego.
5. *Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage*[5] – stanowi modelowy przykład tego, że FR traktuje ataki hybrydowe jako narzędzie destabilizacji w swojej bliskiej zagranicy. Jest to publikacja szczególnie cenna dla rządów i organizacji międzynarodowych stosujących środki zaradcze.
6. *Protecting maritime infrastructure from hybrid threats: legal options*[6] – analizuje zagrożenia hybrydowe dla infrastruktury morskiej, podkreśla luki prawne i wyzwania w zakresie bezpieczeństwa. Wzywa do ściślejszej współpracy międzynarodowej i reform prawnych w celu ochrony krytycznych zasobów podmorskich.

Omawiane badania są ważne dla zrozumienia koncepcji operacji hybrydowych prowadzonych przeciwko szeroko rozumianym państwom zachodnim. Analiza badań pokazuje, w jaki sposób forma i zakres zagrożeń hybrydowych zmieniły się na przestrzeni lat, a także jakie główne wyzwania stoją przed państwami NATO i UE w zakresie reagowania na te zagrożenia. Szczególną uwagę poświęcono działaniom prowadzonym przez FR.

Autor wyodrębnił istotne elementy z każdej publikacji, aby nakreślić mapę analizowanych zagrożeń hybrydowych, podkreślił także ich ewolucję w ostatnich latach. Wskazał, że niektóre z nich pojawią się w przyszłości w różnych formach i lokalizacjach, a obecne działania atakujących (np. uszkodzenia infrastruktury krytycznej, IK) stanowią podstawę do kolejnych ataków.

Analiza empiryczna i przegląd tych dokumentów są istotne dla rozwoju badań nad zagrożeniami hybrydowymi. Przeprowadzane są jednak kolejne badania polegające na analizowaniu z różnych perspektyw

[4] R. Jungwirth i in., *Hybrid threats: a comprehensive resilience ecosystem*, Publications Office of the European Union, Luxembourg 2023, https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE_comprehensive_resilience_ecosystem.pdf [dostęp: 22.01.2025].

[5] H. Praks, *Hybrid CoE Working Paper 32: Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage*, maj 2024, https://www.hybridcoe.fi/wp-content/uploads/2024/05/20240530-Hybrid-CoE-Working-Paper-32-Russias-hybrid-threat-tactics-WEB.pdf [dostęp: 30.01.2025].

[6] A. Sari, *Hybrid CoE Research Report 14: Protecting maritime infrastructure from hybrid threats: legal options*, marzec 2025, https://www.hybridcoe.fi/wp-content/uploads/2025/03/20250306-Hybrid-CoE-Research-Report-14-web.pdf [dostęp: 6.03.2025].

pojawiających się zagrożeń bezpieczeństwa. W związku z tym należy kontynuować dialog na temat zagrożeń hybrydowych, aby wyjaśnić to zjawisko, zwiększyć świadomość społeczną, wzmocnić odporność oraz sformułować najlepsze praktyki i odpowiedzi, zarówno w celu skutecznego reagowania na zagrożenia, jak i zapobiegania im.

Kompleksowy ekosystem odporności

Odporność definiuje się jako zdolność systemu – osobowego, społecznego lub instytucjonalnego – do wytrzymywania zakłóceń, odbudowy po ich wystąpieniu oraz adaptacyjnej zmiany w ich następstwie. Badania akademickie zmieniły z czasem postrzeganie odporności jako czegoś stałego na postrzeganie jej jako dynamicznego procesu, w którym adaptacja i transformacja są dosyć ważne[7]. Odporność staje się filarem bezpieczeństwa narodowego, biorąc pod uwagę rosnącą złożoność ataków, w tym zagrożeń hybrydowych, oraz potrzebę odbudowy i naprawy infrastruktury.

Odporność jest definiowana w zależności od punktów widzenia osób z danego kręgu kulturowego, które wpływają na rozwój i realizację polityk. Na przykład w Rosji odporność jest zwykle łączona z wytrzymałością i stabilnością. Podczas gdy w wielu krajach arabskich odporność kształtują wydarzenia geopolityczne, w Chinach kładzie się nacisk na adaptację[8].

W pierwszej dekadzie XXI w. priorytetami UE były zarządzanie kryzysowe oraz ochrona IK. Formalnie pojęcie odporności zostało włączone do procesu kształtowania unijnej polityki dopiero w 2017 r. za sprawą dokumentu *Wspólna wizja, wspólne działanie: Silniejsza Europa. Globalna strategia na rzecz polityki zagranicznej i bezpieczeństwa Unii Europejskiej*. Komisja Europejska w 2016 r. po raz pierwszy przedstawiła dokument *Wspólny komunikat do Parlamentu Europejskiego i Rady. Wspólne ramy przeciwdziałania zagrożeniom hybrydowym – odpowiedź Unii Europejskiej*. Wymieniono w nim 22 działania mające na celu przeciwdziałanie zagrożeniom hybrydowym. Przyjęty przez Radę Europejską 25 maja 2022 r. *Strategiczny kompas bezpieczeństwa i obrony* jest obecnie koncepcją przewodnią strategii odporności UE[9].

[7] R. Jungwirth i in., *Hybrid threats: a comprehensive resilience ecosystem…*, s. 17.

[8] Tamże, s. 19.

[9] Tamże, s. 26.

Pandemia COVID-19 wpłynęła na strategię NATO. Sojusznicy pracowali nad przygotowaniem sektora opieki zdrowotnej. W 2020 r. NATO przeprowadziło rewizję 7 podstawowych wymogów (z ang. *Seven Baseline Requirements*, 7BLR) dotyczących gotowości cywilnej, aby uwzględnić wpływ pandemii. Podczas szczytu w Brukseli Sojusz postanowił wzmocnić swoją odporność przez (...) *współpracę z sektorem prywatnym i pozarządowym, z programami i centrami wiedzy specjalistycznej ustanowionymi przez członków Sojuszu, a także z naszymi społeczeństwami i populacjami, aby zwiększyć odporność naszych narodów i społeczeństw*[10].

Systemy demokratyczne, oprócz zaufania do społeczeństwa, rządu i instytucji państwowych, opierają się na 7 głównych filarach. Są to:

1) poczucie sprawiedliwości i równego traktowania, obejmujące wiarę w bezstronny system oraz ochronę własności i tożsamości;
2) prawa i wolności obywatelskie, takie jak wolność słowa i prawo do głosowania;
3) odpowiedzialność polityczna, wyrażająca się w wolnych i uczciwych wyborach oraz otwartej debacie publicznej;
4) rządy prawa, czyli równość wszystkich wobec przepisów i niezależność sądownictwa;
5) stabilność polityczna, społeczna i gospodarcza;
6) niezawodność i dostępność, rozumiane jako zagwarantowany dostęp do podstawowych dóbr i usług;
7) zdolność przewidywania, czyli umiejętność identyfikowania zagrożeń, rozwijania współpracy międzysektorowej i wdrażania innowacyjnych rozwiązań.

To właśnie te elementy stanowią fundament odporności i trwałości nowoczesnych demokracji[11].

Podstawą kompleksowego ekosystemu odporności (ang. *A Comprehensive Resilience Ecosystem*, CORE) są 3 najważniejsze obszary: obywatelski (społeczeństwo i kultura), zarządzanie (administracja, procesy polityczne, dyplomacja) oraz usługi (infrastruktura, gospodarka). CORE może promować międzysektorowe wysiłki angażujące całe społeczeństwo przez przedstawienie najważniejszych wzajemnych powiązań. Zapewnia metodologię, która umożliwia lepsze zrozumienie interakcji między systemami, instytucjami i czynnikami społecznymi. Pozwala na prezentację incydentów

[10] Tamże, s. 29. Tłumaczenia w artykule pochodzą od redakcji (dop. red.).

[11] Tamże, s. 33.

i ich konsekwencji, służy jako mechanizm zwiększania odporności na zagrożenia hybrydowe i wzmacniania społeczeństw demokratycznych. Skupienie na zagrożeniach hybrydowych, ukierunkowanych na eksploatację systemowych słabości w różnych skalach – lokalnej, krajowej i międzynarodowej – może stanowić ważny bodziec do dalszego rozwoju i rozszerzania zdolności w obszarze budowania odporności. Wsparcie ze strony decydentów politycznych jest niezbędne do wprowadzenia odpowiednich przepisów i podniesienia świadomości społecznej na temat potencjalnych konsekwencji ataków hybrydowych.

Ponadto niezbędny jest ciągły rozwój technologii wykrywania zagrożeń hybrydowych, ostrzegania przed nimi, przeciwdziałania im i łagodzenia ich w celu zwiększania odporności[12].

Krajobraz zagrożeń hybrydowych

Państwa i regiony w odmienny sposób postrzegają nie tylko bezpieczeństwo, lecz także stale ewoluujące zagrożenia hybrydowe[13]. Są one, wraz z działaniami hybrydowymi, rozumiane jako połączenie działań regularnych i nieregularnych (tj. o różnej intensywności i częstotliwości), podejmowanych zarówno przez siły zbrojne, jak i przestępców, terrorystów, a nawet organizacje polityczne[14]. Zróżnicowany charakter zagrożeń wskazuje na potrzebę weryfikacji zdolności państw do reagowania na tego typu niebezpieczeństwa. Wiąże się to przede wszystkim z działaniami rządów, skutecznością systemów obrony oraz współpracą międzynarodową w zakresie bezpieczeństwa. W tym przypadku istotne jest spojrzenie na obecną sytuację w Ukrainie, na Bałkanach, w Syrii, Libii czy Afryce Środkowej przez pryzmat wyzwań zarówno militarnych, jak i niemilitarnych.

Działania hybrydowe są prowadzone głównie przez aktorów o autorytarnych lub totalitarnych poglądach na władzę, których celem jest skierowanie wszystkich możliwych (autorytarnych) narzędzi przeciwko

[12] Tamże, s. 78.

[13] G. Giannopoulos, H. Smith, M. Theocharidou, *The Landscape of Hybrid Threats: A Conceptual Model…*, s. 9.

[14] A. Olech, *Cooperation between NATO and the European Union against hybrid threats with a particular emphasis on terrorism*, Institute of New Europe, 17.03.2021, https://ine.org.pl/en/cooperation-between-nato-and-the-european-union-against-hybrid-threats-with-a-particular-emphasis-on-terrorism/ [dostęp: 10.02.2025].

systemom demokratycznym[15]. W rezultacie rządy o takim charakterze często trwają przez dziesięciolecia i z czasem są coraz bardziej ugruntowane. Co ważne, jednego autorytarnego przywódcę zastępuje inny.

Podmioty państwowe podejmujące się działań hybrydowych to głównie państwa autorytarne lub totalitarne. Ich wewnętrzna strategia utrzymania władzy jest uważana za identyczną ze strategią wojny hybrydowej, w kontekście której państwa demokratyczne są postrzegane jako egzystencjalne zagrożenie dla tych reżimów. Dlatego też te reżimy próbują podważyć i osłabić zdolności państw demokratycznych. Bardzo ważną rolę odgrywa informacja – jest narzędziem, które umożliwia manipulowanie przekonaniami społecznymi i zniechęca do zbiorowych działań przeciwko reżimowi[16].

Rozwój mediów, w tym mediów społecznościowych, stworzył nowe możliwości prowadzenia działań dezinformacyjnych i propagandowych. Teraz każdy może być nadawcą i publikować z dowolnego miejsca; dostępne są nowe platformy, będące poza kontrolą państwa; pojawiły się nowe możliwości zniekształcania treści; przyspieszyła globalizacja mediów; rozwinęły się nowe modele biznesowe, a struktura gospodarcza opiera się na danych[17]. Dezinformacja z krajów autorytarnych jest znacznie częstsza i silniejsza pod względem zakresu rozpowszechnianych informacji. Wynika to z faktu, że kraje demokratyczne mają wdrożone procesy regulacyjne i weryfikacyjne[18]. Należy zauważyć, że obalanie fałszywych informacji jest trudniejsze niż ich publikowanie.

W przeszłości za zagrożenie hybrydowe było uważane promowanie demokracji, np. wysiłki organizacji pozarządowych podejmowane w tym celu w krajach niedemokratycznych. Gdy władze w tych państwach zaczynają zdawać sobie sprawę z tej działalności, reagują i wprowadzają przepisy dotyczące podmiotów zagranicznych lub zakazują działalności organizacji pozarządowych (ang. *non-governmental organisations*) i think tanków. Obecnie zagrożenie hybrydowe należy zdefiniować jako formę niejawnego użycia siły z możliwością zastosowania korupcji lub zmuszenia kogoś (np. szantażem). W odniesieniu np. do działań organizacji pozarządowych

[15] G. Giannopoulos, H. Smith, M. Theocharidou, *The Landscape of Hybrid Threats: A Conceptual Model...*, s. 15.

[16] Tamże, s. 16.

[17] Tamże, s. 17.

[18] Tamże, s. 18.

mających na celu promowanie demokracji[19] sugerowano również, że za zagrożenia hybrydowe można uznać miękką siłę (ang. *soft power*) i dyplomację publiczną.

Należy zauważyć, że koszty prowadzenia nieregularnych ataków określanych jako działania hybrydowe są znacznie niższe niż w przypadku tradycyjnej wojny. Ponadto atakujący nie jest, przynajmniej nie do końca, narażony na zdecydowaną reakcję społeczności międzynarodowej. Konflikt hybrydowy w Ukrainie to część ewolucji, do której dochodzi w krajach postsowieckich (tak jak dzieje się to obecnie np. w Białorusi). Jest to kryzys wielowymiarowy, składają się na niego działania podmiotów krajowych i ponadnarodowych realizujących swoje interesy polityczne i gospodarcze za pomocą dostępnego wachlarza metod – od konwencjonalnego użycia sił zbrojnych po rozpowszechnianie fake newsów. Dopuszczenie do rozwoju separatystycznych enklaw, takich jak te w Mołdawii, Gruzji i Azerbejdżanie, jest poważnym problemem i wymaga od tych krajów współpracy z państwami członkowskimi NATO i UE oraz stworzenia wspólnej sfery bezpieczeństwa.

Rosja

W Rosji obowiązuje strategia samoregulacji. Oznacza to, że dzięki zakorzenionym wartościom obywatele, a także firmy i inne podmioty niepaństwowe działają bez uprzedniej koordynacji z władzami, wdrażają rozwiązania zgodne z koncepcjami politycznymi proponowanymi przez Moskwę. Takie podejście ułatwia zdecentralizowaną realizację celów strategicznych i pozwala na elastyczność działań. Rosyjskość służy jako element jednoczący, łączący wszystkich Rosjan, aby chronić narodowe interesy strategiczne swojego kraju i realizować cele wyznaczone przez najwyższe kierownictwo – co ma decydujące znaczenie dla mobilizacji społeczeństwa[20].

Zarządzanie refleksyjne jest podstawową koncepcją w rosyjskiej teorii strategicznej, podkreślającą rolę psychologicznej manipulacji przeciwnikami. Celem jest stworzenie okoliczności, w których przeciwnicy dokonują wyborów zbieżnych z planami strategicznymi Rosji, a jednocześnie postrzegają siebie jako działających wbrew interesom Moskwy[21].

[19] Tamże.

[20] Tamże, s. 19.

[21] Tamże, s. 19–20.

Chiny

Chiny opierają swoje próby uzyskania statusu wielkiego mocarstwa na teorii Heartlandu[22] Halforda Mackindera. Aby to osiągnąć, dążą do uzyskania statusu potęgi morskiej[23]. W swoich działaniach kierują się koncepcją sztuki skutecznego oszukiwania wroga autorstwa Sun Zi oraz, w idealnej sytuacji, wygrywania wojny bez konieczności uciekania się do broni[24]. Strategiczne zachowanie chińskich sił zbrojnych determinują 3 czynniki: myślenie strategiczne, środowisko strategiczne i potencjał wojskowy. Ta triada kształtuje kompleksowe planowanie i realizację strategii w odpowiedzi na zagrożenia hybrydowe[25].

Tradycyjna chińska strategia opiera się na myśleniu dialektycznym, które uwzględnia dynamiczne przeciwieństwa, takie jak „słabość" i „siła". Te koncepcje są płynne i elastyczne – funkcjonują zarówno jako abstrakcyjne idee, jak i praktyczne narzędzia w działaniach strategicznych[26]. Chińska koncepcja 3 wojen obejmuje wojnę psychologiczną (osiąganie celów przez wpływanie na psychikę, np. odstraszanie, przymus, oszustwo), wojnę z opinią publiczną (wpływanie na poparcie krajowe i międzynarodowe przez wykorzystanie selektywnych informacji dostarczanych za pośrednictwem różnych mediów, kształtowanie określonego systemu wartości w społeczeństwie) oraz wojnę prawną (działania podejmowane w celu uzyskania przewagi prawnej przez wykorzystanie lub modyfikację prawa krajowego i międzynarodowego, aby osiągnąć przewagę polityczną lub wojskową)[27].

Podmioty niepaństwowe

Państwem działającym za pośrednictwem podmiotu niepaństwowego jest np. Iran, który wykorzystuje Hezbollah. Kolejny przykład to Rosja i Grupa Wagnera. Można wskazać na takie podmioty, jak islamskie milicje w Afryce i na Bliskim Wschodzie, a także grupy terrorystyczne, np. IRA (ang. Irish Republican Army), ETA (bask. Euskadi Ta Askatasuna) czy Tamilskie Tygrysy.

[22] Heartland (czyli „rdzeń lądowy") to według Mackindera obszar Eurazji obejmujący tereny dzisiejszej Rosji i Azji Środkowej, które są mniej podatne na ataki z morza, trudne do zdobycia, ale kluczowe dla panowania nad kontynentem.

[23] G. Giannopoulos, H. Smith, M. Theocharidou, *The Landscape of Hybrid Threats: A Conceptual Model...*, s. 20.

[24] Tamże, s. 21.

[25] Tamże.

[26] Tamże.

[27] Tamże.

Obecnie rozwija się nowa grupa podmiotów niepaństwowych, a mianowicie prywatne grupy wojskowe (z ang. *private military companies*, PMC), które czasami są nazywane firmami ochroniarskimi. Należy do nich także Grupa Wagnera. Rośnie rola PMC w kreowaniu zagrożeń hybrydowych[28].

Niejawne działania państwowe ze strony agresora mają tę zaletę, że państwom stanowiącym cel utrudniają nie tylko wykrycie możliwości przeprowadzenia szkodliwych operacji i zapobieżenie im, lecz także przypisanie odpowiedzialności za te operacje obcemu państwu, np. w przypadku aneksji Krymu – Rosji i klubowi motocyklowemu Nocne Wilki (ros. Ночные Волки). Państwa będące agresorem mogą zaprzeczać i odrzucać oskarżenia, a swoje cele osiągać w tajemnicy, np. zyskiwać dostęp do krytycznych sektorów (m.in. rosyjska ingerencja w wybory prezydenckie w USA w 2016 r.)[29].

Organizacje przestępcze działające w państwach celach są coraz częściej wykorzystywane przez państwa agresorów. Na przykład udostępniają tym państwom istniejące sieci przemytu, dostarczają sfałszowanych dokumentów, dokonują przestępstw finansowych lub po prostu grożą strategicznym państwom, grupom lub jednostkom[30].

Rozumienie zagrożeń hybrydowych jako obecności organizacji przestępczych lub terrorystycznych jest istotne. Jednak tylko niewielka liczba tych podmiotów przeprowadziła operacje przeciwko państwom zachodnim, aby osiągnąć swoje cele. Jak dotąd stosują one przemoc lub groźby jej użycia, ale nie na taką skalę, która pozwalałaby je jednoznacznie zaklasyfikować jako zagrożenia hybrydowe[31].

Domeny zagrożeń hybrydowych

Wyróżnia się 13 domen, w których mogą występować zagrożenia hybrydowe: infrastruktura, gospodarka, wywiad, informacja, cyberprzestrzeń, dyplomacja, polityka, kultura, społeczeństwo, prawo, wojsko/obrona, przestrzeń kosmiczna i administracja[32]. W kontekście zagrożeń hybrydowych najistotniejsze są:

[28] Tamże, s. 23.

[29] Tamże, s. 23–24.

[30] Tamże, s. 24.

[31] Tamże.

[32] Tamże, s. 26.

1. Cyberprzestrzeń – jako nowe pole do stwarzania zagrożeń w postaci cyberprzestępczości, propagandy, szpiegostwa, terroryzmu, a nawet wojny. Mniejsze podmioty mają większe możliwości działania w cyberprzestrzeni niż w świecie rzeczywistym[33].
2. Przestrzeń kosmiczna – działania hybrydowe w tej przestrzeni budzą coraz większe obawy ze względu na fakt, że kilka krajów rozwija w niej swoje zdolności wojskowe. Może to mieć wpływ na inne domeny, np. wojskową, ponieważ sfera kosmiczna jest jej integralną częścią[34].
3. Społeczeństwo – domena społeczna jest zwykle polem do generowania i pogłębiania podziałów społeczno-kulturowych i ich wykorzystywania, co spowoduje wstrząsy społeczne niezbędne do kontynuowania działań związanych z zagrożeniami hybrydowymi i odnoszenia sukcesów[35].
4. Sfera prawna – odnosi się do zbioru regulacji prawnych, działań, procesów i instytucji. Państwa autorytarne mogą stosować kontrustawy, tworzyć je, aby osiągnąć swój cel lub wykorzystywać luki w prawie istniejącym w krajach demokratycznych. Na przykład poleganie na prawie do wolności słowa tworzy przestrzeń dla kampanii dezinformacyjnych[36].
5. Wywiad – państwo zazwyczaj wykorzystuje swoje zdolności wywiadowcze do wspierania działań związanych z zagrożeniami hybrydowymi lub może próbować wpływać na operacje wywiadowcze państwa celu[37].
6. Dyplomacja – zwłaszcza działania hybrydowe w tej sferze mają na celu tworzenie podziałów na poziomie krajowym lub międzynarodowym, wspieranie kampanii informacyjnych i ingerowanie w proces decyzyjny (sankcje dyplomatyczne, wykorzystywanie ambasad)[38]. Dyplomacja przenika się z polityką wewnętrzną, więc decydenci w państwie muszą tworzyć strategie dwupoziomowe. Dyplomacja jest również ściśle powiązana z gospodarką, sferą

[33] Tamże, s. 28.

[34] Tamże.

[35] Tamże, s. 30.

[36] Tamże.

[37] Tamże, s. 31.

[38] Tamże.

społeczną i prawną. Działania w sferze dyplomacji mogą mieć negatywny wpływ na gospodarkę państwa[39].

7. Informacja – jeśli będzie kontrolowana, celowo rozpowszechniana lub będzie inspirowała określone działania, to może stać się elementem wojny hybrydowej i wpływać na przeciwnika.

Od czasu aneksji Krymu przez Rosję w 2014 r. podjęto wiele inicjatyw mających na celu wzmocnienie odporności UE i NATO na zagrożenia hybrydowe. Wysiłki te muszą zostać dostrzeżone przez kraje członkowskie tych struktur, a tempo działań i ich intensywność – utrzymane. Ze względu na stale zmieniający się charakter zagrożeń hybrydowych wymagana jest nieustanna czujność. Niezbędne jest strategiczne podejście do zwalczania zagrożeń hybrydowych, które obejmowałoby nie tylko struktury międzynarodowe, lecz także krajowe, w tym całe społeczeństwa, ponieważ to one są głównymi ofiarami terroryzmu.

Z uwagi na szeroki zakres działań NATO i UE, współcześnie tworzona jest kompleksowa i wielopłaszczyznowa struktura, która umożliwi wielofazowe reagowanie na zagrożenia bezpieczeństwa. Usprawnienie dotychczas istniejących schematów reagowania na ataki hybrydowe, zarówno militarnych, politycznych, gospodarczych, jak i społecznych, pozwala na skuteczną interwencję i tworzy bardzo potrzebny obecnie aparat (ang. *geopolitical apparatus*). Reakcja jest niezbędna, aby sprostać pojawiającym się wyzwaniom związanym z zagrożeniami hybrydowymi.

Rosyjska koncepcja wojny hybrydowej

W toczącej się debacie w Rosji wojna hybrydowa jest określana jako połączenie działań wojskowych i niewojskowych mających na celu osiągnięcie celów politycznych[40]. Należy zauważyć, że wczesne wdrożenie wojny informacyjnej pozwala na osiągnięcie celów politycznych bez użycia sił zbrojnych[41]. Później konieczne jest jedynie utrzymanie autorytarnej władzy. Dlatego w 2014 r. działania wojskowe i niewojskowe zostały połączone i ujęte w ramy wojny hybrydowej z Rosją[42].

[39] Tamże, s. 32.

[40] K. Pynnöniemi, *The concept of hybrid war in Russia: A national security…*, s. 3.

[41] Tamże, s. 4.

[42] Tamże.

Ukraina nie ma już żadnych szans na odzyskanie ziem zajętych przez Rosję w 2014 r. Innymi słowy, operacje hybrydowe, w tym prowadzone w ramach późniejszej i pełnoskalowej inwazji w 2022 r., doprowadziły do całkowitego przejęcia tych terytoriów. Co więcej, znacznie wzmocniły zdolności FR do realizowania dalszych operacji hybrydowych w Ukrainie oraz w całej wschodniej flance UE i NATO.

W Rosji wojna hybrydowa jest traktowana jako próba podważenia jej suwerenności, odrębności cywilizacyjnej i statusu jednego z głównych światowych mocarstw. Strategię tę opisuje się jako kombinację działań destrukcyjnych i konstruktywnych mających na celu doprowadzenie do wewnętrznej dezorganizacji i dezorientacji w państwie przeciwnika. Działania destrukcyjne to te podejmowane przez Zachód w celu podzielenia rosyjskiego społeczeństwa, zniszczenia rosyjskiej kultury i tradycji. Działania konstruktywne z kolei są po prostu obroną Rosji przed tymi działaniami. W debacie prowadzonej przez rosyjskie środowiska naukowe jako głównego aktora stojącego za tymi wysiłkami wskazuje się Stany Zjednoczone. Z kolei w dokumentach państwowych nie tylko USA, lecz także UE są wymieniane jako ci, którzy prowokują napięcia w Eurazji, zwłaszcza w Ukrainie[43].

W 2003 r. generał Machmut Gariejew wyróżnił 3 kategorie zagrożeń dla Rosji:

1) zagrożenia suwerenności politycznej Rosji, a w rezultacie jej statusu wielkiego mocarstwa,
2) możliwość użycia broni nuklearnej przeciwko Rosji,
3) trzecia grupa zagrożeń jest wielopłaszczyznowa – obejmuje szybki rozwój technosfery wojskowej, a także naruszenie równowagi sił w pobliżu granic Rosji[44].

Podział ten jest nadal aktualny. Obecnie zbiega się to z utrzymującym się antagonizmem Rosji wobec państw NATO i UE, zwłaszcza w odniesieniu do sytuacji w Ukrainie. W 2013 r. Gariejew stwierdził, że na świecie doszło do znaczącej transformacji geopolitycznej, która zasadniczo zmieniła równowagę sił i charakter zagrożeń, co wymusiło nowe strategie i metody reagowania. Zaktualizowana typologia zagrożeń obejmuje tworzenie kontrolowanego chaosu w celu wzniecenia różnych form niepokojów w krajach przeciwnika, obalenie od wewnątrz niepożądanych struktur władzy

[43] Tamże.

[44] Tamże, s. 5.

oraz destabilizację spójności wewnętrznej państwa, czego przykładem są sytuacje w Libii i Syrii[45].

Po ataku na Krym Gariejew powiedział, że Rosja powinna być dumna ze swoich działań i poprawić wykorzystanie miękkiej siły wraz z narzędziami politycznymi, dyplomatycznymi i informacyjnymi – te elementy są niezbędne dla systemu strategicznego odstraszania[46]. Jednocześnie wojna hybrydowa jest definiowana jako strategiczne narzędzie przymusu[47].

W rosyjskiej terminologii wojskowej strategiczne odstraszanie obejmuje zbiór ofensywnych i defensywnych instrumentów – jądrowych, niejądrowych i niemilitarnych – które łącznie stanowią „kompleksową strategię powstrzymywania, odstraszania i przymusu"[48]. Rosja postrzega odstraszanie jako środek mający na celu uniknięcie konfliktu. W ramach tego środka stosuje zastraszanie. Moskwa straszy potencjalnymi reperkusjami (np. grozi rozmieszczeniem broni jądrowej, aby odwieść innych od wykorzystania jej przeciwko sobie). Połączenie militarnych i niemilitarnych strategii przymusu jest uważane za strategiczne zagrożenie dla Rosji[49].

Wojna hybrydowa jest definiowana jako rodzaj strategicznego przymusu niemilitarnego, który obejmuje sankcje gospodarcze, cyberataki i operacje informacyjne. Działania te mają na celu zmianę struktury władzy w Rosji, wywołanie niezgody na sąsiednich terytoriach i zakwestionowanie jej pozycji jako dominującej siły w wielobiegunowym świecie[50]. Federacja Rosyjska nie tylko więc określa zagrożenia hybrydowe dla siebie, lecz także w pełni wykorzystuje swoje zdolności do atakowania w ten sposób innych narodów we wszystkich domenach, w których identyfikuje zagrożenia. Robi to, zanim sama stanie się celem.

45 Tamże.

46 Tamże.

47 Tamże.

48 Tamże, s. 6.

49 Tamże.

50 Tamże.

Taktyka działań hybrydowych Rosji wobec państw regionu Morza Bałtyckiego

Modelowym przykładem działań FR w bliskiej zagranicy jest instrumentalizacja ataków hybrydowych jako narzędzia destabilizacji. Różnorodność narzędzi, jakimi dysponuje Rosja – od zagrożeń kinetycznych (takich jak sabotaż) po zagrożenia niekinetyczne (takie jak dezinformacja)[51] – zwiększa się z każdym rokiem, a rosyjskie służby wywiadowcze konsekwentnie intensyfikują swoje operacje, pozornie bez obawy o reperkusje czy środki zaradcze.

Wzrost agresywnych działań jest szczególnie zauważalny od lutego 2022 r. w krajach wschodniej flanki NATO, a mianowicie w Estonii, na Łotwie, Litwie, w Finlandii, Polsce i Szwecji. Celem jest osłabienie poparcia dla Ukrainy, wywołanie wewnętrznej niestabilności w tych krajach i zdestabilizowanie jedności struktur UE i NATO[52]. Z uwagi na nową administrację w Stanach Zjednoczonych oraz niepewną sytuację w Ukrainie kraje wschodniej flanki są prawdopodobnie celami dalszej destabilizacji.

Rosja jest zdeterminowana, aby działać poniżej progu otwartej wojny, ponieważ rozumie, że przedłużający się konflikt z NATO może zakończyć się porażką Moskwy i całkowitą restrukturyzacją rosyjskiego systemu politycznego. Długoterminowym celem Kremla jest reorganizacja europejskiej architektury bezpieczeństwa i rozszerzenie rosyjskich wpływów zarówno przez sprawowanie kontroli nad Europą Środkowo-Wschodnią, jak i pozyskiwanie sprzymierzeńców w krajach Europy Zachodniej[53].

Rosyjska dezinformacja opiera się na tworzeniu fałszywej narracji o nieuchronnej porażce Ukrainy, przedstawianiu rządów krajów UE i NATO jako zaniedbujących własnych obywateli na rzecz wspierania Ukrainy oraz na wykorzystywaniu mediów społecznościowych do manipulowania opinią publiczną i kształtowania nastrojów społecznych[54]. Liczba fałszywych wiadomości mających na celu zniechęcenie do wspierania Ukrainy i podsycanie wrogości wobec jej obywateli rośnie z dnia na dzień. Część społeczeństwa w krajach europejskich wierzy w antyukraińskie narracje. Służy to również Kremlowi do określenia, które grupy są najbardziej podatne na manipulację.

[51] H. Praks, *Hybrid CoE Working Paper 32: Russia's hybrid threat tactics against the Baltic Sea region...*, s. 5.

[52] Tamże, s. 6–7.

[53] Tamże, s. 7–8.

[54] Tamże, s. 9–10.

Jednym z największych atutów Rosji jest jej diaspora w krajach bałtyckich i Azji Środkowej, będąca pozostałością po Imperium Rosyjskim i ZSRR. Moskwa aktywnie wspiera organizacje prorosyjskie, finansuje inicjatywy promujące język rosyjski i zdecydowanie sprzeciwia się usuwaniu sowieckich pomników. Jako narzędzia polityczne wykorzystuje także różne instytucje, m.in. Kościół prawosławny[55]. Ponadto rosyjskie agencje wywiadowcze rekrutują nowych agentów.

Rosja stworzyła kompleksową sieć szpiegowską wzdłuż wschodniej flanki NATO, co było szczególnie widoczne podczas operacji w krajach bałtyckich, które rozpoczęły się pod koniec 2023 r. W styczniu 2024 r. estońska Służba Bezpieczeństwa Wewnętrznego (eston. Kaitsepolitseiamet, KAPO) zatrzymała rosyjskiego profesora nauk politycznych z Uniwersytetu w Tartu, który rzekomo przez ponad dekadę był zaangażowany w szpiegostwo[56]. W podobnym czasie KAPO odkryło grupę podejrzaną o współpracę z rosyjskim wywiadem w celu przeprowadzania aktów wandalizmu i ataków fizycznych w Estonii. Do kwietnia 2024 r. władze aresztowały 13 osób, niektóre z nich były wcześniej karane. Grupa z powodzeniem przeprowadziła kilka ataków, w tym uszkodziła prywatny samochód estońskiego ministra spraw wewnętrznych i zniszczyła pomniki związane z oporem kraju przeciwko Związkowi Radzieckiemu. Estońscy urzędnicy opisali te incydenty jako część strategii wojny hybrydowej[57].

Rosyjski wywiad polega również w dużej mierze na grupach hakerów atakujących IK oraz instytucje rządowe. W raporcie Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (European Union Agency for Cybersecurity, ENISA) z grudnia 2023 r. ujawniono, że połowa wszystkich ataków DDoS w tym roku związana była z wojną w Ukrainie[58]. Ujawnienie nastąpiło, gdy Stany Zjednoczone ogłosiły, że wstrzymują własne operacje cybernetyczne przeciwko Rosji[59].

Od lat Rosja, we współpracy z Białorusią, wykorzystuje migrację jako narzędzie wywierania presji i wpływu na sąsiednie kraje. Moskwa i Mińsk

[55] Tamże, s. 12–13.

[56] Tamże, s. 14.

[57] Tamże, s. 15.

[58] Tamże, s. 18.

[59] M. Untersinger, *Les Etats-Unis ordonnent une pause des cyberopérations contre la Russie, selon plusieurs médias*, Le Monde, 4.03.2025, https://www.lemonde.fr/pixels/article/2025/03/03/les-etats-unis-ordonnent-une-pause-des-operations-cyber-contre-la-russie_6575971_4408996.html [dostęp: 4.03.2025].

manipulują przez dezinformację przepływami migracyjnymi, wykorzystują ludzi z Bliskiego Wschodu, Afryki oraz Azji Środkowej do tworzenia kontrolowanej presji migracyjnej. Zmusza to kraje NATO do wzmocnienia swojej infrastruktury bezpieczeństwa i zintensyfikowania dyskusji na temat aktualizacji przepisów prawnych. Presja migracyjna była wykorzystywana przed inwazją na Ukrainę w celu przetestowania reakcji NATO i poruszenia opinii publicznej, a także przed przystąpieniem Finlandii do Sojuszu[60]. Podobną technikę stosuje się wobec Ukrainy i Gruzji, aby zapobiec bliższej integracji tych państw z NATO lub zachodnimi strukturami w ogóle.

Państwa frontowe są najbardziej narażone na zagrożenia hybrydowe, takie jak sabotaż IK. Wynika to m.in. z tego, że podwodna sieć kabli i rurociągów w Europie nie została zaprojektowana z myślą o zagrożeniach związanych z wojną hybrydową[61]. To samo dotyczy aktów sabotażu oraz wysiłków na rzecz polaryzacji społeczeństw, podżegania do protestów i wywoływania napięć. Wszystko to ma na celu destabilizację krajów, które sprzeciwiają się Rosji.

Morskie zagrożenia hybrydowe oraz prawne aspekty ochrony infrastruktury morskiej

Zgodnie z definicją opracowaną przez Hybrid CoE zagrożeniami hybrydowymi są skoordynowane i zsynchronizowane działania ukierunkowane na słabości systemowe i instytucjonalne przy użyciu szerokiej gamy środków. Ma to też zastosowanie do działań prowadzonych na morzu[62].

Działania hybrydowe, takie jak częściowa blokada tranzytu morskiego lub ograniczenie dostępu do infrastruktury państwowej, mogą stanowić poważne zagrożenie dla małych państw, które zazwyczaj polegają na 1 lub 2 krytycznych obiektach morskich[63]. Jest to teraz bardziej widoczne w kontekście działań mających na celu uszkodzenie kabli (np. światłowodowych, energetycznych) na Morzu Bałtyckim, a także wykorzystywania przez Rosję

[60] H. Praks, *Hybrid CoE Working Paper 32: Russia's hybrid threat tactics against the Baltic Sea region...*, s. 19–20.

[61] Tamże, s. 21.

[62] *Hybrid CoE Paper 16: Handbook on maritime hybrid threats...*

[63] Tamże, s. 19–20.

tzw. floty cieni. Takie działania zmuszają kraje UE do reagowania i ciągłego monitorowania wszystkich ruchów statków na tym akwenie.

Należy podkreślić, że sztandarowym modelem ataku hybrydowego jest atak na podwodną IK (np. rurociągi)[64]. To przykład działania, które niewątpliwie będzie się powtarzać we współczesnej rywalizacji o zasoby.

Coraz bardziej powszechnym zagrożeniem, powiązanym z rozwojem sztucznej inteligencji i innych nowych technologii, są cyberataki, klasyfikowane jako zagrożenia hybrydowe. Takie ataki mogą skutkować utratą kontroli nad statkami, uszkodzeniem infrastruktury portowej i przerwami w łańcuchach dostaw[65]. Cyberprzestrzeń wykazuje wiele cech wspólnych z domeną morską – zwłaszcza pod względem rozproszenia, możliwości manewrowania oraz trudności w sprawowaniu nad nią pełnej kontroli.

Na obszarze morskim istnieją różne możliwości stwarzania w sposób niejawny zagrożeń dla IK, np. uszkodzenia jej bądź unieruchomienia. Państwo przeciwnik może wykorzystać broń podwodną – rozmieścić ją samodzielnie lub za czyimś pośrednictwem i wywołać eksplozje w pobliżu IK celu. Scenariusz zakłada ustanowienie stref kontroli wokół wysp. Chociaż jest to sprzeczne z Konwencją Narodów Zjednoczonych o prawie morza[66] (*United Nations Convention on the Law of the Sea*, UNCLOS), to przeciwnik może przyjąć strategię *faits accomplis* lub zgłaszać roszczenia do takich regionów – zazwyczaj w celu ustanowienia punktu kontrolnego, stworzenia instalacji wojskowej lub zapewnienia dostępu do złóż zasobów, zasobów rybnych lub szlaku transportowego w wyłącznej strefie ekonomicznej[67].

Chiny rozwijają sztuczne wyspy i obiekty wojskowe w regionach, do których roszczenia zgłaszają również Filipiny, Wietnam i Malezja. Wdrażają politykę faktów dokonanych, przez budowanie infrastruktury i zapewnienie sobie kontroli nad żeglugą na obszarach, do których nie mają pełnych praw na mocy UNCLOS. Po aneksji Krymu Rosja ustanowiła strefy kontroli na Morzu Azowskim i wokół Cieśniny Kerczeńskiej i tym samym utrudniła Ukrainie dostęp do jej portów. Japonia i Chiny są uwikłane w konflikty dotyczące wysp Senkaku, ponieważ Chiny konsekwentnie

[64] Tamże, s. 12–13.

[65] Tamże, s. 14–16.

[66] *Konwencja Narodów Zjednoczonych o prawie morza, sporządzona w Montego Bay dnia 10 grudnia 1982 r.*

[67] *Hybrid CoE Paper 16: Handbook on maritime hybrid threats…*, s. 17, 21.

wysyłają tam statki straży przybrzeżnej. Może to doprowadzić do przejęcia kontroli nad regionem.

Antagonista jest również w stanie celowo przeprowadzać nielegalne zatrzymania i inspekcje statków morskich pod pretekstem działań antyterrorystycznych. Wejście na pokład statku może skutkować sabotażem jego infrastruktury lub instalacją szkodliwego i szpiegowskiego oprogramowania[68]. Jest to kolejna metoda negatywnego wpływania na operacje na morzu, gdzie statki pozostają stałym celem wrogich działań.

Wrogie państwa mogą wykorzystywać floty kutrów rybackich (pochodzenia niepaństwowego) lub instrumentalizować grupy niepaństwowe w celu wywierania presji na IK i jednostki morskie[69]. Taktyka ta polega na wykorzystywaniu właścicieli statków, ich flot lub bander w celu stworzenia iluzji, że sprawca pochodzi z innego kraju, a nie np. z Rosji.

Wrogie państwa mogą wykorzystywać technologie modyfikacji pogody, np. przez rozpylanie substancji chemicznych w atmosferze w celu wywołania deszczu, burz czy mgły, a nawet sztucznie inicjować zjawiska o charakterze katastrof naturalnych, by zakłócić funkcjonowanie IK przeciwnika. Wrogie państwo może wykorzystać te działania jako zasłonę dymną do przeprowadzenia ataku hybrydowego, polegającego np. na uszkodzeniu podwodnej infrastruktury telekomunikacyjnej i energetycznej[70].

Atak hybrydowy może wiązać się również z celowym zablokowaniem cieśniny morskiej. Po pierwsze, utrudnia to państwom zagwarantowanie niezakłóconego tranzytu statków morskich, a po drugie, może wywołać międzynarodowy kryzys polityczny, przez sparaliżowanie zarówno stosunków wewnętrznych, jak i zagranicznych państwa będącego celem ataku[71]. Takich działań, zwłaszcza w odniesieniu do Kanału Sueskiego czy cieśniny Bab al-Mandab, należy spodziewać się w przyszłości w związku z powstaniem nowych baz morskich w Rogu Afryki. Jest to zagrożenie, które może pojawić się również na Morzu Bałtyckim.

Kolejne zagrożenia wynikają z naruszeń prawa międzynarodowego, głównie naruszeń UNCLOS. Zalecenia przedstawione w *Handbook on maritime hybrid threats: 15 scenarios and legal scans* kładą nacisk na potencjalne reakcje zgodne z międzynarodowymi normami prawnymi. Zbyt silna

[68] Tamże, s. 27.

[69] Tamże, s. 36.

[70] Tamże, s. 46.

[71] Tamże, s. 31.

zależność od tych ram prawnych niesie ze sobą istotne ryzyko. Powstaje bowiem asymetria: część podmiotów działa w granicach prawa, podczas gdy inni wykorzystują jego ograniczenia, co daje im strategiczną przewagę. W sytuacjach tego rodzaju korzyści osiągane w wyniku skutecznego ataku hybrydowego mogą znacznie przewyższać negatywne konsekwencje wynikające z międzynarodowych sankcji prawnych, co skłania niektóre państwa do świadomego naruszania prawa. Sytuacja ta pokazuje, że w czasie eskalującej rywalizacji geopolitycznej możliwości efektywnego przeciwdziałania agresywnym działaniom są ograniczone, co sprawia, że państwa muszą koncentrować się głównie na łagodzeniu skutków i odbudowie po ataku.

Potencjalna strategia ochronna obejmuje maksymalną marginalizację wrogiego państwa lub podmiotu niepaństwowego, której towarzyszy jego ciągłe monitorowanie. Pomogłoby to ograniczyć wdrażanie szkodliwych działań, szczególnie w obszarze bezpieczeństwa morskiego.

Ochrona morskiej IK stała się pilną kwestią w świetle niedawnych zagrożeń hybrydowych wymierzonych w podmorskie kable i rurociągi. Raport podkreśla rosnącą podatność na zagrożenia w tej domenie, zwłaszcza że podmioty państwowe i niepaństwowe wykorzystują luki i słabości technologiczne do przeprowadzania destrukcyjnych operacji[72]. Zagrożenia te, które mogą mieć znaczące konsekwencje geopolityczne, finansowe czy w zakresie bezpieczeństwa, obejmują sabotaż, cyberataki oraz zakłócenia ruchu morskiego[73]. Zabezpieczenie aktywów morskich stało się główną troską członków UE i sojuszników NATO z uwagi na istotną rolę, jaką infrastruktura morska odgrywa w globalnym handlu, dystrybucji energii i sieciach komunikacyjnych[74].

Systemy prawne mają dużą moc rozwiązywania tych problemów, ale nakładają również poważne ograniczenia. Konwencja UNCLOS przez ustanowienie stref jurysdykcyjnych pozwalających państwom nadbrzeżnym na różny stopień kontroli nad działalnością morską utrudnia państwom podejmowanie zdecydowanych działań przeciwko zagrożeniom hybrydowym powstającym poza ich granicami terytorialnymi, ze względu na rozproszone przepisy prawne. Chociaż obecne narzędzia prawne dają

[72] A. Sari, *Hybrid CoE Research Report 14: Protecting maritime infrastructure from hybrid threats*..., s. 5.

[73] Tamże, s. 6.

[74] Tamże, s. 8.

ogólne uprawnienia do utrzymania świadomości sytuacyjnej, to brakuje jasnych procedur dotyczących reakcji, zwłaszcza w przypadku zagrożeń rozwijających się na wodach międzynarodowych[75].

Podatność na uszkodzenia podmorskich kabli komunikacyjnych, kluczowych dla globalnej łączności internetowej i transakcji finansowych, jest poważnym problemem. Podmioty stanowiące zagrożenie hybrydowe wykazały zdolność do atakowania tych kabli, czego dowodem są niedawne incydenty na Morzu Bałtyckim[76]. Federacja Rosyjska, jak wcześniej wspomniano, nie ma żadnych skrupułów w intensyfikowaniu szkodliwych działań, które prowadziła w Europie Środkowo-Wschodniej w ostatnich latach.

Problem z jednoznacznym przypisaniem odpowiedzialności za ataki hybrydowe utrudnia adekwatną reakcję, ponieważ sprawcy często wykorzystują luki i niejasności w zakresie jurysdykcji międzynarodowej, by uniknąć odpowiedzialności prawnej. Skuteczne przeciwdziałanie tego typu zakłóceniom wymaga bliskiej współpracy międzynarodowej oraz sprawnie funkcjonujących systemów wymiany informacji wywiadowczych, z uwzględnieniem złożonych czynników ryzyka – zarówno gospodarczych, jak i dotyczących bezpieczeństwa – które są z nimi nierozerwalnie związane[77].

Konieczne jest opracowanie i opublikowanie kompleksowej strategii w celu złagodzenia tych słabości. W pierwszej kolejności państwa powinny zagwarantować spójne stosowanie krajowych ram prawnych w celu skutecznego wdrażania jurysdykcji ustawodawczej i wykonawczej, zgodnie z postanowieniami UNCLOS. Wiąże się to z uznaniem, że istnieją niedociągnięcia prawne, które podmioty stwarzające zagrożenia mogą wykorzystać, i dostosowaniem ustawodawstwa krajowego w celu wzmocnienia współpracy transgranicznej w zakresie egzekwowania prawa. Po drugie, interpretacje prawne muszą zostać zmodyfikowane w celu uwzględnienia pojawiających się zagrożeń, w tym celowego atakowania infrastruktury podmorskiej za pomocą metod cybernetycznych i kinetycznych[78].

Kolejnym ważnym zaleceniem jest wzmocnienie wysiłków dyplomatycznych w celu ustanowienia nowych międzynarodowych zasad ochrony krytycznych zasobów morskich. W raporcie zasugerowano, aby członkowie

[75] Tamże, s. 16–17.

[76] Tamże, s. 27.

[77] Tamże, s. 32–36.

[78] Tamże, s. 32.

UE i NATO wspólnie pracowali nad wzmocnieniem środków regulacyjnych, w tym nad przyjęciem wiążących umów, które zwiększą bezpieczeństwo podmorskich kabli i rurociągów. Ponadto wspólne ćwiczenia i inicjatywy wymiany informacji w czasie rzeczywistym powinny zostać rozszerzone, aby poprawić zdolności wykrywania zagrożeń i reagowania na nie[79].

Ewoluujący charakter zagrożeń hybrydowych wymaga proaktywnej i adaptacyjnej strategii prawnej. Państwa muszą być przygotowane na aktualizację i rozszerzenie swoich polityk w odpowiedzi na pojawiające się wyzwania. Ochrona infrastruktury morskiej to nie tylko kwestia bezpieczeństwa narodowego, lecz także globalny imperatyw[80]. Ta kwestia jest szczególnie aktualna w odniesieniu do regionu Morza Bałtyckiego.

Podsumowanie

Analizowane badania, oparte na studiach Hybrid CoE, pozwalają na kompleksowe zrozumienie zagrożeń hybrydowych, zwłaszcza ich implikacji dla IK w UE, przede wszystkim w Europie Środkowo-Wschodniej. Głównym podmiotem podejmującym w ostatnich latach szkodliwe działania pozostaje FR, jednak coraz więcej państw wykorzystuje narzędzia hybrydowe, aby zwiększyć swoją obecność i wpływy. Ponadto charakter zagrożeń hybrydowych szybko ewoluuje.

Badanie *The Landscape of Hybrid Threats: A Conceptual Model* przedstawia szerokie spojrzenie na ewolucję i mechanizmy zagrożeń hybrydowych, stwarzanych zarówno przez podmioty państwowe, jak i niepaństwowe. Z kolei *The concept of hybrid war in Russia: A national security threat and means of strategic coercion* zapewnia zrozumienie strategicznych celów Rosji przez ukazanie jej działań hybrydowych w kontekście rywalizacji geopolitycznej. *Handbook on maritime hybrid threats: 15 scenarios and legal scans* podkreśla potrzebę większego skupienia się na obszarze morskim (głównie na Morzu Bałtyckim), który jest istotny dla UE i NATO pod względem infrastruktury, stabilności gospodarczej i transportowej, a także bezpieczeństwa regionalnego. Równie ważny jest raport *A comprehensive resilience ecosystem,* który podkreśla potrzebę odporności na zmieniające się zagrożenia hybrydowe i wspiera w ten sposób krajowe i międzynarodowe struktury

[79] Tamże, s. 36.

[80] Tamże.

bezpieczeństwa. Jest to szczególnie ważne teraz, gdy Europa musi skoncentrować się na własnym bezpieczeństwie i nie może polegać wyłącznie na wsparciu USA. *Russia's Hybrid Threat Tactics Against the Baltic Sea Region* jest niezbędnym narzędziem do zrozumienia ataków i aktów sabotażu. Należy wziąć je pod uwagę przy tworzeniu nowych polityk, ponieważ oferuje konkretne studium przypadku rosyjskich taktyk hybrydowych wraz z ich wpływem i wymaganymi środkami zaradczymi. *Protecting maritime infrastructure from hybrid threats: legal options* wskazuje na istotne słabości prawne w zakresie bezpieczeństwa morskiego, wspierając tym samym globalną współpracę i zmiany prawne.

Podkreślając potrzebę proaktywnych polityk bezpieczeństwa, działań budujących odporność i zmian prawnych w celu skutecznego sprostania pojawiającym się wyzwaniom, badania te dostarczają istotnych informacji dla zrozumienia i minimalizowania zagrożeń hybrydowych dla IK krajów UE. Należy również dodać, że państwa na wschodniej flance zmagają się z wyzwaniem w postaci odpowiedzi na działania FR i podmiotów niepaństwowych oraz muszą zadbać o własne bezpieczeństwo.

Obecne badania nad zagrożeniami hybrydowymi ujawniają liczne dysfunkcje w systemie przeciwdziałania tym zagrożeniom w UE, utrudniające skuteczne działania. Muszą one zostać natychmiast wyeliminowane przez:

a) wypracowanie transkontynentalnego porozumienia mającego na celu przeciwdziałanie zagrożeniom hybrydowym,
b) wyznaczenie konkretnych państw, organizacji i frakcji, które mogą być źródłem zagrożeń hybrydowych,
c) rewizję istniejących definicji zagrożeń hybrydowych, z uwzględnieniem ciągłej ewolucji tego zjawiska,
d) zatwierdzenie terminologii i wspólnych cech zagrożeń hybrydowych, działań wojennych i terroryzmu,
e) standaryzacja systemów prawnych społeczności międzynarodowej w zakresie przestępstw oraz działań związanych z zagrożeniami hybrydowymi, jak również innych czynów przestępczych,
f) utrzymanie spójnej polityki przeciwdziałania zagrożeniom hybrydowym w ramach sojuszy międzynarodowych,
g) ponowną ocenę planów i strategii w państwowych programach przeciwdziałania zagrożeniom hybrydowym, co zwiększyłoby orientację na cel i finansowanie odpowiednich organizacji zaangażowanych w zwalczanie zagrożeń hybrydowych,

h) wdrożenie długoterminowej polityki przeciwdziałania zagrożeniom hybrydowym z ciągłym finansowaniem i szkoleniami dla podstawowych jednostek przeciwdziałających zagrożeniom hybrydowym,
i) gruntowną edukację społeczeństwa, zwłaszcza dzieci i młodzieży, w zakresie istniejących zagrożeń hybrydowych, a także postrzegania i rozumienia różnych religii i kultur[81].

Znalezienie odpowiedniego sposobu zwalczania zagrożeń hybrydowych stanowi najważniejszy cel zarówno na poziomie krajowym, jak i międzynarodowym. Obiektywna ocena ewolucji tego zjawiska pozostaje ściśle powiązana z rozwojem oraz koordynacją polityk przeciwdziałania zagrożeniom hybrydowym, a także z podnoszeniem świadomości społecznej w tym zakresie. Charakter tych zagrożeń determinuje kierunek działań państw oraz kształt tworzonych regulacji prawnych stanowiących odpowiedź na pojawiające się wyzwania. Powielane stereotypy powinny zostać zastąpione pogłębionymi analizami, które pozwolą uznać zagrożenia hybrydowe za nadrzędne wyzwanie dla bezpieczeństwa państwa – szczególnie z uwagi na ich zróżnicowaną formę, zależną od specyfiki terytorium, na którym występują. Zagrożenia hybrydowe mogą przybierać odmienne formy w krajach bałtyckich, Francji, Polsce i Ukrainie. Należy być świadomym ich istnienia, ewolucji i coraz częstszego występowania. Sposobom przeciwdziałania zagrożeniom hybrydowym należy poświęcić więcej uwagi w debatach politycznych, eksperckich i badaniach naukowych, co ułatwi wyciągnięcie właściwych wniosków i konceptualizację praktycznych działań, również na poziomie międzynarodowym.

Unia Europejska i NATO pokazały, że istnieje silna wola wzmocnienia bezpieczeństwa w obszarze euroatlantyckim i wspólnego zwalczania zagrożeń hybrydowych. Potrzebny jest czas na wypracowanie konkretnych rozwiązań. W dynamicznym środowisku geopolitycznym tylko wielopoziomowa polityka bezpieczeństwa umożliwi osiągnięcie celów. Zarówno UE, jak i NATO dysponują instrumentami współpracy wojskowej i politycznej umożliwiającymi skuteczną reakcję. Niezwykle istotne jest nie tylko eliminowanie pojawiających się zagrożeń, lecz także podejmowanie globalnych inicjatyw mających im zapobiegać[82]. W tym zakresie szczególny nacisk należy położyć na wyzwania w Europie Środkowo-Wschodniej.

[81] A. Olech, *French and Polish fight against terrorism*, Poznań 2022, s. 198.

[82] A. Olech, *Cooperation between NATO and the European*...

Do ich skutecznej realizacji niezbędne jest jednak zaangażowanie każdego z państw członkowskich. Bez stałej i niezachwianej współpracy obecne wysiłki struktur międzynarodowych mogą okazać się daremne.

Hybrid CoE powinno zainicjować badania nad zagrożeniami hybrydowymi pochodzącymi od zewnętrznych aktorów w Afryce i na Bliskim Wschodzie, szczególnie w kontekście Europy. Konieczne jest także coroczne przygotowywanie oceny zagrożeń hybrydowych dla państw członkowskich UE, z wykorzystaniem raportów krajowych agencji bezpieczeństwa. Korzystne byłoby również organizowanie dyskusji okrągłego stołu, zarówno w formie stacjonarnej, jak i zdalnej, dla unijnych ekspertów specjalizujących się w zagrożeniach hybrydowych. Rezultatem omówienia przez nich najpilniejszych wyzwań i koncepcji może być raport zawierający różne perspektywy dotyczące zagrożeń hybrydowych, uwzględniające uwarunkowania każdego kraju. Zdaniem autora Hybrid CoE jest gotowe do ustanowienia ponadnarodowej strategii przeciwdziałania zagrożeniom hybrydowym.

W 2025 r., ponad dekadę po rosyjskim ataku na Ukrainę i 3 lata po rozpoczęciu pełnoskalowej inwazji oraz serii ataków hybrydowych wymierzonych w państwa członkowskie UE, konieczne staje się nie tylko wzmocnienie polityki bezpieczeństwa i odporności na zagrożenia hybrydowe, lecz także rozwinięcie skuteczniejszych mechanizmów reagowania. Charakterystyka tych zagrożeń jednoznacznie wskazuje, że wojna hybrydowa już trwa, co znajduje potwierdzenie w analizach prowadzonych przez Hybrid CoE. W obecnej sytuacji równie istotne jak diagnozowanie i opisywanie natury tych działań jest wdrażanie proaktywnych środków zaradczych oraz budowanie odporności systemowej.

Bibliografia

Olech A., *French and Polish fight against terrorism*, Poznań 2022.

Źródła internetowe

Giannopoulos G., Smith H., Theocharidou M., *The Landscape of Hybrid Threats: A Conceptual Model Public Version*, Publications Office of the European Union, Luxembourg 2021, https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf [dostęp: 2.01.2025].

Hybrid CoE Paper 16: Handbook on maritime hybrid threats: 15 scenarios and legal scans, marzec 2023, https://www.hybridcoe.fi/wp-content/uploads/2023/03/NEW_web_Hybrid_CoE_Paper-16_rgb.pdf [dostęp: 17.01.2025].

Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G., *Hybrid threats: a comprehensive resilience ecosystem*, Publications Office of the European Union, Luxembourg 2023, https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE_comprehensive_resilience_ecosystem.pdf [dostęp: 22.01.2025].

Olech A., *Cooperation between NATO and the European Union against hybrid threats with a particular emphasis on terrorism*, Institute of New Europe, 17.03.2021, https://ine.org.pl/en/cooperation-between-nato-and-the-european-union-against-hybrid-threats-with-a-particular-emphasis-on-terrorism/ [dostęp: 10.02.2025].

Praks H., *Hybrid CoE Working Paper 32: Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage*, maj 2024, https://www.hybridcoe.fi/wp-content/uploads/2024/05/20240530-Hybrid-CoE-Working-Paper-32-Russias-hybrid-threat-tactics-WEB.pdf [dostęp: 30.01.2025].

Pynnöniemi K., *The concept of hybrid war in Russia: A national security threat and means of strategic coercion*, Hybrid CoE Strategic Analysis / 27, maj 2021, https://www.hybridcoe.fi/wp-content/uploads/2021/05/20210518_Hybrid_CoE_Strategic_Analysis_27_The_concept_of_hybrid_war_in_Russia_WEB.pdf [dostęp: 10.01.2025].

Sari A., *Hybrid CoE Research Report 14: Protecting maritime infrastructure from hybrid threats: legal options*, marzec 2025, https://www.hybridcoe.fi/wp-content/uploads/2025/03/20250306-Hybrid-CoE-Research-Report-14-web.pdf [dostęp: 6.03.2025].

Untersinger M., *Les Etats-Unis ordonnent une pause des cyberopérations contre la Russie, selon plusieurs médias*, Le Monde, 4.03.2025, https://www.lemonde.fr/pixels/article/2025/03/03/les-etats-unis-ordonnent-une-pause-des-operations-cyber-contre-la-russie_6575971_4408996.html [dostęp: 4.03.2025].

Akty prawne

Konwencja Narodów Zjednoczonych o prawie morza, sporządzona w Montego Bay dnia 10 grudnia 1982 r. (DzU z 2002 poz. 543).

Dr Aleksander Olech

Szef Działu Współpracy Międzynarodowej Defence24. Wykładowca na uczelniach polskich 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 i polityka bezpieczeństwa NATO.

Kontakt: a.olech@defence24.pl

Terroryzm – studia, analizy, prewencja, 2025, wydanie specjalne: 167–193

https://doi.org/10.4467/27204383TER.25.006.21509

Artykuł

Prawne i techniczne metody ochrony obiektów infrastruktury krytycznej przed zagrożeniami ze strony bezzałogowych statków powietrznych – przykład Polski

Legal and technical methods of protecting critical infrastructure facilities against threats from unmanned aerial vehicles – the Polish example

JĘDRZEJ ŁUKASIEWICZ
https://orcid.org/0000-0002-7082-8511
Autor niezależny

DAMIAN SZLACHTER
https://orcid.org/0000-0003-2763-9325
Agencja Bezpieczeństwa Wewnętrznego

Abstrakt

Celem artykułu jest omówienie zmian prawnych wprowadzonych w Polsce w odpowiedzi na rosnące zagrożenie dla obiektów infrastruktury krytycznej ze strony bezzałogowych statków powietrznych oraz przedstawienie rekomendowanej metody oceny skuteczności systemów detekcji i neutralizacji tych statków opracowanej przez Rządowe Centrum Bezpieczeństwa. Autorzy omawiają nowelizację *Ustawy z dnia 3 lipca 2002 r. Prawo lotnicze*, w której zawarto przepisy istotne dla bezpieczeństwa wykonywania lotów platform bezzałogowych, zapewniające operatorom infrastruktury krytycznej prawo do obrony chronionego obiektu przed atakami z wykorzystaniem bezzałogowych statków powietrznych, oraz nowelizację *Ustawy z dnia*

24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej, w ramach której poszerzono katalog środków przymusu bezpośredniego o zniszczenie albo unieruchomienie bezzałogowego statku powietrznego albo przejęcie kontroli nad jego lotem oraz wskazano środki jego neutralizacji.

Słowa kluczowe

infrastruktura krytyczna, bezzałogowe statki powietrzne, ustawa – Prawo lotnicze, systemy detekcji i neutralizacji dronów

Abstract

The aim of this article is to discuss the legal changes introduced in Poland in response to the growing threat to critical infrastructure facilities from unmanned aerial vehicles (UAVs) and to present a recommended method for assessing the effectiveness of UAV detection and neutralisation systems developed by the Government Centre for Security (RCB). The authors discuss the amendment of the *Act of 3 July 2002 – Aviation Law*, which includes provisions relevant to the safety of unmanned platform flights, ensuring that operators of critical infrastructure have the right to defend the protected facility against attacks using unmanned aircraft, and the amendment of the *Act of 24 May 2013 on direct coercive measures and firearms*, which expanded the catalogue of direct coercive measures to include the destruction or immobilisation of UAV or the seizure of control over its flight, and indicated the means of its neutralisation.

Keywords

critical infrastructure, unmanned aerial vehicles, Aviation Law, drone detection and neutralisation systems

Wprowadzenie

Miniaturyzacja elektroniki, skonstruowanie wydajnych źródeł energii wykorzystywanych w bezzałogowych statkach powietrznych oraz stosunkowo prosty proces szkolenia pilotów przyczyniły się do rozwoju i popularyzacji lotnictwa bezzałogowego. Dostępność w sprzedaży różnych modeli tych statków oraz części i instrukcji pozwalających na samodzielną i anonimową budowę platformy bezzałogowej, jak również dostęp do technologii druku 3D, umożliwiającej wykonanie nawet skomplikowanych

elementów, spowodowały, że bezzałogowe statki powietrzne zaczęły być wykorzystywane na dużą skalę m.in. w działaniach sabotażowych, w tym w atakach na obiekty infrastruktury krytycznej (IK). Działania mające na celu wprowadzenie w Polsce rozwiązań prawno-organizacyjnych zapewniających operatorom IK szanse na zbudowanie skutecznych systemów antydronowych trwały w Polsce kilka lat[1]. Finalizacją tych działań jest wejście w życie nowelizacji prawa lotniczego (luty 2025 r.), która wprowadza duże zmiany w obszarze stosowania systemów antydronowych przez operatorów IK. Celem artykułu jest omówienie tych zmian oraz przedstawienie rekomendacji Rządowego Centrum Bezpieczeństwa (RCB) dotyczących metody oceny skuteczności systemów detekcji oraz neutralizacji platform bezzałogowych.

Bezzałogowe statki powietrzne jako narzędzie ataku na obiekt infrastruktury krytycznej

Bezzałogowe statki powietrzne są coraz powszechniej wykorzystywane jako narzędzie do rozpoznania systemów lub obiektów IK oraz do ataków na nie. W badaniach ankietowych przeprowadzonych wśród przedstawicieli służb i instytucji systemu AT w RP oraz analityków rządowych think tanków bezzałogowe statki powietrzne zostały wskazane jako narzędzie stanowiące największe wyzwanie dla służb, organów i instytucji mających zapewniać bezpieczeństwo obiektom mogącym być celem ataku terrorystycznego. Wraz z drukiem 3D stanowiły one 77,66% wszystkich wskazań[2]. Do czasu pełnoskalowej rosyjskiej inwazji na Ukrainę wykorzystanie dronów w atakach na IK zdarzało się rzadko. Działania wojenne przyczyniły się do gwałtownego rozwoju technologii bezzałogowych, a także do opracowania nowych taktyk ataków z wykorzystaniem platform bezzałogowych.

[1] Autorzy artykułu brali udział w pracach kilku międzyresortowych grup roboczych (pod egidą Ministerstwa Spraw Wewnętrznych i Administracji lub Agencji Bezpieczeństwa Wewnętrznego) czy zespołów wewnętrznych tworzonych przez Rządowe Centrum Bezpieczeństwa lub organy Komisji Europejskiej.

[2] D. Szlachter, *Terroryzm w Polsce i kierunki jego rozwoju. Wyniki badań ankietowych (skrócony raport)*, „Terroryzm – studia, analizy, prewencja" 2022, nr 2, s. 148–176. https://doi.org/10.4467/27204383TER.22.022.16342.

Zgodnie z obecnie obowiązującymi w Polsce przepisami prawa infrastrukturą krytyczną są systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Infrastruktura krytyczna obejmuje systemy:

a) zaopatrzenia w energię, surowce energetyczne i paliwa,
b) łączności,
c) sieci teleinformatycznych,
d) finansowe,
e) zaopatrzenia w żywność,
f) zaopatrzenia w wodę,
g) ochrony zdrowia,
h) transportowe,
i) ratownicze,
j) zapewniające ciągłość działania administracji publicznej,
k) produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych[3].

System bezzałogowego statku powietrznego to bezzałogowy statek powietrzny (platforma unosząca się w powietrzu) wraz z wyposażeniem do jego zdalnego sterowania (stacją naziemną, za pomocą której pilot może sterować statkiem w czasie lotu)[4]. Przepisy prawa nie rozróżniają typów statków powietrznych. Do najczęściej wykorzystywanych typów platform bezzałogowych należą multirotory, samoloty, śmigłowce oraz hybrydy, których konstrukcja łączy cechy pozostałych typów statków. Hybrydą może być np. samolot wyposażony w dodatkowe silniki umożliwiające pionowy start i lądowanie. Będzie to zatem hybryda samolotu i multirotora. Statki te mogą mieć różne masy. Przepisy polskiego prawa wyróżniają masy statku do 0,25 kg, do 0,9 kg, do 4 kg oraz do 25 kg. Statki o masie większej niż 25 kg wymagają specjalnego zezwolenia na wykonanie operacji wydawanego przez Prezesa Urzędu Lotnictwa Cywilnego[5].

[3] Artykuł 3 ust. 2 *Ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*.

[4] *Rozporządzenie wykonawcze Komisji Europejskiej (UE) 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych*.

[5] *Ustawa z dnia 3 lipca 2002 r. Prawo lotnicze*; *Rozporządzenie wykonawcze Komisji (UE) 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji*

Za pomocą systemu bezzałogowego statku powietrznego można zrealizować praktycznie każdy scenariusz ataku lotniczego. O ich uniwersalności decydują m.in. następujące cechy:

1. Mogą być wykorzystane w misjach obarczonych dużo wyższym ryzykiem neutralizacji platformy niż w przypadku statków załogowych. Z tej przyczyny wykorzystuje się bezzałogowce w misjach samobójczych, w których ceną sukcesu jest utrata platformy, a nie pilota.
2. Mogą wykonywać misje sterowane bezpośrednio przez pilota, w locie automatycznym lub w locie autonomicznym. Bezpośrednie sterowanie przez pilota odbywa się za pomocą sygnału radiowego lub przez światłowód. Lot automatyczny to taki, którego trasa, parametry lotu oraz zadania wykonane przez statek zostały zaprogramowane przez pilota przed startem. Taki lot odbywa się z wykorzystaniem sensorów wspomagających komputer pokładowy platformy. W tym typie lotu pilot wskazuje zadanie, ale sposób wykonania misji zależy od algorytmów AI zaimplementowanych na komputerze pokładowym platformy. Dodatkowo komputery pokładowe przed podjęciem decyzji o ataku na podstawie danych z sensorów, z wykorzystaniem algorytmów AI, określają wartość celu i potencjalne straty przeciwnika i podejmują decyzję[6].
3. Mają zdolność do utrzymania się w jednym punkcie przestrzeni przez długi czas, przez co mogą być wykorzystane do obserwacji dużego obszaru dookoła punktu zawisu. Bezzałogowce typu samolot mogą przenosić ładunek wybuchowy na duże odległości i atakować cele zlokalizowane daleko od miejsca startu (czyli miejsca, w którym znajduje się pilot). Potwierdzone odległości, na które latają bezzałogowe samoloty, sięgają kilkuset kilometrów[7].

---

bezzałogowych statków powietrznych; Wytyczne nr 15/2023 Prezesa Urzędu Lotnictwa Cywilnego z dnia 1 czerwca 2023 r. w sprawie sposobów wykonywania operacji przy użyciu systemów bezzałogowych statków powietrznych w związku z wejściem w życie przepisów rozporządzenia wykonawczego Komisji (UE) nr 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych.

[6] J. Łukasiewicz, M. Piekarski, M. Kluczyński, *Bezpieczeństwo infrastruktury krytycznej wobec zagrożeń ze strony platform bezzałogowych*, Raport PTBN t. 2, Polskie Towarzystwo Bezpieczeństwa Narodowego 2021.

[7] *Timeline: UAE under drone, missile attacks*, Al Jazeera, 3.02.2022, https://www.aljazeera.com/news/2022/2/3/timeline-uae-drone-missile-attacks-houthis-yemen [dostęp:

4. Mogą być napędzane silnikami elektrycznymi, tłokowymi silnikami spalinowymi, a także silnikami turboodrzutowymi. Silniki elektryczne wymagają źródeł prądu, czyli baterii, ogniwa paliwowego lub generatora zasilanego silnikiem spalinowym, są za to stosunkowo ciche. Silniki spalinowe pozwalają na wykonanie misji na bardzo dalekie dystanse, a silniki turboodrzutowe – na rozpędzenie platformy do prędkości nieosiągalnych dla innych napędów.
5. Mogą być sterowane za pomocą różnych częstotliwości, w przypadku gdy łączność odbywa się drogą radiową bezpośrednio pomiędzy lecącą platformą a stacją naziemną. Ze względu na możliwość zagłuszenia sygnału radiowego wypracowano mechanizm zmian częstotliwości w locie. Loty na dalekie odległości mogą być realizowane z wykorzystaniem innych statków powietrznych przenoszących urządzenie zwane *repeater*, pracujące jako stacja pośrednia pomiędzy stacją naziemną a platformą. Bezzałogowym statkiem powietrznym można także sterować z wykorzystaniem łączności GSM. Warunkiem skutecznego połączenia jest nasycenie rejonu lotu dostateczną liczbą stacji przekaźnikowych (ang. *base transceiver station*, BTS). Coraz popularniejszym, a czasami jedynym możliwym, sposobem łączności pomiędzy stacją bazową a lecącym statkiem jest łączność satelitarna. Pozwala ona na realizowanie misji, której czas trwania zależy tylko od zasobów energii koniecznej do napędzania silników statku powietrznego[8]. W przypadku gdy jedną z metod obrony atakowanego obiektu jest zagłuszanie częstotliwości radiowych, na których realizuje się połączenie statku ze stacją naziemną, można wykorzystać połączenie światłowodowe. Zgodnie z doniesieniami maksymalna długość światłowodu nawiniętego na szpulę to obecnie 41 km[9]. Oczywiście konieczność

21.02.2025]; G. Faulconbridge, L. Kelly, *Ukrainian drone strikes trigger fires at major oil and gas facilities in Russia*, Reuters, 3.02.2025, https://www.reuters.com/world/europe/ukraines-drone-attack-sparks-fire-forces-flight-suspensions-several-russian-2025-02-03/ [dostęp: 21.02.2025].

[8] C. Koulouris i in., *A Survey Study and Comparison of Drones Communication Systems*, w: *Flexible Electronics for Electric Vehicles. Proceedings of the 3rd International Conference, FlexEV 2022*, S.K. Goyal i in. (red.), seria: „Lecture Notes in Electrical Engineering", t. 1065, Springer, Singapore. https://doi.org/10.1007/978-981-99-4795-9_33.

[9] *Jam-Proof Fiber Optics for Drones: Revolutionizing Secure Communications*, Linden Photonics Inc, 22.08.2024, https://www.lindenphotonics.com/jam-proof-fiber-optics-for-drones-

przeniesienia szpuli ze światłowodem powoduje ograniczenie masy ładunku wybuchowego. Zaletą tego rozwiązania jest jednak to, że statek porusza się w całkowitej ciszy radiowej.

6. Mogą być budowane z wykorzystaniem wielu materiałów. Najpopularniejsze to plastik formowany w formach wtryskowych, laminat szklany lub węglowy formowany lub cięty za pomocą frezarek CNC, aluminium cięte frezarkami CNC, druk 3D. Do konstrukcji bezzałogowców stosuje się także drewno, sklejkę i ebonit.
7. Mogą przenosić dowolny ładunek użyteczny. Ładunkiem użytecznym mogą być urządzenia pomiarowe, urządzenia rejestrujące obraz oraz zasobniki z materiałami wybuchowymi lub środkami chemicznymi. Do przeprowadzania ataków są wykorzystywane ręczne granaty, głowice RPG i inne materiały wybuchowe. Możliwość przenoszenia ładunku zapewnił druk 3D.
8. Proste konstrukcje przystosowane do lotów z ładunkiem wybuchowym i dające możliwość obserwacji celu ataku (tzw. drony FPV) można zbudować już za ok. 200 dolarów[10]. Konstrukcje bardziej zaawansowane i te przeznaczone do celów wojskowych są znacznie droższe.
9. Zdobycie umiejętności sterowania platformą nie jest skomplikowane. Dzięki wykorzystaniu akcelerometrów i żyroskopów, a także barometrów i odbiorników GPS, czyli systemów stabilizujących platformę, pilot może nabyć takie umiejętności w ciągu kilku godzin.

W związku z wymienionymi cechami systemów bezzałogowych statków powietrznych operator IK przy budowaniu systemu ich detekcji i neutralizacji powinien rozważyć następujące scenariusze oraz konsekwencje ataku przeprowadzonego za pomocą tych urządzeń:

1. Zakłócenie działania atakowanego obiektu lub instalacji przez nieautoryzowany przelot w rejonie obiektu. Konsekwencjami ataku mogą być: wywołanie niepokoju personelu, zakłócenie jego pracy,

revolutionizing-secure-communications [dostęp: 21.02.2025]; *Ukrainians Made an FPV With Fiber-Optic Cord Stretching For 41 km*, Defence Express, 26.01.2025, https://en.defence-ua.com/industries/ukrainians_made_an_fpv_with_fiber_optic_cord_stretching_for_41_km-13327.html [dostęp: 21.02.2025].

[10] B. Wang, *Ukraine's One Million FPV Drones Is Outnumbered by 5 Million Russian Drones*, Next Big Future, 27.01.2024, https://www.nextbigfuture.com/2024/01/ukraines-one-million-fpv-drones-will-be-outnumbered-by-5-million-russian-drones.html [dostęp: 21.02.2025].

oderwanie go od rutynowych czynności, a także zaangażowanie służb państwowych w czynności mające na celu ustalenie sprawcy ataku[11].

2. Działalność szpiegowska. Konsekwencją takiego ataku może być rozpoznanie: cech konstrukcyjnych obiektu lub instalacji przemysłowych wykorzystywanych w obiekcie, producenta urządzeń wykorzystywanych w procesach technologicznych, procedur obowiązujących na terenie atakowanego obiektu, tożsamości pracowników oraz metod komunikacji pomiędzy pracownikami zatrudnionymi w obiekcie[12].
3. Uderzenie kinetyczne, rozbicie platformy, zrzucenie ładunku, który mechanicznie uszkodzi urządzenia i instalacje, a następnie wstrzyma ich działanie, zawieszenie na urządzeniach elektrycznych elementów przewodzących prąd elektryczny takich jak przewody, włókna węglowe lub pył węglowy. Konsekwencjami ataku mogą być: uszkodzenia instalacji, obrażenia u ludzi, panika, a także spowodowanie zwarcia instalacji elektrycznej zasilającej obiekt lub instalację[13].
4. Przeniesienie ładunku wybuchowego i wywołanie jego eksplozji. Konsekwencjami ataku mogą być: utrata zdrowia lub życia przez pracowników, zniszczenie instalacji powodujące długotrwałą przerwę w działaniu obiektu, panika, stres, a w dalszej perspektywie niepokój społeczny[14].
5. Przeniesienie broni chemicznej, biologicznej, radiologicznej lub innej substancji drażniącej. Konsekwencjami ataku mogą być: długotrwała kontaminacja obszaru obiektu uniemożliwiająca jego funkcjonowanie, uszkodzenie instalacji wymaganych w procesie

[11] *It is still unclear whose drone is blocking 6 flights at Sofia Airport*, Fakti.bg, 9.02.2025, https://fakti.bg/en/bulgaria/948414-it-is-still-unclear-whose-drone-is-blocking-6-flights-at-sofia-airport [dostęp: 21.02.2025].

[12] *Sweden drones: Sightings reported over nuclear plants and palace*, BBC, 18.01.2022, https://www.bbc.com/news/world-europe-60035446 [dostęp: 21.02.2025].

[13] S. Lyngaas, *Drone at Pennsylvania electric substation was first to 'specifically target energy infrastructure', according to federal law enforcement bulletin*, CNN, 4.11.2021, https://edition.cnn.com/2021/11/04/politics/drone-pennsylvania-electric-substation/index.html [dostęp: 21.02.2025]; B. Barrett, *A Drone Tried to Disrupt the Power Grid. It Won't Be the Last*, Wired, 5.11.2021, https://www.wired.com/story/drone-attack-power-substation-threat/ [dostęp: 21.02.2025].

[14] G. Faulconbridge, L. Kelly, *Ukrainian drone strikes trigger fires*...

technologicznym, spowodowanie pożarów, w tym na obszarze otaczającym chroniony obiekt[15].

6. Przemyt niedozwolonych ładunków zarówno na teren obiektu, jak i z obiektu poza jego ogrodzenie. Konsekwencjami mogą być: pojawienie się na terenie obiektu broni palnej, materiałów wybuchowych, środków walki elektronicznej, narkotyków itp.[16] Przemyt z obiektu może spowodować utratę kontroli nad informacjami niejawnymi, których nie wolno przenosić poza teren obiektu, utratę chronionych środków chemicznych, biologicznych lub jądrowych itp.

Zmiany legislacyjne w zakresie ochrony infrastruktury krytycznej przed bezzałogowymi statkami powietrznymi

Obowiązujące dotychczas w Polsce przepisy prawa praktycznie nie uwzględniały możliwości zwalczania bezzałogowych statków powietrznych, nawet w przypadku gdy stanowiły one zagrożenie dla chronionych obiektów, ruchu lotniczego, zdrowia lub życia ludzkiego. Na świecie konsekwencją braku właściwych przepisów były przeloty bezzałogowych statków powietrznych nad chronionymi obiektami, a nawet loty na kursach kolizyjnych z załogowymi statkami powietrznymi[17]. Zdarzały się także pojedyncze przypadki użycia bezzałogowych platform w atakach na ludzi[18]. Tego rodzaju sytuacje, wojna w Ukrainie, liczne doniesienia o atakach na obiekty IK na świecie, a także działania hybrydowe na Bałtyku pokazały, że zapewnienie w Polsce bezpieczeństwa IK, dla której źródłem zagrożeń są bezzałogowe statki powietrzne, wymaga poważnych zmian prawnych.

[15] *Drone 'containing radiation' lands on roof of Japanese PM's office*, The Guardian, 22.04.2015, https://www.theguardian.com/world/2015/apr/22/drone-with-radiation-sign-lands-on-roof-of-japanese-prime-ministers-office [dostęp: 21.02.2025].

[16] *Cheap and They Don't Snitch: Drones Are the New Drug Mules*, RUSI, 5.01.2024, https://www.rusi.org/news-and-comment/in-the-news/cheap-and-they-dont-snitch-drones-are-new-drug-mules [dostęp: 21.02.2025].

[17] S. McKenzie, G. Mezzofiore, *Police hunt drone pilots in unprecedented Gatwick Airport disruption*, CNN, 20.12.2018, https://edition.cnn.com/2018/12/20/uk/gatwick-airport-drones-gbr-intl/index.html [dostęp: 21.02.2025]; *Drones paralyzed Stockholm-Arlanda Airport*, Kronen Zeitung, 9.09.2024, https://www.krone.at/3519874 [dostęp: 21.02.2025].

[18] *Venezuela President Maduro survives 'drone assassination attempt'*, BBC, 5.08.2018, https://www.bbc.com/news/world-latin-america-45073385 [dostęp: 21.02.2025].

Odpowiedzią na te zagrożenia są nowe przepisy zapisane w ustawie o zmianie ustawy – Prawo lotnicze oraz niektórych innych ustaw[19]. Projekt wpłynął do Sejmu Rzeczypospolitej 24 listopada 2024 r.[20] W dniu 24 stycznia 2025 r. został przekazany prezydentowi RP, który podpisał ustawę 6 lutego 2025 r. Wdraża ona te przepisy prawa unijnego, które dotyczą bezzałogowych statków powietrznych[21]. Ustawa uporządkowała dotychczasowy stan prawny, na którego podstawie wykonywano w Polsce loty bezzałogowych statków powietrznych. Nowością w stosunku do obowiązującej wcześniej ustawy – Prawo lotnicze jest wprowadzenie działu VIa całkowicie poświęconego bezzałogowym statkom powietrznym. Zawarto w nim m.in. rozdział 2, dotyczący stref geograficznych dla bezzałogowych statków powietrznych, oraz rozdział 6, odnoszący się do zapobiegania bezprawnemu wykonywaniu operacji z użyciem systemu bezzałogowego statku powietrznego.

Przestrzeń powietrzna przeznaczona do wykonywania lotów statkami powietrznymi zgodnie z zapisami ustawy – Prawo lotnicze dzieli się na przestrzeń kontrolowaną i przestrzeń niekontrolowaną[22]. Struktura przestrzeni jest określona, w drodze rozporządzenia, przez ministra właściwego do spraw transportu, ale w porozumieniu z ministrem obrony narodowej i przy uwzględnieniu zasad wynikających z przepisów oraz umów międzynarodowych. Zgodnie z rozporządzeniem ministra infrastruktury z 27 grudnia 2018 r.[23] przestrzeń kontrolowana to taka, w której wszystkim statkom powietrznym zapewnia się służbę kontroli ruchu lotniczego (Air Traffic Control), na podstawie klasyfikacji Organizacji Międzynarodowego Lotnictwa Cywilnego (International Civil Aviation Organization). Ta służba gwarantuje separację pomiędzy statkami powietrznymi, służbę alarmową oraz służbę informacji powietrznej. W przestrzeni niekontrolowanej zapewnione są tylko służba alarmowa oraz służba informacji powietrznej, a separację

[19] *Ustawa z dnia 24 stycznia 2025 r. o zmianie ustawy – Prawo lotnicze oraz niektórych innych ustaw*.

[20] *Rządowy projekt ustawy o zmianie ustawy – Prawo lotnicze oraz niektórych innych ustaw*, druk nr 810, https://www.sejm.gov.pl/sejm10.nsf/PrzebiegProc.xsp?nr=810 [dostęp: 21.02.2025].

[21] *Rozporządzenie delegowane Komisji (UE) 2019/945 z dnia 12 marca 2019 r. w sprawie bezzałogowych systemów powietrznych oraz operatorów bezzałogowych systemów powietrznych z państw trzecich*; *Rozporządzenie wykonawcze Komisji Europejskiej (UE) 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych*.

[22] Artykuł 121 ust. 5 pkt 1 *Ustawy z dnia 3 lipca 2002 r. Prawo lotnicze*.

[23] *Rozporządzenie Ministra Infrastruktury z dnia 27 grudnia 2018 r. w sprawie struktury polskiej przestrzeni powietrznej oraz szczegółowych warunków i sposobu korzystania z tej przestrzeni*.

pomiędzy statkiem a innymi statkami powietrznymi wykonującymi przelot w tej przestrzeni samodzielnie zapewnia pilot statku powietrznego. W Polsce przestrzeń kontrolowana rozciąga się od pułapu FL095 do FL660 (Flight Level 660 – poziom lotu wynoszący 66000 stóp), przestrzeń niekontrolowana natomiast – od ziemi do pułapu FL095 (Flight Level 095 – poziom lotu wynoszący 9500 stóp). W przestrzeniach kontrolowanej i niekontrolowanej dla zapewnienia bezpieczeństwa lotów, efektywniejszego wykorzystania przestrzeni powietrznej oraz optymalizacji zarządzania ruchem lotniczym wydziela się dodatkowo elementy stałe i elastyczne przestrzeni powietrznej. Elementy stałe to takie, których granice poziome i pionowe są określone i niezmienne. Należą do nich np.: drogi lotnicze (Airways, AWY), strefy kontrolowane lotnisk cywilnych (Control Zones, CTR), strefy zakazane (Prohibited Area, P). Elementy elastyczne, wydzielane tylko na czas określony, to np. strefy czasowo wydzielone (Temporary Segregated Areas, TSA) czy strefy ruchu lotniskowego (Aerodrome Traffic Zones, ATZ).

Wymienione elementy stałe i elastyczne powstały w czasach, gdy lotnictwo bezzałogowe nie było powszechne, a zasady wykonywania lotów obowiązujące w tych elementach były dostosowane do lotnictwa załogowego. Gwałtowny rozwój lotnictwa bezzałogowego spowodował konieczność uporządkowania struktury przestrzeni powietrznej na potrzeby wykonywania operacji bezzałogowych. Wobec braku odpowiednich zapisów w polskich ustawach i rozporządzeniach na mocy wytycznych Prezesa Urzędu Lotnictwa Cywilnego rozpoczęto wyznaczanie stref geograficznych dla systemów bezzałogowych statków powietrznych[24]. Nowelizacja ustawy – Prawo lotnicze pozwoliła na zapis treści tych wytycznych w rozdziale 2 ustawy. Zgodnie z nowymi przepisami za wyznaczenie strefy geograficznej odpowiada Polska Agencja Żeglugi Powietrznej (dalej: Agencja), która określa okres obowiązywania strefy, obszar strefy geograficznej oraz warunki, na jakich należy wykonywać loty bezzałogowymi statkami powietrznymi w danej strefie[25].

Zgodnie z nowymi przepisami wniosek o wyznaczenie strefy geograficznej może złożyć uprawniony podmiot, którym jest:

1) organ administracji publicznej, organ Sił Zbrojnych Rzeczypospolitej Polskiej, przewodniczący Państwowej Komisji Badania

[24] *Wytyczne nr 17/2023 Prezesa Urzędu Lotnictwa Cywilnego z dnia 6 czerwca 2023 r. w sprawie wyznaczania stref geograficznych dla systemów bezzałogowych statków powietrznych*. Wytyczne te zostały zaktualizowane w dokumencie z 21 lutego 2025 r.

[25] Artykuł 156h ust. 13 *Ustawy z dnia 3 lipca 2002 r. Prawo lotnicze.*

Wypadków Lotniczych, przewodniczący Komisji Badania Wypadków Lotniczych Lotnictwa Państwowego, Dyrektor Generalny Państwowego Gospodarstwa Leśnego Lasy Państwowe, podmiot uprawniony do wykonywania ratownictwa wodnego, podmiot uprawniony do wykonywania ratownictwa górskiego i dyrektor Rządowego Centrum Bezpieczeństwa – w przypadku konieczności zabezpieczenia przestrzeni powietrznej w celu realizacji zadań ustawowych;

2) zarządzający IK, w tym lotniczą, morską, kolejową lub energetyczną, lub terenem górniczym – w przypadku konieczności zabezpieczenia przestrzeni powietrznej w celu wykonania obowiązków tego zarządzającego;
3) organizator ćwiczeń, treningów, zawodów, pokazów lotniczych lub przelotów okolicznościowych – w przypadku konieczności zabezpieczenia przestrzeni powietrznej na potrzeby wykonania lotów w czasie ćwiczeń, treningów, zawodów, pokazów lotniczych lub przelotów okolicznościowych;
4) operator systemu bezzałogowego statku powietrznego zamierzający wykonywać operację w kategorii „szczególnej", w przypadku gdy konieczność wyznaczenia strefy geograficznej wynika z zezwolenia na operację, certyfikatu LUC, scenariusza standardowego lub krajowego scenariusza standardowego;
5) uznany podmiot, który prowadzi szkolenie praktyczne i ocenę umiejętności praktycznych pilota bezzałogowego statku powietrznego do wykonywania operacji w kategorii „szczególnej" i producent systemów bezzałogowych statków powietrznych[26].

Powyższe zapisy znowelizowanej ustawy zezwalają operatorowi IK na wyznaczenie dronowej strefy geograficznej nad obszarem, na którym znajduje się chroniony obiekt IK.

Rodzaje stref geograficznych, szczegółowe warunki i sposób korzystania z nich określi minister właściwy do spraw transportu na drodze rozporządzenia. Aktualnie w Polsce wyróżnia się następujące rodzaje stref geograficznych:

1) DRA-P – strefę, w której operacje z użyciem systemów bezzałogowych statków powietrznych nie mogą być wykonywane, z wyjątkiem operacji wykonywanych na warunkach określonych przez

[26] Artykuł 156h ust. 4 *Ustawy z dnia 3 lipca 2002 r. Prawo lotnicze.*

Agencję, Dowódcę Generalnego Rodzaju Sił Zbrojnych, Dowódcę Operacyjnego Rodzajów Sił Zbrojnych, Komendanta Głównego Żandarmerii Wojskowej, Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Agencji Wywiadu, Szefa Centralnego Biura Antykorupcyjnego, Szefa Służby Kontrwywiadu Wojskowego, Szefa Służby Wywiadu Wojskowego, Komendanta Głównego Policji, Komendanta Głównego Straży Granicznej, Dyrektora Generalnego Służby Więziennej, Szefa Krajowej Administracji Skarbowej, Komendanta Służby Ochrony Państwa lub Komendanta Głównego Państwowej Straży Pożarnej – na warunkach określonych przez Agencję;

2) DRA-R – strefę ograniczoną dla systemów bezzałogowych statków powietrznych, w której operacje z użyciem systemów bezzałogowych statków powietrznych mogą być wykonywane za zgodą i na warunkach określonych przez Agencję lub podmiot uprawniony, na wniosek którego strefa geograficzna została wyznaczona, w tym:
   a) DRA-RH – strefę ograniczoną dla systemów bezzałogowych statków powietrznych o wysokim prawdopodobieństwie uzyskania zgody zarządzającego strefą geograficzną na przeprowadzenie operacji,
   b) DRA-RM – strefę ograniczoną dla systemów bezzałogowych statków powietrznych o średnim prawdopodobieństwie uzyskania zgody zarządzającego strefą geograficzną na przeprowadzenie operacji,
   c) DRA-RL – strefę ograniczoną dla systemów bezzałogowych statków powietrznych o niskim prawdopodobieństwie uzyskania zgody zarządzającego strefą geograficzną na przeprowadzenie operacji;
3) DRA-T – strefę ograniczoną dla systemów bezzałogowych statków powietrznych, w której operacje z użyciem systemów bezzałogowych statków powietrznych mogą być wykonywane wyłącznie z użyciem systemów bezzałogowych statków powietrznych spełniających wymagania techniczne wskazane przez Agencję oraz na warunkach określonych przez Agencję, dla strefy DRA-T dopuszcza się wprowadzenie dodatkowych warunków wykonywania operacji, w tym obowiązku uzyskania zgody zarządzającego strefą geograficzną;
4) DRA-I – strefę informacyjną dla bezzałogowych statków powietrznych, zawierającą informacje konieczne dla zapewnienia

bezpieczeństwa wykonywania operacji przy użyciu systemów bezzałogowych statków powietrznych, w tym ostrzeżenia nawigacyjne[27].

Znowelizowana ustawa – Prawo lotnicze wprowadza także zapisy mające na celu umożliwienie zniszczenia, unieruchomienia bezzałogowego statku powietrznego lub przejęcia nad nim kontroli w przypadkach, gdy pilot wykonuje operację lotniczą w taki sposób, że przebieg operacji lub działanie bezzałogowego statku powietrznego:

1) zagraża lub może zagrozić życiu lub zdrowiu ludzi lub zwierząt,
2) stwarza lub może stworzyć zagrożenie dla chronionych obiektów, urządzeń lub obszarów,
3) zakłóca lub może zakłócić przebieg imprezy masowej albo zagraża bezpieczeństwu jej uczestników,
4) stwarza lub może stworzyć uzasadnione podejrzenie, że może zostać użyty jako środek ataku terrorystycznego,
5) stwarza lub może stworzyć zagrożenie bezpieczeństwa ruchu lotniczego, statku powietrznego lub życia lub zdrowia załogi lub pasażerów znajdujących się na jego pokładzie,
6) utrudnia lub może utrudnić ruch lotniczy lub powoduje lub może spowodować jego wstrzymanie lub ograniczenie[28].

Bezzałogowy statek powietrzny może być także zniszczony, unieruchomiony lub nad jego lotem może zostać przejęta kontrola, jeśli wbrew zakazowi wykonuje operację w strefie geograficznej ustanowionej nad: chronionymi obiektami Sił Zbrojnych RP oraz jednostek organizacyjnych podległych lub podporządkowanych ministrowi obrony narodowej lub przez niego nadzorowanych lub obiektami, urządzeniami lub obszarami istotnymi dla bezpieczeństwa lub obronności państwa, bezpieczeństwa publicznego lub nienaruszalności granicy państwowej[29].

Wymienione zapisy znowelizowanej ustawy wprowadzają duże zmiany w odniesieniu do bezpieczeństwa obiektów IK. Do czasu nowelizacji prawo pozwalało na detekcję bezzałogowych statków powietrznych, ale nie dawało operatorowi narzędzi pozwalających na neutralizację statków naruszających strefę geograficzną wyznaczoną nad obiektami chronionymi

[27] *Wytyczne nr 4/2025 Prezesa Urzędu Lotnictwa Cywilnego z dnia 21 lutego 2025 r. w sprawie wyznaczania stref geograficznych dla systemów bezzałogowych statków powietrznych.*

[28] Artykuł 156ze ust. 1 pkt 1 *Ustawy z dnia 3 lipca 2002 r. Prawo lotnicze.*

[29] Artykuł 156ze ust. 1 pkt 2 *Ustawy z dnia 3 lipca 2002 r. Prawo lotnicze*.

tą strefą. Z powodu braku podstaw prawnych oraz przede wszystkim z obawy przed odpowiedzialnością za potencjalne straty spowodowane neutralizacją bezzałogowego statku powietrznego wielu operatorów IK nie instalowało systemów detekcji i neutralizacji tych statków. Znowelizowana ustawa jednoznacznie wskazuje na pilota lub operatora statku powietrznego wykonującego operację w sposób naruszający przepisy prawa jako odpowiedzialnego za szkody powstałe wskutek neutralizacji statku powietrznego[30].

W przypadku gdy bezzałogowy statek powietrzny:

- zagraża lub może zagrozić życiu lub zdrowiu ludzi lub zwierząt,
- stwarza lub może stworzyć zagrożenie dla chronionych obiektów, urządzeń lub obszarów,
- stwarza lub może stworzyć uzasadnione podejrzenie, że może zostać użyty jako środek ataku terrorystycznego,
- stwarza lub może stworzyć zagrożenie bezpieczeństwa ruchu lotniczego, statku powietrznego lub życia lub zdrowia załogi lub pasażerów znajdujących się na jego pokładzie,
- utrudnia lub może utrudnić ruch lotniczy lub powoduje lub może spowodować jego wstrzymanie lub ograniczenie

do zniszczenia, unieruchomienia lub przejęcia kontroli nad statkiem są uprawnieni funkcjonariusze Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, Centralnego Biura Antykorupcyjnego, Policji, Straży Granicznej, Służby Ochrony Państwa, Służby Celno-Skarbowej, Służby Więziennej, Straży Marszałkowskiej, inspektorzy Biura Nadzoru Wewnętrznego, żołnierze zawodowi wyznaczeni na stanowiska służbowe w Służbie Kontrwywiadu Wojskowego albo Służbie Wywiadu Wojskowego, żołnierze Żandarmerii Wojskowej i Sił Zbrojnych Rzeczypospolitej Polskiej, pracownicy służby ochrony lotniska, strażnicy leśni, pracownicy ochrony specjalistycznych uzbrojonych formacji ochronnych, a także pracownicy wewnętrznych służb ochrony działających na terenach jednostek organizacyjnych podległych lub podporządkowanych ministrowi obrony narodowej lub przez niego nadzorowanych[31].

Znowelizowana ustawa przewiduje kary za naruszenie przepisów dotyczących operacji z użyciem bezzałogowych statków powietrznych. W Dziale XIa – Administracyjne kary pieniężne – dodano zapisy zezwalające

[30] Artykuł 156ze ust. 4 *Ustawy z dnia 3 lipca 2002 r. Prawo lotnicze.*

[31] Artykuł 156ze ust. 2 *Ustawy z dnia 3 lipca 2002 r. Prawo lotnicze.*

na nałożenie kary na każdego, kto wykonuje operacje z użyciem systemu bezzałogowego statku powietrznego niezgodnie z warunkami wykonywania operacji w danej strefie geograficznej. Wysokość takiej kary to 10 000 zł za każde naruszenie.

Kolejną ważną nowelizacją jest zmiana ustawy z 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej[32]. Poszerzono w niej katalog środków przymusu bezpośredniego o zniszczenie albo unieruchomienie bezzałogowego statku powietrznego albo przejęcie kontroli nad jego lotem[33]. Ustawa ta została także uzupełniona o wskazanie środków neutralizacji bezzałogowego statku powietrznego, do których zaliczono:

1) urządzenie wykorzystujące lub zakłócające fale radiowe,
2) siatkę obezwładniającą,
3) inne bezzałogowe statki powietrzne,
4) pociski niepenetrujące lub inne przedmioty miotane za pomocą przeznaczonych do tego urządzeń oraz za pomocą broni palnej i broni pneumatycznej,
5) urządzenia emitujące skumulowaną wiązkę energii lub fal elektromagnetycznych[34].

Lista środków zawiera wszystkie znane obecnie metody neutralizacji bezzałogowych statków powietrznych.

Rekomendacje Rządowego Centrum Bezpieczeństwa dotyczące oceny skuteczności systemów detekcji i neutralizacji bezzałogowych statków powietrznych

W związku z doniesieniami o wykorzystaniu bezzałogowych platform do paraliżu pracy systemów technicznych odpowiedzialnych za ciągłość działania IK[35], niepokojenia personelu obiektu[36] czy wręcz atakach z użyciem

[32] *Ustawa z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej*.

[33] Tamże, art. 11.

[34] Tamże, art. 33a ust. 2.

[35] *Drones paralyzed Stockholm-Arlanda Airport…*; S. Lyngaas, *Drone at Pennsylvania electric substation…*

[36] H. Altman, *Nuclear Power Plants Report Massive Uptick In Drone Sightings*, The Warzone, 21.12.2024, https://www.twz.com/news-features/massive-uptick-in-official-drone-sightings-by-nuclear-power-plants [dostęp: 21.02.2025].

materiałów wybuchowych[37] operatorzy IK powinni rozważyć budowę systemów detekcji i neutralizacji bezzałogowych statków powietrznych.

Proces budowy systemu detekcji i neutralizacji bezzałogowych statków powietrznych rozpoczyna się od analizy ryzyka zagrożeń systemu lub obiektu, dla którego źródłem zagrożeń są platformy bezzałogowe. Jeśli operator IK uzna, że chroniony przez niego system lub obiekt jest podatny na atak, to budowa systemu detekcji i neutralizacji jest nieodzowna.

Systemy detekcji są zbudowane z wielu urządzeń wykorzystujących różne metody wykrywania platform bezzałogowych[38]. Najprostszą i wydaje się najczęściej wykorzystywaną metodą detekcji jest wykrywanie komunikacji pomiędzy lecącą platformą a stacją naziemną. Jest ona uniwersalna, ponieważ można w jej ramach zastosować urządzenia detekcyjne zarówno stacjonarne, jak i przenośne. Zaawansowane urządzenia wykorzystujące algorytmy AI potrafią na podstawie pomiaru charakterystyki sygnału komunikacji określić model statku powietrznego[39]. Te łatwe w konstrukcji urządzenia działają na zasadzie wskaźnika wydającego sygnał dźwiękowy w momencie detekcji lecącego statku. Ich wadą jest brak możliwości detekcji bezzałogowych statków lecących w ciszy radiowej, np. sterowanych za pomocą światłowodu, a także brak możliwości detekcji platform, których komunikacja odbywa się na częstotliwościach nieobsługiwanych przez urządzenie detekcyjne.

Kolejna metoda detekcji wykorzystuje urządzenia radarowe. Jej zaletą jest szeroki zasięg radaru – jego dystans detekcji znacznie przewyższa odległości, na których można wykryć bezzałogowca innymi metodami. Prawdopodobieństwo wykrycia statku powietrznego zależy jednak od kilku czynników, m.in. od wielkości wykrywanego obiektu oraz od wysokości, na której się on porusza[40]. Nowoczesne systemy radarowe wspomagane algorytmami AI potrafią określić, czy śledzony obiekt to platforma bezzałogowa czy ptak. Zaletą opisywanej metody jest także możliwość wykrycia obiektu bez względu na porę dnia lub nocy. Wady detekcji radarowej to

[37] L. Kelly, *Ukrainian drone strikes trigger fires*...

[38] J. Łukasiewicz, M. Piekarski, M. Kluczyński, *Bezpieczeństwo infrastruktury krytycznej*...

[39] M.F. Al-Sa'd i in., *RF-based drone detection and identification using deep learning approaches: An initiative towards a large open-source drone database*, „Future Generation Computer Systems" 2019, t. 100, s. 86–97. https://doi.org/10.1016/j.future.2019.05.007.

[40] M. Ezuma i in., *Comparative Analysis of Radar Cross Section Based UAV Classification Techniques*, preprint, https://arxiv.org/abs/2112.09774 [dostęp: 21.02.2025]. https://doi.org/10.48550/arXiv.2112.09774.

duży koszt urządzenia oraz niemożność wykrycia lecącego obiektu w przypadku, gdy chowa się on za przeszkodami terenowymi lub leci bardzo nisko nad ziemią.

Coraz częściej stosowana jest metoda akustyczna[41]. Koszt detektora akustycznego jest niższy niż detektora radarowego i, co ważniejsze, ten detektor jest pasywny, tzn. nie emituje sygnału w żadnej formie, by dokonać detekcji. Metoda ta staje się coraz popularniejsza w systemach detekcji dronów w Ukrainie, gdzie duże platformy wykorzystywane do przenoszenia dużych ładunków wybuchowych są napędzane głośnymi silnikami spalinowymi. Wadą metody akustycznej może być nieskuteczna detekcja w miejscu, w którym występują inne źródła hałasu niż tylko platforma bezzałogowa.

Ostatnią metodą detekcji jest analiza obrazu rejestrowanego przez kamerę pracującą w świetle widzialnym lub w podczerwieni[42]. Taka kamera jest wyposażona w algorytmy AI pozwalające na rozpoznanie kształtu lecącego obiektu. Kamery działające w podczerwieni analizują jego temperaturę, co pozwala na rozróżnienie między bezzałogową platformą a ptakami. Wadą kamer działających w obszarze widzialnym jest brak możliwości rejestracji obrazu w warunkach braku światła, np. w nocy. Z kolei mankamentem kamer działających w podczerwieni jest brak możliwości detekcji obiektu w przypadku, gdy ten jest wyposażony w izolatory termiczne.

Wszystkie opisane metody wykorzystywane w budowie systemu detekcji pozwalają na wykrywanie platform bezzałogowych w różnych warunkach. Metoda oceny skuteczności tego systemu została opisana w przygotowanym przez RCB dokumencie będącym załącznikiem do Narodowego Programu Ochrony Infrastruktury Krytycznej 2023 (NPOIK)[43]. Zakłada ona badanie prawdopodobieństwa detekcji przez poszczególne urządzenia systemu. Prawdopodobieństwo to określa się na podstawie

[41] H. Altman, T. Rogoway, *Ukraine's Acoustic Drone Detection Network Eyed By U.S. As Low-Cost Air Defense Option*, The Warzone, 24.07.2024, https://www.twz.com/air/ukraines-acoustic-drone-detection-network-eyed-by-u-s-as-low-cost-air-defense-option [dostęp: 21.02.2025].

[42] Y. Wu, Y. Sui, G. Wang, *Vision-Based Real-Time Aerial Object Localization and Tracking for UAV Sensing System*, „IEEE Access" 2017, t. 5, s. 23969–23978. https://doi.org/10.1109/ACCESS.2017.2764419.

[43] *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.

zliczeń skutecznych detekcji na 100 prób. Próby te muszą się odbywać w różnych warunkach, tzn. bada się prawdopodobieństwo wykrycia dla danej lokalizacji w różnych warunkach pogodowych, w warunkach występowania zewnętrznych źródeł promieniowania elektromagnetycznego, dla różnych typów bezzałogowych statków powietrznych, dla różnych scenariuszy ataku, dla różnych kompetencji personelu ochrony. Gdy zna się prawdopodobieństwo detekcji każdego urządzenia w danych warunkach, można wyznaczyć całkowite prawdopodobieństwo detekcji przez cały system za pomocą wzoru:

$$P_{CAŁK\_D} = 1 - (1 - P_{1D})(1 - P_{2D})(1 - P_{3D})(1 - P_{4D}) \ldots (1 - P_{ND})$$

gdzie:

$P_{CAŁK\_D}$ – prawdopodobieństwo detekcji przez cały system,
P_{1D} – prawdopodobieństwo detekcji przez pierwsze urządzenie detekcyjne,
P_{2D} – prawdopodobieństwo detekcji przez drugie urządzenie detekcyjne,
P_{3D} – prawdopodobieństwo detekcji przez trzecie urządzenie detekcyjne,
P_{4D} – prawdopodobieństwo detekcji przez czwarte urządzenie detekcyjne,
P_{ND} – prawdopodobieństwo detekcji przez n-te urządzenie detekcyjne.

Zadaniem operatora IK jest zbudowanie takiego systemu detekcji, by wartość prawdopodobieństwa $P_{CAŁK\_D}$ była wyższa niż założona przez operatora wartość progowa.

Do budowy systemów neutralizacji dronów stosuje się również urządzenia działające na różnych zasadach, aby zwiększyć prawdopodobieństwo neutralizacji. Jedną z najbardziej popularnych metod jest zagłuszenie sygnału komunikacji między bezzałogową platformą a stacją naziemną. Zagłuszenie odbywa się przez emisję w kierunku lecącej platformy fali elektromagnetycznej o takiej samej częstotliwości jak częstotliwość wykorzystywana do komunikacji. Wadą tego rozwiązania jest pojawiający się coraz częściej mechanizm hoppingowy, który polega na zmianie częstotliwości komunikacji pomiędzy platformą a stacją naziemną w czasie lotu. Urządzenie zagłuszające musi zatem emitować fale o różnych częstotliwościach, by przerwać komunikację. Takie urządzenie nie jest skuteczne w walce z bezzałogową platformą lecącą w ciszy radiowej albo w trybie automatycznym lub autonomicznym.

Inna metoda to zagłuszenie lub zafałszowanie sygnału nawigacji satelitarnej[44], czego rezultatem będzie pogubienie się platformy bezzałogowej w przestrzeni powietrznej lub przelot platformy do miejsca wskazanego zafałszowanym sygnałem nawigacji satelitarnej. Rozwiązanie to okaże się nieskuteczne w przypadku zastosowania na bezzałogowej platformie urządzeń do nawigacji zliczeniowej, zwanej inercyjną. W takim przypadku bezzałogowiec nawiguje na podstawie obliczeń, koryguje swoje położenie geograficzne przez okresowe odczyty położenia z satelit.

Trzecią metodą jest stosowanie systemów siatkowych, które można wystrzelić ze specjalnych urządzeń pod nazwą *net guns*, w które jest wyposażony personel ochrony, lub z urządzeń przenoszonych przez bezzałogowce obsługiwane przez personel ochrony[45]. Wadą tej metody jest konieczność oddania strzału z bliskiej odległości od platformy.

Kolejną metodą neutralizacji jest zniszczenie bezzałogowego statku powietrznego przez wyemitowanie w jego kierunku impulsu elektromagnetycznego o dużej energii[46]. Taki impuls niszczy elementy półprzewodnikowe układów elektronicznych zamontowanych na platformie. Wadą tego rozwiązania jest możliwość umieszczenia wrażliwych elementów elektronicznych w klatce Faradaya, czyli w opakowaniu, które izoluje urządzenia elektroniczne od wpływu zewnętrznych pól elektromagnetycznych.

Do zwalczania systemów bezzałogowych coraz częściej stosuje się systemy laserowe. Laserów można użyć jako źródeł światła, które świecąc wprost w obiektyw kamery bezzałogowca, uniemożliwiają pilotowi prawidłowe sterowanie nim. Coraz częściej stosuje się też lasery do fizycznego zniszczenia platformy przez spalenie[47]. Systemy laserowe nie są popularne,

[44] M. Sahmoudi, M.G. Amin, *Robust tracking of weak GPS signals in multipath and jamming environments*, „Signal Processing" 2009, t. 89, nr 7, s. 1320–1333. https://doi.org/10.1016/j.sigpro.2009.01.001.

[45] D. Hambling, *Webslingers: How Net-Launching Drones Are Downing Russian Quadcopters*, Forbes, 12.11.2024, https://www.forbes.com/sites/davidhambling/2024/11/12/webslingers-how-net-launching-drones-are-downing-russian-quadcopters/ [dostęp: 21.02.2025].

[46] O.D. Razooqi, A.H. Ali, *Drones neutralized by utilize electromagnetic pulse (EMP) system*, w: *2022 5th International Conference on Engineering Technology and its Applications (IICETA)*, Al-Najaf 2022, s. 487–492. https://doi.org/10.1109/IICETA54559.2022.9888673.

[47] J. Saballa, *Ukraine Announces Successful Use of First Laser Weapon on Battlefield*, The Defense Post, 6.02.2025, https://thedefensepost.com/2025/02/06/ukraine-laser-weapon-battlefield/ [dostęp: 21.02.2025].

ponieważ wymagają dużych gabarytowo i wydajnych źródeł energii, a ich skuteczność w znacznym stopniu zależy od przejrzystości powietrza[48].

Żaden z opisanych sposobów nie gwarantuje neutralizacji, dlatego należy budować systemy wykorzystujące różne metody. Propozycja sposobu oceny skuteczności systemu neutralizacji platform bezzałogowych została opisana we wspomnianym załączniku do NPOIK 2023[49]. Metoda zakłada badanie prawdopodobieństwa neutralizacji z wykorzystaniem poszczególnych urządzeń systemu. Prawdopodobieństwo to określa się na podstawie zliczeń skutecznych neutralizacji na 100 prób. Próby te muszą się odbywać w różnych warunkach, tzn. bada się prawdopodobieństwo neutralizacji dla danej lokalizacji w różnych warunkach pogodowych, dla różnych typów bezzałogowych statków powietrznych, dla różnych scenariuszy ataku, dla różnych kompetencji personelu ochrony. Gdy zna się prawdopodobieństwo neutralizacji każdego urządzenia systemu w danych warunkach, można wyznaczyć całkowite prawdopodobieństwo neutralizacji przez cały system za pomocą wzoru:

$$P_{CAŁK\_N} = 1 - (1 - P_{1N})(1 - P_{2N})(1 - P_{3N})(1 - P_{4N}) \ldots (1 - P_{NN})$$

gdzie:

$P_{CAŁK\_N}$ – prawdopodobieństwo neutralizacji przez cały system,
P_{1N} – prawdopodobieństwo neutralizacji przez pierwsze urządzenie neutralizacyjne,
P_{2N} – prawdopodobieństwo neutralizacji przez drugie urządzenie neutralizacyjne,
P_{3N} – prawdopodobieństwo neutralizacji przez trzecie urządzenie neutralizacyjne,
P_{4N} – prawdopodobieństwo neutralizacji przez czwarte urządzenie neutralizacyjne,
P_{NN} – prawdopodobieństwo neutralizacji przez n-te urządzenie neutralizacyjne.

Zadaniem operatora infrastruktury krytycznej jest zbudowanie takiego systemu neutralizacji, by wartość prawdopodobieństwa $P_{CAŁK\_N}$ była wyższa niż założona przez operatora minimalna wartość progowa.

[48] R. Ceder, *US Navy hits drone with HELIOS laser in successful test*, Navy Times, 4.02.2025, https://www.navytimes.com/news/your-navy/2025/02/04/us-navy-hits-drone-with-helios-laser-in-successful-test/ [dostęp: 21.02.2025]; M. Knight, *Ukraine says it has a laser that can shoot down aircraft a mile away. It's called 'Tryzub'*, CNN, 18.12.2024, https://edition.cnn.com/2024/12/18/europe/ukrainian-tryzub-laser-weapon-intl-latam/index.html [dostęp: 21.02.2025].

[49] *Standardy służące zapewnieniu sprawnego funkcjonowania...*

Podsumowanie

Nowelizacja polskiej ustawy – Prawo lotnicze była wyczekiwana przez operatorów IK. Zapewnia im ona duże możliwości i podstawy formalnoprawne do zwalczania dronów, które w sposób nieautoryzowany naruszają strefę geograficzną wyznaczoną nad obiektem IK. Nowe przepisy wskazują jednoznacznie na pilota bezzałogowej platformy naruszającego zasady wykonywania lotów jako na osobę, która ponosi konsekwencje potencjalnego upadku drona, w którego wyniku zostaną poniesione straty. Wprowadzone w tym zakresie kary można ocenić jako bardzo dotkliwe. Ponadto nowelizacja ustawy o środkach przymusu bezpośredniego i broni palnej poszerza katalog tych środków o urządzenia, które można wykorzystać do zwalczania platform bezzałogowych. Omawiana nowelizacja ustawy – Prawo lotnicze powinna zostać uzupełniona o nowelizację ustawy o zarządzaniu kryzysowym, by zobowiązać operatorów IK do prowadzenia analiz ryzyka zagrożeń dla obiektów i w konsekwencji do budowy systemów detekcji i neutralizacji bezzałogowych statków powietrznych.

Wobec gwałtownego rozwoju technologii bezzałogowej, pojawienia się amunicji do dronów, coraz powszechniej nabywanej umiejętności pilotażu bezzałogowych statków powietrznych zarówno instytucje unijne, jak i państwa członkowskie UE powinny zachęcać instytucje badawcze, laboratoria, centra technologiczne oraz prywatnych inwestorów do lokowania środków finansowych w badania i rozwój nowoczesnych systemów detekcji i neutralizacji platform bezzałogowych. Na podstawie obserwacji konfliktu zbrojnego w Ukrainie można uznać, że aktualne systemy detekcji i neutralizacji nie gwarantują bezpieczeństwa chronionych obiektów.

Technologiczna przepaść między możliwościami atakowania obiektów IK za pomocą bezzałogowych statków powietrznych a systemami do ich wykrywania i neutralizacji się powiększa. Do takiego samego wniosku można dojść po porównaniu kosztów pozyskania bezzałogowca zdolnego do ataku na obiekt IK z kosztami pozyskania, obsługi i serwisu systemu antydronowego zmniejszającego ryzyko ataku do poziomu akceptowalnego dla operatora IK. Nie można pozwolić, aby ten dystans rósł. Zwiększenie odporności obiektów IK na ataki z wykorzystaniem bezzałogowych systemów statków powietrznych zależy od działań operatorów IK, którzy otrzymali postulowane od lat ramy prawne i organizacyjne.

Bibliografia

Al-Sa'd M.F., Al-Ali A., Mohamed A., Khattab T., Erbad A., *RF-based drone detection and identification using deep learning approaches: An initiative towards a large open-source drone database*, „Future Generation Computer Systems" 2019, t. 100, s. 86–97. https://doi.org/10.1016/j.future.2019.05.007.

Ezuma M., Anjinappa C.K., Semkin V., Guvenc I., *Comparative Analysis of Radar Cross Section Based UAV Classification Techniques*, preprint, https://arxiv.org/abs/2112.09774 [dostęp: 21.02.2025]. https://doi.org/10.48550/arXiv.2112.09774.

Koulouris C., Dimitrios P., Al-Darraji I., Tsaramirsis G., Khadidos A.O., Khadidos A.O., Papageorgasi P., *A Survey Study and Comparison of Drones Communication Systems*, w: *Flexible Electronics for Electric Vehicles. Proceedings of the 3rd International Conference, FlexEV 2022*, S.K. Goyal, D.K. Palwalia, R. Tiwari, Y. Gupta (red.), seria: „Lecture Notes in Electrical Engineering", t. 1065, Springer, Singapore. https://doi.org/10.1007/978-981-99-4795-9_33.

Łukasiewicz J., Piekarski M., Kluczyński M., *Bezpieczeństwo infrastruktury krytycznej wobec zagrożeń ze strony platform bezzałogowych*, Raport PTBN, t. 2, Polskie Towarzystwo Bezpieczeństwa Narodowego 2021.

Razooqi O.D., Ali A.H., *Drones neutralized by utilize electromagnetic pulse (EMP) system*, w: *2022 5th International Conference on Engineering Technology and its Applications (IICETA)*, Al-Najaf 2022, s. 487–492. https://doi.org/10.1109/IICETA54559.2022.9888673.

Sahmoudi M., Amin M.G., *Robust tracking of weak GPS signals in multipath and jamming environments*, „Signal Processing" 2009, t. 89, nr 7, s. 1320–1333. https://doi.org/10.1016/j.sigpro.2009.01.001.

Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje, załącznik 1 do Narodowego Programu Ochrony Infrastruktury Krytycznej, Rządowe Centrum Bezpieczeństwa, 2023.

Szlachter D., *Terroryzm w Polsce i kierunki jego rozwoju. Wyniki badań ankietowych (skrócony raport)*, „Terroryzm – studia, analizy, prewencja" 2022, nr 2, s. 148–176. https://doi.org/10.4467/27204383TER.22.022.16342.

Wu Y., Sui Y., Wang G., *Vision-Based Real-Time Aerial Object Localization and Tracking for UAV Sensing System*, „IEEE Access" 2017, t. 5, s. 23969–23978. https://doi.org/10.1109/ACCESS.2017.2764419.

Źródła internetowe

Altman H., *Nuclear Power Plants Report Massive Uptick In Drone Sightings*, The Warzone, 21.12.2024, https://www.twz.com/news-features/massive-uptick-in-official-drone-sightings-by-nuclear-power-plants [dostęp: 21.02.2025].

Altman H., Rogoway T., *Ukraine's Acoustic Drone Detection Network Eyed By U.S. As Low-Cost Air Defense Option*, The Warzone, 24.07.2024, https://www.twz.com/air/ukraines-acoustic-drone-detection-network-eyed-by-u-s-as-low-cost-air-defense-option [dostęp: 21.02.2025].

Barrett B., *A Drone Tried to Disrupt the Power Grid. It Won't Be the Last*, Wired, 5.11.2021, https://www.wired.com/story/drone-attack-power-substation-threat/ [dostęp: 21.02.2025].

Ceder R., *US Navy hits drone with HELIOS laser in successful test*, Navy Times, 4.02.2025, https://www.navytimes.com/news/your-navy/2025/02/04/us-navy-hits-drone-with-helios-laser-in-successful-test/ [dostęp: 21.02.2025].

Cheap and They Don't Snitch: Drones Are the New Drug Mules, RUSI, 5.01.2024, https://www.rusi.org/news-and-comment/in-the-news/cheap-and-they-dont-snitch-drones-are-new-drug-mules [dostęp: 21.02.2025].

Drone 'containing radiation' lands on roof of Japanese PM's office, The Guardian, 22.04.2015, https://www.theguardian.com/world/2015/apr/22/drone-with-radiation-sign-lands-on-roof-of-japanese-prime-ministers-office [dostęp: 21.02.2025].

Faulconbridge G., Kelly L., *Ukrainian drone strikes trigger fires at major oil and gas facilities in Russia*, Reuters, 3.02.2025, https://www.reuters.com/world/europe/ukraines-drone-attack-sparks-fire-forces-flight-suspensions-several-russian-2025-02-03/ [dostęp: 21.02.2025].

Hambling D., *Webslingers: How Net-Launching Drones Are Downing Russian Quadcopters*, Forbes, 12.11.2024, https://www.forbes.com/sites/davidhambling/2024/11/12/webslingers-how-net-launching-drones-are-downing-russian-quadcopters/ [dostęp: 21.02.2025].

It is still unclear whose drone is blocking 6 flights at Sofia Airport, Fakti.bg, 9.02.2025, https://fakti.bg/en/bulgaria/948414-it-is-still-unclear-whose-drone-is-blocking-6-flights-at-sofia-airport [dostęp: 21.02.2025].

Jam-Proof Fiber Optics for Drones: Revolutionizing Secure Communications, Linden Photonics Inc., 22.08.2024, https://www.lindenphotonics.com/jam-proof-fiber-optics-for-drones-revolutionizing-secure-communications [dostęp: 21.02.2025].

Knight M., *Ukraine says it has a laser that can shoot down aircraft a mile away. It's called 'Tryzub'*, CNN, 18.12.2024, https://edition.cnn.com/2024/12/18/europe/ukrainian-tryzub-laser-weapon-intl-latam/index.html [dostęp: 21.02.2025].

Lyngaas S., *Drone at Pennsylvania electric substation was first to 'specifically target energy infrastructure', according to federal law enforcement bulletin*, CNN, 4.11.2021, https://edition.cnn.com/2021/11/04/politics/drone-pennsylvania-electric-substation/index.html [dostęp: 21.02.2025].

McKenzie S., Mezzofiore G., *Police hunt drone pilots in unprecedented Gatwick Airport disruption*, CNN, 20.12.2018, https://edition.cnn.com/2018/12/20/uk/gatwick-airport-drones-gbr-intl/index.html [dostęp: 21.02.2025].

Saballa J., *Ukraine Announces Successful Use of First Laser Weapon on Battlefield, The Defense Post*, 6.02.2025, https://thedefensepost.com/2025/02/06/ukraine-laser-weapon-battlefield/ [dostęp: 21.02.2025].

Sweden drones: Sightings reported over nuclear plants and palace, BBC, 18.01.2022, https://www.bbc.com/news/world-europe-60035446 [dostęp: 21.02.2025].

Timeline: UAE under drone, missile attacks, Al Jazeera, 3.02.2022, https://www.aljazeera.com/news/2022/2/3/timeline-uae-drone-missile-attacks-houthis-yemen [dostęp: 21.02.2025].

Ukrainians Made an FPV With Fiber-Optic Cord Stretching For 41 km, Defence Express, 26.01.2025, https://en.defence-ua.com/industries/ukrainians_made_an_fpv_with_fiber_optic_cord_stretching_for_41_km-13327.html [dostęp: 21.02.2025].

Venezuela President Maduro survives 'drone assassination attempt', BBC, 5.08.2018, https://www.bbc.com/news/world-latin-america-45073385 [dostęp: 21.02.2025].

Wang B., *Ukraine's One Million FPV Drones Is Outnumbered by 5 Million Russian Drones*, Next Big Future, 27.01.2024, https://www.nextbigfuture.com/2024/01/ukraines-one-million-fpv-drones-will-be-outnumbered-by-5-million-russian-drones.html [dostęp: 21.02.2025].

Akty prawne

Rozporządzenie wykonawcze Komisji Europejskiej (UE) 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych (Dz. Urz. UE L 152/45 z 11.06.2019).

Rozporządzenie delegowane Komisji (UE) 2019/945 z dnia 12 marca 2019 r. w sprawie bezzałogowych systemów powietrznych oraz operatorów bezzałogowych systemów powietrznych z państw trzecich (Dz. Urz. UE L 152/1 z 11.06.2019).

Ustawa z dnia 24 stycznia 2025 r. o zmianie ustawy – Prawo lotnicze oraz niektórych innych ustaw (DzU z 2025 poz. 179).

Ustawa z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (t.j. DzU z 2024 poz. 383, ze zm.).

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. DzU z 2023 poz. 122, ze zm.).

Ustawa z dnia 3 lipca 2002 r. Prawo lotnicze (t.j. DzU z 2023 poz. 2110, ze zm.).

Rozporządzenie Ministra Infrastruktury z dnia 27 grudnia 2018 r. w sprawie struktury polskiej przestrzeni powietrznej oraz szczegółowych warunków i sposobu korzystania z tej przestrzeni (DzU z 2019 poz. 619).

Wytyczne nr 4/2025 Prezesa Urzędu Lotnictwa z dnia 21 lutego 2025 r. w sprawie wyznaczania stref geograficznych dla systemów bezzałogowych statków powietrznych (Dz. Urz. ULC z 2025 poz. 13).

Wytyczne nr 17/2023 Prezesa Urzędu Lotnictwa Cywilnego z dnia 6 czerwca 2023 r. w sprawie wyznaczania stref geograficznych dla systemów bezzałogowych statków powietrznych (Dz. Urz. ULC z 2023 poz. 42).

Wytyczne nr 15/2023 Prezesa Urzędu Lotnictwa Cywilnego z dnia 1 czerwca 2023 r. w sprawie sposobów wykonywania operacji przy użyciu systemów bezzałogowych statków powietrznych w związku z wejściem w życie przepisów rozporządzenia wykonawczego Komisji (UE) nr 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych (Dz. Urz. ULC z 2023 poz. 39).

Inne dokumenty

Rządowy projekt ustawy o zmianie ustawy – Prawo lotnicze oraz niektórych innych ustaw, druk nr 810, https://www.sejm.gov.pl/sejm10.nsf/PrzebiegProc.xsp?nr=810 [dostęp: 21.02.2025].

Dr Jędrzej Łukasiewicz

Doktor nauk fizycznych. Były pracownik Politechniki Poznańskiej, na której był zatrudniony na stanowisku adiunkta. Konstruktor i pilot bezzałogowych statków powietrznych. Instruktor w ośrodku szkolenia pilotażu dronów Politechniki Poznańskiej. Specjalizuje się w bezpieczeństwie obiektów infrastruktury krytycznej, dla których źródłem zagrożeń są bezzałogowe statki powietrzne. Autor metody oceny skuteczności systemów detekcji oraz neutralizacji bezzałogowych statków powietrznych. Metoda ta została opisana w Załączniku 1 do Narodowego Programu Ochrony Infrastruktury Krytycznej zatytułowanym *Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje*. Autor artykułów naukowych publikowanych w czasopismach o zasięgu międzynarodowym. Uczestnik prac zespołów resortowych wspierających administrację państwową w zwiększaniu odporności państwa na zagrożenia hybrydowe.

Kontakt: jedrzej.lukasiewicz@tlen.pl

Dr Damian Szlachter

Redaktor naczelny czasopisma naukowego ABW „Terroryzm – studia, analizy, prewencja". Członek komitetu sterującego unijnej grupy doradców ds. budowania odporności na zagrożenia (EU Protective Security Advisors). Ekspert narodowy w Dyrekcji Generalnej ds. Migracji i Spraw Wewnętrznych Komisji Europejskiej (Directorate-General for Migration and Home Affairs) w ramach grupy roboczej ds. ochrony antyterrorystycznej przestrzeni publicznych (Policy Group on Public Spaces Protection). Audytor krajowy kontroli jakości w zakresie ochrony lotnictwa cywilnego (Urzędu Lotnictwa Cywilnego). Uczestnik prac kilkunastu zespołów międzyresortowych oraz grup roboczych administracji państwowej, których zadaniem było budowanie odporności na zagrożenia terrorystyczne i hybrydowe obiektów strategicznych dla bezpieczeństwa państwa oraz infrastruktury krytycznej. Członek zespołu do spraw badania wyzwań inżynierii bezpieczeństwa obiektów budowlanych infrastruktury krytycznej przy Głównym Urzędzie Nadzoru Budowlanego. Autor blisko 40 artykułów naukowych oraz współautor kilku książek i raportów specjalistycznych na temat bezpieczeństwa wewnętrznego.

Kontakt: d.szlachter@abw.gov.pl

Terroryzm – studia, analizy, prewencja, 2025, wydanie specjalne: 195–218

https://doi.org/10.4467/27204383TER.25.007.21510

Artykuł

Polskie indywidualne środki ograniczające zastosowane wobec podmiotów gospodarczych w kontekście wojny w Ukrainie oraz sytuacji w Rosji i Białorusi

Polish individual restrictive measures applied to economic entities in the context of the war in Ukraine and the situation in Russia and Belarus

MARIUSZ CICHOMSKI
https://orcid.org/0000-0003-3707-7856
Ministerstwo Spraw Wewnętrznych i Administracji

KONRAD KACZOR
https://orcid.org/0009-0009-7182-4027
Autor niezależny

Abstrakt

Polska, podobnie jak kilka innych państw Unii Europejskiej, przyjęła indywidualne środki ograniczające w związku z agresją Federacji Rosyjskiej na Ukrainę w 2022 r. oraz naruszeniami praw człowieka wobec społeczeństwa obywatelskiego i opozycji demokratycznej w Rosji i Białorusi. Celem artykułu jest charakterystyka podmiotów gospodarczych objętych stosowanymi w Polsce środkami ograniczającymi. Uwzględniono rodzaj działalności prowadzonej przez te podmioty, państwa ich rejestracji oraz powiązania z Rosją lub Białorusią jako powód zamrożenia ich działalności na podstawie polskiej listy sankcyjnej oraz decyzji administracyjnych, na mocy których dokonano wpisu na tę listę. Jako przykład autorzy zanalizowali przypadek podmiotu gospodarczego

wpisanego na listę, z uwzględnieniem opisu przesłanek wpisu, ustalonego zakresu środków ograniczających oraz dodatkowych mechanizmów prawnych zastosowanych w celu minimalizowania negatywnych skutków dla państwa nakładającego te środki. Analiza przypadku pozwoliła odpowiedzieć na pytanie o zasadność wprowadzania indywidualnych środków ograniczających na poziomie krajowym oraz na pytanie, czy ich stosowanie może mieć znaczenie dla bezpieczeństwa dostaw surowców energetycznych, funkcjonowania infrastruktury przesyłowej i infrastruktury krytycznej.

Słowa kluczowe

środki ograniczające, lista sankcyjna, sankcje, wojna w Ukrainie

Abstract

Poland, like several other European Union countries, adopted restrictive measures in response to the Russian Federation's aggression against Ukraine in 2022, as well as serious human rights violations against civil society and the democratic opposition in Russia and Belarus. The aim of this article is to characterise the economic entities subject to the restrictive measures applied in Poland. The type of activities carried out by these entities, the countries of their registration and their links with Russia or Belarus were taken into account as reasons for freezing their activities on the basis of the Polish sanctions list and the administrative decisions by which the list was entered. As an example, the authors analysed the case of an economic entity listed on the sanctions list, taking into account both the rationale for its inclusion and the established scope of restrictive measures, as well as additional legal mechanisms implemented to minimise the negative effects of these measures. The case analysis allowed for answering the question of the legitimacy of introducing individual restrictive measures at the national level and whether the application of such measures can impact the security of energy resource supplies, the functioning of transmission infrastructure, and critical infrastructure.

Keywords

restrictive measures, sanctions list, sanctions, war in Ukraine

Środki ograniczające w Unii Europejskiej

Wprowadzone dotychczas pakiety środków ograniczających Unii Europejskiej związanych z agresją Federacji Rosyjskiej (FR) na Ukrainę (16 pakietów

na czas przygotowania artykułu) i wsparciem udzielonym w tym zakresie Rosji przez Białoruś, mają swoje podstawy prawne w art. 29 Traktatu o Unii Europejskiej[1]. Umożliwia on Radzie UE nakładanie środków ograniczających przeciwko rządom państw niebędących państwami członkowskimi UE, podmiotom niepaństwowym, np. podmiotom gospodarczym, a także osobom fizycznym w celu wywołania zmian w ich działaniach. Drugi fundament traktatowy stosowania przez UE środków ograniczających to art. 215 ust. 2 Traktatu o funkcjonowaniu Unii Europejskiej[2], zgodnie z którym Rada UE może przyjąć niezbędne środki w celu wykonania decyzji przyjętych wynikających z art. 29 Traktatu o Unii Europejskiej, aby zagwarantować ich jednolite stosowanie we wszystkich państwach członkowskich[3]. Odnosi się to do możliwości stosowania środków ograniczających o charakterze gospodarczym (sektorowym), jak zakazy przywozu z państw objętych tymi środkami określonych rodzajów produktów czy surowców, oraz o charakterze finansowym. Są to zwłaszcza stosowane w odniesieniu do konkretnych osób lub podmiotów gospodarczych zamrożenia środków finansowych i zasobów gospodarczych będących w posiadaniu tych osób lub podmiotów bądź znajdujących się pod ich kontrolą. Oddzielne zagadnienie stanowią sankcje dyplomatyczne, w tym zawieszenie oficjalnych wizyt, dwustronnej lub wielostronnej współpracy z UE, bojkot wydarzeń[4].

Problemem nie jest jednak znalezienie istotnych pod względem ekonomicznym słabych punktów państwa, wobec którego mają być stosowane środki ograniczające. Głębokość powiązań międzynarodowych jest na tyle duża, że stosunkowo łatwo można określić, jakie ograniczenia byłyby przez

[1] *Traktat o Unii Europejskiej* (wersja skonsolidowana) – Tytuł V – Postanowienia ogólne o działaniach zewnętrznych Unii i postanowienia szczególne dotyczące wspólnej polityki zagranicznej i bezpieczeństwa – Rozdział 2 – Postanowienia szczególne dotyczące wspólnej polityki zagranicznej i bezpieczeństwa – Sekcja 1 – Postanowienia wspólne – Artykuł 29 (dawny artykuł 15 TUE).

[2] *Traktat o funkcjonowaniu Unii Europejskiej* (wersja skonsolidowana) – Część 5 – Działania zewnętrzne Unii – Tytuł IV – Środki ograniczające – Artykuł 215 (dawny artykuł 301 Traktatu ustanawiającego Wspólnotę Europejską).

[3] Zob. 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. 95–96. https://doi.org/10.4467/27204383TER.24.003.19391; *Ogólne ramy dla sankcji unijnych*, Unia Europejska, https://eur-lex.europa.eu/PL/legal-content/summary/general-framework-for-eu-sanctions.html [dostęp: 20.02.2025].

[4] *Ogólne ramy dla sankcji unijnych*...

to państwo najbardziej odczuwalne. Przyjęcie środków ograniczających na poziomie UE wymaga jednak uzgodnienia tego między państwami członkowskimi, co jest dużym wyzwaniem nie tylko w wymiarze politycznym, lecz także gospodarczym. Stosowanie środków ograniczających o charakterze zarówno sektorowym, jak i indywidualnym wymaga ze strony każdego z państw członkowskich UE starannej analizy skutków wprowadzenia tych środków[5]. O złożoności procesu wprowadzania kolejnych restrykcji i jego stopniowalności świadczy wskazana wcześniej dotychczasowa liczba 16 tzw. pakietów sankcyjnych[6] wprowadzonych w związku z konfliktem w Ukrainie. Podstawą ich wprowadzenia była nowelizacja 3 głównych w tym zakresie aktów prawnych, tj. *Rozporządzenia Rady (WE) nr 765/2006 z dnia 18 maja 2006 r. dotyczącego środków ograniczających w związku z sytuacją na Białorusi i udziałem Białorusi w agresji Rosji wobec Ukrainy* (dalej: rozporządzenie 765/2006), *Rozporządzenia Rady (UE) nr 269/2014 z dnia 17 marca 2014 r. w sprawie środków ograniczających w odniesieniu do działań podważających integralność terytorialną, suwerenność i niezależność Ukrainy lub im zagrażających* (dalej: rozporządzenie 269/2014) oraz *Rozporządzenia Rady (UE) nr 833/2014 z dnia 31 lipca 2014 r. dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie* (dalej: rozporządzenie 833/2014).

Przykładem wspomnianej stopniowalności wprowadzania środków ograniczających mogą być restrykcje dotyczące rosyjskiego gazu płynnego (LPG). Dopiero *Rozporządzeniem Rady (UE) 2023/2878 z dnia 18 grudnia 2023 r. zmieniającym rozporządzenie (UE) nr 833/2014 dotyczące środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie*, będącym 12 pakietem sankcji UE przeciwko FR, wprowadzono zakaz importu z Rosji LPG i jego składników, czyli surowca, którego eksport stanowi jedno z najistotniejszych źródeł dochodu tego państwa

[5] Zob. szerzej: M. Cichomski, *Między konfliktem zbrojnym a terroryzmem państwowym…*, s. 96; P. Pospieszna, *Sankcje Unii Europejskiej wobec Rosji: proces decyzyjny, trwałość i rola państw członkowskich*, „Rocznik Integracji Europejskiej" 2018, nr 12, s. 311–321. https://doi.org/10.14746/rie.2018.12.21.

[6] Na temat relacji pojęć: sankcje, środki ograniczające, środki odwetowe na poziomie UE zob. szerzej: M. Cichomski, *Między konfliktem zbrojnym a terroryzmem państwowym…*, s. 99–100; P. Kobza, *Środki restrykcyjne jako instrument Wspólnej Polityki Zagranicznej i Bezpieczeństwa Unii Europejskiej*, „Studia Europejskie" 2006, nr 3, s. 10–14. Temat genezy pojęcia sankcji w wymiarze prawa międzynarodowego został podjęty w: M. Sułek, *Zachodnie sankcje wobec Rosji – sens i skuteczność*, „Rocznik Strategiczny" 2014/2015, t. 20, s. 398–400.

i przekłada się na zwiększanie jego zdolności militarnych. Jednocześnie przyjęto okres przejściowy, który pozwalał na sprowadzanie LPG z Rosji do 20 grudnia 2024 r. na mocy praw nabytych, czyli kontraktów zawartych przed wejściem w życie środków ograniczających. W efekcie realny zakaz zaczął obowiązywać dopiero po prawie 3 latach od wybuchu pełnoskalowego konfliktu zbrojnego w Ukrainie.

W tego typu przypadkach to możliwości lub interesy państwa, które ma zastosować restrykcje, wpływają na zgodę na wprowadzenie określonych ograniczeń, a nie miarkowanie środków ograniczających ze względu na adekwatność do zmieniającej się sytuacji będącej powodem wprowadzenia ograniczeń (np. zmiany na froncie i działania agresora). Przy podejmowaniu tej decyzji najważniejszy jest poziom uzależnienia danego kraju od dostaw określonych surowców czy towarów z państwa, wobec którego mają być zastosowane środki ograniczające. Brak realnej dywersyfikacji źródeł dostaw może przekształcić się w sytuację kryzysową (brak odporności państwa w danym zakresie). Może nastąpić także ograniczenie dochodów państwa, czego przykładem jest długotrwała dyskusja na poziomie wspólnotowym nad wprowadzeniem ograniczeń w zakresie importu diamentów z FR.

W związku z konsensusem państw członkowskich wymaganym do wprowadzenia środków ograniczających nie powinny zaskakiwać ograniczona skuteczność tych środków w wymiarze wspólnotowym czy długotrwałość procesu decyzyjnego. Dotyczy to determinantów tego konsensusu, jakimi są zarówno partykularne interesy ekonomiczne państw, jak i ich odporność wewnętrzna na odcięcie dostaw określonych surowców bądź towarów z kraju objętego sankcjami. Ponadto ma znaczenie odległość od danego państwa do miejsca stanowiącego źródło wprowadzania ograniczeń (np. miejsce konfliktu, położenie kraju, na które chce się wywrzeć presję). Z oczywistych względów percepcja zagrożenia ze strony FR jest inna w Polsce czy na Łotwie niż w Hiszpanii lub Portugalii, tak samo jak różne jest podejście tych państw do zagrożeń z kontynentu afrykańskiego[7]. Przekłada się to również na gotowość na ponoszenie konsekwencji wprowadzania środków ograniczających. Ta różnica w percepcji powoduje potrzebę znalezienia krajowych środków ograniczających, które będą uzupełnieniem środków wspólnotowych i pozwolą na dostosowanie wykorzystywanych rozwiązań w wymiarze geopolitycznym. Właśnie z tej przyczyny w kontekście konfliktu

[7] M. Cichomski, *Między konfliktem zbrojnym a terroryzmem państwowym...*, s. 124.

w Ukrainie takie państwa, jak Polska, Czechy[8] czy Łotwa[9] stosują własne środki ograniczające o charakterze subsydiarnym względem unijnych.

Powstaje pytanie, jaka powinna być wzajemna relacja wspólnotowych i krajowych środków ograniczających[10]. Odwołanie do niej znajduje się w art. 4 ust. 2 Traktatu o Unii Europejskiej, zgodnie z którym UE: (...) *Szanuje podstawowe funkcje państwa, zwłaszcza funkcje mające na celu zapewnienie jego integralności terytorialnej, utrzymanie porządku publicznego oraz ochronę bezpieczeństwa narodowego. W szczególności bezpieczeństwo narodowe pozostaje w zakresie wyłącznej odpowiedzialności każdego Państwa Członkowskiego*.

Należy podkreślić, że kompetencja w zakresie wspólnej polityki zagranicznej i bezpieczeństwa UE, w tym do przyjmowania środków ograniczających, nie ma charakteru wyłącznego, a państwa członkowskie zachowują samodzielne uprawnienia w tych obszarach i mają prawo przyjmować własne środki ograniczające, niezależne od środków UE, tak jak zrobiły to Polska, Czechy i Łotwa. Źródłem kompetencji państw członkowskich w tym zakresie są wyłącznie przepisy prawa krajowego. Przy przyjmowaniu własnych środków ograniczających państwa członkowskie muszą zapewnić, że te środki nie zagrażają urzeczywistnieniu celów, którym mają służyć środki przyjęte przez UE.

Warto też wspomnieć o wytycznych Rady UE pt. *Aktualizacja dobrych praktyk UE w zakresie skutecznego wprowadzania w życie środków ograniczających*. Wskazano w nich, że państwa członkowskie, oprócz prawodawstwem przyjętym na poziomie unijnym, powinny w razie potrzeby dysponować także takimi rozwiązaniami prawnymi, które na szczeblu krajowym umożliwiałyby im zamrażanie środków finansowych i aktywów finansowych oraz zasobów gospodarczych osób i podmiotów podlegających unijnym środkom ograniczającym. Przepisy krajowe powinny ponadto umożliwiać zakaz udostępniania środków finansowych i zasobów gospodarczych tym podmiotom i osobom lub na ich korzyść, w tym przez administracyjne środki oddziaływania lub stosowanie sądowych postanowień

[8] *Zákon o omezujících opatřeních proti některým závažným jednáním uplatňovaných v mezinárodních vztazích (sankční zákon)*, https://www.mzv.cz/jnp/cz/o_ministerstvu/legislativa/pravni_predpisy_v_pusobnosti_mzv/zakon_c_1_2023_sb_o_omezujicich.html [dostęp: 26.02.2025].

[9] *Starptautisko un Latvijas Republikas nacionālo sankciju likums*, https://likumi.lv/doc.php?id=280278 [dostęp: 26.02.2025].

[10] Zob. szerzej: M. Cichomski, *Między konfliktem zbrojnym a terroryzmem państwowym...*, s. 102–107.

o zabezpieczeniu[11]. Wyjaśniono, że środki te powinny umożliwić krajowym organom nakazywanie i realizację zamrażania środków finansowych i zasobów gospodarczych w ramach jurysdykcji państwa członkowskiego, należących do danej osoby lub podmiotu będących ich własnością, kontrolowanych lub posiadanych przez nie, a także powinny być skierowane do osób lub podmiotów pochodzących z UE i prowadzących tam główną działalność[12].

Polskie rozwiązania w zakresie stosowania indywidualnych środków ograniczających w związku z konfliktem w Ukrainie

Polską regulacją określającą zasady stosowania krajowych indywidualnych środków ograniczających w związku z konfliktem w Ukrainie jest *Ustawa z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego* (dalej: ustawa szczególna). Zapewniła ona stosowanie unijnych rozporządzeń 765/2006, 269/2014 oraz 833/2014 – określiła sankcje karne lub prawno-administracyjne za naruszenie środków ograniczających opisanych w tych rozporządzeniach, wskazała organy właściwe do stosowania tych rozporządzeń na gruncie krajowym oraz niezbędne procedury. Ponadto określiła ramy stosowania krajowych środków ograniczających przy uwzględnieniu podstawowych zasad wynikających z rozporządzeń 765/2006 oraz 269/2014.

Ustawa ta w wymiarze stosowania indywidualnych środków ograniczających jest autonomicznym aktem prawa krajowego, wykorzystującym jedynie mechanizmy stosowane przez UE (przez odesłanie do nich, a nie powielanie ich treści). Wynika to wprost z brzmienia art. 1 pkt 1 i 2 ustawy szczególnej, odwołujących się do wspólnotowych środków ograniczających określonych w art. 2 ust. 1–3 rozporządzenia 765/2006 oraz w art. 2 i 9 rozporządzenia 269/2014. Zgodnie z art. 2 ust. 2 ustawy szczególnej nakładane środki nie mogą się dublować: *Zakres środków, o których mowa w art. 1, stosowanych wobec osób i podmiotów wpisanych na listę nie może powielać zakresu*

[11] *Aktualizacja dobrych praktyk UE w zakresie skutecznego wprowadzania w życie środków ograniczających*, Bruksela, 4.05.2018, dokument nr 8519/18, http://data.consilium.europa.eu/doc/document/ST-8519-2018-INIT/pl/pdf [dostęp: 20.02.2025].

[12] Tamże.

środków określonych względem tych osób i podmiotów w wykazach określonych w rozporządzeniu 765/2006 lub rozporządzeniu 269/2014.

Rozwiązania krajowe w zakresie określania indywidualnych środków ograniczających zostały oparte na liście osób i podmiotów (dalej: lista) prowadzonej przez ministra właściwego do spraw wewnętrznych. Jest ona dostępna na jego stronie podmiotowej w Biuletynie Informacji Publicznej[13]. Przed wpisem na listę minister wydaje decyzję, zindywidualizowaną i zaskarżalną do sądu administracyjnego, o wprowadzeniu indywidualnych środków ograniczających wobec danej osoby lub podmiotu oraz o zakresie tych środków.

Minister właściwy do spraw wewnętrznych podejmuje decyzję w sprawie wpisu względem osób i podmiotów dysponujących środkami finansowymi, funduszami oraz zasobami gospodarczymi w rozumieniu odpowiednio rozporządzenia 765/2006 lub rozporządzenia 269/2014, bezpośrednio lub pośrednio wspierających:

1) agresję FR na Ukrainę rozpoczętą w dniu 24 lutego 2022 r. lub
2) poważne naruszenia praw człowieka lub represje wobec społeczeństwa obywatelskiego i opozycji demokratycznej lub których działalność stanowi inne poważne zagrożenie dla demokracji lub praworządności w FR lub Białorusi

– lub bezpośrednio związanych z takimi osobami lub podmiotami, w szczególności ze względu na powiązania o charakterze osobistym, organizacyjnym, gospodarczym lub finansowym, lub wobec których istnieje prawdopodobieństwo wykorzystania w tym celu dysponowanych przez nie takich środków finansowych, funduszy lub zasobów gospodarczych[14].

Spełnienie którejś z wymienionych przesłanek musi być wykazane w ramach wydawanej przez ministra właściwego do spraw wewnętrznych decyzji o wpisie na listę. W odniesieniu do wpisanych na nią osób lub podmiotów stosuje się:

– odpowiednio środki określone w art. 2 ust. 1–3 rozporządzenia 765/2006 lub określone w art. 2 i 9 rozporządzenia 269/2014, w ramach których zamraża się odpowiednio środki finansowe, fundusze i zasoby gospodarcze będące własnością, pozostające w posiadaniu,

[13] *Lista osób i podmiotów objętych sankcjami*, Ministerstwo Spraw Wewnętrznych i Administracji, https://www.gov.pl/web/mswia/lista-osob-i-podmiotow-objetych-sankcjami [dostęp: 24.02.2025].

[14] Artykuł 3 ust. 2 ustawy szczególnej.

w faktycznym władaniu lub pod kontrolą osób fizycznych lub prawnych, podmiotów i organów wymienionych na liście sankcyjnej prowadzonej przez ministra właściwego do spraw wewnętrznych. Z tym środkiem ograniczającym jest skorelowany zakaz bezpośredniego oraz pośredniego udostępniania środków finansowych, funduszy lub zasobów gospodarczych wymienionym na liście sankcyjnej osobom fizycznym lub prawnym, podmiotom i organom ani na ich rzecz, a także zakaz świadomego i umyślnego udziału w działaniach, których celem lub skutkiem jest bezpośrednie lub pośrednie obejście środków;

– wykluczenie z postępowania o udzielenie zamówienia publicznego lub konkursu prowadzonego na podstawie *Ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych*[15].

Ponadto w stosunku do osób wpisanych na listę może zostać zastosowany środek ograniczający w postaci wpisu do wykazu cudzoziemców, których pobyt na terytorium RP jest niepożądany (art. 434 *Ustawy z dnia 12 grudnia 2013 r. o cudzoziemcach*).

Decyzję w sprawie wpisu na listę lub wykreślenia z niej minister właściwy do spraw wewnętrznych wydaje z urzędu lub na uzasadniony wniosek ustawowo wskazanych podmiotów. Uprawnienie dotyczące wnioskowania o dokonanie wpisu przyznano służbom specjalnym mogącym pozyskiwać informacje o istniejących powiązaniach zarówno na podstawie czynności operacyjno-rozpoznawczych, jak i analityczno-informacyjnych oraz od służb partnerskich z innych krajów. Ponadto uprawnienie to przysługuje dwóm służbom o charakterze policyjnym, tj. Policji i Straży Granicznej, podmiotom dysponującym wiedzą o transferach środków finansowych, tj. Generalnemu Inspektorowi Informacji Finansowej (czyli krajowej jednostce analityki finansowej), Komisji Nadzoru Finansowego, Prezesowi Narodowego Banku Polskiego czy Szefowi Krajowej Administracji Skarbowej (KAS) oraz Prokuratorowi Krajowemu, a także Przewodniczącemu Komitetu Rady Ministrów właściwego w sprawach bezpieczeństwa i obrony państwa, ze względu na rolę koordynacyjną tego komitetu[16].

Należy podkreślić, że analogicznie jak w przypadku środków ograniczających stosowanych przez UE, polskie krajowe środki ograniczające

[15] Artykuł 1 ustawy szczególnej.

[16] Zob. szerzej: M. Cichomski, *Między konfliktem zbrojnym a terroryzmem państwowym...*, s. 109–114.

mają charakter zapobiegawczy, a nie represyjny czy konfiskacyjny[17]. Ich celem jest uniemożliwienie dostarczenia środków finansowych, funduszy czy zasobów gospodarczych do FR czy Białorusi.

Zakres podmiotowy i przedmiotowy zastosowanych krajowych indywidualnych środków ograniczających

Na dzień 31 stycznia 2025 r. na krajowej liście środków ograniczających figurowały łącznie **523 osoby i podmioty gospodarcze**[18]. Na **428 osób** wpisanych na listę 379 to osoby powiązane z Białorusią (obywatele Białorusi, w tym parlamentarzyści, dziennikarze propagandyści, funkcjonariusze służb, prokuratorzy i sędziowie), 49 natomiast to osoby powiązane z FR (47 obywateli Rosji, 1 obywatel Mołdawii i 1 obywatel Polski).

Na **95 podmiotów gospodarczych** wpisanych na listę:

- 14 to podmioty powiązane z Białorusią, w tym zarejestrowane:
  - w Polsce – 6,
  - w Białorusi – 5,
  - na Węgrzech – 1,
  - w Zjednoczonych Emiratach Arabskich – 1,
  - na Cyprze – 1.
- 81 to podmioty powiązane z FR, w tym zarejestrowane:
  - w Polsce – 49,
  - w FR – 18,
  - na Cyprze – 7,
  - w Kazachstanie – 4,
  - w Luksemburgu – 1,
  - w Turcji – 1,
  - na Łotwie – 1.

Wszystkie dotychczasowe wpisy na liście dotyczyły łącznie 535 osób i podmiotów (430 osób i 105 podmiotów). Od momentu przyjęcia ustawy szczególnej wydano łącznie **12 decyzji o wykreśleniu z listy w odniesieniu do:**

- 2 osób (1 osoba w związku z wpisem na listę UE, 1 osoba w związku z ustaniem przesłanek stosowania środków ograniczających),

[17] *Opinia Komisji z dnia 19 czerwca 2020 r. w sprawie art. 2 rozporządzenia Rady (UE) nr 269/2014*, Bruksela, 19.06.2020, C (2020) 4117 final, s. 6. Taka sama opinia w tym zakresie została przedstawiona w pkt 28 dokumentu *Aktualizacja dobrych praktyk UE*...

[18] Wyróżnienia w tekście pochodzą od autorów (przyp. red.).

– 10 podmiotów (1 wykreślenie nastąpiło w związku z wpisem na listę UE, 9 było związanych ze zmianami w strukturze własnościowej oraz zakończeniem współpracy z kontrahentami powiązanymi z FR lub Białorusią).

W związku z wydaniem decyzji o dokonaniu wpisu na listę środków ograniczających do wojewódzkiego sądu administracyjnego skierowano łącznie 96 skarg, z tego 37 zostało oddalonych (12 prawomocnie, w tym 3 po wyrokach Naczelnego Sądu Administracyjnego, NSA), 4 – uchylono, 10 – odrzucono, 8 – umorzono, a 37 pozostaje w toku. Do NSA skierowano 28 skarg kasacyjnych.

Na potrzeby analizy opisywanego zagadnienia, mając na uwadze konieczność przedstawienia całości dotychczas zastosowanych środków ograniczających, w dalszej części artykułu uwzględniono zarówno podmioty gospodarcze, które znajdowały się na liście 31 stycznia 2025 r., jak i wykreślone z niej do tego dnia. Pozwoli to na przedstawienie pełnego spektrum zastosowanych do tej pory krajowych środków ograniczających.

Jak wskazano, stosowanie środków ograniczających na poziomie UE wymaga pełnego konsensusu państw członkowskich, co z założenia powoduje rozciągnięcie w czasie procesu nakładania tych środków – od momentu wytypowania podmiotu do objęcia restrykcjami do ich wprowadzenia w życie aktem prawa unijnego. Jest to także duże wyzwanie dla samej UE w kontekście stosunków bilateralnych z państwami trzecimi. Polityka zagraniczna prowadzona przez państwa członkowskie nie jest jednolita – kierują się one przede wszystkim własnymi interesami. Przyczyn tej niejednolitości jest wiele, od położenia geograficznego (bliskość FR i Białorusi) przez posiadane zasoby i bogactwa naturalne (złoża paliw kopalnych, minerałów oraz możliwość ich szybkiego nabycia w przypadku zastosowania środków ograniczających) aż do możliwości zapewnienia bezpieczeństwa wewnętrznego państwa w wielu wymiarach (infrastruktura przesyłowa, zapewnienie mieszkańcom ochrony i zaspokojenie ich potrzeb).

Wprowadzanie przez państwa krajowych środków ograniczających daje realne szanse na szybsze reagowanie na zmieniającą się sytuację nie tylko polityczną, lecz przede wszystkim gospodarczą, co pozwala na elastyczne kształtowanie zakresu podmiotowego i przedmiotowego stosowanych środków ograniczających. Jednocześnie zapewnia łatwość dotarcia do podmiotów gospodarczych przez krajowe mechanizmy oddziaływania (kontrola skarbowa, system bankowy, koncesje, itp.). Wprowadzenie takich rozwiązań to niewątpliwie duże wyzwanie dla państw. Należy wziąć pod

uwagę szerokie spektrum zagrożeń dla państwa członkowskiego UE, które decyduje się na wprowadzenie tych środków. W pierwszej kolejności należy wskazać ryzyko obniżenia dochodów państwa związanych z prowadzeniem działalności przez podmiot (lub podmioty w przypadku wprowadzenia sankcji sektorowych) objęty środkami ograniczającymi, tj. obniżenie dotychczasowych wpływów podatkowych związanych ze skalą prowadzonej działalności gospodarczej, czy też zmniejszenie wolumenu określonych produktów na rynku, co również – przez zmniejszone zakupy – spowoduje mniejsze wpływy do budżetu za pośrednictwem podatku VAT.

Drugi obszar zagrożeń dotyczy infrastruktury posiadanej przez podmioty objęte środkami ograniczającymi. Zastosowanie takich środków może powodować zakłócenia w liniach przesyłowych użytkowanych przez te podmioty, np. gazu ziemnego, paliw płynnych czy sieci energetycznych. Może to prowadzić m.in. do wstrzymania produkcji w zakładach produkcyjnych, niedostarczania dostaw paliw do odbiorców indywidualnych (np. ogrzewanie domów), a także do zaprzestania działalności szpitali i innych podmiotów świadczących usługi dla ludności, których nieprzerwana praca jest niezbędna dla zapewnienia prawidłowego funkcjonowania państwa i bezpieczeństwa jego obywateli.

Kolejne zagrożenia państwa mają związek z pracownikami podmiotów objętych środkami ograniczającymi. Rolą państwa, z przyczyn ekonomicznych i społecznych, jest takie kształtowanie rynku, aby jego obywatel nie tylko mógł podjąć zatrudnienie, lecz także by było ono stabilne. Niewątpliwie objęcie danego podmiotu gospodarczego środkami ograniczającymi, pomimo braku ich charakteru represyjnego, przy jednoczesnym ograniczeniu możliwości dalszego prowadzenia działalności może spowodować redukcję zatrudnienia czy też opóźnienia w wypłacie wynagrodzeń lub innych świadczeń pracowniczych. Konsekwencje wpisu na listę ponoszą zatem zarówno właściciele firm, jak i pośrednio pracownicy.

Polska ustawa szczególna pozwala na złagodzenie tych niedogodności przez wprowadzenie instytucji tymczasowego zarządu przymusowego (art. 6a). Zadaniem tego zarządu jest zbycie środków finansowych, funduszy lub zasobów gospodarczych w rozumieniu rozporządzenia 765/2006 lub rozporządzenia 269/2014, gdy jest to niezbędne dla zapewnienia funkcjonowania podmiotu gospodarczego prowadzącego przedsiębiorstwo na terytorium RP w celu:

1) utrzymania miejsc pracy w tym przedsiębiorstwie lub
2) utrzymania w zakresie działalności tego przedsiębiorstwa świadczenia usług użyteczności publicznej lub wykonywania innych zadań o charakterze publicznym, lub
3) ochrony interesu ekonomicznego państwa.

Artykuł 6b pozwala natomiast na wprowadzenie tymczasowego zarządu przymusowego w celu przejęcia na rzecz Skarbu Państwa lub innego podmiotu własności środków finansowych, funduszy lub zasobów gospodarczych w rozumieniu rozporządzenia 765/2006 lub rozporządzenia 269/2014, należących do osoby albo podmiotu wpisanych na listę, jeżeli jest to niezbędne dla ochrony ważnego interesu publicznego, ochrony interesu ekonomicznego państwa lub ze względu na zapewnienie jego bezpieczeństwa. Tymczasowy zarządca przymusowy ma na celu zapewnienie dalszego funkcjonowania podmiotu gospodarczego do czasu zbycia środków finansowych, funduszy lub zasobów gospodarczych objętych zarządem, a zatem ich odcięcia od powiązania z osobami i podmiotami wspierającymi działalność reżimów w Rosji i Białorusi. Środki ze sprzedaży są zamrożone na rachunkach dotychczasowych właścicieli objętych sankcjami[19].

Aby zadbać o interes społeczny, tj. interes pracowników przedsiębiorstw prowadzonych przez podmioty gospodarcze objęte środkami ograniczającymi, w art. 6e ustawy szczególnej wprowadzono także możliwość wystąpienia przez podmiot objęty środkami ograniczającymi z wnioskiem o przyznanie świadczeń z Funduszu Gwarantowanych Świadczeń Pracowniczych na zaspokojenie należności pracowniczych. W przypadku niewystąpienia przez pracodawcę z powyższym wnioskiem wypłata świadczeń może nastąpić również na podstawie indywidualnego wniosku pracownika.

Przedstawione rozwiązania pozwalają na zachowanie ciągłości prowadzenia działalności podmiotu wpisanego na listę oraz ochronę praw jego pracowników. W pewien sposób minimalizują one również zagrożenia, jakie przyjęło na siebie państwo wprowadzające własne restrykcje, które są z natury szersze niż rozwiązania unijne. Za przykład mogą posłużyć wspomniane polskie rozwiązania w postaci wykluczenia z postępowania o udzielenie zamówienia publicznego lub konkursu oraz wpis do wykazu cudzoziemców, których pobyt na terytorium RP jest niepożądany.

[19] Zob. szerzej: M. Cichomski, *Między konfliktem zbrojnym a terroryzmem państwowym...*, s. 121–122.

Podział środków ograniczających zastosowanych przez ministra spraw wewnętrznych na dzień 31 stycznia 2025 r. ze względu na państwo rejestracji podmiotów gospodarczych przedstawiał się następująco (w nawiasach podano udział procentowy w ogólnej liczbie podmiotów gospodarczych objętych środkami ograniczającymi):

- Polska – 64 podmioty (60,95%),
- FR – 19 podmiotów (18,10%),
- Cypr – 8 podmiotów (7,62%),
- Białoruś – 5 podmiotów (4,76%),
- Kazachstan – 4 podmioty (3,81%).

Ponadto zastosowano środki wobec pojedynczych podmiotów gospodarczych zarejestrowanych w Luksemburgu, Turcji, Zjednoczonych Emiratach Arabskich oraz na Węgrzech i Łotwie (4,76%).

Należy zauważyć, że RP wpisała na listę nie tylko podmioty zarejestrowane w FR i Białorusi, co wynika z celu stosowania środków ograniczających na poziomie europejskim (ograniczenie finansowania agresji FR na Ukrainę oraz finansowania reżimu Aleksandra Łukaszenki), lecz przede wszystkim podmioty zarejestrowane w Polsce.

Stosowanie środków ograniczających w stosunku do podmiotów gospodarczych zarejestrowanych w RP należy rozpatrywać także w aspekcie ich beneficjentów rzeczywistych oraz osób nimi zarządzających. To, że podmiot jest zarejestrowany w Polsce, nie oznacza, że ma on polski kapitał. Z uwagi na swobodę prowadzenia działalności gospodarczej ta okoliczność nie ma żadnego znaczenia prawnego. Spełnienie ustawowych przesłanek rejestracji podmiotu gospodarczego (zarówno w formie spółki, jak i działalności gospodarczej prowadzonej przez osobę fizyczną) powoduje, że podlega on wpisowi do Krajowego Rejestru Sądowego lub Centralnej Ewidencji i Informacji o Działalności Gospodarczej. W związku z tym spółka zarejestrowana w Polsce nie musi być spółką „polską" w kontekście jej kapitału założycielskiego i środków na prowadzenie działalności. Konsekwencją takiego stanu rzeczy jest dowolność w obsadzie jej kadry zarządzającej.

Podobna sytuacja dotyczy beneficjentów rzeczywistych podmiotów gospodarczych. Zgodnie z *Ustawą z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* beneficjentem rzeczywistym jest każda osoba fizyczna sprawująca bezpośrednio lub pośrednio kontrolę nad spółką przez posiadane uprawnienia, które wynikają z okoliczności prawnych lub faktycznych. Umożliwiają one wywieranie decydującego wpływu na czynności lub działania podejmowane przez spółkę lub każdą

osobę fizyczną, w imieniu której są nawiązywane stosunki gospodarcze lub jest przeprowadzana transakcja okazjonalna. Zatem beneficjentem podmiotów gospodarczych zarejestrowanych w Polsce mogą być zarówno podmioty gospodarcze, jak i osoby fizyczne, powiązane z dowolnym państwem na świecie czy też podmiotem gospodarczym w nich zarejestrowanym. Mogą to być zatem osoby powiązane z reżimem w FR lub Białorusi. Implikuje to możliwość dowolnego transferu środków do tych państw i w konsekwencji przeznaczenie ich na wspieracie agresji na Ukrainę lub represji wobec opozycji demokratycznej w Rosji i Białorusi.

Środki ograniczające zastosowane przez ministra spraw wewnętrznych na dzień 31 stycznia 2025 r. dotyczą podmiotów gospodarczych prowadzących działalność gospodarczą w następujących obszarach (w nawiasach podano udział procentowy w ogólnej liczbie podmiotów gospodarczych objętych środkami ograniczającymi):

- przemysł chemiczny (w tym produkcja i dystrybucja nawozów) – 17 podmiotów (16,20%),
- transport i spedycja – 11 podmiotów (10,48%),
- produkcja, eksport i dystrybucja gazu ziemnego (w tym posiadacze infrastruktury przesyłowej) – 9 podmiotów (8,57%),
- produkcja i dystrybucja chemii budowlanej – 8 podmiotów (7,62%),
- produkcja i dystrybucja oprogramowania – 6 podmiotów (5,71%),
- przemysł petrochemiczny – 5 podmiotów (4,76%),
- organizacja imprez masowych – 5 podmiotów (4,76%),
- produkcja i dystrybucja maszyn rolniczych – 5 podmiotów (4,76%),
- produkcja i dystrybucja gazów przemysłowych i medycznych – 4 podmioty (3,81%),
- obrót sklejką brzozową – 4 podmioty (3,81%),
- import i dystrybucja węgla – 3 podmioty (2,86%),
- przemysł hutniczy i wydobywczy – 3 podmioty (2,86%),
- sprzedaż pojazdów i części samochodowych – 3 podmioty (2,86%),
- sprzedaż sprzętu elektronicznego i telekomunikacyjnego – 3 podmioty (2,86%),
- produkcja artykułów higienicznych – 2 podmioty (1,90%),
- przemysł samochodowy – 2 podmioty (1,90%),
- przemysł maszynowy – 2 podmioty (1,90%),
- sektor finansowy – 2 podmioty (1,90%),
- produkcja i dystrybucja artykułów spożywczych – 2 podmioty (1,90%).

Terroryzm – studia, analizy, prewencja
2025, wydanie specjalne: 195–218

Ponadto środki ograniczające były zastosowane w stosunku do pojedynczych podmiotów prowadzących działalność w zakresie: sprzedaży artykułów sportowych, dystrybucji energii elektrycznej, produkcji maszyn, sprzedaży internetowej, produkcji akumulatorów, produkcji i dystrybucji soli, obrotu maszynami przemysłowymi, prowadzenia rozliczeń w ramach dystrybucji paliw oraz dystrybucji alkoholu metylowego. Łącznie stanowią one 8,57% podmiotów, wobec których zastosowano środki ograniczające.

W kontekście zakresu tematycznego niniejszego opracowania, a zatem podmiotów sprowadzających surowce energetyczne czy posiadaczy infrastruktury przesyłowej, dalsza analiza polskiej listy podmiotów objętych środkami ograniczającymi wskazuje, że zastosowano je w stosunku do (w nawiasach podano udział procentowy w ogólnej liczbie podmiotów gospodarczych objętych środkami ograniczającymi):

- 5 podmiotów sprowadzających surowce energetyczne, w tym 3 zajmujące się importem węgla (4,76%),
- 5 podmiotów posiadających infrastrukturę przesyłową (4,76%).

Wpis na listę objął również 4 podmioty gospodarcze, które były na wstępnym etapie prowadzenia działalności w zakresie importu i dystrybucji gazu. Nałożenie środków ograniczających na te podmioty miało charakter zapobiegawczy i uniemożliwiło im rozwinięcie pełnoskalowej działalności.

Jedna z zamrożonych spółek wpisanych na listę nie posiadała własnych sieci przesyłowych, niemniej jednak wpis na listę uniemożliwił jej dokonywanie transakcji hurtowych sprzedaży lub zakupu energii elektrycznej oraz korzystanie z sieci przesyłowych posiadacza infrastruktury krytycznej.

W odniesieniu do podmiotów sprowadzających surowce energetyczne czy posiadaczy infrastruktury przesyłowej, pod względem miejsca ich rejestracji ograniczenia te zastosowano wobec (w nawiasach podano udział procentowy w ogólnej liczbie podmiotów gospodarczych objętych środkami ograniczającymi):

- 9 podmiotów zarejestrowanych w Polsce, tj. 3 zajmujących się importem węgla, 2 importujących gaz ziemny oraz 4 planujących rozpoczęcie działalności gospodarczej w zakres importu i dystrybucji gazu (8,57%),
- 3 podmiotów zarejestrowanych w FR (2,86%).

Wobec wskazanych 12 podmiotów gospodarczych zastosowano środki w rozumieniu rozporządzenia 269/2014, co stanowi 13,79% z wszystkich 87 podmiotów, wobec których zastosowano środki w nim określone.

Wskazane podmioty mają istotne znaczenie dla funkcjonowania państwa i jego infrastruktury w związku z przedmiotem ich działalności, który jest krytyczny w odniesieniu do zapewnienia bezpieczeństwa energetycznego państwa. Stosowanie środków ograniczających wobec tych firm niosło za sobą zagrożenie zakłócenia dostaw energii oraz paliw. Z jednej strony pokazuje to ryzyko, jakie podejmuje państwo wprowadzające takie rozwiązania na poziomie krajowym. Z drugiej strony daje realne szanse na wywarcie presji na państwo, względem którego są stosowane środki ograniczające. Stosowanie indywidualnych środków ograniczających może mieć znaczenie w kontekście bezpieczeństwa dostaw surowców energetycznych, funkcjonowania infrastruktury przesyłowej i infrastruktury krytycznej i z tej perspektywy należy je oceniać.

Studium przypadku

W kolejnej części artykułu dokonano analizy przypadku jednego z podmiotów wpisanych na krajową listę środków ograniczających. Analiza ta uwzględnia zarówno opis przesłanek wpisu, jak i zastosowanego zakresu środków ograniczających, a także dodatkowych mechanizmów prawnych zastosowanych w celu minimalizowania negatywnych skutków społecznych i gospodarczych związanych z wpisem tego podmiotu na listę. Analiza została przeprowadzona na podstawie decyzji ministra spraw wewnętrznych i administracji umieszczonych na stronie podmiotowej MSWiA. W artykule zrezygnowano z posługiwania się autentycznymi nazwami podmiotów gospodarczych.

Spółka A działała na rynku polskim od kilkunastu lat. Główny profil jej działalności to import i sprzedaż LPG oraz skroplonego gazu ziemnego (LNG), również na rynku europejskim. Ponadto prowadziła działalność w zakresie budowy instalacji regazyfikacji LNG, stacji tankowania LNG i dostaw skroplonego gazu ziemnego. Posiadała terminale przeładunkowe LPG oraz rozlewnię LPG w butlach. W zakres jej działalności wchodziło także dostarczanie gazu własnymi sieciami przesyłowymi do kilkunastu gmin gazyfikowanych w technologii LNG. Profil działalności spółki A, zwłaszcza w kontekście dostaw gazu do podmiotów indywidualnych, sytuował ją

Terroryzm – studia, analizy, prewencja
2025, wydanie specjalne: 195–218

w sektorze podmiotów mających istotne znaczenie dla zapewnienia bezpieczeństwa energetycznego państwa, przy czym nie był to poziom krytyczny.

Spółka A była podmiotem zależnym w grupie kapitałowej B, kontrolowanej przez rosyjski koncern C, od którego importowała gaz na terytorium Polski. Koncern C to jeden z największych producentów gazu ziemnego w Rosji oraz jeden z największych podmiotów gospodarczych w FR, objęty środkami ograniczającymi rządu Stanów Zjednoczonych Ameryki wprowadzanymi przez OFAC (Specially Designated Nationals and Blocked Persons List U.S. Department of the Treasury's Office of Foreign Assets Control). Koncern C jest powiązany z osobą X, objętą środkami ograniczającymi rządu Wielkiej Brytanii na podstawie *Sanctions and Anti-Money Laundering Act 2018* – nr 996. Ponadto członkiem zarządu koncernu C był Y, jeden z zaufanych współpracowników Władimira Putina, objęty środkami ograniczającymi na podstawie rozporządzenia 269/2014. Z uwagi na sektor, w którym koncern C prowadził działalność, jak również jego wielkość, zapewniał on istotne źródło dochodów rządowi FR.

Te powiązania w sposób kompletny wypełniały ustawowe przesłanki zastosowania środków ograniczających wobec spółki A. W efekcie minister spraw wewnętrznych i administracji wydał decyzję administracyjną i na jej mocy wpisał spółkę A na listę, o której mowa w art. 2 ust. 1 ustawy szczególnej, oraz zastosował pierwotnie w stosunku do niej:

- zamrożenie środków finansowych i zasobów gospodarczych w rozumieniu rozporządzenia 269/2014, będących własnością, pozostających w posiadaniu, pozostających w faktycznym władaniu lub pod kontrolą podmiotu, w pełnym zakresie,
- zakaz udostępniania podmiotowi, lub na jego rzecz – bezpośrednio lub pośrednio – jakichkolwiek środków finansowych lub zasobów gospodarczych w rozumieniu rozporządzenia 269/2014,
- zakaz świadomego i umyślnego udziału w działaniach, których celem lub skutkiem jest ominięcie ww. środków,
- wykluczenie z postępowania o udzielenie zamówienia publicznego lub konkursu prowadzonego na podstawie ustawy – prawo zamówień publicznych.

Uzasadnieniem wydania decyzji i zastosowania środków ograniczających było stwierdzenie, że spółka A jest podmiotem dysponującym odpowiednio środkami finansowymi oraz zasobami gospodarczymi w rozumieniu rozporządzenia 269/2014, bezpośrednio lub pośrednio wspierającym agresję FR na Ukrainę. Przesłanki faktyczne natomiast to powiązania

osobiste, organizacyjne, gospodarcze i finansowe z podmiotem rosyjskim (koncern C), zapewniającym środki finansowe wykorzystywane do wspierania agresji na Ukrainę. Ponadto osoby związane z koncernem C (powiązania zarówno właścicielskie, jak i decyzyjne) należą do grona bliskich współpracowników Putina oraz są beneficjentami decyzji rządu FR.

Jak wskazano, spółka A działała na terenie Polski w segmencie importu gazu ziemnego i jego dalszej dystrybucji do odbiorców końcowych (podmioty sektora publicznego i prywatnego). W związku z istotnym znaczeniem tej działalności, w celu zapewnienia nieprzerwanych dostaw gazu ziemnego realizowanych przez spółkę, minister spraw wewnętrznych i administracji wziął pod uwagę potrzebę przeciwdziałania skutkom ewentualnej sytuacji kryzysowej[20], jaka mogła powstać w związku z realizacją środków przewidzianych w pierwotnej decyzji dotyczącej wpisu spółki A na listę. Wydał decyzję, w której zmodyfikował zakres środków dotyczących zamrożenia środków finansowych i zasobów gospodarczych spółki, oraz zakazu ich udostępniania, przez wyłączenie zakresu związanego z czynnościami wykonywanymi w ramach realizacji poleceń wydanych przez Prezesa Rady Ministrów w trybie art. 7a *Ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*.

Celem wydania wskazanej decyzji było zwolnienie środków finansowych i zasobów gospodarczych pozostających we władaniu spółki, w celu umożliwienia dysponowania nimi w takim zakresie, aby zachować ciągłość dostaw gazu do odbiorców za pośrednictwem infrastruktury należącej do spółki. Należy zauważyć, że konstrukcja ustawy szczególnej – a w konsekwencji również decyzji wydanej na jej podstawie – powoduje, że zwolnienie środków finansowych i zasobów gospodarczych podmiotu objętego środkami ograniczającymi wymaga każdorazowego uzyskania zgody szefa KAS. Zgodnie bowiem z tą ustawą zadania i kompetencje, o których mowa w art. 4 ust. 1 rozporządzenia 269/2014, wobec osób i podmiotów wpisanych na listę wykonuje szef KAS. Może on na uzasadniony wniosek wyrazić zgodę na zwolnienie określonych zamrożonych środków finansowych lub zasobów gospodarczych lub też udostępnienie określonych środków finansowych lub zasobów gospodarczych, w odniesieniu do osób i podmiotów objętych środkami ograniczającymi. Biorąc jednak pod uwagę niezbędność zapewnienia ciągłych dostaw gazu, każdorazowe wystąpienie z wnioskiem do szefa KAS i konieczność oczekiwania na wydanie pozytywnej decyzji mogłoby zakłócić dostawy.

[20] W rozumieniu art. 7a pkt 1 *Ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*.

Konsekwencją wydania ww. decyzji dotyczącej wyłączenia zakresu stosowania środków ograniczających w stosunku do spółki A było wydanie przez Prezesa Rady Ministrów decyzji na podstawie art. 7a i 7b ustawy o zarządzaniu kryzysowym. Na jej mocy polecił on spółce wydanie określonym podmiotom gospodarczym, realizującym działalność w zakresie dystrybucji paliwa gazowego, wszelkiej dokumentacji dotyczącej infrastruktury posiadanej i użytkowanej przez spółkę do przesyłu gazu oraz dokumentacji niezbędnej do zapewnienia niezakłóconych dostaw gazu odbiorcom końcowym, a przede wszystkim do wydania, na zasadach bezpłatnego użyczenia, sieci oraz instalacji służących do dystrybucji gazu. Wskazane podmioty gospodarcze, które miały przejąć obowiązki spółki A, zostały natomiast zobowiązane m.in. do sprzedaży gazu odbiorcom końcowym dotychczas obsługiwanym przez spółkę oraz do zapewnienia warunków technicznych do przeprowadzenia tych działań.

Podjęte działania pozwoliły na niezakłócone i niecierpiące zwłoki dostawy gazu do podmiotów gospodarczych, szkół, przedszkoli i innych instytucji użyteczności publicznej, do których gaz był dostarczany dotychczasowo przez spółkę A. Ponadto pomimo zastosowania wobec niej środków ograniczających, a co za tym idzie – faktycznego zakazu importu gazu przez ten podmiot, nie odnotowano braków LPG na polskim rynku paliwowym.

Spółka A, korzystając z uprawnień zawartych w ustawie szczególnej oraz przepisach prawa administracyjnego, wniosła do wojewódzkiego sądu administracyjnego skargi na decyzje wydane przez ministra spraw wewnętrznych i administracji. Zostały one oddalone zarówno przez sąd I instancji, jak i NSA. Ponadto spółka wniosła do ministra wniosek o wykreślenie z listy sankcyjnej, który został rozpatrzony negatywnie. W konsekwencji spółka wniosła skargę do sądu, która również została oddalona przez sądy I i II instancji.

Korzystając z uprawnień ustawowych, minister rozwoju i technologii na wniosek złożony przez szefa Centralnego Biura Antykorupcyjnego wprowadził w spółce tymczasowy zarząd przymusowy i określił zakres objętych nim środków finansowych, funduszy i zasobów gospodarczych, tj. rzeczowych aktywów trwałych, wartości niematerialnych i prawnych, aktywów ruchomych i nieruchomych oraz aktywów finansowych. Uznał on, że zastosowanie tego środka jest niezbędne do zapewnienia funkcjonowania podmiotu w zakresie świadczenia usług użyteczności publicznej lub wykonywania innych zadań o charakterze publicznym oraz dla ochrony interesów ekonomicznych państwa. Jako kluczowe zadanie ustanowionego zarządu wskazano w decyzji zabezpieczenie mienia należącego do spółki

w celu zapewnienia ciągłości świadczonych usług z zakresu dostaw gazu. Zarządca tymczasowy podjął działania zmierzające do zbycia spółki, które trwają do chwili obecnej.

Podsumowanie

Przedstawiona analiza wskazuje jednoznacznie, że wprowadzenie środków ograniczających na poziomie krajowym, niezależnie od środków stosowanych przez UE na poziomie wspólnotowym, jest niezbędne dla realnego odcinania od dochodów państw stanowiących cel wywierania presji. Szczególne znaczenie w tym zakresie ma polityka sankcyjna krajów leżących blisko państwa będącego celem bezpośrednich działań restrykcyjnych. Krajowe środki ograniczające stanowią cenne uzupełnienie dla środków unijnych, są bardziej elastyczne i mają większą możliwość oddziaływania. Znaczenie mają także możliwość skrócenia czasu reakcji na zmieniające się okoliczności oraz skala ich oddziaływania na terenie państwa, które je wprowadziło.

Należy przy tym zauważyć, że o ile środki ograniczające wprowadzone przez UE w zdecydowanej większości dotyczą podmiotów gospodarczych zarejestrowanych w FR i Białorusi, o tyle w przypadku środków wprowadzonych przez Polskę są to podmioty przede wszystkim zarejestrowane w tym państwie. Istotne pozostaje w tym kontekście położenie RP, jako kraju graniczącego zarówno z FR, jak i Białorusią, a także Ukrainą, gdzie trwa pełnoskalowa wojna. Ta bliskość z jednej strony skutkuje większą liczbą powiązań gospodarczych o wymiarze lokalnym, które mogą być postrzegane jako marginalne z perspektywy celów wspólnotowych, z drugiej zaś strony determinuje wprowadzanie restrykcji. Przykład Polski w kontekście konfliktu w Ukrainie wskazuje, że zastosowanie krajowych środków ograniczających wobec niektórych podmiotów może mieć znaczenie dla bezpieczeństwa dostaw surowców energetycznych, funkcjonowania infrastruktury przesyłowej i infrastruktury krytycznej.

O znaczeniu i skuteczności krajowych środków ograniczających świadczą również dane statystyczne. Według danych KAS łączna wartość zamrożonych dotychczas w Polsce aktywów wynosi ponad 1,3 mld euro, w tym 885,4 mln na podstawie przepisów krajowych[21].

[21] Zapis przebiegu posiedzenia Sejmowej Komisji Finansów z dnia 18 grudnia 2024 r., https://www.sejm.gov.pl/sejm10.nsf/biuletyn.xsp?documentId=EECD190CFA2CF2EFC1258C44004F3194 [dostęp: 12.03.2025].

Bibliografia

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.

Kobza P., *Środki restrykcyjne jako instrument Wspólnej Polityki Zagranicznej i Bezpieczeństwa Unii Europejskiej*, „Studia Europejskie" 2006, nr 3, s. 9–31.

Pospieszna P., *Sankcje Unii Europejskiej wobec Rosji: proces decyzyjny, trwałość i rola państw członkowskich*, „Rocznik Integracji Europejskiej" 2018, nr 12, s. 311–321. https://doi.org/10.14746/rie.2018.12.21.

Sułek M., *Zachodnie sankcje wobec Rosji – sens i skuteczność*, „Rocznik Strategiczny" 2014/2015, t. 20, s. 398–410.

Akty prawne

Traktat o funkcjonowaniu Unii Europejskiej (wersja skonsolidowana) – (Dz. Urz. UE C 202/47 z 7.06.2016).

Traktat o Unii Europejskiej (wersja skonsolidowana) – (Dz. Urz. UE C 202/13 z 7.06.2016).

Rozporządzenie Rady (UE) nr 833/2014 z dnia 31 lipca 2014 r. dotyczące środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz. Urz. UE L 229/1 z 31.07.2014).

Rozporządzenie Rady (UE) nr 269/2014 z dnia 17 marca 2014 r. w sprawie środków ograniczających w odniesieniu do działań podważających integralność terytorialną, suwerenność i niezależność Ukrainy lub im zagrażających (Dz. Urz. UE L 78/6 z 17.03.2014, ze zm.).

Rozporządzenie Rady (WE) nr 765/2006 z dnia 18 maja 2006 r. dotyczące środków ograniczających w związku z sytuacją na Białorusi i udziałem Białorusi w agresji Rosji wobec Ukrainy (Dz. Urz. UE L 134/1 z 20.05.2006, ze zm.).

Rozporządzenie Rady (WE) nr 2580/2001 z 27 grudnia 2001 r. w sprawie szczególnych środków restrykcyjnych skierowanych przeciwko niektórym osobom i podmiotom mających na celu zwalczanie terroryzmu (Dz. Urz. UE L 344/70 z 28.12.2001).

Opinia Komisji z dnia 19 czerwca 2020 r. w sprawie art. 2 rozporządzenia Rady (UE) nr 269/2014, Bruksela, 19.06.2020, C (2020) 4117 final.

Ustawa z dnia 5 sierpnia 2022 r. o zmianie ustawy o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego oraz ustawy o Krajowej Administracji Skarbowej (DzU z 2022 poz. 1713).

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 poz. 507, ze zm.).

Ustawa z dnia 11 września 2019 r. – Prawo zamówień publicznych (t.j. DzU z 2024 poz. 1320).

Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. DzU z 2023 poz. 1124, ze zm.).

Ustawa z dnia 12 grudnia 2013 r. o cudzoziemcach (t.j. DzU z 2024 poz. 769, ze zm.).

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. DzU z 2023 poz. 122, ze zm.).

Starptautisko un Latvijas Republikas nacionālo sankciju likums, https://likumi.lv/doc.php?id=280278 [dostęp: 26.02.2025].

Zákon o omezujících opatřeních proti některým závažným jednáním uplatňovaných v mezinárodních vztazích (sankční zákon), https://www.mzv.cz/jnp/cz/o_ministerstvu/legislativa/pravni_predpisy_v_pusobnosti_mzv/zakon_c_1_2023_sb_o_omezujicich.html [dostęp: 26.02.2025].

Inne dokumenty

Aktualizacja dobrych praktyk UE w zakresie skutecznego wprowadzania w życie środków ograniczających, Bruksela, 4.05.2018, dokument nr 8519/18, http://data.consilium.europa.eu/doc/document/ST-8519-2018-INIT/pl/pdf [dostęp: 20.02.2025].

Lista osób i podmiotów objętych sankcjami, Ministerstwo Spraw Wewnętrznych i Administracji, https://www.gov.pl/web/mswia/lista-osob-i-podmiotow-objetych-sankcjami [dostęp: 24.02.2025].

Ogólne ramy dla sankcji unijnych, Unia Europejska, https://eur-lex.europa.eu/PL/legal-content/summary/general-framework-for-eu-sanctions.html [dostęp: 20.02.2025].

Zapis przebiegu posiedzenia Sejmowej Komisji Finansów z dnia 18 grudnia 2024 r., https://www.sejm.gov.pl/sejm10.nsf/biuletyn.xsp?documentId=EECD190CFA2CF2EFC1258C44004F3194 [dostęp: 12.03.2025].

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.

Konrad Kaczor

Były funkcjonariusz Policji oraz były pracownik Ministerstwa Spraw Wewnętrznych i Administracji. Ma ponadtrzydziestoletnie doświadczenie w zakresie zwalczania przestępczości ekonomicznej i zorganizowanej. Zajmuje się zagadnieniami związanymi z międzynarodową sytuacją geopolityczną.

Terroryzm – studia, analizy, prewencja, 2025, wydanie specjalne: 219–235

https://doi.org/10.4467/27204383TER.25.008.21511

Artykuł

Hybrydowy wymiar współczesnego terroryzmu a infrastruktura krytyczna. Analiza raportów Europolu TE-SAT z lat 2021–2024

The hybrid dimension of contemporary terrorism and critical infrastructure. Analysis of Europol's TE-SAT reports from 2021–2024

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

Uniwersytet im. Adama Mickiewicza w Poznaniu
Instytut Zachodni w Poznaniu

Abstrakt

Na podstawie raportów Europolu TE-SAT z lat 2021–2024 autor dokonuje analizy współczesnych przejawów terroryzmu w Unii Europejskiej, ze zwróceniem szczególnej uwagi na jego hybrydowy charakter oraz wpływ na bezpieczeństwo infrastruktury krytycznej. Punktem wyjścia rozważań jest charakterystyka nowej – zgodnie z typologią Davida Rapoporta – piątej fali terroryzmu. Cechuje ją m.in. łączenie tradycyjnych i nowoczesnych metod działania, powiązania terrorystów z przestępczością zorganizowaną oraz służbami specjalnymi państw wrogich, a także aktywność w przestrzeni cyfrowej. Analiza raportów TE-SAT ukazuje zmienność dynamiki zamachów i aresztowań w UE, różne motywacje ideologiczne sprawców (dżihadystyczna, separatystyczna, prawicowa, lewicowo-anarchistyczna) oraz wzrost znaczenia tzw. samotnych wilków. Autor wskazuje na rosnącą rolę państw takich jak Rosja, Białoruś czy Iran w stosowaniu instrumentarium terrorystycznego w wymiarze proxy i cybernetycznym oraz podkreśla potrzebę redefinicji unijnej polityki antyterrorystycznej, rozszerzenia mandatu

Europolu (z uwzględnieniem terroryzmu państwowego), intensyfikacji współpracy z NATO oraz rozwoju wielowymiarowych zdolności obronnych UE, w tym zwiększenia ochrony europejskiej infrastruktury krytycznej.

Słowa kluczowe

terroryzm, Europol, zagrożenia hybrydowe, infrastruktura krytyczna

Abstract

On the basis of Europol TE-SAT reports from 2021-2024, the author analyses contemporary manifestations of terrorism in the European Union, paying particular attention to its hybrid nature and its impact on the security of critical infrastructure (CI). The starting point of the considerations is the characterisation of the new – according to David Rapoport's typology – fifth wave of terrorism. It is characterised by, among other things, combining traditional and modern methods of operation, links between terrorists and organised crime and the special services of hostile states, as well as activity in the digital space. Analysis of TE-SAT reports reveals the changing dynamics of attacks and arrests in the EU, the different ideological motivations of the perpetrators (jihadist, separatist, right-wing, left-anarchist) and the rise of so-called "lone wolves". The author points to the growing role of countries such as Russia, Belarus and Iran in the use of proxy and cyber terrorist instrumentation and emphasises the need to redefine the EU's counter-terrorism policy, extend Europol's mandate (including state terrorism), intensify cooperation with NATO and develop the EU's multidimensional defence capabilities, including enhanced protection of European CI.

Keywords

terrorism, Europol, hybrid threats, critical infrastructure

Nowa fala zagrożenia terrorystycznego

Terroryzm[1] nie tylko nadal jest obecny w świecie, lecz ponownie eskaluje w różnych częściach globu, np. na Bliskim Wschodzie, w Afryce i Unii

[1] Na temat definiowania pojęcia terroryzm zob. np. A. Richards, *Defining terrorism*, w: *Routledge Handbook of Terrorism and Counterterrorism*, A. Silke (red.), New York 2019; S. Wojciechowski, *The Hybridity of Terrorism: Understanding Contemporary Terrorism*, Berlin 2013.

Europejskiej[2]. Świat mierzy się zarówno z jego nasileniem, jak i z ewoluowaniem – na tyle znaczącym, że zasadne jest rozpatrzenie hipotezy o nowej fali terroryzmu. Zgodnie z typologią zaproponowaną przez Davida Rapoporta[3] będzie to piąta fala zagrożenia terrorystycznego, po wcześniejszych jego formach: anarchistycznej, antykolonialnej, lewicowej oraz religijnej erze dżihadu[4]. W większym lub mniejszym stopniu koresponduje ona lub wręcz przenika się ze swoimi poprzedniczkami, choćby w kontekście występowania ideologii dżihadu. Łączy stare i nowe aspekty taktyki czy strategii i ma wyjątkowo silny charakter hybrydowy. Stąd jej nazwa – hybrydowa fala terroryzmu. Jej główne cechy to m.in.:

1. Coraz częstsze wykorzystywanie przez terrorystów z jednej strony prostych i łatwo dostępnych narzędzi, m.in. noża czy samochodu, a z drugiej nowoczesnych technologii, np. dronów czy sztucznej inteligencji (hybrydowość środków), szczególnie na etapie planowania zamachu. Towarzyszy temu relatywnie łatwy dostęp do broni palnej, masowo przemycanej z obszarów konfliktogennych – w Afryce, na Bliskim Wschodzie czy w Europie (kazus Bałkanów lub Ukrainy), oraz do broni wytwarzanej, w tym w technologii 3D.
2. Kształtowanie się coraz silniejszych powiązań w triadzie: terrorysta/terroryści – grupy przestępcze – służby specjalne wrogich państw. Jest to kolejny element hybrydowy, szczególnie niebezpieczny w przypadku terroryzmu państwowego, gdy podmiot państwowy wspiera lub stosuje ten rodzaj aktywności (od działań kinetycznych

[2] Na temat obecnej eskalacji terroryzmu zob. szerzej: R. Gunaratna, *Global Terrorism Threat Forecast 2025*, „RSIS Commentary" 2025, nr 002, https://dr.ntu.edu.sg/bitstream/10356/182595/2/CO25002.pdf [dostęp: 9.03.2025]; *Security Council debates growing terrorism threat in Africa*, United Nations, 21.01.2025, https://news.un.org/en/story/2025/01/1159246 [dostęp: 5.03.2025]; Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2024*, https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2024-eu-te-sat [dostęp: 4.02.2025]; Institute for Economics & Peace, *Global Terrorism Index 2025*, https://www.economicsandpeace.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf [dostęp: 10.03.2025].

[3] D. Rapoport, *Waves of Global Terrorism: From 1879 to the Present*, Columbia University Press 2022.

[4] Koncepcja fal terroryzmu wywołuje polemiki. Zob. np. T. Parker, N. Sitter, *The Four Horsemen of Terrorism: It's Not Waves, It's Strains*, „Terrorism and Political Violence" 2016, t. 28, nr 2, s. 197–216. https://doi.org/10.1080/09546553.2015.1112277; D. Rapoport, *It Is Waves, Not Strains*, „Terrorism and Political Violence" 2016, t. 28, nr 2, s. 217–224. https://doi.org/10.1080/09546553.2015.1112278.

po operacje prowadzone w cyberprzestrzeni), połączony z terrorem kryminalnym, czego przykładem są działania Rosji, Białorusi, Iranu i Korei Północnej (hybrydowość sprawców).

3. Coraz skuteczniejsze propagowanie przez terrorystów swojej narracji w sieci. Internet oraz inne nowoczesne technologie, np. sztuczna inteligencja, stały się ważnym narzędziem wykorzystywanym w celach propagandowych, werbunkowych, dezinformacyjnych czy do pozyskiwania środków finansowych oraz organizowania zaplecza logistycznego. Służą one także do radykalizowania postaw i propagowania mowy nienawiści (hybrydowość celów), co prowadzi do tworzenia środowiska sprzyjającego wzrostowi poziomu ekstremizmu w państwach będących celem wrogich działań. Coraz niższy jest też wiek sprawców – nazywanych pokoleniem terrorystów z Tik-Toka. Na przykład w sierpniu 2024 r. policja aresztowała dwóch nastolatków w wieku 19 i 17 lat, którzy planowali ataki podczas koncertu Taylor Swift w Wiedniu. Z kolei podczas świąt Bożego Narodzenia w 2024 r. niemiecka policja zatrzymała 15-letniego terrorystę, który planował zamach na kościół w Berlinie.
4. Połączenie powyższych elementów skutkuje pojawieniem się nowych zagrożeń oraz modyfikacją już istniejących, w tym zagrożeń dla obiektów spełniających kryteria narodowej lub europejskiej infrastruktury krytycznej (IK). Cele te mogą być atakowane zarówno fizycznie, jak i z wykorzystaniem cyberprzestrzeni oraz we wszystkich domenach: lądowej, powietrznej, morskiej, cybernetycznej, kosmicznej i kognitywnej[5] (hybrydowość obszarów działania). Potwierdzają to m.in. przypadki niszczenia czy zakłócania działania podwodnej IK czy infrastruktury komunikacyjnej, a także ich lądowych, powietrznych, a nawet kosmicznych odpowiedników.

Celem artykułu jest analiza zagrożenia terrorystycznego w UE w latach 2020–2023 przeprowadzona na podstawie dorocznych raportów Europolu pt. *European Union Terrorism Situation and Trend Report*. Uwzględniono w niej kilka ważnych kategorii, takich jak: ataki przeprowadzone, nieudane oraz udaremnione, liczba osób aresztowanych z powodu działalności

[5] Za: *Multi-Domain Operations in NATO – Explained*, NATO, 5.10.2023, https://www.act.nato.int/article/mdo-in-nato-explained/ [dostęp: 2.03.2025].

terrorystycznej, postępowania sądowe dotyczące zatrzymań za popełnienie w krajach członkowskich UE przestępstw o charakterze terrorystycznym oraz formy terroryzmu: dżihadystyczny, prawicowy, lewicowy i anarchistyczny, etnonacjonalistyczny i separatystyczny. Najważniejszym punktem odniesienia jest analiza zagrożeń terrorystycznych dotyczących obiektów, które można klasyfikować jako IK. Poważnym ograniczeniem opracowania jest zakres mandatu Europolu. Do działań przeciwko terroryzmowi sponsorowanemu przez państwo może on być angażowany tylko pośrednio[6]. Bezpośrednia dyplomatyczna lub militarna reakcja na terroryzm państwowy podlega jurysdykcji instytucji odpowiedzialnej za politykę zagraniczną UE lub NATO, a nie Europolu. Ma to przełożenie również na jego aktywność informacyjną oraz zbierane przez niego dane, które są prezentowane w dorocznym raporcie. Warto dodać, że część państw UE podejmuje obecnie inicjatywę mającą na celu rozszerzenie mandatu Europolu o kwestie terroryzmu, którego źródłem są podmioty państwowe.

Terroryzm w Unii Europejskiej w 2020 roku

Pomimo globalnych ograniczeń wynikających z pandemii COVID-19 w 2020 r. nie zaobserwowano znaczącego spadku aktywności terrorystycznej na terenie UE. Według raportu TE-SAT 2021[7] poziom zagrożenia w 2020 r. był porównywalny z tym w 2019 r., a nawet nastąpił niewielki wzrost liczby ataków i prób ich przeprowadzenia. W UE (bez Wielkiej Brytanii) odnotowano 57 ataków terrorystycznych (ta liczba obejmuje również ataki udaremnione), o 2 więcej niż w 2019 r.

W 2020 r. najwięcej ataków terrorystycznych dokonano we Włoszech (24 przypadki), następnie we Francji (15) i Hiszpanii (9). Na dalszych

[6] Zagrożenie terroryzmem ma wymiar nie tylko wewnętrzny, lecz także geopolityczny, ponieważ w tle działają aktorzy państwowi, którzy mogą wspierać lub wykorzystywać terrorystów do własnych celów. Na terytorium UE istnieje terroryzm państwowy, np. Iran od lat sponsoruje ugrupowania zbrojne (jak Hezbollah) i dokonuje za granicą zamachów na przeciwników politycznych. Rosja z kolei prowadzi agresywną politykę hybrydową wobec państw Zachodu, m.in. propagandowo i finansowo wspiera skrajne ruchy ekstremistyczne w Europie, a jej służby specjalne prowadzą działania o charakterze terrorystycznym (np. zlecają zabójstwa dysydentów na terenie UE).

[7] Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2021*, https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2021-te-sat [dostęp: 4.02.2025].

miejscach znalazły się Niemcy (6), Belgia (2) i Austria (1). Po dołączeniu danych z Wielkiej Brytanii całkowita liczba zamachów w Europie wyniosła 119. Dane te potwierdzają, że nawet w okresie obowiązywania powszechnych restrykcji sanitarnych i ograniczeń związanych z możliwościami przemieszczania się aktywność terrorystyczna nie została zahamowana.

W analizowanym okresie zidentyfikowano 4 główne źródła ideologiczne działań ekstremistycznych. Ataki miały podłoże: lewicowe i anarchistyczne (25 ataków), dżihadystyczne (14), separatystyczne i etnonacjonalistyczne (14) oraz prawicowe (4). Utrzymująca się duża liczba ataków o podłożu lewicowym i anarchistycznym potwierdza, że jest to zjawisko o względnie stabilnym poziomie aktywności od kilku lat.

Chociaż w 2020 r. odnotowano spadek liczby przeprowadzonych zamachów inspirowanych ideologią dżihadystyczną (z 18 w 2019 r. do 14 w 2020 r.), to według Europolu nadal można je uznawać za najbardziej niebezpieczne. Ich realizacja zazwyczaj kończyła się sukcesem, co świadczy o coraz większej skuteczności sprawców i zwiększa ryzyko dla ludności cywilnej. Potencjał eskalacyjny tego zagrożenia wzrósł w związku z wydarzeniami geopolitycznymi, w tym wycofaniem sił międzynarodowych z Afganistanu i szybkim przejęciem władzy przez Talibów. Sukces ten został wykorzystany przez środowiska ekstremistyczne do wspierania narracji o trwałości i skuteczności islamistycznego oporu. Mogło to mieć wpływ także na nasilenie się nastrojów radykalnych w kręgach ekstremistów w Europie.

Z perspektywy działań antyterrorystycznych istotnym zjawiskiem był zauważalny spadek liczby zatrzymań osób podejrzanych o powiązania z działalnością terrorystyczną – z ponad 700 przypadków w 2019 r. do poniżej 450 w 2020 r. Kwestią dyskusyjną jest jednak to, czy mniejsza liczba zatrzymań świadczy o mniejszej aktywności terrorystycznej, czy może o utrudnionej pracy służb w warunkach pandemii. Wśród zatrzymanych dominowali podejrzani o związki z terroryzmem dżihadystycznym (57%), na kolejnych miejscach były osoby powiązane z terroryzmem o charakterze lewicowym i anarchistycznym (12%), separatystycznym (8%) oraz prawicowym (7%). Charakterystyka metod działania sprawców ujawnia, że ataków najczęściej dokonywały jednostki działające samodzielnie, tzw. samotne wilki, posługujące się łatwo dostępnymi środkami, takimi jak broń biała czy palna.

Należy podkreślić rosnącą rolę cyberprzestrzeni jako obszaru działania terrorystów. Pandemia wpłynęła na zwiększenie ruchu w sieci, co ekstremiści wykorzystali do szerzenia ideologii, prowadzenia rekrutacji

oraz konsolidacji swoich sympatyków. W raporcie zwrócono uwagę na to, że w przekazach terrorystycznych coraz częściej pojawiały się aktualne społecznie wątki, takie jak pandemia, kryzys ekologiczny czy zagrożenia związane z nowymi technologiami. Autorzy tych treści próbowali zyskać w ten sposób rozgłos i zainteresowanie nowych odbiorców. Wzrost znaczenia cyberprzestrzeni może mieć kilka przyczyn, poczynając od ograniczeń i utrudnień pandemicznych, przez osłabienie zdolności logistycznych terrorystów, a kończąc na instrukcjach przekazywanych np. przez ISIS, aby przeprowadzać zamachy z wykorzystaniem najprostszych środków. Należy zwrócić uwagę, że w związku z utrudnionym dostępem do popularnych komunikatorów terroryści cały czas poszukują nowych form komunikacji. Dotyczy to nie tylko islamistów, lecz także innych nurtów zagrożenia terrorystycznego.

Terroryzm w Unii Europejskiej w 2021 roku

Raport TE-SAT 2022[8] wskazał, że w porównaniu z wcześniejszymi latami rok 2021 przyniósł wyraźne osłabienie aktywności terrorystycznej w Europie. Istotnie spadła zarówno liczba zamachów – z ponad 50 w 2019 r. do 15 w 2021 r., jak i liczba aresztowań. Najwięcej incydentów odnotowano we Francji – 5. W Niemczech doszło do 3 ataków, w Szwecji do 2. Austria, Dania, Węgry, Belgia i Hiszpania zaraportowały po 1 ataku.

Mimo że liczba zamachów powiązanych z ideologią dżihadystyczną ponownie była niższa niż w latach poprzednich, ten typ zagrożenia nadal – według Europolu – uznaje się za najgroźniejszy. W 2021 r. spośród 11 zdarzeń tego typu 3 zakończyły się powodzeniem, a 8 zostało skutecznie udaremnionych. Na niezmiennym poziomie pozostała liczba prób zamachów o charakterze prawicowym (3 przypadki), spadła natomiast niemal zupełnie aktywność ekstremistycznych ruchów lewicowych i anarchistycznych – tylko 1 przypadek. Warto zwrócić uwagę na prawie całkowity zanik terroryzmu o podłożu separatystycznym i etnonacjonalistycznym, który jeszcze w 2020 r. stanowił istotną część tego zjawiska. Zmiana ta może być po części spowodowana ewolucją kryteriów klasyfikacyjnych stosowanych

[8] Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2022*, https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2022-te-sat [dostęp: 4.02.2025].

przez niektóre państwa członkowskie, w wyniku czego pewne działania ekstremistyczne nie są kwalifikowane już jako terroryzm.

Dominującą liczebnie grupą zatrzymanych w 2021 r. były osoby podejrzewane o związek z dżihadyzmem – 260 aresztowań, głównie we Francji, Hiszpanii i Austrii. Drugą najliczniejszą kategorią byli przedstawiciele nurtów skrajnie prawicowych (64 osoby). Mniej liczne grupy aresztowanych stanowiły osoby powiązane z ruchami separatystycznymi i etnonacjonalistycznymi (26) oraz z terroryzmem lewicowym i anarchistycznym (19).

Autorzy raportu zwracają uwagę, że pandemia COVID-19 mogła w dużym stopniu przyczynić się do spadku aktywności terrorystycznej w wymiarze fizycznym, gdyż ograniczyła mobilność, komunikację i możliwości organizacyjne ugrupowań ekstremistycznych. Miała także wpływ na zmianę sposobu działania organizacji terrorystycznych. Zintensyfikowały się natomiast działania prowadzone w przestrzeni cyfrowej – m.in. w zakresie rekrutacji, radykalizacji, szerzenia propagandy i zbierania funduszy. Wymaga to od służb bezpieczeństwa wypracowania metod przeciwdziałania dostosowanych do nowych uwarunkowań. Spadku fizycznej aktywności terrorystycznej nie należy jednak interpretować jako trwałego zaniku zagrożenia. Wzrost liczby zamachów na świecie, odbudowa struktur ISIS i Al-Kaidy, rozwój skrajnej prawicy, a także nowe formy terroryzmu – takie jak ataki przy użyciu dronów, działania w cyberprzestrzeni czy współpraca struktur państwowych z grupami terrorystycznymi – wskazują na ewolucyjny charakter zagrożenia.

Terroryzm w Unii Europejskiej w 2022 roku

Jak podano w raporcie TE-SAT z 2023 r.[9], w 2022 r. na terenie państw UE doszło do 28 zdarzeń zaklasyfikowanych jako ataki terrorystyczne. Liczba ta obejmuje ataki udane, nieudane oraz udaremnione (18). Jest to istotny wzrost procentowy w stosunku do 2021 r., kiedy to odnotowano 15 takich przypadków. Jednocześnie w 2022 r. było ich znacznie mniej niż w latach wcześniejszych (zwłaszcza przed pandemią COVID-19 – w 2019 r. przeprowadzono 55 ataków[10]). Do największej liczby incydentów doszło

[9] Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2023,* https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2023-te-sat [dostęp: 4.02.2025].

[10] Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2022*…, s. 8–9.

we Włoszech (12), a także we Francji (6), Grecji (4) i Belgii (3), pojedyncze przypadki odnotowano w Niemczech, Hiszpanii i na Słowacji.

Pod względem ideologicznym największą aktywność wykazywały ugrupowania skrajnie lewicowe i anarchistyczne (18 incydentów). Działania motywowane dżihadem stanowiły 6 przypadków, a ideologią skrajnie prawicową – 4 przypadki. W rezultacie tych zdarzeń zginęły 4 osoby: 2 w wyniku ataków islamistycznych, 2 w związku z przemocą motywowaną ekstremizmem prawicowym.

W analizowanym okresie organy ścigania państw UE zatrzymały łącznie 380 osób podejrzewanych o działalność o charakterze terrorystycznym. Najwięcej zatrzymań było we Francji (93), Hiszpanii (46), Niemczech (30), Belgii (22) oraz we Włoszech i Holandii (po 21). Zdecydowana większość aresztowań dotyczyła terroryzmu dżihadystycznego (266 osób). W związku z terroryzmem prawicowym dokonano 45 zatrzymań, a lewicowym i anarchistycznym – 19. Ujęto także 18 osób powiązanych z terroryzmem separatystycznym i etnonacjonalistycznym, 26 – powiązanych z innymi formami terroryzmu oraz 6 osób, w przypadku których forma terroryzmu nie została określona.

W 2022 r. zakończono 427 postępowań sądowych związanych z przestępstwami o charakterze terrorystycznym, nieco więcej niż w poprzednich latach (w 2020 r. – 422 i w 2021 r. – 423). Najwięcej procesów odbyło się we Francji (110). Następne w kolejności były: Belgia (81), Niemcy (54), Austria (48), Hiszpania (42), Węgry, Holandia (po 26) i Włochy (21). Wskaźnik wyroków skazujących był wysoki, dla spraw związanych z terroryzmem lewicowym i prawicowym wyniósł 100%, a dla przypadków motywowanych ideologią dżihadystyczną – 84%. Procesy dotyczące terroryzmu separatystycznego zakończyły się wyrokiem skazującym w 68% przypadków.

Z analizy metod stosowanych przez sprawców wynika, że najczęściej wybierali oni prymitywne, lecz skuteczne środki ataku. Ekstremiści lewicowi i anarchistyczni wykorzystywali przede wszystkim improwizowane ładunki zapalające oraz materiały wybuchowe domowej konstrukcji. Dżihadyści używali głównie noży oraz przemocy fizycznej (np. uduszenia), a sprawcy związani z prawicowym ekstremizmem sięgali po broń palną. Z uwagi na to, że podejmowane działania nie wymagały ani zaawansowanych zasobów, ani skomplikowanej logistyki, czyniło je to trudnymi do przewidzenia i zapobieżenia.

Niezmiennie istotnym elementem działalności terrorystycznej była przestrzeń cyfrowa. Internet służył terrorystom nie tylko do szerzenia

propagandy i ideologii, lecz także do rekrutacji, pozyskiwania funduszy oraz planowania ataków. W tym celu były wykorzystywane zarówno popularne platformy mediów społecznościowych, jak i zamknięte fora dyskusyjne, szyfrowane komunikatory oraz gry wideo. Zwiększająca się decentralizacja kanałów komunikacji utrudnia służbom bezpieczeństwa efektywne działania, a w związku z tym ryzyko radykalizacji rośnie.

Dane z 2022 r. wskazują, że terroryzm pozostaje istotnym zagrożeniem dla państw członkowskich UE. Mimo że liczba aresztowań i wyroków skazujących utrzymuje się na stabilnym poziomie, a aktywność organizacji takich jak ISIS czy Al-Kaida w UE słabnie, zagrożenie ewoluuje. Oprócz klasycznych form przemocy coraz istotniejsze staje się monitorowanie przestrzeni cyfrowej, gdzie radykalizacja następuje w sposób szybki, rozproszony i często trudny do wykrycia. Służby bezpieczeństwa muszą stale dostosowywać swoje działania do zmieniającej się dynamiki współczesnego terroryzmu, jest to także wyzwanie dla systemów prawnych.

Terroryzm w Unii Europejskiej w 2023 roku

W 2023 r. odnotowano łącznie 120 incydentów terrorystycznych w 7 państwach członkowskich UE, z czego 98 zakończyło się realizacją ataku, 9 prób było nieudanych, a 13 udaremniły służby bezpieczeństwa. Największą aktywność wykazały grupy separatystyczne, odpowiedzialne za 70 ataków, oraz grupy lewicowe i anarchistyczne, które przeprowadziły 32 ataki. Ataków o podłożu dżihadystycznym było 14. Zginęło w nich 6 osób, a 12 zostało rannych. Były to zdarzenia o największej liczbie ofiar. Ponadto udaremniono 2 ataki planowane przez ekstremistów prawicowych.

Większość ataków w 2023 r. była skierowana przeciwko: IK (15 zdarzeń), firmom prywatnym (7), ludności cywilnej (4) i funkcjonariuszom policji (3). Wśród zgłoszonych form ataków najczęstsze były: podpalenia (20), zamachy bombowe (8), niszczenie mienia (6), ataki z użyciem noża (6) i broni palnej (5).

Z analizy raportu TE-SAT 2024[11] wynika, że zagrożenie terrorystyczne w UE ma różne podłoża ideologiczne. Oprócz dżihadystycznych grup terrorystycznych aktywność wykazują organizacje o charakterze separatystycznym, lewicowym, anarchistycznym oraz prawicowym. Różnorodność

[11] Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2024*...

motywacji ideologicznych przekłada się na zróżnicowane cele i metody działania, co utrudnia możliwości przeciwdziałania i prewencji.

Terroryści coraz częściej wykorzystują nowoczesne technologie, w tym sztuczną inteligencję i narzędzia cyfrowe, do planowania ataków, prowadzenia rekrutacji oraz propagandy. Zauważalny jest wzrost zainteresowania pozyskiwaniem informacji na temat produkcji broni przy użyciu drukarek 3D, a także instrukcji dotyczących użycia dronów, materiałów wybuchowych i broni chemicznej. Takie działania są obserwowane w środowiskach skupionych wokół różnych ideologii, co oznacza potrzebę szerokiego podejścia do monitorowania tych zagrożeń i przeciwdziałania im.

Raport TE-SAT 2024 wskazuje na istotny wpływ wydarzeń geopolitycznych na dynamikę zagrożeń terrorystycznych w UE. Na przykład atak Hamasu na Izrael w październiku 2023 r. i eskalacja konfliktu w Strefie Gazy wpłynęły na wzrost napięć i aktywności ekstremistycznej w Europie. Tego rodzaju wydarzenia mogą prowadzić do zwiększonej radykalizacji i mobilizacji zwolenników różnych ideologii ekstremistycznych.

Zagrożenia terrorystyczne w Unii Europejskiej. Wyzwania i postulaty

Raporty Europolu potwierdzają, że obszar UE jest jednym z regionów bardziej zagrożonych terroryzmem. Wśród państw europejskich o podwyższonym poziomie ryzyka należy wskazać zarówno te już wcześniej często atakowane, np. Francję, Włochy czy Niemcy, jak i inne, np. Polskę, Czechy czy państwa bałtyckie. Kazus Polski – chociaż w raporcie Europolu z 2024 r. nie odnotowano żadnej próby ataku w Polsce i tylko 1 aresztowanie z powodu działalności terrorystycznej – jest ważny m.in. ze względu na wzrost zainteresowania międzynarodowej opinii publicznej państwem polskim. Wynika ono nie tylko z jego prezydencji w Radzie UE czy zaangażowania na rzecz wspierania Ukrainy, lecz także z innych polityczno-dyplomatycznych działań Polski.

Nasilanie się zagrożenia terrorystycznego potwierdzają dane Europolu. W 2021 r. na terytorium państw członkowskich UE odnotowano 18 ataków, w 2022 r. – 28, a w 2023 r. było ich aż 120, co oznacza ponadczterokrotny wzrost względem roku poprzedniego. Na uwagę zasługuje również duża dysproporcja w 2023 r. między liczbą ataków przeprowadzonych (98) a udaremnionych (13). Ponad 90% wszystkich ataków w analizowanym roku

dotyczyło 2 państw: Francji i Włoch. Wskazuje to, do pewnego stopnia, na ograniczone geograficznie występowanie zagrożeń terrorystycznych. Wzrost zagrożenia terrorystycznego jest dostrzegany również przez opinię publiczną w UE. Jak wynika z badań ankietowych przeprowadzonych w 2024 r. na terytorium UE oraz Wielkiej Brytanii przez Fundację Bertelsmanna, w których wzięło udział 26 000 osób, terroryzm to drugie – zdaniem ankietowanych – największe zagrożenie pokoju i bezpieczeństwa. Takiej odpowiedzi udzieliło 21% badanych. Na pierwszym miejscu (25% respondentów) wskazano niedostateczną ochronę granic[12].

W odniesieniu do źródeł zjawiska terroryzmu w UE należy zwrócić uwagę, że w raportach Europolu podkreślono różnorodność przyczyn terroryzmu w UE. Ma on nie tylko, jak nadal dość często błędnie się uważa, podłoże islamistyczne. Na przykład w 2023 r. odnotowano aż 70 ataków o podłożu separatystycznym oraz etnonacjonalistycznym, 32 o podłożu lewicowym oraz anarchistycznym i 14 o charakterze dżihadystycznym. Możliwa jest dalsza eskalacja różnych nurtów terroryzmu, państwowego (inspirowanego np. przez Rosję czy Białoruś) i pozapaństwowego, podsycanego m.in. przez służby specjalne wrogich państw, choćby w odpowiedzi na zintensyfikowaną politykę antyrosyjską, wsparcie dla Ukrainy czy programy zbrojeniowe realizowane w UE. Generuje to również groźbę częstszego atakowania (fizycznego i w cybersferze) obiektów związanych z przemysłem zbrojeniowym, w tym zaliczanych do IK. Groźne jest też odradzanie się ISIS i towarzysząca temu ofensywa operacyjno-propagandowa w różnych częściach świata. Jest to spowodowane różnymi czynnikami, w tym spektakularnym sukcesem islamistów w Syrii.

W ostatnich latach celem o zwiększonym poziomie narażenia na ataki stała się IK. Terroryści dostrzegli, że uderzenie w sieci energetyczne, transport czy łączność może sparaliżować państwo równie skutecznie jak zamach na ludzi, a bywa łatwiejsze do przeprowadzenia. Raport TE-SAT 2024 wskazuje, że w 2023 r. aż 15 ataków terrorystycznych w UE było wymierzonych w IK (najwięcej w historii tych raportów). Były to głównie ataki na sieci przesyłowe, podpalenia masztów telekomunikacyjnych (ruch przeciwko 5G) czy próby zakłócenia transportu kolejowego. Za większością tych czynów stali separatyści i anarchiści – np. korsykańscy nacjonaliści atakowali obiekty związane z funkcjonowaniem francuskiej administracji rządowej,

[12] *Survey: Border security and terrorism top threats for EU citizens*, Yahoo, 20.11.2024, https://www.yahoo.com/news/survey-border-security-terrorism-top-092813566.html [dostęp: 4.02.2025].

a anarchiści we Włoszech niszczyli stacje energetyczne i linie kolejowe. Chociaż ataki na IK rzadko powodują ofiary śmiertelne, ich skutki społeczne są poważne – przerwy w dostawach prądu, transporcie czy komunikacji wywołują chaos i straty ekonomiczne. Są to zatem bardzo atrakcyjne cele z perspektywy terrorystów chcących uderzyć w społeczeństwo jako całość. Zagrożenia dla IK są ściśle powiązane z koncepcją zagrożeń hybrydowych. Atak terrorystyczny na sieć gazową czy system finansowy może być elementem szerszej kampanii terrorystycznej prowadzonej przez wrogie państwo lub grupę. Rok 2023 dowiódł, że w nadchodzących latach IK będzie w centrum strategii antyterrorystycznej UE (nowa agenda antyterrorystyczna UE ukaże się w drugiej połowie 2025 r.). Wiele nowych lub zmodyfikowanych zagrożeń dla obiektów IK wiąże się z opisaną na początku artykułu specyfiką piątej fali terroryzmu oraz z kształtowaniem się triady: terrorysta/terroryści – grupy przestępcze – służby specjalne wrogich państw. Jest to szczególnie niebezpieczne w przypadku terroryzmu państwowego, czego przykładem są m.in. działania Rosji, Białorusi czy Iranu. Państwa te korzystają z szerokiego spektrum narzędzi operacyjnych, w tym z podmiotów zastępczych lub pośredników, w celu m.in. zatarcia śladów. Zwraca na to uwagę m.in. fińska służba specjalna SUPO (fin. Suojelupoliisi) w raporcie obejmującym 2024 r.[13]

Warto podkreślić znaczny wzrost przestępczości w UE. Europol wskazuje wprost, że głównym zagrożeniem bezpieczeństwa wewnętrznego państw UE jest terror gangów kryminalnych. W Europie Środkowo-Wschodniej dotyczy to zwłaszcza grup pochodzących z obszaru postradzieckiego, np. ukraińskich czy gruzińskich. To zagrożenie może się nasilić wraz z zakończeniem wojny w Ukrainie, tak jak to się działo w byłej Jugosławii. Należy się liczyć m.in. ze wzmożonym przemytem broni, materiałów wybuchowych oraz współpracą grup przestępczych z terrorystami czy służbami specjalnymi wrogich państw. Świadczą o tym np. relacje gangów gruzińskich z rosyjskimi, a pośrednio też z tamtejszymi służbami specjalnymi.

W podsumowaniu należy podkreślić, że UE potrzebuje nie tylko nowego spojrzenia na problematykę zagrożenia terrorystycznego, lecz wręcz nowej filozofii antyterrorystycznej na poziomie strategicznym, tak jak

[13] SUPO, *National Security Overview 2025*, https://katsaus.supo.fi/documents/62399122/236002257/National%20Security%20Overview%202025.pdf/a4480ede-834e-6cc3-3c08-f3b762d06253/National%20Security%20Overview%202025.pdf?t=1741941168438 [dostęp: 4.02.2025].

w przypadku kompasu konkurencyjności i doktryny gospodarczej UE czy kształtowania obecnej polityki obronnej, w tym produkcji uzbrojenia. Potrzeba zmiany wynika nie tylko z raportów Europolu, Mario Draghiego[14] czy Sauliego Niinistö[15], lecz przede wszystkim z ponownej eskalacji i ewolucji zagrożenia terrorystycznego. Oznacza to również nowe wyzwania związane z ochroną IK przed aktywnością o charakterze terrorystycznym, wspieraną pośrednio przez podmioty państwowe, wrogie UE. Raporty TE-SAT wskazują, że Europol nie ma mandatu do bezpośredniego przeciwdziałania terroryzmowi państwowemu. Konieczna jest więc rewizja uprawnień agencji UE w tym zakresie oraz wzmocnienie współpracy z NATO w obszarze budowania odporności IK na ataki o charakterze terrorystycznym wspierane przez podmioty państwowe.

Nowe podejście do bezpieczeństwa w UE powinno dotyczyć nie tylko np. zagrożeń ze strony Rosji i jej sojuszników, rozwiązania problemu migrantów czy bezpieczeństwa energetycznego, lecz także wielu innych kwestii, w tym efektywnego zwalczania terroryzmu. Skuteczne przeciwdziałanie zagrożeniu terrorystycznemu wymaga pogłębienia współpracy (w tym wywiadowczej, logistycznej, prawnej, politycznej) wszystkich państw członkowskich UE oraz rozszerzonego współdziałania z NATO oraz z innymi sojusznikami w różnych częściach świata. Celem jest budowanie odporności nie tylko w wymiarze zewnętrznym, lecz także wewnętrznym.

Zagrożeniem dla spójnej polityki antyterrorystycznej UE mogą być partykularne interesy poszczególnych państw członkowskich, trwający w niektórych z nich kryzys polityczny, rozdźwięk w relacjach transatlantyckich, brak środków finansowych czy krach ekonomiczny zapowiadany przez różnych specjalistów. Na szczególne rozpatrzenie zasługuje scenariusz zakładający ograniczenie współpracy wywiadowczej pomiędzy USA a europejskimi partnerami, co mogłoby m.in. znacznie zmniejszyć efektywność działań antyterrorystycznych prowadzonych przez UE.

[14] 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: 4.02.2025].

[15] S. Niinistö, *Safer Together. Strengthening Europe's Civilian and Military Preparedness and Readiness*, European Commission, https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf [dostęp: 4.02.2025].

Bibliografia

Parker T., Sitter N., *The Four Horsemen of Terrorism: It's Not Waves, It's Strains*, „Terrorism and Political Violence" 2016, t. 28, nr 2, s. 197–216. https://doi.org/10.1080/09546553.2015.1112277.

Rapoport D., *It Is Waves, Not Strains*, „Terrorism and Political Violence" 2016, t. 28, nr 2, s. 217–224. https://doi.org/10.1080/09546553.2015.1112278.

Rapoport D., *Waves of Global Terrorism: From 1879 to the Present*, Columbia University Press 2022.

Richards A., *Defining terrorism*, w: *Routledge Handbook of Terrorism and Counterterrorism*, A. Silke (red.), New York 2019.

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

Źródła internetowe

Gunaratna R., *Global Terrorism Threat Forecast 2025*, „RSIS Commentary" 2025, nr 002, https://dr.ntu.edu.sg/bitstream/10356/182595/2/CO25002.pdf [dostęp: 9.03.2025].

Multi-Domain Operations in NATO – Explained, NATO, 5.10.2023, https://www.act.nato.int/article/mdo-in-nato-explained/ [dostęp: 2.03.2025].

Security Council debates growing terrorism threat in Africa, United Nations, 21.01.2025, https://news.un.org/en/story/2025/01/1159246 [dostęp: 5.03.2025].

SUPO, *National Security Overview 2025*, https://katsaus.supo.fi/documents/62399122/236002257/National%20Security%20Overview%202025.pdf/a4480ede-834e-6cc3-3c08-f3b762d06253/National%20Security%20Overview%202025.pdf?t=1741941168438 [dostęp: 4.02.2025].

Survey: Border security and terrorism top threats for EU citizens, Yahoo, 20.11.2024, https://www.yahoo.com/news/survey-border-security-terrorism-top-092813566.html [dostęp: 4.02.2025].

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: 4.02.2025].

Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2020*, https://www.europol.europa.eu/publications-events/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2020 [dostęp: 4.02.2025].

Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2021*, https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2021-te-sat [dostęp: 4.02.2025].

Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2022*, https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2022-te-sat [dostęp: 4.02.2025].

Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2023*, https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2023-te-sat [dostęp: 4.02.2025].

Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2024*, https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2024-eu-te-sat [dostęp: 4.02.2025].

Institute for Economics & Peace, *Global Terrorism Index 2025*, https://www.economicsandpeace.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf [dostęp: 10.03.2025].

Niinistö S., *Safer Together. Strengthening Europe's Civilian and Military Preparedness and Readiness*, European Commission, https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf [dostęp: 4.02.2025].

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 Organizacji Bezpieczeństwa i Współpracy w Europie ds. bezpieczeństwa, w tym terroryzmu. 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. Były dziekan Wydziału Politologii i Stosunków Międzynarodowych Wyższej Szkoły Nauk Humanistycznych i Dziennikarstwa w Poznaniu. Członek m.in.: Komisji Bałkanistyki PAN, Rady Naukowej Centrum Badań nad Terroryzmem Collegium Civitas, Rady Programowej Projektu budowy Centralnego Okręgu Przemysłowego 2 (COP 2). Autor wielu ekspertyz i analiz przygotowanych dla polskich i zagranicznych instytucji, a także publikacji z zakresu stosunków międzynarodowych oraz bezpieczeństwa wewnętrznego i międzynarodowego, ze szczególnym uwzględnieniem problematyki: twardych i miękkich zagrożeń bezpieczeństwa, NATO, polityki bezpieczeństwa Polski i UE, hybrydowości terroryzmu. Ekspert NATO DEEP eAcademy ds. bezpieczeństwa wewnętrznego i międzynarodowego.

Kontakt: wojciechowski.s@wp.pl

Terroryzm – studia, analizy, prewencja, 2025, wydanie specjalne: 237–262

https://doi.org/10.4467/27204383TER.25.009.21512

Artykuł

Cyberzagrożenia jako działalność hybrydowa przeciwko Unii Europejskiej w świetle obecnej sytuacji geopolitycznej

Cyber threats as hybrid activity against the European Union in light of the current geopolitical situation

MONIKA STODOLNIK

https://orcid.org/0009-0000-5319-7968

Agencja Bezpieczeństwa Wewnętrznego

Abstrakt

W artykule została przedstawiona analiza cyberzagrożeń jako przejawu zagrożeń hybrydowych, z którymi zmaga się Europa. Autorka przeanalizowała raporty państw Unii Europejskiej i NATO pod kątem tego, w jaki sposób wskazane zagrożenia są prezentowane przez służby wywiadowcze, rządy oraz krajowe zespoły CERT (Computer Emergency Response Team) i CSIRT (Computer Security Incident Response Team). Omówiła również kategoryzację cyberzagrożeń na podstawie ich źródła pochodzenia oraz celu działania, z uwzględnieniem grup sponsorowanych przez państwa, haktywistycznych oraz cyberprzestępczych. Wskazała na wzrastającą częstość cyberataków, prowadzonych zwłaszcza z Rosji i Chin, oraz omówiła ich wpływ na infrastrukturę krytyczną i stabilność polityczną państw. Zaprezentowała zmieniający się krajobraz cyberzagrożeń w Europie, podała przykłady cyberataków oraz opisała sposoby raportowania o tych zdarzeniach przyjęte w Danii, Niemczech, Estonii, Litwie, Łotwie oraz Polsce.

Słowa kluczowe

zagrożenia hybrydowe, cyberatak, cyberbezpieczeństwo, dezinformacja, operacje informacyjne

Abstract

The article presents analysis of cyber threats as a manifestation of the hybrid threats facing Europe. The author analysed reports from European Union and NATO countries in terms of how the identified threats are presented by intelligence services, governments and national CERTs (Computer Emergency Response Teams) and CSIRTs (Computer Security Incident Response Teams). She also discussed the categorisation of cyber threats based on their source of origin and their purpose, including state-sponsored, hacktivist and cybercriminal groups. She pointed to the increasing frequency of cyber attacks, especially those conducted from Russia and China, and discussed their impact on the critical infrastructure (CI) and political stability of states. She presented the changing landscape of cyber threats in Europe, gave examples of cyber attacks and described the methods of reporting these incidents adopted in Denmark, Germany, Estonia, Lithuania, Latvia and Poland.

Keywords

hybrid threats, cyber attack, cyber security, disinformation, information operations

Wprowadzenie

Współczesna sytuacja geopolityczna sprawia, że zagrożenia hybrydowe stają się jednym z najpoważniejszych wyzwań dla bezpieczeństwa i stabilności Europy. Zagrożenia hybrydowe stanowią połączenie taktyk konwencjonalnych oraz niekonwencjonalnych i mają na celu m.in. destabilizację państwa, jego demokracji oraz podważenie zaufania społecznego. Odwołując się do definicji Francisa Fukuyamy, którego zdaniem (...) *zaufanie to mechanizm oparty na założeniu, że innych członków danej społeczności cechuje uczciwe i kooperatywne zachowanie oparte na wyznawanych normach*[1], można zauważyć, że manipulacyjne działania psychologiczne, dezinformacyjne naruszają ten

[1] F. Fukuyama, *Zaufanie. Kapitał społeczny a droga do dobrobytu*, Warszawa 1997, s. 38.

właśnie mechanizm i pogłębiają podziały w społeczeństwie. W 2025 r. Europa jest szczególnie narażona na tego rodzaju zagrożenia ze względu na bliskie sąsiedztwo z możliwym przeciwnikiem, a także rozwój technologiczny, którego potencjał może być wykorzystany zarówno do obrony, jak i ataku. Obserwacje i lekcje wynoszone z wojny w Ukrainie wskazują prawdopodobne wektory działalności Federacji Rosyjskiej (FR) w sytuacji rozszerzenia konfliktu na inne państwa europejskie. Dynamiczny rozwój sztucznej inteligencji w ostatnich latach wspiera wrogą działalność w cyberprzestrzeni, pod kątem generowania treści dezinformacyjnych oraz rozwoju narzędzi służących do ataków na infrastrukturę teleinformatyczną.

Standard życia rośnie wraz z postępem technologicznym. Rozwój technologii informacyjno-telekomunikacyjnych (ang. *information and communication technologies*, ICT) oraz rosnąca zależność od automatyzacji różnych sektorów, zwłaszcza systemów kontroli przemysłowej (ang. *industrial control systems*, ICS), powodują, że ryzyko narażenia społeczeństwa na zagrożenia pochodzące z cyberprzestrzeni się zwiększyło. Destrukcyjne działania są kierowane zwłaszcza na sektor energetyczny, będący kluczowym filarem gospodarki każdego nowoczesnego państwa[2]. Jak wskazuje EnergiCERT, duński zespół reagowania na incydenty komputerowe sektora energii, liczba ataków na ten sektor w Europie stale wzrastała w latach 2015–2022[3]. Ataki na podmioty sektora energii mogą doprowadzić do paraliżu kraju – niezależnie od tego, czy sprawcy kierują się pobudkami finansowymi, ideologicznymi czy politycznymi. Jednocześnie liczba oraz charakter oficjalnych dokumentów i korespondencji tworzonych i przetwarzanych w formie elektronicznej sprawiają, że jest to główny cel operacji szpiegowskich stwarzających zagrożenie bezpieczeństwa narodowego.

W artykule został przeanalizowany wielowymiarowy charakter zagrożeń hybrydowych, przed którymi stoi Europa. Dokonano tego na podstawie przeglądu raportów dotyczących cyberzagrożeń oraz cyberataków jako przejawów działalności hybrydowej, sporządzonych w wybranych krajach Unii Europejskiej i NATO. Przedmiotem analizy był sposób, w jaki te zagrożenia są przedstawiane przez służby wywiadowcze, rządy oraz

[2] *Cybersecurity of Critical Sectors – Energy*, ENISA, https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors/energy [dostęp: 8.04.2025].

[3] *Cyber attacks against European energy & utility companies*, EnergiCERT, wrzesień 2022, https://sektorcert.dk/wp-content/uploads/2022/09/Attacks-against-European-energy-and-utility-companies-2020-09-05-v3.pdf [dostęp: 8.04.2025].

zespoły CERT i CSIRT Danii, Niemiec, Estonii, Litwy, Łotwy i Polski – państw zlokalizowanych w niedużej odległości od FR i będących w zainteresowaniu rosyjskich grup cyberofensywnych.

Krajobraz cyberzagrożeń jako zagrożeń hybrydowych

Zgodnie z definicją NATO: *Zagrożenia hybrydowe łączą środki wojskowe i niewojskowe, jawne i niejawne, w tym dezinformację, cyberataki, presję ekonomiczną, użycie nieregularnych formacji zbrojnych i wojsk regularnych. Metody hybrydowe służą do zacierania granic między wojną a pokojem oraz mają na celu sianie wątpliwości w umysłach ludzi będących grupą docelową. Ich celem jest destabilizacja i podważanie fundamentów społeczeństw*[4]. Unia Europejska w dokumencie opracowanym przez Komisję Europejską, zatytułowanym *Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym – odpowiedź Unii Europejskiej* (*Joint framework on countering hybrid threats – a European Union response*), podkreśla, że (...) *zagrożenia hybrydowe są różnie definiowane i definicje te należy formułować w sposób elastyczny, tak by uwzględniały one zmienny charakter tego rodzaju zagrożeń*[5]. Z kolei Europejskie Centrum Doskonalenia ds. Przeciwdziałania Zagrożeniom Hybrydowym (European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE) przedstawia zagrożenia hybrydowe jako (...) *działania podejmowane przez państwa autorytarne oraz podmioty niepaństwowe, które często działają jako pełnomocnicy reżimów autorytarnych. Przykładami aktorów stwarzających zagrożenia hybrydowe są Rosja, Chiny i Iran. Podmioty niepaństwowe mogą obejmować grupy, ruchy lub inne jednostki wykorzystywane lub podporządkowane w celu realizacji określonych celów strategicznych*[6].

[4] *Countering hybrid threats*, NATO, 7.05.2024, https://www.nato.int/cps/en/natohq/topics_156338.htm? [dostęp: 19.03.2025]. Tłumaczenia w artykule pochodzą od redakcji (dop. red.).

[5] *Wspólny komunikat do Parlamentu Europejskiego i Rady. Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym – odpowiedź Unii Europejskiej*, Bruksela, 6.04.2016, JOIN(2016) 18 final, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52016JC0018, s. 2 [dostęp: 19.03.2025].

[6] *Frequently asked questions on hybrid threats*, Hybrid CoE, https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ [dostęp: 19.03.2025].

Rozważając cyberzagrożenia w tym kontekście, można je podzielić na ogólne kategorie w zależności od tego, kto jest ich źródłem oraz jakimi metodami posługuje się do osiągnięcia obranego celu:

- Podmioty państwowe (aktorzy państwowi), często wysoce zaawansowane technologicznie i operacyjnie:
  - cyberszpiegostwo,
  - cybersabotaż,
  - operacje informacyjne w cyberprzestrzeni.
- Grupy hakerskie (haktywiści) motywowane ideologicznie:
  - zakłócanie funkcjonowania systemów i usług IT (ataki typu DDoS),
  - cybersabotaż (ataki zmieniające parametry, niszczące, wpływające na świadczenie usługi w sposób inny niż przez niedostępność),
  - podmiana zawartości strony (ang. *defacement*),
  - ataki typu *hack-and-leak* (włamanie i wyciek danych).
- Cyberprzestępcy działający dla korzyści finansowych:
  - wymuszenia finansowe z wykorzystaniem oprogramowania ransomware,
  - wymuszenia finansowe przez groźbę ujawnienia danych.

Podmioty państwowe, nazywane również grupami sponsorowanymi przez państwo, często utożsamiane z grupami APT (ang. *advanced persistent threat*)[7], to jednostki wspierane przez rząd, często będące częścią służb specjalnych prowadzące ofensywne działania cybernetyczne w interesie państwa[8]. Cyberszpiegostwo, będące naturalnym rozszerzeniem tradycyjnych metod wywiadowczych, stanowi trzon ich działalności – zarówno jako cel sam w sobie, jak i środek do przeprowadzania rozpoznania, niezbędnego do pozostania niezauważonym. Cyberszpiegostwo jest najczęściej realizowane za pomocą ataków phishingowych lub spearphishingowych, czyli wykorzystujących techniki inżynierii społecznej do manipulowania za pośrednictwem poczty e-mail w celu pozyskania określonych informacji lub infekowania stacji roboczych złośliwym oprogramowaniem. Cyberszpiegostwo oprócz phishingu może obejmować również naruszenie bezpieczeństwa urządzenia lub sieci przez wykorzystanie luki w zabezpieczeniach, czyli słabości systemu IT (może to być

[7] Grupy APT – zorganizowane jednostki realizujące wyrafinowane i długo trwające ataki w cyberprzestrzeni.

[8] J. Kose, *Cyber Warfare: An Era of Nation-State Actors And Global Corporate Espionage*, „ISSA Journal" 2021, t. 19, nr 4, s. 12–15.

zarejestrowana, dobrze znana podatność, luka typu zero-day, nadużycie funkcji systemu lub błąd użytkownika). Tego rodzaju ataki podważają jeden z 3 kluczowych filarów cyberbezpieczeństwa – poufność[9]. W odniesieniu do integralności danych takie ataki są uznawane za cybersabotaż – mają charakter destrukcyjny i niosą ze sobą znacznie poważniejsze konsekwencje. Mogą zakłócić życie codzienne obywateli, np. przez przerwanie dostaw energii elektrycznej czy opóźnienia w transporcie, gdy zostaną wymierzone w infrastrukturę krytyczną. Mogą nawet spowodować ofiary śmiertelne, zwłaszcza gdy celem staną się systemy nawigacyjne lub systemy ochrony zdrowia.

Operacje informacyjne to (...) *działania podejmowane w celu wpływania na informacje i systemy informacyjne przeciwnika przy jednoczesnej ochronie własnych zasobów informacyjnych i systemów*[10]. Operacje informacyjne wspomagane cyberatakami, znane również jako kampanie wpływu – terminy te są stosowane zamiennie – (...) *znajdują się na styku oszustw opartych na danych wywiadowczych i efektów wywołanych z myślą o strategii*[11]. Polegają na (...) *celowym wykorzystaniu informacji przez jedną stronę, aby zdezorientować przeciwnika, wprowadzić w błąd i ostatecznie wpłynąć na dokonywane przez niego wybory oraz podejmowane decyzje*[12]. Tego rodzaju działalność może obejmować naruszanie systemów IT mediów informacyjnych w celu publikowania spreparowanych treści w renomowanych źródłach, tworzenie własnych stron internetowych i profili w mediach społecznościowych oraz masowe wysyłanie wiadomości e-mail czy SMS.

Słowo haktywizm powstało z połączenia słów *hacking* i *activism*. Oznacza ono (...) *połączenie oddolnego protestu politycznego z hakowaniem komputerowym*[13]. W ostatnim czasie na czele haktywistów znajdują się grupy prorosyjskie i propalestyńskie, organizujące się i komunikujące przez

[9] Triada CIA: poufność, integralność, dostępność (ang. *confidentiality, integrity, availability*).

[10] D.T. Kuehl, *Information Operations, Information Warfare, and Computer Network Attack: Their Relationship to National Security in the Information Age*, „International Law Studies" 2022, t. 76, s. 36.

[11] J. Vićić, R. Harknett, *Identification-imitation-amplification: understanding divisive influence campaigns through cyberspac*e, „Intelligence and National Security" 2024, t. 39, nr 5, s. 897–914. https://doi.org/10.1080/02684527.2023.2300933.

[12] H. Lin, J. Kerr, *On Cyber-Enabled Information/Influence Warfare and Manipulation*, w: *The Oxford Handbook of Cyber Security*, P. Cornish (red.), Oxford University Press 2021, s. 251–272. https://doi.org/10.1093/oxfordhb/9780198800682.013.15.

[13] T. Jordan, P. Taylor, *Hacktivism and Cyberwars. Rebels with a cause?*, London 2004, s. 1.

aplikację Telegram oraz przeprowadzające różnego rodzaju cyberataki o różnej skuteczności. Oddolny charakter tych działań bywa kwestionowany. Niektórzy eksperci uważają, że grupy takie jak XakNet Team, Infoccentr, Solntsepek i Cyber Army of Russia Reborn współpracują z rosyjskim Głównym Zarządem Wywiadowczym (GRU) oraz z powiązanymi z nim grupami cyberzagrożeń, takimi jak APT28[14] i APT44[15].

Najbardziej znane grupy haktywistyczne stosują głównie ataki typu *distributed denial-of-service* (DDoS), których celem jest uniemożliwienie dostępu do wybranych stron internetowych lub usług dla ogółu użytkowników. Grupy te naruszają również infrastrukturę przez nieautoryzowany dostęp. Często nie chodzi im przy tym o osiągnięcie jakiegoś złożonego celu, a jedynie o zademonstrowanie swoich możliwości technicznych. Narzędzia wykorzystywane przez te grupy do rozpowszechniania swoich przekazów to również *defacement* stron internetowych oraz ataki typu *hack-and-leak*. Pierwsze działanie polega na zastąpieniu treści strony internetowej wiadomością od hakera, drugie na upublicznieniu danych wykradzionych z sieci i serwerów zaatakowanego podmiotu[16].

Podobnie jak haktywizm jest aktywizmem w cyberprzestrzeni, tak cyberprzestępczość (...) *składa się z czynów przestępczych popełnianych online przy użyciu sieci łączności elektronicznej i systemów informatycznych*[17]. Takimi czynami są np. ataki na systemy informatyczne jako najbardziej krytyczne dla państwa, a nie dla samych obywateli. Najczęściej zgłaszane incydenty związane z cyberprzestępczością dotyczą oprogramowania ransomware, które (...) *stało się dominującym zagrożeniem dla cyberbezpieczeństwa*[18]. Ransomware to rodzaj złośliwego oprogramowania, które jest

[14] Mandiant Intelligence, *Hacktivists Collaborate with GRU-sponsored APT28*, Mandiant, 23.09.2022, https://cloud.google.com/blog/topics/threat-intelligence/gru-rise-telegram-minions [dostęp: 19.03.2025].

[15] G. Roncone i in., *APT44: Unearthing Sandworm*, Mandiant, 17.04.2024, https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf [dostęp: 19.03.2025].

[16] D. Sancho, *Understanding Hacktivists. The Overlap of Ideology and Cybercrime*, Trend Micro, 4.02.2025, https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/understanding-hacktivists-the-overlap-of-ideology-and-cybercrime [dostęp: 19.03.2025].

[17] *Cybercrime*, European Commission, 31.10.2024, https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en [dostęp: 19.03.2025].

[18] T. McIntosh i in., *Ransomware Reloaded: Re-examining Its Trend, Research and Mitigation in the Era of Data Exfiltration*, „ACM Computing Surveys" 2024, t. 57, nr 1, s. 1. https://doi.org/10.1145/3691340.

wykorzystywane po to, aby wymusić od zaatakowanego okup przez odmowę dostępu do systemów i danych. Większość obecnie dokonywanych ataków ransomware to ataki podwójnego wymuszenia, w których atakujący szyfruje dane i je kradnie. Żąda przy tym okupu nie tylko za odszyfrowanie, lecz także za uniemożliwienie ich sprzedaży czy publikacji[19]. Takie oprogramowanie może zakłócać operacyjność podmiotu, a ze względu na skutki w postaci przerwy w świadczeniu usług oraz wycieku danych, w tym klientów, może powodować utratę zaufania ze strony potencjalnych partnerów do współpracy.

W latach 2014–2024 częstość ataków hybrydowych, zwłaszcza w cyberprzestrzeni, rosła. Federacja Rosyjska jest jak dotąd największym sprawcą sponsorowanych przez państwo cyberataków – włączając w to ataki prorosyjskich haktywistów – przeciwko krajom europejskim[20]. Były one wymierzone głównie w systemy rządowe i strony internetowe, infrastrukturę krytyczną, firmy państwowe i prywatne, think tanki, organizacje pozarządowe, dziennikarzy i polityków. W 2022 r. grupy haktywistów działających na rzecz Rosji przeprowadziły 61% cyberataków na świecie[21]. Największym katalizatorem takiej aktywności jest wojna w Ukrainie. Od początku 2022 r. różne podmioty deklarują wsparcie dla Rosji i działają w jej interesie, prowadząc cyberszpiegostwo, cybersabotaż i operacje informacyjne przeciwko krajom UE i NATO[22]. Powiązani z Rosją cyberprzestępcy dokonujący ataków na Europę i USA działają nie tylko z pobudek politycznych. Niektórzy z nich to Hunters International[23],

[19] *What is data exfiltration?*, IBM, https://www.ibm.com/think/topics/data-exfiltration [dostęp: 19.03.2025].

[20] *Microsoft Digital Defense Report 2024, The foundations and new frontiers of cybersecurity*, https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024, s. 13 [dostęp: 19.03.2025].

[21] Thales Cyber Threat Intelligence, *From Ukraine to the whole of Europe: cyber conflict reaches a turning point*, Thales, 29.03.2023, https://www.thalesgroup.com/en/worldwide/security/press_release/ukraine-whole-europecyber-conflict-reaches-turning-point [dostęp: 8.04.2025].

[22] S.G. Jones, *Russia's Shadow War Against the West*, Center for Strategic & International Studies, 18.03.2025, https://www.csis.org/analysis/russias-shadow-war-against-west [dostęp: 19.03.2025].

[23] R. Wolert, *RaaS group profile Hunters International*, CERT Orange, 28.10.2024, https://cert.orange.pl/wp-content/uploads/2024/11/CERTOPL_CTI_Hunters_International_en.pdf [dostęp: 19.03.2025].

Hive[24] czy Conti[25]. Niezależnie od przypisania haktywisty czy grupy cyberprzestępczej do APT, w przypadku rosyjskiej aktywności w cyberprzestrzeni należy również rozważyć działania pod obcą flagą. Jeśli uwzględni się takie przykłady jak aktywność grupy identyfikującej się jako Cyber Berkut w 2014 r., działania Cyber Caliphate w 2015 r. i ataki ransomware w 2016 r. i 2017 r., wszystkie przypisywane rosyjskiemu wywiadowi wojskowemu GRU[26], to zasięg działania rosyjskich służb specjalnych może być szerszy niż można było początkowo przypuszczać.

Kolejnym poważnym źródłem cyberzagrożeń są Chiny, które realizują swoje cele polityczne i ideologiczne, m.in. dążą do uzyskania statusu supermocarstwa[27]. Działania hakerskie, które prowadzą, służą strategicznym celom ekonomicznym. Zgodnie z chińską strategią wojskową (...) *cyberprzestrzeń stała się nowym filarem rozwoju gospodarczego i społecznego*[28]. W ocenie ekspertów NATO (...) *Części chińskiego wojska stały się dla rządu użytecznymi narzędziami do prowadzenia politycznego i gospodarczego cyberszpiegostwa, a także do pomocy w zmniejszeniu technologicznych i strategicznych braków ChALW* [Chińskiej Armii Ludowo-Wyzwoleńczej] *w stosunku do konkurentów*[29]. Sektory gospodarki państw europejskich najbardziej narażone na ataki to: energetyka, telekomunikacja i transport[30].

---

[24] *Russian National Charged with Ransomware Attacks Against Critical Infrastructure*, U.S. Department of Justice, 16.05.2023, https://www.justice.gov/archives/opa/pr/russian-national-charged-ransomware-attacks-against-critical-infrastructure [dostęp: 19.03.2025].

[25] *Multiple Foreign Nationals Charged in Connection with Trickbot Malware and Conti Ransomware Conspiracies*, U.S. Department of Justice, 7.09.2023, https://www.justice.gov/archives/opa/pr/multiple-foreign-nationals-charged-connection-trickbot-malware-and-conti-ransomware [dostęp: 19.03.2025].

[26] A. Greenberg, *A Brief History of Russian Hackers' Evolving False Flags*, Wired, 21.10.2019, https://www.wired.com/story/russian-hackers-false-flags-iran-fancy-bear/ [dostęp: 19.03.2025].

[27] A.H. Cordesman, *China's Emergence as a Superpower*, Center for Strategic & International Studies, 15.08.2023, https://www.csis.org/analysis/chinas-emergence-superpower [dostęp: 19.03.2025].

[28] *China's Military Strategy*, Ministry of National Defense of the People's Republic of China, 23.06.2021, http://eng.mod.gov.cn/xb/Publications/WhitePapers/4887928.html [dostęp: 19.03.2025].

[29] M. Raud, *China and Cyber: Attitudes, Strategies, Organization*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn 2016, https://ccdcoe.org/uploads/2018/10/CS_organisation_CHINA_092016_FINAL.pdf, s. 21 [dostęp: 19.03.2025].

[30] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2024 roku*, w przygotowaniu.

Dania

Do jednego z największych cyberataków na duńską IK doszło w maju 2023 r. Aktor, którego nie wiąże się otwarcie z GRU, ale SektorCERT podejrzewa, że jest powiązany z grupą Sandworm[31], przeprowadził dokładny rekonesans przed atakiem. Mógł on obejmować, oprócz cyberszpiegostwa, również tradycyjne sposoby gromadzenia danych wywiadowczych. W raporcie SektorCERT poinformował, że w czasie ataku informacje o podatnych urządzeniach nie były dostępne w serwisach publicznych (takich jak Censys lub Shodan), co dowodzi, że atakujący uzyskali je w inny sposób[32]. Luka oprogramowania urządzenia brzegowego firmy Zyxel, która została wykorzystana podczas tego ataku (CVE-2023-28771), otrzymała ocenę 9,8 na 10. Czyni to z niej lukę krytyczną – łatwą do wykorzystania i pozwalającą na naruszenie bezpieczeństwa, które ma poważne konsekwencje. Podatne na ataki urządzenia wyprodukowane przez Zyxel były używane w tym czasie w dużej mierze przez niewielkich duńskich operatorów IK w ich środowiskach OT[33]. W sumie udało się zagrozić bezpieczeństwu 22 firm energetycznych, a kilka z nich odnotowało zakłócenia w działalności.

Najnowsza ocena Danii dotycząca zagrożeń hybrydowych ze strony Rosji jest taka, że (...) *wykorzystuje ona środki hybrydowe zarówno w okresie poprzedzającym bezpośredni konflikt zbrojny, jak i w jego trakcie* (...) *środki hybrydowe obejmują narzędzia polityczne, gospodarcze, informacyjne i wojskowe, które mogą być wykorzystywane w sposób skoordynowany w celu maksymalizacji ich wpływu*[34]. Duńska Służba Wywiadu Obronnego (dun. Forsvarets Efterretningstjeneste) wskazuje, że w rosyjskie operacje hybrydowe są angażowane zarówno władze państwowe, jak i podmioty prywatne, przy czym te pierwsze koordynują działania. W przypadku tego rodzaju operacji często jest ukrywane, kto za nimi stoi[35]. Duńskie Centrum Cyberbezpieczeństwa (dun. Center

[31] *The attack against Danish, critical infrastructure*, SektorCERT, listopad 2023, https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf, s. 15 [dostęp: 19.03.2025].

[32] Tamże, s. 10.

[33] Operational technology – systemy i urządzenia wykorzystywane do monitorowania, kontrolowania i zarządzania procesami technologicznymi, takimi jak maszyny produkcyjne, pompy, urządzenia pomiarowe czy systemy zarządzania ruchem.

[34] *Intelligence Outlook 2024*, Danish Defence Intelligence Service, 22.01.2025, https://www.fe-ddis.dk/en/produkter/Risk_assessment/riskassessment/Intelligenceoutlook2024/, s. 26 [dostęp: 19.03.2025].

[35] Tamże.

for Cybersikkerhed), które obecny poziom zagrożenia i cele Rosji ocenia podobnie jak wywiad, wskazuje, że (...) *jest prawdopodobne, że sponsorowani przez państwo rosyjscy hakerzy prowadzą cyberszpiegostwo przeciwko duńskiej infrastrukturze krytycznej w ramach przygotowań do destrukcyjnych cyberataków w przyszłości*[36]. Jednocześnie podejrzewa się, że cyberszpiegostwo w celu uzyskania informacji na temat technologii i polityki prowadzą również Chiny. Centrum to jest zdania, że największe ryzyko cyberataków, które skutkują ofiarami śmiertelnymi lub rannymi, znacznymi szkodami materialnymi, zniszczeniem informacji, danych, oprogramowania czy manipulacją nimi, wiąże się z Rosją, a głównie z grupami sponsorowanymi przez państwo.

Niemcy

W maju 2023 r. niemiecka federalna minister spraw wewnętrznych stwierdziła: *Absolutnie nie damy się zastraszyć rosyjskiemu reżimowi*[37]. Słowa te padły w odniesieniu do cyberataków przeprowadzanych przez FR. Przyczyną takiej reakcji było podanie do wiadomości, że GRU i jego grupa zagrożeń APT28 stały za cyberatakami ze stycznia 2023 r. Celem tych ataków były systemy partii SPD oraz firm z sektora logistyki, obronności, lotnictwa i IT. Atak był możliwy ze względu na lukę w zabezpieczeniach programu Microsoft Outlook, która spowodowała, że nieautoryzowany aktor mógł uzyskać dostęp do kont e-mail tych podmiotów. Niemcy podtrzymały opinię, że ten atak był (...) *poważną ingerencją w struktury demokratyczne*[38]. Federalne Ministerstwo Spraw Wewnętrznych i Ojczyzny (niem. Bundesministerium des Innern und für Heimat) ocenia, że wojna w Ukrainie zmieniła sytuację bezpieczeństwa w Niemczech w taki sposób, że kraj ten potrzebuje lepszej ochrony i większej świadomości na temat podatności na cyberataki i rosyjską dezinformację[39].

[36] *Threat assessment: the cyber Threat against Denmark 2024*, Centre for Cyber Security, wrzesień 2024, https://www.cfcs.dk/link/472c3cc8872446e59fa59eaf0f7ad945.aspx, s. 8 [dostęp: 19.03.2025].

[37] *Cyber attacks traced to Russian military intelligence agency*, Federal Ministry of the Interior and Community, 3.05.2024, https://www.bmi.bund.de/SharedDocs/kurzmeldungen/EN/2024/05/schutzmassnahmen-cyberangriffe-en.html [dostęp: 19.03.2025].

[38] Tamże.

[39] *Heightened security situation in Germany*, Federal Ministry of the Interior and Community, https://www.bmi.bund.de/SharedDocs/schwerpunkte/EN/ukrain/security_meldung.html [dostęp: 19.03.2025].

Niemieckie służby wywiadowcze twierdzą, że rosyjskie działania szpiegowskie dotyczą rządu i administracji, a także wojska, technologii, badań, biznesu i przemysłu. *Rosyjskie cyberataki, niezależnie od tego, czy są skierowane na osoby fizyczne, organizacje czy instytucje rządowe, mają przede wszystkim na celu zdobycie stałego źródła informacji wywiadowczych. Oprócz takiego szpiegostwa, ataki te mogą być również wykorzystywane do sabotażu, operacji wywierania wpływu, dezinformacji lub celów propagandowych*[40].

W kwestii cyberzagrożeń ze strony Chin Niemcy uważają, że działania służb wywiadowczych służą realizacji celu Komunistycznej Partii Chin, którym jest status Chin jako globalnego lidera i światowej potęgi[41]. Federalny Urząd Ochrony Konstytucji (niem. Bundesamt für Verfassungsschutz) bezpośrednio wskazuje na grupy APT15 i APT31 jako wymagające uwagi ze względu na złożone techniki i narzędzia, jakimi się posługują. Na początku 2023 r. celem ataku na łańcuch dostaw przeprowadzonego przez sprawcę z Chin stali się niemieccy dostawcy usług IT dla sieci rządowych[42]. W raporcie nie sprecyzowano jednak, na czym ten atak polegał.

Estonia

Pierwszy cyberatak, o którym publicznie poinformowały estońskie władze, został przeprowadzony w 2020 r. przez GRU, a konkretnie Jednostkę 29155. Zespół CERT-EE, zajmujący się obsługą incydentów w estońskim Urzędzie ds. Systemów Informacyjnych, poinformował, że systemy komputerowe Ministerstwa Gospodarki i Komunikacji zostały naruszone za pomocą złośliwego oprogramowania typu backdoor. Spowodowało to wyciek 350 GB danych, w tym poufnych informacji wewnętrznych – dokumentów strategicznych i roboczych, danych osobowych i korespondencji z firmami[43]. Ten sam podmiot zaatakował także Ministerstwo Spraw Zagranicznych oraz Centrum Systemów Informacyjnych o Zdrowiu i Opiece Społecznej.

[40] *Brief summary 2023 Report on the Protection of the Constitution (Facts and Trends)*, Bundesamt für Verfassungsschutz, https://www.verfassungsschutz.de/SharedDocs/publikationen/EN/reports-on-the-protection-of-the-constitution/2024-06-brief-summary-2023-report-on-the-protection-of-the-constitution.pdf, s. 60 [dostęp: 19.03.2025].

[41] Tamże.

[42] Tamże, s. 62.

[43] *Cyber Security in Estonia 2025*, Republic of Estonia Information System Authority, https://www.ria.ee/en/cyber-security-estonia-2025 [dostęp: 19.03.2025].

Podanie tych informacji do publicznej wiadomości i przypisanie ataków nastąpiło dopiero pod koniec 2024 r. w wyniku operacji Toy Soldier przeprowadzonej przez Estonię i kilka innych krajów. Dzięki niej połączono Jednostkę 29155 z wieloma cyberatakami na Ukrainę, kraje NATO i UE. *Cele komórki cybernetycznej GRU, Jednostki 29155, obejmują gromadzenie danych wywiadowczych, naruszanie dobrego imienia przez kradzież i wyciek poufnych informacji oraz systematyczny sabotaż przez niszczenie danych i systemów komputerowych*[44].

W 2023 r. CERT-EE opublikował szczegółową analizę ataków DDoS przeprowadzonych przez haktywistów w 2022 r., których celem były strony internetowe sektora publicznego, transportowego i finansowego Estonii. Ataki nasilały się w związku z pewnymi wydarzeniami, takimi jak przeniesienie radzieckich pomników w Narwie czy oświadczenie estońskiego parlamentu Riigikogu, że rosyjski reżim jest terrorystyczny[45]. CERT-EE ogłosił, że były to działania o marginalnym znaczeniu i dał do zrozumienia, że Estonia nie uznała ich za poważne zagrożenie, lecz za utrudnienie. Co najważniejsze, CERT-EE nie przypisał tych ataków Rosji, lecz ideologicznie zmotywowanym hakerom, dla których wojna była katalizatorem. Często były one wynikiem i działań niezgodnych z oficjalną rosyjską narracją.

Prezentując ogólne postrzeganie zagrożeń sponsorowanych w cyberprzestrzeni, estońska Służba Bezpieczeństwa Wewnętrznego (eston. Kaitsepolitseiamet, KAPO) stwierdziła, że wrogie działania cyberwywiadowcze są prowadzone zwykle przez (...) *wojskowe i specjalne jednostki cyberwywiadowcze wrogich państw, które wytrwale działają na rzecz interesów swojego kraju*[46]. Według KAPO (...) *zarówno instytucje państwowe, jak i firmy świadczące usługi kluczowe muszą zdawać sobie sprawę, że ich status jako takich czyni je potencjalnymi celami ataków* [cybernetycznego sabotażu][47]. KAPO uważa za wysoce prawdopodobne, że (...) *rosyjskie służby specjalne nadal będą próbowały uzyskać nielegalny dostęp do sieci komputerowych estońskich dostawców usług kluczowych oraz najważniejszych firm transportowych*

[44] Tamże.

[45] *Cyber Security in Estonia 2023*, Republic of Estonia Information System Authority, https://www.ria.ee/sites/default/files/documents/2023-02/Cyber-Security-in-Estonia-2023.pdf, s. 17 [dostęp: 19.03.2025].

[46] *Annual review 2023–2024*, Estonian Internal Security Service, https://kapo.ee/sites/default/files/content_page_attachments/annual-review-2023-2024.pdf, s. 26 [dostęp: 19.03.2025].

[47] Tamże.

i logistycznych w celu zebrania informacji i przygotowania się do zakłócenia ich działalności za pomocą środków cybernetycznych, jeśli zajdzie taka potrzeba[48].

Ważnym spostrzeżeniem dotyczącym nastawienia opinii publicznej i postrzegania przez nią aktorów prezentujących się jako niepaństwowi, takich jak cyberprzestępcy czy haktywiści, jest to, że (...) *rosyjskie służby specjalne również korzystają z usług hakerów, którzy są z nimi pośrednio powiązani i wydają się działać niezależnie*[49]. KAPO ocenia, że takie ataki o niskim poziomie zaawansowania i niewielkim wpływie, w przeciwieństwie do grup APT bezpośrednio powiązanych ze służbami specjalnymi, umożliwiają Rosji tworzenie iluzji silnego wsparcia i dużych możliwości[50].

Estonia wskazuje również na zagrożenia ze strony Chin. KAPO zwraca uwagę, że produkowana tam technologia może zawierać złośliwe oprogramowanie i sprzętowe backdoory, pozwalające Chińczykom na nieautoryzowany dostęp do estońskich sieci i urządzeń[51]. Dlatego pomimo konkurencyjnych cen tych technologii należy rozpatrywać rozwiązania pochodzące z Chin jako potencjalne zagrożenie dla informacji przetwarzanych w docelowych systemach i każdorazowo przeprowadzać analizę ryzyka wynikającego z ich zastosowania.

Litwa

Przed wojną w Ukrainie Litwa była jednym z głównych celów operacji „Ghostwriter", przypisywanej grupie UNC1151, w tamtym czasie łączonej z Rosją[52]. Działalność ta, prowadzona w dalszym ciągu, chociaż na mniejszą skalę, łączy w sobie dwie sfery – cyberataki i operacje informacyjne, w których zaatakowana infrastruktura jest wykorzystywana do szerzenia w społeczeństwie dezinformacji. Wiele operacji dotyczyło stosunków między Litwą a Polską, np. operacje informacyjne pod hasłem „Wyciek odpadów radioaktywnych z litewskiej elektrowni jądrowej stanowi

[48] *Annual review 2022–2023,* Estonian Internal Security Service, https://kapo.ee/sites/default/files/content_page_attachments/Annual%20Review%202022-23_0.pdf, s. 22 [dostęp: 19.03.2025].

[49] *Annual review 2023–2024*..., s. 26.

[50] Tamże, s. 27.

[51] *Annual review 2022–2023*..., s. 24.

[52] Obecnie eksperci uważają, że równie prawdopodobne są powiązania tej grupy i z Rosją, i z Białorusią. Możliwe jest również, że działa ona pod obcą flagą.

zagrożenie dla Polaków mieszkających w pobliżu granicy" czy „Polska szkoliła ekstremistów w celu destabilizacji Litwy", a także między Litwą a Niemcami lub USA[53]. W oświadczeniu z 23 września 2021 r. wiceminister obrony narodowej Margiris Abukevičius stwierdził, że (...) *Litwa zdecydowanie popiera wspólną deklarację Unii Europejskiej wydaną w ramach stanowczego potępienia cyberataków informacyjnych Ghostwritera powiązanych z Rosją, które są wymierzone w procesy demokratyczne, instytucje, polityków, przedstawicieli mediów i ogólnie społeczeństwa państw członkowskich UE*[54]. W 2023 r. litewskie służby wywiadowcze – Drugi Departament Służb Operacyjnych (lit. Antrojo Operatyvinių Tarnybų Departamento, AOTD) oraz Departament Bezpieczeństwa Państwa (lit. Valstybės Saugumo Departamentas, VSD) poinformowały, że cybernetyczne operacje informacyjne przeciwko Litwie prowadzone przez grupę Ghostwriter ustały z powodu przekierowania działań na Ukrainę.

Litewskie służby wywiadowcze oceniły, że w związku z masowymi wydaleniami rosyjskich dyplomatów, a właściwie oficerów rosyjskiego wywiadu działających pod przykryciem dyplomatycznym, Rosja będzie poszukiwać innych sposobów gromadzenia informacji i uprawiać m.in. cyberszpiegostwo. AOTD i VSD odnotowały, że ataki są coraz częstsze. Ich celem są przede wszystkim organizacje rządowe i infrastruktura krytyczna.

Litwa podobnie jak Estonia wskazuje na współpracę cyberprzestępców i nienadzorowanych przez państwo hakerów z rosyjskimi służbami specjalnymi. Przestępcy osiągają dzięki niej korzyści finansowe i mają technologiczne wsparcie, a państwa zyskują na tym, że przypisanie atrybucji staje się trudniejsze[55].

W 2024 r. Litwa skoncentrowała się w swoich raportach na zagrożeniu ze strony Chin. Wskazano, że (...) *ich aktywność w litewskiej cyberprzestrzeni wzrosła, szczególnie od 2021 r., kiedy to Litwa ogłosiła otwarcie*

[53] *GhostWriter Update: Cyber Espionage Group UNC1151 Likely Conducts GhostWriter Influence Activity*, Mandiant, 28.04.2021, https://services.google.com/fh/files/misc/ghostwriter_update_report.pdf, s. 12–14 [dostęp: 19.03.2025].

[54] *Lithuania supports the EU declaration condemning Ghostwriter malicious cyber activities and calls to use more political tools*, Ministerstwo Obrony Narodowej Republiki Litwy, 23.09.2021, https://kam.lt/en/lithuania-supports-the-eu-declaration-condemning-ghostwriter-malicious-cyber-activities-and-calls-to-use-more-political-tools/ [dostęp: 8.04.2025].

[55] *National Threat Assessment 2023*, https://kam.lt/wp-content/uploads/2023/03/Assessment-of-Threats-to-National-Security-2022-published-2023.pdf, s. 55 [dostęp: 19.03.2025].

przedstawicielstwa Tajwanu na Litwie[56]. Nastąpiła zmiana celów ataków – z sektora prywatnego na instytucje rządowe zajmujące się sprawami wewnętrznymi i polityką zagraniczną. Taktyka ewoluowała w kierunku inżynierii społecznej, działania są prowadzone za pośrednictwem sieci społecznościowych.

Łotwa

Łotewski rząd niechętnie ujawnia sprawców cyberataków, chociaż wskazuje sektory, które są najbardziej narażone. W 2022 r. ci sami aktorzy stojący za atakami na infrastrukturę Ukrainy próbowali zaatakować łotewskie podmioty z sektora telekomunikacyjnego i energetycznego. Ze względów bezpieczeństwa nazwy czy też powiązania atakujących nie zostały ujawnione[57]. Zgodnie z przewidywaniami łotewskiej Służby Bezpieczeństwa Państwowego (łot. Valsts drošības dienests, VDD) z 2022 r.[58] i potwierdzonymi zdarzeniami w latach 2023[59] i 2024[60] za atakami na łańcuchy dostaw przy użyciu sprzętu lub oprogramowania zainfekowanego złośliwym kodem, a także aktualizacji oprogramowania bądź usług serwisowych, stały grupy wywodzące się z Rosji i wspierane przez to państwo. Według Biura Ochrony Konstytucji (łot. Satversmes aizsardzības birojs, SAB) tego typu ataki na łańcuch dostaw były wymierzone m.in. w satelitę telewizyjnego łotewskiego operatora telekomunikacyjnego – firmę Tet. Skutkiem tych ataków była krótka emisja rosyjskiej propagandy. Hakerzy uzyskali również dostęp do serwerów wynajętych przez operatora telekomunikacyjnego – firmę Balticom, obsługiwanych przez zewnętrznego dostawcę usług z Bułgarii,

[56] *National Threat Assessment 2024*, https://www.vsd.lt/wp-content/uploads/2024/03/GR-2024-02-15-EN-1.pdf, s. 57 [dostęp: 19.03.2025].

[57] D. Antoniuk, *Latvia's cyberspace faces new challenges amid war in Ukraine*, The Record, 28.10.2022, https://therecord.media/latvias-cyberspace-faces-new-challenges-amid-war-in-ukraine [dostęp: 19.03.2025].

[58] *Annual Report on the activities of Latvian State Security Service (VDD) in 2022*, https://vdd.gov.lv/uploads/materials/33/en/annual-report-2022.pdf, s. 13–14 [dostęp: 19.03.2025].

[59] *Annual Report on the activities of Latvian State Security Service (VDD) in 2023*, https://vdd.gov.lv/uploads/materials/37/en/annual-report-2023.pdf, s. 15 [dostęp: 19.03.2025].

[60] *Annual report on the activities of Latvian State Security Service (VDD) in 2024*, https://vdd.gov.lv/uploads/materials/40/en/annual-report-2024.pdf, s. 17 [dostęp: 19.03.2025].

i wyemitowali nagranie z rosyjskiej parady wojskowej[61]. W żadnym z tych przypadków infrastruktura nie znajdowała się na terenie Łotwy[62]. Niemniej jednak zespół CERT.LV podkreślił, że (...) *kluczowe jest zapobieganie zaangażowaniu łotewskiej infrastruktury IT w cyberataki oraz możliwości przeprowadzania ataków z terytorium kraju, ponieważ firmy telekomunikacyjne powiązane z Rosją celowo budują swoją obecność na Łotwie i w innych państwach członkowskich UE*[63].

Ataki naruszające infrastrukturę transmisyjną w celu szerzenia propagandy zacierają granice między cyberatakiem a operacją informacyjną, w której podmiot zostaje przejęty po to, aby wykorzystać jego zasięg i zaufanie, jakim się cieszy, do rozpowszechniania dezinformacji. W porównaniu z innymi metodami wykorzystywanymi w tego typu działaniach operacje informacyjne wspierane cyberatakami mogą znacznie szybciej dotrzeć do grupy docelowej, co dla sprawców czyni je atrakcyjnym narzędziem.

Podobnie jak inne kraje europejskie Łotwa również podziela przekonanie, że prorosyjscy haktywiści są (...) *prawdopodobnie koordynowani i finansowani w celu realizowania rosyjskich operacji wpływu, zarówno w polityce wewnętrznej, jak i zagranicznej*[64]. Jednocześnie, po przeanalizowaniu wydarzeń z 2022 r., VDD zweryfikowało, że informacje publikowane przez takie grupy na ich kanałach na Telegramie często są dezinformacją, ponieważ zgłaszane przez nie szkody w rzeczywistości nie zaistniały[65].

W odniesieniu do chińskiego wywiadu VDD ocenia, że Chiny nadal postrzegają Łotwę przede wszystkim jako część NATO i UE, które uznają za głównych rywali w globalnej rywalizacji o wpływy[66]. Gdy weźmie się to pod uwagę, ich cel jest jasny – jest nim gromadzenie informacji wywiadowczych na temat strategicznych decyzji i polityki dotyczącej relacji między Chinami a krajami przeciwnymi. Łotewskie służby wywiadowcze obserwują próby nawiązywania i wzmacniania przez przedstawicieli Chin

[61] *Latvia mulls tightening security after recent TV propaganda hacks*, LSM+, 20.05.2024, https://eng.lsm.lv/article/society/crime/20.05.2024-latvia-mulls-tightening-security-after-recent-tv-propaganda-hacks.a554618/ [dostęp: 19.03.2025].

[62] *2024 Annual Report*, Republic of Latvia Constitution Protection Bureau, https://www.sab.gov.lv/files/uploads/2025/02/SAB-gada-parskats_2024_ENG.pdf, s. 36 [dostęp: 19.03.2025].

[63] *Latvian Cybersecurity and CERT.LV Technical Activities Annual Report 2023*, 26.07.2024, https://cert.lv/uploads/eng/Annual_Report_CERT-LV_2023.pdf, s. 4–5 [dostęp: 19.03.2025].

[64] Tamże, s. 6.

[65] *Annual Report on the activities of Latvian State Security Service (VDD) in 2022...*, s. 13.

[66] Tamże.

pozytywnych relacji i wpływów wśród łotewskich polityków, naukowców i badaczy, co potwierdza ich zainteresowanie nowymi technologiami, innowacjami i polityką. Zainteresowanie to dotyczy również kwestii cybernetycznych – chińskie grupy cybernetyczne prowadzą działania hakerskie.

Polska

Polskie instytucje bezpieczeństwa państwa nie udostępniają informacji w formie okresowych raportów dotyczących kwestii strategicznych czy operacyjnych (jedynie raporty poświęcone zagadnieniom technicznym), dlatego w celu oceny stanowiska rządu wobec zagrożeń hybrydowych konieczne było sięgnięcie po doraźne komunikaty rzeczników bądź publikacje ukazujące się na oficjalnej stronie rządowej gov.pl.

Pod koniec 2022 r. ukazał się komunikat Pełnomocnika Rządu ds. Bezpieczeństwa Przestrzeni Informacyjnej Rzeczypospolitej Polskiej, w którym kilka cyberataków przypisano rosyjskim hakerom: (...) *przez wrogie operacje w cyberprzestrzeni Rosja chce wywierać presję na Polskę jako kraj frontowy i kluczowego sojusznika Ukrainy na wschodniej flance NATO*[67]. Obejmowały one ataki DDoS przeprowadzone przez prorosyjską grupę haktywistów NoName057(16) w odpowiedzi na uchwałę Sejmu RP z grudnia 2022 r. uznającą Rosję za państwo sponsorujące terroryzm[68], a także tworzenie stron do zbierania danych za pomocą phishingu.

Podobnie rzecznik prasowy ministra koordynatora służb specjalnych Polski stwierdził w połowie 2022 r.: *Operacje wywiadowcze polegające na atakach hakerskich, przejmowaniu zasobów informacyjnych i wykorzystywaniu ich do manipulowania opinią publiczną są w ostatnich latach wykorzystywane przez Kreml w ramach walki z NATO*[69]. Jednoznacznie przypisał więc te działania Rosji.

---

[67] *Russian cyberattacks*, Serwis Rzeczypospolitej Polskiej, 30.12.2022, https://www.gov.pl/web/special-services/russian-cyberattacks [dostęp: 19.03.2025].

[68] *Sejm uznał Rosję za państwo wspierające terroryzm*, Sejm Rzeczypospolitej Polskiej, 14.12.2022, https://www.sejm.gov.pl/sejm9.nsf/komunikat.xsp?documentId=4774505381CECC-10C1258918007022FA [dostęp: 8.04.2025].

[69] *Ataki hakerskie na RP operacją rosyjskich służb*, Serwis Rzeczypospolitej Polskiej, 20.07.2022, https://www.gov.pl/web/sluzby-specjalne/ataki-hakerskie-na-rp-operacja-rosyjskich-sluzb [dostęp: 19.03.2025].

Rok 2024 był pierwszym, w którym sprawozdanie Pełnomocnika Rządu ds. Cyberbezpieczeństwa za poprzedni rok zostało przedstawione publicznie[70]. Wcześniej był to w pełni tajny dokument. Tym samym, wraz z corocznymi raportami CERT Polska i CSIRT GOV, stało się jednym z nielicznych oficjalnych źródeł podsumowujących rok 2023.

W miesiącach poprzedzających wybory parlamentarne w 2023 r. grupa hakerska UNC1151 kontynuowała spersonalizowane ataki phishingowe (spearphishing) wymierzone w polityków, personel wojskowy, dziennikarzy, prawników oraz inne osoby mogące mieć powiązania z Rosją i Białorusią. Celem tych kampanii było cyberszpiegostwo i dezinformacja i w raporcie o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 r. zostały one przypisane Białorusi. Ta sama grupa jest podejrzewana o przeprowadzenie operacji informacyjnej wspieranej cyberatakami tuż przed wyborami, w ramach której wykorzystywano e-maile, wiadomości tekstowe oraz ekrany informacyjne w centrach handlowych do szerzenia dezinformacji[71].

Minister cyfryzacji nie wskazał bezpośrednio sprawców, ale zasugerował, że cyberatak na Polską Agencję Prasową i fałszywa depesza o częściowej mobilizacji w Polsce, która to informacja została opublikowana na stronie PAP w wyniku włamania, ma rosyjskie źródło. Minister stwierdził, że celem tego incydentu było (...) *szerzenie dezinformacji przed wyborami i „sparaliżowanie" społeczeństwa*[72]. Chodziło o wybory do Parlamentu Europejskiego w 2024 r.

Raportowanie w Polsce koncentruje się głównie na samych incydentach, np. przypadkach e-maili phishingowych rozsyłanych przez grupy APT powiązane z Rosją, takie jak APT28, APT29 czy Gamaredon, w celu prowadzenia cyberszpiegostwa. Krajowe zespoły CSIRT prezentują te incydenty w swoich raportach. W Polsce o zagrożeniach hybrydowych niewiele się mówi z perspektywy kontrwywiadu, mimo że jeden z krajowych zespołów CSIRT działa w strukturach Agencji Bezpieczeństwa Wewnętrznego.

[70] *Sprawozdanie Pełnomocnika Rządu do spraw Cyberbezpieczeństwa za 2023 rok*, Ministerstwo Cyfryzacji, 11.04.2024, https://www.gov.pl/web/cyfryzacja/krajobraz-cyberprzestrzeni [dostęp: 8.04.2025].

[71] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 roku*, CSIRT GOV, https://csirt.gov.pl/download/3/220/RaportostaniebezpieczenstwacyberprzestrzeniRPw2023.pdf, s. 6 [dostęp: 19.03.2025].

[72] *Fake PAP report looks like cyberattack, says gov't official*, Polska Agencja Prasowa, 31.05.2024, https://www.pap.pl/en/news/fake-pap-report-looks-cyberattack-says-govt-official [dostęp: 19.03.2025].

Na temat zagrożeń pochodzących z Chin w Polsce publikuje się nieliczne informacje. W źródłach rządowych można znaleźć jedynie kilka przykładów takich incydentów. Ocena sytuacji w 2023 r. wskazywała, że ze względu na poziom współpracy propagandowej między Chinami a Rosją (...) *należy oczekiwać, że zainteresowanie i aktywność chińskiego wywiadu nie ulegną zmianie, głównie ze względu na skalę wsparcia, jakie Rzeczpospolita Polska udziela Ukrainie w odpieraniu rosyjskiej agresji, sojusz Warszawy z Waszyngtonem oraz sytuację wokół Tajwanu*[73].

Wnioski

Wyniki zaprezentowanych badań przedstawiają szczegółowy przegląd aktualnych zagrożeń cybernetycznych, z którymi mierzy się Unia Europejska. Analizowane państwa prezentują stanowisko, że od początku wojny w Ukrainie w 2022 r. ataki z Rosji nasilają się i nie ma sygnałów wskazujących, że mogą osłabnąć. Wręcz przeciwnie, możliwości aktorów będących źródłem zagrożeń ewoluują wraz z ich doświadczeniem, a ataki stają się coraz trudniej wykrywalne i coraz bardziej wyrafinowane. W przypadku Chin jednogłośna opinia jest taka, że zagrożenia pochodzące z tego kraju intensyfikują się i mogą się przekształcić z gromadzenia informacji w działania destrukcyjne. Dwa pozostałe państwa z Wielkiej Czwórki[74], czyli Iran i Korea Północna, rzadko są wspominane w kontekście zagrożeń cybernetycznych.

Strategie dotyczące raportowania i przypisywania ataków przyjęte w analizowanych krajach można podzielić na 3 kategorie: minimalna, ostrożna i bezpośrednia. Łotwa w przypadku ataków na swój sektor telekomunikacyjny i energetyczny jedynie informowała, że ten sam aktor stał za atakami na infrastrukturę Ukrainy. Skłaniała opinię publiczną ku przekonaniu, że był on powiązany z Rosją, ale nie wskazała go bezpośrednio. Dania ostrożnie wskazywała nazwę grupy potencjalnie stojącej za atakiem na infrastrukturę krytyczną, przy czym podkreślała dużą niepewność i poszlakowość atrybucji. Niemcy natomiast bezpośrednio przypisały ataki

[73] *China's propaganda offensive*, 17.02.2023, https://www.gov.pl/web/special-services/Chinas-propaganda-offensive [dostęp: 19.03.2025].

[74] Wielka Czwórka (ang. Big Four) aktorów państwowych, tj. Chiny, Rosja, Korea Północna, Iran, to grupa państw identyfikowanych przez analityków cyberbezpieczeństwa jako największe źródła zagrożeń w cyberprzestrzeni.

na różne sektory grupie APT28 kierowanej przez GRU i otwarcie mówiły o rosyjskiej aktywności. Jednocześnie rodzą się pytania o to, ile podobnych ataków nie upubliczniono. Ile zakłóceń raportowanych jako wypadki i awarie w rzeczywistości było poważnymi cyberatakami ze strony zagranicznych aktorów?

Każdy raport dotyczący szczegółów ataków jest ważnym źródłem informacji dla analityków cyberbezpieczeństwa, a każdy raport służb wywiadowczych poszerza wiedzę badaczy bezpieczeństwa i umożliwia lepsze zrozumienie krajobrazu zagrożeń nie tylko w pojedynczym kraju, lecz także w całym regionie. Bardzo ważne jest, aby dla dobra wspólnego Europa wypracowała jednolite i spójne stanowisko wobec zagrożeń cybernetycznych.

Bibliografia

Fukuyama F., *Zaufanie. Kapitał społeczny a droga do dobrobytu*, Warszawa 1997.

Jordan T., Taylor P., *Hacktivism and Cyberwars. Rebels with a cause?*, London 2004.

Kose J., *Cyber Warfare: An Era of Nation-State actors And Global Corporate Espionage*, „ISSA Journal" 2021, t. 19, nr 4, s. 12–15.

Kuehl D.T., *Information Operations, Information Warfare, and Computer Network Attack: Their Relationship to National Security in the Information Age*, „International Law Studies" 2022, t. 76, s. 35–58.

Lin H., Kerr J., *On Cyber-Enabled Information/Influence Warfare and Manipulation*, w: *The Oxford Handbook of Cyber Security*, P. Cornish (red.), Oxford University Press 2021, s. 251–272. https://doi.org/10.1093/oxfordhb/9780198800682.013.15.

McIntosh T. i in., *Ransomware Reloaded: Re-examining Its Trend, Research and Mitigation in the Era of Data Exfiltration*, „ACM Computing Surveys" 2024, t. 57, nr 1. https://doi.org/10.1145/3691340.

Vićić J., Harknett R., *Identification-imitation-amplification: understanding divisive influence campaigns through cyberspac*e, „Intelligence and National Security" 2024, t. 39, nr 5, s. 897–914. https://doi.org/10.1080/02684527.2023.2300933.

Źródła internetowe

Antoniuk D., *Latvia's cyberspace faces new challenges amid war in Ukraine*, The Record, 28.10.2022, https://therecord.media/latvias-cyberspace-faces-new-challenges-amid-war-in-ukraine [dostęp: 19.03.2025].

Ataki hakerskie na RP operacją rosyjskich służb, Serwis Rzeczypospolitej Polskiej, 20.07.2022, https://www.gov.pl/web/sluzby-specjalne/ataki-hakerskie-na-rp-operacja-rosyjskich-sluzb [dostęp: 19.03.2025].

Brief summary 2023 Report on the Protection of the Constitution (Facts and Trends), Bundesamt fur Verfassungsschutz, https://www.verfassungsschutz.de/SharedDocs/publikationen/EN/reports-on-the-protection-of-the-constitution/2024-06-brief-summary-2023-report-on-the-protection-of-the-constitution.pdf [dostęp: 19.03.2025].

China's propaganda offensive, 17.02.2023, https://www.gov.pl/web/special-services/Chinas-propaganda-offensive [dostęp: 19.03.2025].

Cordesman A.H., *China's Emergence as a Superpower*, Center for Strategic & International Studies, 15.08.2023, https://www.csis.org/analysis/chinas-emergence-superpower [dostęp: 19.03.2025].

Countering hybrid threats, NATO, 7.05.2024, https://www.nato.int/cps/en/natohq/topics_156338.htm [dostęp: 19.03.2025].

Cyber attacks against European energy & utility companies, EnergiCERT, wrzesień 2022, https://sektorcert.dk/wp-content/uploads/2022/09/Attacks-against-European-energy-and-utility-companies-2020-09-05-v3.pdf [dostęp: 8.04.2025].

Cyber attacks traced to Russian military intelligence agency, Federal Ministry of the Interior and Community, 3.05.2024, https://www.bmi.bund.de/SharedDocs/kurzmeldungen/EN/2024/05/schutzmassnahmen-cyberangriffe-en.html [dostęp: 19.03.2025].

Cybercrime, European Commission, 31.10.2024, https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en [dostęp: 19.03.2025].

Cybersecurity of Critical Sectors – Energy, ENISA, https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors/energy [dostęp: 8.04.2025].

Fake PAP report looks like cyberattack, says gov't official, Polska Agencja Prasowa, 31.05.2024, https://www.pap.pl/en/news/fake-pap-report-looks-cyberattack-says-govt-official [dostęp: 19.03.2025].

Frequently asked questions on hybrid threats, Hybrid CoE, https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ [dostęp: 19.03.2025].

Greenberg A., *A Brief History of Russian Hackers' Evolving False Flags*, Wired, 21.10.2019, https://www.wired.com/story/russian-hackers-false-flags-iran-fancy-bear/ [dostęp: 19.03.2025].

Heightened security situation in Germany, Federal Ministry of the Interior and Community, https://www.bmi.bund.de/SharedDocs/schwerpunkte/EN/ukrain/security_meldung.html [dostęp: 19.03.2025].

Intelligence Outlook 2024, Danish Defence Intelligence Service, 22.01.2025, https://www.fe-ddis.dk/link/905eb443324b4db1be29f0546e275183.aspx [dostęp: 19.03.2025].

Jones S.G., *Russia's Shadow War Against the West*, Center for Strategic & International Studies, 18.03.2025, https://www.csis.org/analysis/russias-shadow-war-against-west [dostęp: 19.03.2025].

Latvia mulls tightening security after recent TV propaganda hacks, LSM+, 20.05.2024, https://eng.lsm.lv/article/society/crime/20.05.2024-latvia-mulls-tightening-security-after-recent-tv-propaganda-hacks.a554618/ [dostęp: 19.03.2025].

Lithuania supports the EU declaration condemning Ghostwriter malicious cyber activities and calls to use more political tools, Ministerstwo Obrony Narodowej Republiki Litwy, 23.09.2021, https://kam.lt/en/lithuania-supports-the-eu-declaration-condemning-ghostwriter-malicious-cyber-activities-and-calls-to-use-more-political-tools/ [dostęp: 8.04.2025].

Mandiant Intelligence, *GhostWriter Update: Cyber Espionage Group UNC1151 Likely Conducts GhostWriter Influence Activity*, Mandiant, 28.04.2021, https://services.google.com/fh/files/misc/ghostwriter_update_report.pdf [dostęp: 19.03.2025].

Mandiant Intelligence, *Hacktivists Collaborate with GRU-sponsored APT28*, Mandiant, 23.09.2022, https://cloud.google.com/blog/topics/threat-intelligence/gru-rise-telegram-minions [dostęp: 19.03.2025].

Microsoft Digital Defense Report 2024, *The foundations and new frontiers of cybersecurity*, https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024 [dostęp: 19.03.2025].

Multiple Foreign Nationals Charged in Connection with Trickbot Malware and Conti Ransomware Conspiracies, U.S. Department of Justice, 7.09.2023, https://www.justice.gov/archives/opa/pr/multiple-foreign-nationals-charged-connection-trickbot-malware-and-conti-ransomware [dostęp: 19.03.2025].

Raud M., *China and Cyber: Attitudes, Strategies, Organization*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn 2016, https://ccdcoe.org/uploads/2018/10/CS_organisation_CHINA_092016_FINAL.pdf [dostęp: 19.03.2025].

Roncone G. i in., *APT44: Unearthing Sandworm*, Mandiant, 17.04.2024, https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf [dostęp: 19.03.2025].

Russian cyberattacks, Serwis Rzeczypospolitej Polskiej, 30.12.2022, https://www.gov.pl/web/special-services/russian-cyberattacks [dostęp: 19.03.2025].

Russian National Charged with Ransomware Attacks Against Critical Infrastructure, U.S. Department of Justice, 16.05.2023, https://www.justice.gov/archives/opa/pr/russian-national-charged-ransomware-attacks-against-critical-infrastructure [dostęp: 19.03.2025].

Sancho D., *Understanding Hacktivists. The Overlap of Ideology and Cybercrime*, Trend Micro, 4.02.2025, https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/understanding-hacktivists-the-overlap-of-ideology-and-cybercrime [dostęp: 19.03.2025].

Sejm uznał Rosję za państwo wspierające terroryzm, Sejm Rzeczypospolitej Polskiej, 14.12.2022, https://www.sejm.gov.pl/sejm9.nsf/komunikat.xsp?documentId=4774505381CECC10C1258918007022FA [dostęp: 8.04.2025].

Thales Cyber Threat Intelligence, *From Ukraine to the whole of Europe: cyber conflict reaches a turning point*, Thales, 29.03.2023, https://www.thalesgroup.com/en/worldwide/security/press_release/ukraine-whole-europecyber-conflict-reaches-turning-point [dostęp: 8.04.2025].

The attack against Danish, critical infrastructure, SektorCERT, listopad 2023, https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf [dostęp: 19.03.2025].

What is data exfiltration?, IBM, https://www.ibm.com/think/topics/data-exfiltration [dostęp: 19.03.2025].

Wolert R., *RaaS group profile Hunters International*, CERT Orange, 28.10.2024, https://cert.orange.pl/wp-content/uploads/2024/11/CERTOPL_CTI_Hunters_International_en.pdf [dostęp: 19.03.2025].

Inne dokumenty

2024 Annual Report, Republic of Latvia Constitution Protection Bureau, https://www.sab.gov.lv/files/uploads/2025/02/SAB-gada-parskats_2024_ENG.pdf [dostęp: 19.03.2025].

Annual Report on the activities of Latvian State Security Service (VDD) in 2022, https://vdd.gov.lv/uploads/materials/33/en/annual-report-2022.pdf [dostęp: 19.03.2025].

Annual Report on the activities of Latvian State Security Service (VDD) in 2023, https://vdd.gov.lv/uploads/materials/37/en/annual-report-2023.pdf [dostęp: 19.03.2025].

Annual report on the activities of Latvian State Security Service (VDD) in 2024, https://vdd.gov.lv/uploads/materials/40/en/annual-report-2024.pdf [dostęp: 19.03.2025].

Annual review 2022–2023, Estonian Internal Security Service, https://kapo.ee/sites/default/files/content_page_attachments/Annual%20Review%202022-23_0.pdf [dostęp: 19.03.2025].

Annual review 2023–2024, Estonian Internal Security Service, https://kapo.ee/sites/default/files/content_page_attachments/annual-review-2023-2024.pdf [dostęp: 19.03.2025].

China's Military Strategy, Ministry of National Defense of the People's Republic of China, 23.06.2021, http://eng.mod.gov.cn/xb/Publications/WhitePapers/4887928.html [dostęp: 19.03.2025].

Cyber Security in Estonia 2023, Republic of Estonia Information System Authority, https://www.ria.ee/sites/default/files/documents/2023-02/Cyber-Security-in-Estonia-2023.pdf [dostęp: 19.03.2025].

Cyber Security in Estonia 2025, Republic of Estonia Information System Authority, https://www.ria.ee/en/cyber-security-estonia-2025 [dostęp: 19.03.2025].

Latvian Cybersecurity and CERT.LV Technical Activities Annual Report 2023, 26.07.2024, https://cert.lv/uploads/eng/Annual_Report_CERT-LV_2023.pdf [dostęp: 19.03.2025].

National Threat Assessment 2023, https://kam.lt/wp-content/uploads/2023/03/Assessment-of-Threats-to-National-Security-2022-published-2023.pdf [dostęp: 19.03.2025].

National Threat Assessment 2024, https://www.vsd.lt/wp-content/uploads/2024/03/GR-2024-02-15-EN-1.pdf [dostęp: 19.03.2025].

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 roku, CSIRT GOV, https://csirt.gov.pl/download/3/220/RaportostaniebezpieczenstwacyberprzestrzeniRPw2023.pdf [dostęp: 19.03.2025].

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2024 roku, w przygotowaniu.

Sprawozdanie Pełnomocnika Rządu do spraw Cyberbezpieczeństwa za 2023 rok, Ministerstwo Cyfryzacji, 11.04.2024, https://www.gov.pl/web/cyfryzacja/krajobraz-cyberprzestrzeni [dostęp: 8.04.2025].

Threat assessment: the cyber Threat against Denmark 2024, Centre for Cyber Security, wrzesień 2024, https://www.cfcs.dk/link/472c3cc8872446e59fa59eaf0f7ad945.aspx [dostęp: 19.03.2025].

Wspólny komunikat do Parlamentu Europejskiego i Rady. Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym, Bruksela, 6.04.2016, JOIN(2016) 18 final, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52016JC0018 [dostęp: 19.03.2025].

Monika Stodolnik

Funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego.

Kontakt: monika.stodolnik@abw.gov.pl

Terroryzm – studia, analizy, prewencja, 2025, wydanie specjalne: 263–287

https://doi.org/10.4467/27204383TER.25.010.21513

Artykuł

Wyniki badania ankietowego dotyczącego percepcji zagrożeń terrorystycznych i sabotażowych wśród ekspertów EU Protective Security Advisors

Results of the survey on the perception of terrorist and sabotage threats among the experts of the EU Protective Security Advisors

KAROLINA WOJTASIK https://orcid.org/0000-0002-1215-5005

Stałe Przedstawicielstwo RP przy Unii Europejskiej
Rządowe Centrum Bezpieczeństwa

DAMIAN SZLACHTER https://orcid.org/0000-0003-2763-9325

Agencja Bezpieczeństwa Wewnętrznego

Abstrakt

Artykuł przedstawia wyniki badań ankietowych dotyczących postrzegania zagrożeń terrorystycznych i sabotażowych przez ekspertów uczestniczących w inicjatywie DG Home Komisji Europejskiej – EU Protective Security Advisors (EU PSA). Ankieta została przeprowadzona w lutym 2025 r. na próbie 50 osób reprezentujących EU PSA, instytucje UE i partnerów strategicznych projektu. Kwestionariusz obejmował kilka ważnych aspektów zagrożeń terrorystycznych i sabotażowych, w tym rodzaje potencjalnych celów, metody ataków i przewidywany rozwój zagrożeń hybrydowych. Respondenci mieli również ocenić, które systemy infrastruktury krytycznej wymagają przyznania im najwyższego priorytetu w działaniach na rzecz

budowania odporności, a także to, jakie środki zwalczania terroryzmu powinny być traktowane priorytetowo na szczeblu UE. Ponadto za pomocą ankiety zbadano czynniki, które mogłyby poprawić bezpieczeństwo chronionych obiektów, i zidentyfikowano najbardziej prawdopodobnych sprawców ataków na infrastrukturę krytyczną UE. Wyniki ankiety dostarczają cennych spostrzeżeń dla kształtowania polityki antyterrorystycznej i antysabotażowej na poziomie UE. Autorzy podkreślają konieczność standaryzacji środków bezpieczeństwa fizycznego i rozwijania inicjatyw edukacyjnych w celu budowania kultury bezpieczeństwa.

Słowa kluczowe

infrastruktura krytyczna, przestrzeń publiczna, terroryzm, sabotaż, odporność, cele miękkie, cele twarde, Komisja Europejska, DG HOME, EU PSA, ochrona infrastruktury krytycznej, zagrożenia hybrydowe, wojna hybrydowa

Abstract

This article presents the results of a survey on the perception of terrorist and sabotage threats by experts participating in the European Commission's EU Protective Security Advisors (EU PSA) initiative. The survey was conducted in February 2025 on a sample of 50 individuals representing EU PSA, EU institutions, and strategic project partners. The questionnaire covered several key aspects of terrorist and sabotage threats, including the types of potential targets, attack methods, and expected developments in hybrid threats. Respondents were also asked to assess which critical infrastructure systems require the highest priority in resilience-building efforts, as well as which counter-terrorism measures should be prioritised at the EU level. Additionally, the survey explored factors that could improve the security of protected facilities and identified the most likely perpetrators of attacks on EU critical infrastructure. The survey results provide valuable insights for shaping counter-terrorism and counter-sabotage policies at the EU level. The authors emphasise the necessity of standardising physical security measures and developing educational initiatives to build a security culture.

Keywords

critical infrastructure, public space, terrorism, sabotage, resilience, soft targets, hard targets, European Commission, DG HOME, EU PSA, critical infrastructure protection, hybrid threats, hybrid warfare

Wprowadzenie

Ochrona przestrzeni publicznej i infrastruktury krytycznej (IK) jest podstawowym obowiązkiem państw członkowskich Unii Europejskiej. W odpowiedzi na rosnące zagrożenia terrorystyczne UE podejmuje inicjatywy wspierające państwa członkowskie w wysiłkach na rzecz ochrony obywateli i IK. Jedną z takich inicjatyw jest unijny program doradców ds. budowania odporności na zagrożenia – EU Protective Security Advisors (EU PSA)[1], stworzony przez Directorate-General for Migration and Home Affairs (DG HOME) Komisji Europejskiej.

Inicjatywa EU PSA ma swoje źródło w pracach UE nad ochroną przestrzeni publicznej, które rozpoczęły się w 2012 r. Impulsem do tych działań było wsparcie eksperckie udzielone Polsce podczas Mistrzostw Europy w Piłce Nożnej UEFA Euro 2012. Pozytywne doświadczenia z tego wydarzenia zaowocowały zaproszeniami z innych krajów UE do współpracy przy wzmacnianiu bezpieczeństwa podczas wydarzeń politycznych wysokiego szczebla i dużych zgromadzeń publicznych. Ważnym momentem w rozwoju unijnej polityki ochrony przestrzeni publicznej było przyjęcie w październiku 2017 r. planu działania poświęconego tym zagadnieniom. W jego ramach UE opracowała narzędzie do oceny podatności na zagrożenia. Finalnie doprowadziło to do stworzenia grupy specjalistów i ustanowienia unijnego programu PSA. Grupa EU PSA składa się z ok. 130 specjalistów z Komisji Europejskiej i państw członkowskich UE. Mają oni doświadczenie zawodowe w zakresie ochrony przestrzeni publicznej oraz wiedzę specjalistyczną na temat różnych obszarów bezpieczeństwa. Wdrożenie inicjatywy EU PSA do oficjalnego dorobku prawnego UE w dziedzinie walki z terroryzmem nastąpiło w grudniu 2020 r., wraz z publikacją agendy antyterrorystycznej UE.

Program EU PSA ma na celu udzielenie wsparcia państwom członkowskim UE na ich wniosek. Działania prowadzone w ramach tej inicjatywy obejmują:

- podnoszenie świadomości na temat słabych punktów bezpieczeństwa w przestrzeni publicznej i IK przez zapewnienie wspólnego systemu jego oceny,

[1] *EU Protective Security Advisors (EU PSA)*, https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/eu-protective-security-advisors-eu-psa_en [dostęp: 26.02.2025].

- dzielenie się najlepszymi praktykami i zachęcanie do wymiany wiedzy w celu wyeliminowania zidentyfikowanych słabych punktów bezpieczeństwa,
- dostarczanie państwom członkowskim wskazówek dotyczących zapewniania bezpieczeństwa podczas imprez masowych i ochrony miejsc wysokiego ryzyka,
- budowanie sieci ekspertów przez organizowanie międzynarodowych sesji szkoleniowych i wspieranie inicjatyw przyczyniających się do rozwoju wspólnej kultury bezpieczeństwa w UE.

Program EU PSA obejmuje ochronę przestrzeni publicznej i IK, w tym:

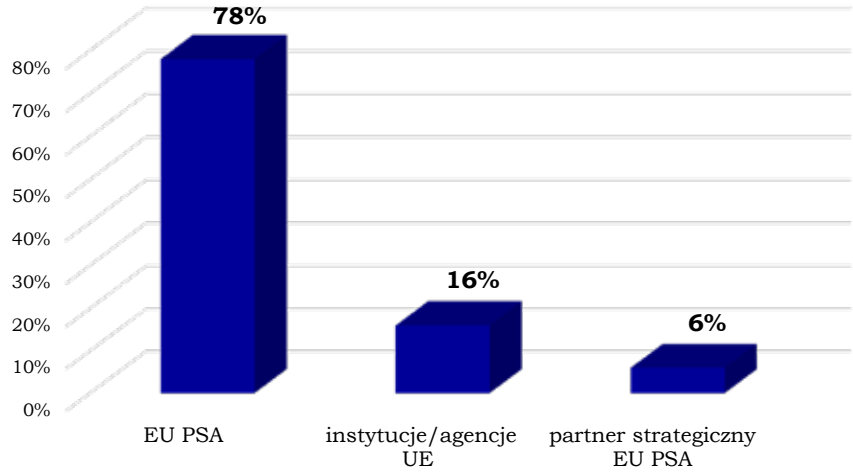
- miejsc kultu i instytucji religijnych,
- wydarzeń kulturalnych, takich jak np. duże festiwale muzyczne,
- wydarzeń z udziałem VIP-ów, takich jak np. szczyty UE,
- dużych obiektów przemysłowych niezaliczanych do IK,
- lotnisk, portów morskich, obiektów z sektora energetycznego oraz innych obiektów zaliczanych do IK.

Ze względu na rosnące uznanie dla programu EU PSA wśród władz państw członkowskich oraz niestabilną sytuację geopolityczną oczekuje się, że zainteresowanie działaniami tej grupy wzrośnie. Państwa członkowskie wyraziły zamiar zaproszenia ekspertów EU PSA do oceny krajowych obiektów IK, szczególnie w kontekście dyrektywy UE w sprawie odporności podmiotów krytycznych. Program EU PSA jest kluczową inicjatywą UE wspierającą państwa członkowskie w ochronie przestrzeni publicznej i IK przed zagrożeniami terrorystycznymi. Podnosząc świadomość, dzieląc się najlepszymi praktykami i zapewniając wsparcie ekspertów, EU PSA przyczynia się do poprawy bezpieczeństwa obywateli i infrastruktury w całej UE. To była przesłanka, dla której autorzy artykułu zdecydowali, że badanie ankietowe dotyczące postrzegania zagrożeń terrorystycznych i sabotażowych zostanie przeprowadzone wśród wspólnoty EU PSA. Składają się na nią członkowie EU PSA, przedstawiciele instytucji i agencji UE współpracujących z EU PSA oraz partnera strategicznego tej inicjatywy.

Wyniki badania ankietowego

Badanie przeprowadzono w lutym 2025 r., z wykorzystaniem standaryzowanego kwestionariusza składającego z 8 pytań[2]. Miało ono charakter anonimowy. W ankiecie wzięło udział 50 osób[3]. Respondenci reprezentowali: EU PSA (78%), instytucje i agencje UE wspierające tę inicjatywę (16%) oraz partnera strategicznego projektu EU PSA (6%). Podział respondentów obrazuje wykres 1.

Wykres 1. Podział respondentów ze względu na reprezentowane przez nich środowisko.



Pytanie nr 1 kwestionariusza brzmiało: *Jakimi obiektami interesują się terroryści/sabotażyści planujący swoje działania w Unii Europejskiej?*

Zadaniem respondentów było uszeregowanie odpowiedzi w kolejności od 1 do 10 miejsca, przy czym 1 miejsce oznaczało obiekt, którym terroryści/sabotażyści interesują sią najbardziej, 10 – najmniej[4]. Respondenci mieli

[2] Załącznik: wzór kwestionariusza ankiety.

[3] Stanowi to ok. 40% liczby członków EU PSA.

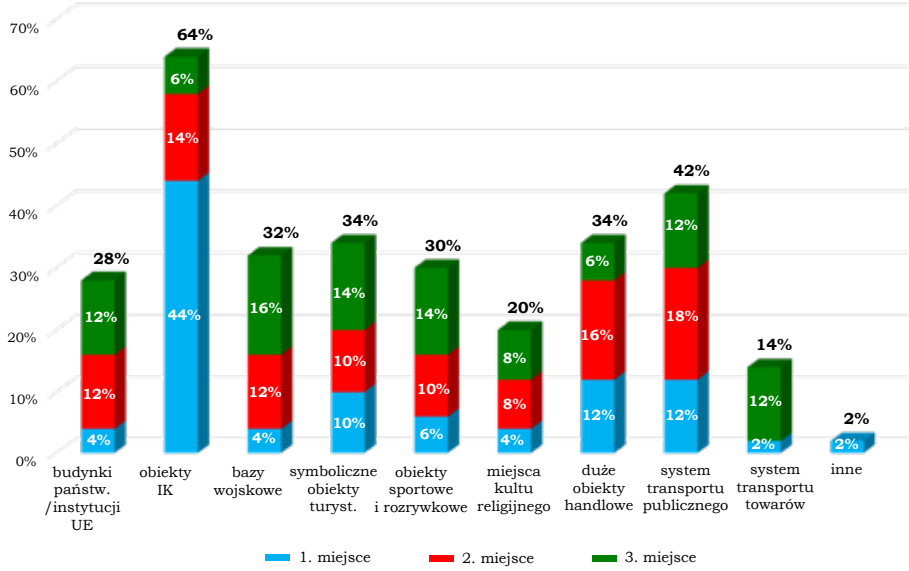
[4] Przy pytaniach, w których zadaniem respondentów było uszeregowanie odpowiedzi, przedstawiono wyniki tylko dla miejsc od 1 do 3. Z tego względu dane na wykresach prezentujących te wyniki nie sumują się do 100%.

podane następujące obiekty: budynki urzędów państwowych i instytucji UE, obiekty IK, bazy wojskowe, symboliczne obiekty turystyczne, obiekty sportowe i rozrywkowe, miejsca kultu religijnego, wielkopowierzchniowe obiekty handlowe, system transportu publicznego, system transportu towarów handlowych, inne.

W grupie obiektów, które respondenci wytypowali na 1 miejscu, najczęściej były wskazywane: obiekty IK (44%), wielkopowierzchniowe obiekty handlowe i system transportu publicznego (oba po 12%) oraz symboliczne obiekty turystyczne (10%). Widoczna jest zatem zdecydowana różnica w częstości wskazań dla IK i kolejnych obiektów. Wśród obiektów, którym uczestnicy badania przyporządkowali 2 miejsce, najczęściej były wskazywane: system transportu publicznego (18%), wielkopowierzchniowe obiekty handlowe (16%) oraz obiekty infrastruktury krytycznej (14%). Wśród obiektów, które respondenci wskazali na 3 miejscu, najczęstszą odpowiedzią były bazy wojskowe (16%). Wyniki dla kolejnych obiektów były takie same – symboliczne obiekty turystyczne oraz obiekty sportowe i rozrywkowe wskazało 14% ankietowanych. W przypadku obiektów, które respondenci wskazali na 2 i 3 miejscu, nie można zatem stwierdzić wyraźnej przewagi jednego z nich.

Zsumowano wyniki z miejsc 1–3 dla poszczególnych odpowiedzi i sprawdzono, które obiekty były najczęściej wskazywane przez respondentów w ramach pierwszej trójki. Z uzyskanych danych wynika, że są to: obiekty IK (64%), system transportu publicznego (42%) oraz ex aequo symboliczne obiekty turystyczne i wielkopowierzchniowe obiekty handlowe (po 34%). Szczegółowe wyniki zostały przedstawione na wykresie 2.

Wykres 2. Obiekty, którymi interesują się terroryści/sabotażyści planujący działania w UE.



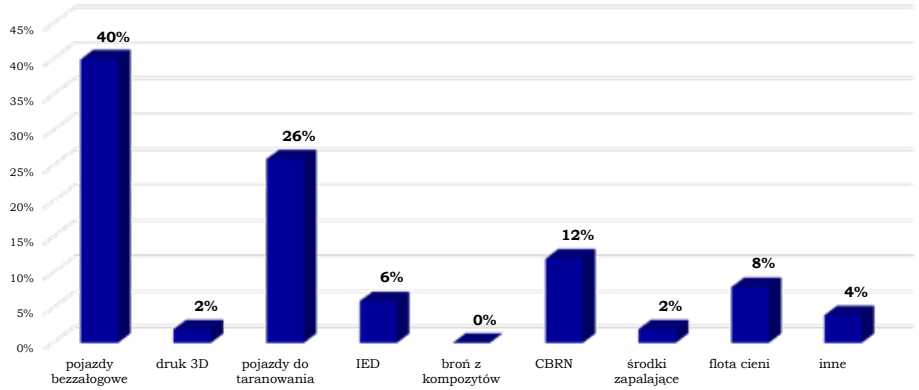
Pytanie nr 2 kwestionariusza brzmiało: *Jakie metody ataku i sabotażu mogą być największym wyzwaniem dla organów ścigania i instytucji zapewniających bezpieczeństwo ludzi i obiektów?*

Respondenci mogli wybrać jedną odpowiedź spośród następujących kategorii: pojazdy bezzałogowe (powietrzne, lądowe, wodne), druk 3D, pojazdy używane do taranowania, improwizowane ładunki wybuchowe (IED), broń wykonana z kompozytów, CBRN, środki zapalające, tzw. flota cieni/ciemna flota (ang. *shadow fleet/dark fleet*), inne.

Najwięcej respondentów (40%) wskazało pojazdy bezzałogowe (powietrzne, lądowe, wodne). W drugiej kolejności ankietowani wskazali pojazdy używane do taranowania (26%), następnie CBRN (12%). Wszystkie wyniki zostały przedstawione na wykresie 3.

Terroryzm – studia, analizy, prewencja
2025, wydanie specjalne: 263–287

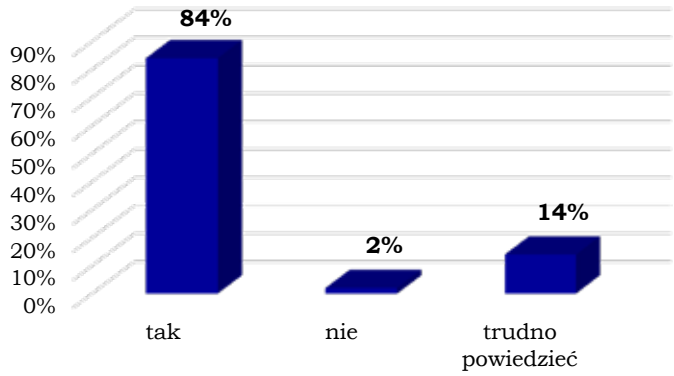
Wykres 3. Metody ataku i sabotażu, które mogą być największym wyzwaniem dla organów ścigania i instytucji zapewniających bezpieczeństwo ludzi i obiektów.



Pytanie nr 3 kwestionariusza brzmiało: *Czy w perspektywie 3 lat należy spodziewać się wykorzystania działań terrorystycznych/sabotażowych w ramach zagrożeń hybrydowych podejmowanych na terytorium UE przez obce państwo?*

Respondenci mogli wybrać jedną odpowiedź spośród: tak, nie, trudno powiedzieć. Twierdząco odpowiedziało 84% respondentów, 14% nie zajęło konkretnego stanowiska, a tylko 2% udzieliło odpowiedzi przeczącej. Wyniki przedstawiono na wykresie 4.

Wykres 4. Czy w perspektywie 3 lat działania terrorystyczne/sabotażowe mogą zostać wykorzystane jako narzędzie operacji hybrydowych w UE?



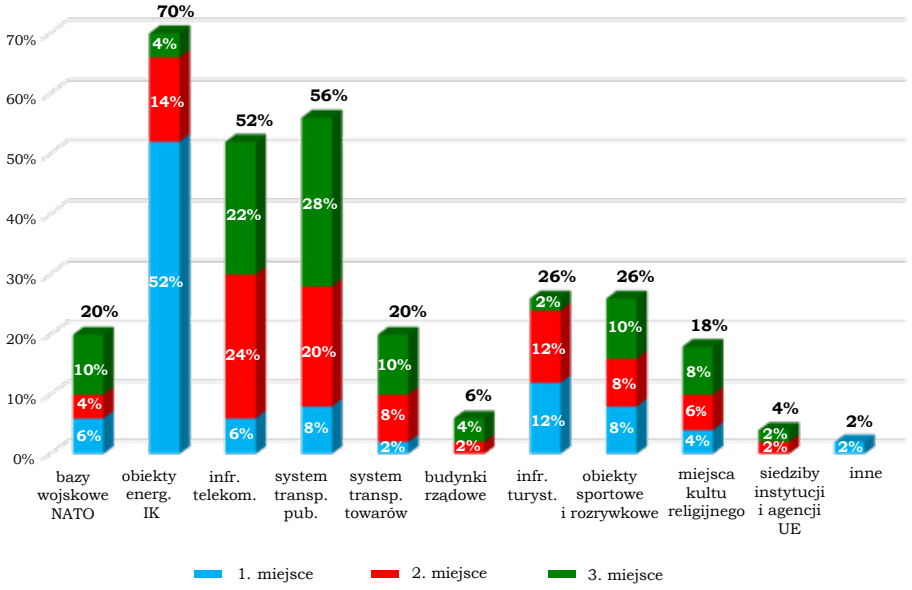
Pytanie nr 4 kwestionariusza brzmiało: *Które obiekty w perspektywie 3 lat będą charakteryzowały się najwyższym poziomem zagrożenia atakami terrorystycznymi/sabotażowymi w UE?*

Zadaniem respondentów było uszeregowanie odpowiedzi w kolejności od 1 do 11 miejsca, przy czym 1 miejsce oznaczało obiekt charakteryzujący się najwyższym poziomem zagrożenia terrorystycznego/sabotażowego, a 11 – najniższym. Respondenci mieli podane następujące obiekty: bazy wojskowe NATO, obiekty energetycznej IK, infrastruktura telekomunikacyjna, system transportu publicznego, system transportu towarów handlowych, budynki rządowe, infrastruktura turystyczna, obiekty sportowe i rozrywkowe, miejsca kultu religijnego, siedziby instytucji i agencji UE, inne.

W grupie obiektów, które respondenci wytypowali na 1 miejscu, najczęściej były wskazywane: obiekty energetycznej IK (52%), infrastruktura turystyczna (12%) oraz obiekty sportowe i rozrywkowe (8%). Należy podkreślić zdecydowaną przewagę IK – następne w kolejności obiekty miały znacznie mniejszą liczbę wskazań. Wśród obiektów, którym uczestnicy badania przyporządkowali 2 miejsce, najczęściej były wskazywane: infrastruktura telekomunikacyjna (24%), system transportu publicznego (20%) oraz obiekty energetycznej IK (14%). Wśród obiektów, które respondenci wskazali na 3 miejscu, najczęstszymi odpowiedziami były: system transportu publicznego (28%), infrastruktura telekomunikacyjna (22%) oraz bazy wojskowe NATO, system transportu towarów handlowych i obiekty sportowe i rozrywkowe (wszystkie po 10%). Zatem w przypadku 2 i 3 miejsca zjawisko przewagi jednego typu obiektu nie wystąpiło.

Zsumowano wyniki z miejsc 1–3 dla poszczególnych odpowiedzi i sprawdzono, które obiekty były najczęściej wskazywane przez respondentów w ramach pierwszej trójki. Z uzyskanych danych wynika, że są to: obiekty energetycznej IK (70%), system transportu publicznego (56%) oraz infrastruktura telekomunikacyjna (52%). Szczegółowe wyniki zostały przedstawione na wykresie 5.

Wykres 5. Obiekty, które będą charakteryzowały się najwyższym poziomem zagrożenia atakami terrorystycznymi/sabotażowymi.



Pytanie nr 5 kwestionariusza brzmiało: *Które systemy infrastruktury krytycznej w perspektywie 3 lat powinny być traktowane priorytetowo w zakresie budowania ich odporności na zagrożenia hybrydowe?*

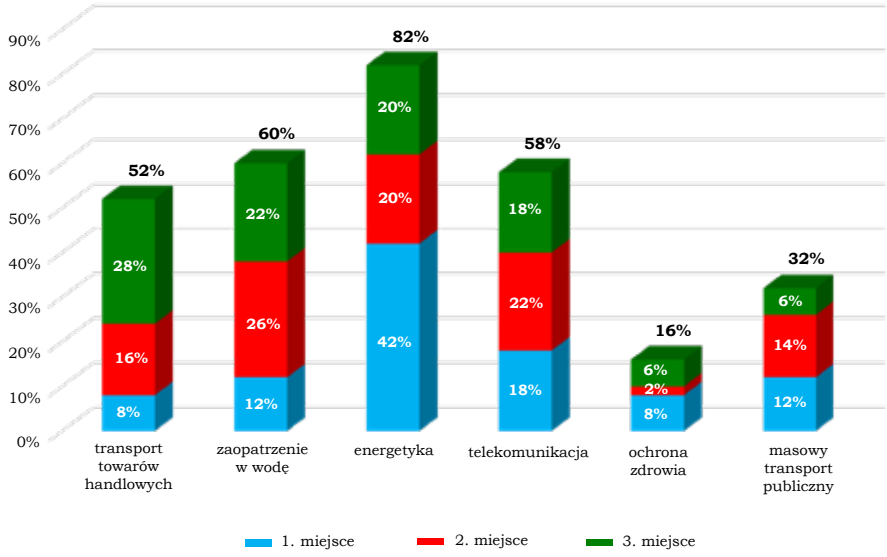
Zadaniem respondentów było uszeregowanie odpowiedzi w kolejności od 1 do 7 miejsca, przy czym 1 miejsce oznaczało system IK o najwyższym priorytecie, a 7 – o najniższym. Respondenci mieli podane następujące systemy: transport towarów handlowych (szlaki komunikacyjne i węzły przeładunkowe), zaopatrzenie w wodę, energetyka, telekomunikacja, ochrona zdrowia, masowy transport publiczny, inne.

W grupie systemów IK, które respondenci wytypowali na 1 miejscu, zdecydowanie najwięcej badanych wskazało system energetyczny (42%), następne w kolejności były system telekomunikacyjny (18%) oraz system zaopatrzenia w wodę i system masowego transportu publicznego (oba po 12%). W przypadku 2 i 3 miejsca odpowiedzi respondentów rozkładają się bardziej równomiernie. Wśród systemów, którym uczestnicy badania przyporządkowali 2 miejsce, najczęściej były wskazywane: system zaopatrzenia w wodę (26%), system telekomunikacyjny (22%) i system energetyczny (20%). Wśród systemów, które respondenci wskazali na 3 miejscu,

najczęstszymi odpowiedziami były: transport towarów handlowych (28%), system zaopatrzenia w wodę (22%) i system energetyczny (20%).

Zsumowano wyniki z miejsc 1–3 dla poszczególnych odpowiedzi i sprawdzono, które systemy IK były najczęściej wskazywane przez respondentów w ramach pierwszej trójki. Z uzyskanych danych wynika, że są to: system energetyczny (82%), system zaopatrzenia w wodę (60%) oraz system telekomunikacyjny (58%). Szczegółowe wyniki zostały przedstawione na wykresie 6 (odpowiedź „inne" nie padła).

Wykres 6. Priorytetowe systemy IK w budowaniu odporności na zagrożenia hybrydowe.



Pytanie nr 6 kwestionariusza brzmiało: *Który z obszarów przeciwdziałania działalności terrorystycznej wymaga obecnie priorytetowego traktowania na poziomie UE?*

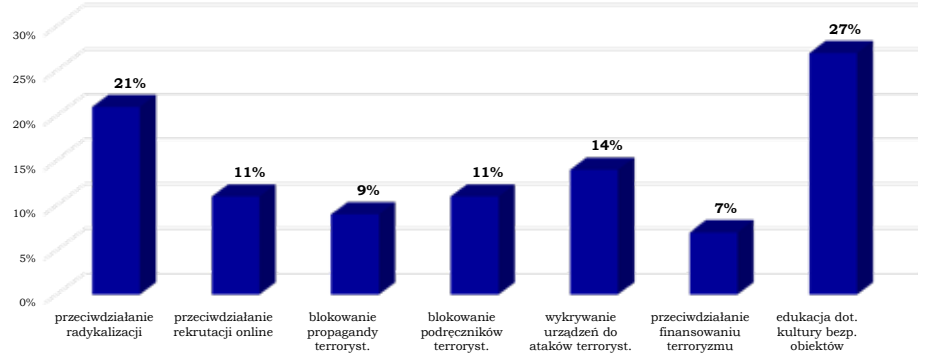
Respondenci mogli wybrać jedną odpowiedź spośród: przeciwdziałanie radykalizacji prowadzącej do działań terrorystycznych, przeciwdziałanie rekrutacji online do działań terrorystycznych/sabotażowych, wykrywanie i blokowanie propagandy terrorystycznej, wykrywanie i blokowanie podręczników terrorystycznych/sabotażowych publikowanych w internecie, rozwijanie technologii wykrywania urządzeń wykorzystywanych

Terroryzm – studia, analizy, prewencja
2025, wydanie specjalne: 263–287

do przeprowadzania ataków terrorystycznych, przeciwdziałanie finansowaniu terroryzmu, inicjatywy edukacyjne dotyczące kultury bezpieczeństwa obiektów narażonych na ataki terrorystyczne/sabotażowe, inne.

W przypadku odpowiedzi na to pytanie zdania ankietowanych były podzielone. Najwięcej respondentów wskazało na działania edukacyjne i budowanie kultury bezpieczeństwa w obiektach, które mogłyby być celem działań terrorystycznych bądź sabotażowych (27%). W drugiej kolejności ankietowani wskazali przeciwdziałanie radykalizacji prowadzącej do działań terrorystycznych (21%), a następnie rozwijanie technologii wykrywania urządzeń wykorzystywanych do przeprowadzania ataków terrorystycznych (14%). Wszystkie wyniki zostały przedstawione na wykresie 7.

Wykres 7. Priorytety w przeciwdziałaniu terroryzmowi.



Pytanie nr 7 kwestionariusza brzmiało: *Co może zwiększyć poziom odporności chronionych obiektów na ataki terrorystyczne i działania sabotażowe?*

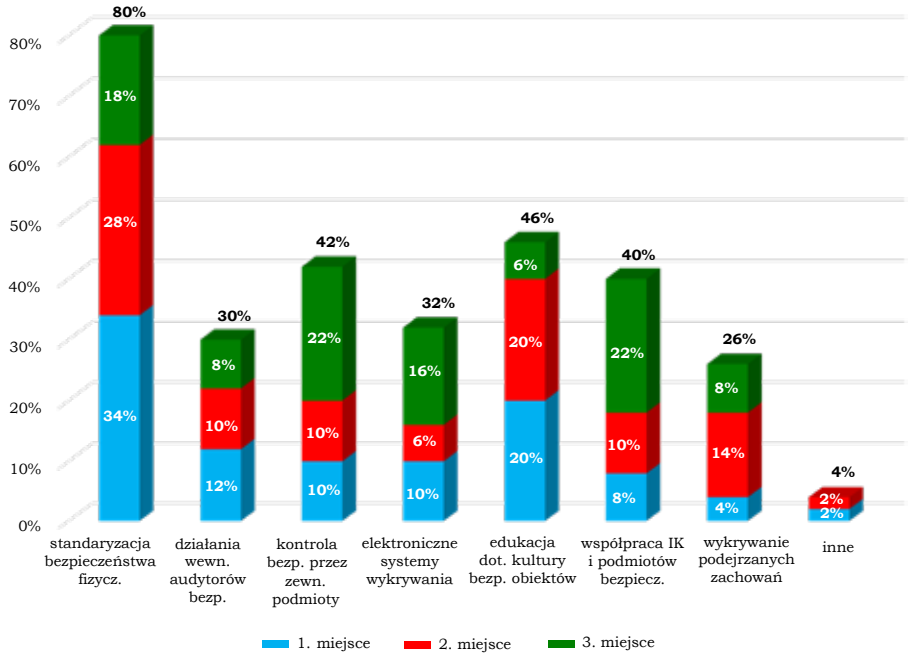
Zadaniem respondentów było uszeregowanie odpowiedzi w kolejności od 1 do 8 miejsca, przy czym 1 miejsce oznaczało działania najważniejsze, a 8 – najmniej ważne. Respondenci mieli podane następujące odpowiedzi: standaryzacja bezpieczeństwa fizycznego (także procedur dotyczących pracowników ochrony), zadania wykonywane przez wewnętrznych audytorów bezpieczeństwa, testy kontroli bezpieczeństwa przeprowadzane przez zewnętrzne podmioty nadzorujące (takie jak: instytucje UE, państwowe organy kontrolne), rozwój inteligentnych elektronicznych systemów

wykrywania zdarzeń zagrażających bezpieczeństwu, rozwój inicjatyw związanych z prewencją terrorystyczną jako elementem kultury bezpieczeństwa obiektu (edukacja dla bezpieczeństwa), poprawa współpracy pomiędzy podmiotami IK a podmiotami odpowiedzialnymi za bezpieczeństwo, wykrywanie podejrzanych zachowań przez przeszkolonych pracowników ochrony, inne.

W grupie działań, które respondenci wytypowali na 1 miejscu, najczęściej były wskazywane: standaryzacja bezpieczeństwa fizycznego (34%), rozwój inicjatyw związanych z prewencją terrorystyczną (20%) oraz zadania wykonywane przez wewnętrznych audytorów bezpieczeństwa (12%). Przy czym różnica między kolejnymi wskazanymi działaniami – testami kontrolnymi bezpieczeństwa przeprowadzanymi przez zewnętrznych nadzorców (takich jak: instytucje UE, państwowe organy kontroli) oraz rozwojem inteligentnych elektronicznych systemów wykrywania zdarzeń zagrażających bezpieczeństwu była niewielka – obie opcje uzyskały po 10% wskazań. Wśród działań, którym uczestnicy badania przyporządkowali 2 miejsce, najczęściej były wskazywane: standaryzacja bezpieczeństwa fizycznego (28%), rozwój inicjatyw związanych z prewencją terrorystyczną (20%) i wykrywanie podejrzanych zachowań przez przeszkolonych pracowników ochrony (14%). Wśród działań, które respondenci wskazali na 3 miejscu, najczęstszymi odpowiedziami były: testy kontroli bezpieczeństwa przeprowadzane przez zewnętrzne podmioty nadzorujące oraz poprawa współpracy pomiędzy podmiotami IK a podmiotami odpowiedzialnymi za bezpieczeństwo (oba po 22%). Kolejną odpowiedzią była standaryzacja bezpieczeństwa fizycznego (18%).

Zsumowano wyniki z miejsc 1–3 dla poszczególnych odpowiedzi i sprawdzono, które działania były najczęściej wskazywane przez respondentów w ramach pierwszej trójki. Z uzyskanych danych wynika, że są to: standaryzacja bezpieczeństwa fizycznego (80%), rozwój inicjatyw związanych z prewencją terrorystyczną (46%), testy kontroli bezpieczeństwa przeprowadzane przez zewnętrzne podmioty (42%). Szczegółowe wyniki zostały przedstawione na wykresie 8.

Wykres 8. Działania mające na celu zwiększenie odporności obiektów na ataki terrorystyczne i działania sabotażowe.

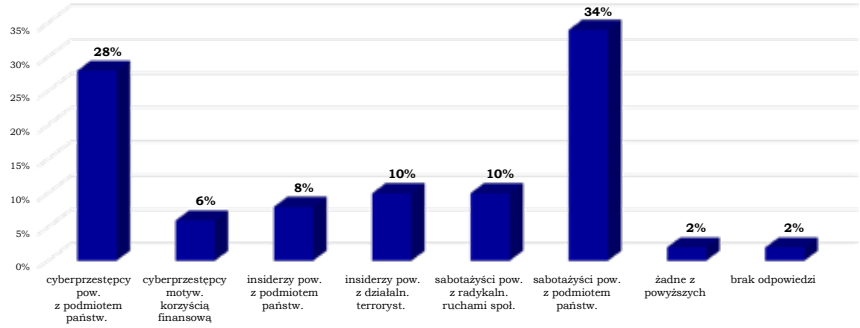


Pytanie nr 8 kwestionariusza dotyczyło sprawców ataków na IK.

Respondenci mogli wybrać jedną odpowiedź spośród: cyberprzestępcy powiązani z podmiotem państwowym, cyberprzestępcy kierujący się wyłącznie chęcią osiągnięcia korzyści finansowych, tzw. insiderzy powiązani z podmiotem państwowym, tzw. insiderzy powiązani z działalnością terrorystyczną, sabotażyści powiązani z działalnością radykalnych ruchów społecznych, sabotażyści powiązani z podmiotem państwowym, żadne z powyższych.

Najwięcej respondentów (34%) wskazało sabotażystów powiązanych z podmiotem państwowym. W drugiej kolejności badani wskazali cyberprzestępców powiązanych z podmiotem państwowym (28%), a następnie ex aequo insiderów powiązanych z działalnością terrorystyczną oraz sabotażystów powiązanych z działalnością radykalnych ruchów społecznych (po 10%). Wszystkie wyniki zostały przedstawione na wykresie 9.

Wykres 9. Potencjalni sprawcy ataków na obiekty IK.



Podsumowanie wyników badań ankietowych

Eksperci zaangażowani w EU PSA wskazali obiekty IK (64% wszystkich odpowiedzi), system transportu publicznego (42%) oraz symboliczne obiekty turystyczne i wielkopowierzchniowe obiekty handlowe (oba 34%) jako najbardziej prawdopodobne cele ataku terrorystycznego/sabotażowego w UE. Należy podkreślić, że przy konstruowaniu kwestionariusza ankiety autorzy artykułu skupili się przede wszystkim na celu ataku, a nie na metodzie. Wnioski wynikające z badań ankietowych nie odbiegają od innych danych. Najnowszy raport TE-SAT przedstawia informacje dotyczące ataków terrorystycznych, do których doszło w 2023 r. W 45 ze 120 przypadków podano bardziej szczegółowe dane, z których wynika, że w 1/3 tych ataków celem była IK[5].

Jeśli chodzi o metody ataku i sabotażu, które mogą być największym wyzwaniem dla organów ścigania, władz i instytucji odpowiedzialnych za zapewnienie bezpieczeństwa fizycznego, najczęstszym wskazaniem respondentów były pojazdy bezzałogowe (powietrzne, lądowe, wodne). Takiej odpowiedzi udzieliło 40% ankietowanych. Ostatnie lata to czas intensywnego rozwoju dronów. Coraz częściej są one wykorzystywane do popełniania przestępstw. Warto podkreślić, że podwodne drony mogą w przyszłości stanowić poważne zagrożenie dla morskiej IK. We wspomnianym raporcie TE-SAT podano również, że osoby z różnych środowisk ideologicznych mogące stanowić zagrożenie aktywnie poszukują materiałów szkoleniowych online i instrukcji obsługi zawierających informacje na temat taktyki

[5] *European Union Terrorism Situation and Trend Report* (EU TE-SAT) 2024, https://www.europol.europa.eu/cms/sites/default/files/documents/TE-SAT%202024.pdf, s. 12 [dostęp: 26.02.2025].

przeprowadzania ataków i tworzenia broni, w tym chemicznej, konstruowania dronów, bomb[6]. Na drugim miejscu uczestnicy badania ankietowego wskazali pojazdy używane do taranowania (26% respondentów), co prawdopodobnie ma związek z ostatnimi wydarzeniami (atak w Magdeburgu w grudniu 2024 r. i atak w Mannheim w marcu 2025 r.)[7].

84% respondentów uważa, że w perspektywie 3 lat działania terrorystyczne i sabotażowe zostaną wykorzystane w ramach działań hybrydowych podejmowanych na terytorium UE przez obce państwo.

Jeśli chodzi o rodzaje obiektów w UE, które w ciągu najbliższych 3 lat będą charakteryzować się najwyższym poziomem zagrożenia atakiem terrorystycznym/sabotażowym, to respondenci najczęściej wskazywali: obiekty energetycznej IK (70%), system transportu publicznego (56%) oraz infrastrukturę telekomunikacyjną (52%). Liczba ataków, głównie cybernetycznych, na infrastrukturę energetyczną i telekomunikacyjną stale rośnie[8] i staje się podstawą wojny hybrydowej. Ataki na transport publiczny są powszechną taktyką stosowaną przez grupy dżihadystów[9].

Większość respondentów wskazała, że systemem IK, który w perspektywie 3 lat powinien być traktowany priorytetowo przy budowaniu odporności na zagrożenia hybrydowe, jest system energetyczny (82%). Sprawne funkcjonowanie infrastruktury energetycznej jest warunkiem

---

[6] Tamże, s. 7.

[7] Atak w Magdeburgu – 20 grudnia 2024 r. kierowca wjechał w grupę ludzi na jarmarku bożonarodzeniowym. Zginęło 6 osób, ponad 100 zostało rannych. Sprawcą był 50-letni lekarz pochodzenia saudyjskiego, mieszkający w Niemczech od 2006 r. Atak w Mannheim – 3 marca 2025 r. 40-letni obywatel Niemiec wjechał samochodem w grupę ludzi na deptaku. Zabił 2 osoby i ranił kilka innych. Sprawca został zatrzymany przez policję wkrótce po zdarzeniu.

[8] B. Nieróbca, *Energetyka w sieci cyberzagrożeń*, EY, 14.08.2024, https://www.ey.com/pl_pl/insights/cybersecurity/energetyka-w-siecicyberzagrozen [dostęp: 26.02.2025]; *Raport: cyberbezpieczeństwo w energetyce*, https://www.inteligentnaenergetyka.pl/enereka/wp-content/uploads/2024/02/Raport_Cyberbezpiecze%C5%84stwo-w-energetyce_ARTSMART_29.02.2024.pdf [dostęp: 26.02.2025]; K. Pohoska, *Cyberprzestępczość – prognozy na 2025 rok*, Stołeczny Magazyn Policyjny, 3.03.2025, https://magazyn-ksp.policja.gov.pl/mag/technologie/137761,Cyberprzestepczosc-prognozy-na-2025-rok.html [dostęp: 20.03.2025].

[9] *The Tactics and Targets of Domestic Terrorists*, Center for Strategic and International Studies, 30.07.2020, https://www.csis.org/analysis/tactics-and-targets-domestic-terrorists [dostęp: 26.02.2025]; B.M. Jenkins, B.R. Butterworth, K.S. Shrum, *Terrorist Attacks On Public Bus Transportation: A Preliminary Empirical Analysis*, https://transweb.sjsu.edu/research/Terrorist-Attacks-Public-Bus-Transportation-Preliminary-Empirical-Analysis [dostęp: 26.02.2025].

funkcjonowania nowoczesnego społeczeństwa. Skutki ataku na system energetyczny są wielopoziomowe. Z tego względu jest on uznawany za najbardziej narażony na ataki.

W przypadku pytania o obszar przeciwdziałania działalności terrorystycznej, który dziś wymaga priorytetowego potraktowania przez UE, zdania respondentów były podzielone. Najwięcej ankietowanych (27%) wskazało jednak na działania edukacyjne i budowanie kultury bezpieczeństwa w obiektach, które mogą stać się celem ataku. Będzie to istotne wyzwanie dla operatorów IK i instytucji sprawujących nad nimi nadzór.

Przedsięwzięciami, które w największym stopniu mogą zwiększyć poziom odporności na ataki terrorystyczne i działania sabotażowe w chronionych obiektach, są: standaryzacja ochrony fizycznej (80%), rozwój inicjatyw prewencji terrorystycznej w ramach kultury bezpieczeństwa obiektu (46%) oraz testy kontroli bezpieczeństwa przeprowadzane przez zewnętrzne podmioty (42%).

Najwięcej respondentów uważa, że sprawcami przeprowadzanych obecnie ataków na systemy IK są sabotażyści powiązani z podmiotem państwowym (34%) lub cyberprzestępcy powiązani z podmiotem państwowym (28%).

Wyniki przeprowadzonego badania jednoznacznie wskazują na zagrożenie atakami terrorystycznymi i sabotażowymi, wymierzonymi zwłaszcza w IK, system transportu publicznego oraz system telekomunikacyjny. Respondenci, reprezentujący środowisko ekspertów ds. bezpieczeństwa, podkreślili potrzebę priorytetowego traktowania działań mających na celu wzmacnianie odporności obiektów o kluczowym znaczeniu dla funkcjonowania państwa i społeczeństwa.

Na podstawie analizy wyników ankiety można zauważyć, że w najbliższych latach będzie konieczne dalsze rozwijanie środków służących zapobieganiu atakom, obejmujących: standaryzację ochrony fizycznej, wdrażanie nowoczesnych technologii wykrywania zagrożeń oraz inicjatywy edukacyjne w zakresie prewencji terrorystycznej. Ponadto istotne znaczenie będzie miała współpraca między operatorami IK a organami odpowiedzialnymi za bezpieczeństwo, co pozwoli na lepszą koordynację działań i skuteczniejsze reagowanie na incydenty.

Badanie potwierdza również, że zagrożenia terrorystyczne i sabotażowe coraz częściej stanowią element strategii działań hybrydowych podejmowanych przez podmioty państwowe i niepaństwowe. W obliczu dynamicznie zmieniającego się środowiska bezpieczeństwa państwa

członkowskie UE powinny dążyć do wdrażania kompleksowych strategii ochrony, uwzględniających zarówno aspekty fizyczne, jak i cyberbezpieczeństwo.

Bibliografia

EU Protective Security Advisors (EU PSA), https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/eu-protective-security-advisors-eu-psa_en [dostęp: 26.02.2025].

Jenkins B.M., Butterworth B.R., Shrum K.S., *Terrorist Attacks On Public Bus Transportation: A Preliminary Empirical Analysis*, https://transweb.sjsu.edu/research/Terrorist-Attacks-Public-Bus-Transportation-Preliminary-Empirical-Analysis [dostęp: 26.02.2025].

Nieróbca B., *Energetyka w sieci cyberzagrożeń*, EY, 14.08.2024, https://www.ey.com/pl_pl/insights/cybersecurity/energetyka-w-siecicyberzagrozen [dostęp: 26.02.2025].

Pohoska K., *Cyberprzestępczość – prognozy na 2025 rok*, Stołeczny Magazyn Policyjny, 3.03.2025, https://magazyn-ksp.policja.gov.pl/mag/technologie/137761,Cyberprzestepczosc-prognozy-na-2025-rok.html [dostęp: 20.03.2025].

The Tactics and Targets of Domestic Terrorists, Center for Strategic and International Studies, 30.07.2020, https://www.csis.org/analysis/tactics-and-targets-domestic-terrorists [dostęp: 26.02.2025].

Inne dokumenty

European Union Terrorism Situation and Trend Report (EU TE-SAT) 2024, https://www.europol.europa.eu/cms/sites/default/files/documents/TE-SAT%202024.pdf [dostęp: 26.02.2025].

Raport: cyberbezpieczeństwo w energetyce, https://www.inteligentnaenergetyka.pl/enereka/wp-content/uploads/2024/02/Raport_Cyberbezpiecze%C5%84stwo-w-energetyce_ARTSMART_29.02.2024.pdf [dostęp: 26.02.2025].

Załącznik

Wzór kwestionariusza ankiety wykorzystanego w lutym 2025 r.

BADANIE EU PSA 2025

Niniejsza ankieta jest przeprowadzana wśród przedstawicieli państw członkowskich UE i Komisji Europejskiej uczestniczących w projekcie budowania odporności na ataki terrorystyczne w przestrzeni publicznej – EU PSA (Protective Security Advisors) w DG HOME Komisji Europejskiej. Ankieta jest anonimowa, a jej wyniki zostaną zebrane w sposób uniemożliwiający identyfikację osoby ją wypełniającej.

Celem ankiety jest uzyskanie opinii respondentów na temat najbardziej prawdopodobnych sposobów rozwoju zagrożeń terrorystycznych/sabotażowych w UE.

Wyniki ankiety zostaną opublikowane w numerze specjalnym czasopisma naukowego „Terroryzm – studia, analizy, prewencja", który będzie poświęcony zagrożeniom terrorystycznym i hybrydowym dla infrastruktury krytycznej. Wydanie specjalne ukaże się w maju 2025 r. i będzie dystrybuowane na posiedzeniach grup roboczych Rady UE: WPT, PROCIV CER w ramach polskiej prezydencji w Radzie UE.

Naszym zdaniem wyniki tego badania mogą przyczynić się do dyskusji na temat rozwoju inicjatyw antyterrorystycznych i antysabotażowych, w tym do zapobiegania zagrożeniom i podnoszenia świadomości na ich temat na poziomie UE i w państwach członkowskich.

Terroryzm – studia, analizy, prewencja
2025, wydanie specjalne: 263–287

Początek kwestionariusza ankiety

1. Jakimi obiektami interesują się terroryści/sabotażyści planujący swoje działania w Unii Europejskiej?

   Podczas wypełniania kwestionariusza za pomocą telefonu komórkowego: przeciągnij opcję i upuść ją, aby ułożyć kolejność.

   W przypadku wypełniania kwestionariusza na komputerze: ponumeruj opcje za pomocą przycisku po lewej stronie lub przeciągnij opcję i upuść ją, aby ułożyć kolejność.

   - budynki urzędów państwowych i instytucji UE,
   - obiekty infrastruktury krytycznej,
   - bazy wojskowe,
   - symboliczne obiekty turystyczne,
   - obiekty sportowe i rozrywkowe,
   - miejsca kultu religijnego,
   - wielkopowierzchniowe obiekty handlowe,
   - system transportu publicznego,
   - system transportu towarów handlowych,
   - inne.

2. Jakie metody ataku i sabotażu mogą być największym wyzwaniem dla organów ścigania i instytucji zapewniających bezpieczeństwo ludzi i obiektów?

   Wybierz jedną odpowiedź:

   - pojazdy bezzałogowe (powietrzne, lądowe, wodne),
   - druk 3D,
   - pojazdy używane do taranowania,
   - improwizowane ładunki wybuchowe,
   - broń wykonana z kompozytów,
   - CBRN,
   - środki zapalające,
   - tzw. flota cieni/ciemna flota,
   - inne.

3. Czy w perspektywie 3 lat należy spodziewać się wykorzystania działań terrorystycznych/sabotażowych w ramach zagrożeń hybrydowych podejmowanych na terytorium UE przez obce państwo?

   Wybierz jedną odpowiedź:

   - tak,
   - nie,
   - trudno powiedzieć.

4. Które obiekty w perspektywie 3 lat będą charakteryzowały się najwyższym poziomem zagrożenia atakami terrorystycznymi/sabotażowymi w UE?

   Podczas wypełniania kwestionariusza za pomocą telefonu komórkowego: przeciągnij opcję i upuść ją, aby ułożyć kolejność.

   W przypadku wypełniania kwestionariusza na komputerze: ponumeruj opcje za pomocą przycisku po lewej stronie lub przeciągnij opcję i upuść ją, aby ułożyć kolejność.

   - bazy wojskowe NATO,
   - obiekty energetycznej infrastruktury krytycznej,
   - infrastruktura telekomunikacyjna,
   - system transportu publicznego,
   - system transportu towarów handlowych,
   - budynki rządowe,
   - infrastruktura turystyczna,
   - obiekty sportowe i rozrywkowe,
   - miejsca kultu religijnego,
   - siedziby instytucji i agencji UE,
   - inne.

5. Które systemy infrastruktury krytycznej w perspektywie 3 lat powinny być traktowane priorytetowo w zakresie budowania ich odporności na zagrożenia hybrydowe?

   Podczas wypełniania kwestionariusza za pomocą telefonu komórkowego: przeciągnij opcję i upuść ją, aby ułożyć kolejność.

Terroryzm – studia, analizy, prewencja
2025, wydanie specjalne: 263–287

W przypadku wypełniania kwestionariusza na komputerze: ponumeruj opcje za pomocą przycisku po lewej stronie lub przeciągnij opcję i upuść ją, aby ułożyć kolejność.

- transport towarów handlowych (szlaki komunikacyjne i węzły przeładunkowe),
- zaopatrzenie w wodę,
- energetyka,
- telekomunikacja,
- ochrona zdrowia,
- masowy transport publiczny,
- inne.

6. Który z obszarów przeciwdziałania działalności terrorystycznej wymaga obecnie priorytetowego traktowania na poziomie UE?

   Wybierz jedną odpowiedź:

   - przeciwdziałanie radykalizacji prowadzącej do działań terrorystycznych,
   - przeciwdziałanie rekrutacji online do działań terrorystycznych/sabotażowych,
   - wykrywanie i blokowanie propagandy terrorystycznej,
   - wykrywanie i blokowanie podręczników terrorystycznych/sabotażowych publikowanych w internecie,
   - rozwijanie technologii wykrywania urządzeń wykorzystywanych do przeprowadzania ataków terrorystycznych,
   - przeciwdziałanie finansowaniu terroryzmu,
   - inicjatywy edukacyjne dotyczące kultury bezpieczeństwa obiektów narażonych na ataki terrorystyczne/sabotażowe,
   - inne.

7. Co może zwiększyć poziom odporności chronionych obiektów na ataki terrorystyczne i działania sabotażowe?

   Podczas wypełniania kwestionariusza za pomocą telefonu komórkowego: przeciągnij opcję i upuść ją, aby ułożyć kolejność.

W przypadku wypełniania kwestionariusza na komputerze: ponumeruj opcje za pomocą przycisku po lewej stronie lub przeciągnij opcję i upuść ją, aby ułożyć kolejność.

- standaryzacja bezpieczeństwa fizycznego (także procedur dotyczących pracowników ochrony),
- zadania wykonywane przez wewnętrznych audytorów bezpieczeństwa,
- testy kontroli bezpieczeństwa przeprowadzane przez zewnętrzne podmioty nadzorujące (takie jak: instytucje UE, państwowe organy kontrolne),
- rozwój inteligentnych elektronicznych systemów wykrywania zdarzeń zagrażających bezpieczeństwu,
- rozwój inicjatyw związanych z prewencją terrorystyczną jako elementem kultury bezpieczeństwa obiektu (edukacja dla bezpieczeństwa),
- poprawa współpracy między podmiotami IK a podmiotami odpowiedzialnymi za bezpieczeństwo,
- wykrywanie podejrzanych zachowań przez przeszkolonych pracowników ochrony,
- inne.

8. Ataki na infrastrukturę krytyczną są obecnie przeprowadzane przez:

Wybierz jedną odpowiedź:

- cyberprzestępców powiązanych z podmiotem państwowym,
- cyberprzestępców kierujących się wyłącznie chęcią osiągnięcia korzyści finansowych,
- tzw. insiderów powiązanych z podmiotem państwowym,
- tzw. insiderów powiązanych z działalnością terrorystyczną,
- sabotażystów powiązanych z działalnością radykalnych ruchów społecznych,
- sabotażystów powiązanych z podmiotem państwowym,
- żadne z powyższych.

Terroryzm – studia, analizy, prewencja
2025, wydanie specjalne: 263–287

UZUPEŁNIJ INFORMACJE

Wybierz jedną odpowiedź:

- przedstawiciel państwa członkowskiego UE,
- przedstawiciel instytucji lub agencji UE,
- przedstawiciel kraju będącego partnerem strategicznym projektu EU PSA.

Koniec kwestionariusza ankiety

Dr Karolina Wojtasik, MBA

Specjalista ds. bezpieczeństwa, biegły sądowy, pracownik naukowy, wiceprezes ds. naukowych Polskiego Towarzystwa Bezpieczeństwa Narodowego, główny specjalista w Rządowym Centrum Bezpieczeństwa. Podczas polskiej prezydencji w Radzie Unii Europejskiej pełni funkcję przewodniczącej grupy roboczej PROCIV CER. Zajmuje się szeroko pojętym bezpieczeństwem infrastruktury krytycznej, szczególnie w kontekście zagrożeń bezpieczeństwa fizycznego i osobowego. Ponadto analizuje działalność salafickich organizacji terrorystycznych, modus operandi sprawców zamachów terrorystycznych w UE i USA, a także publikacje instruktażowe dotyczące metod przeprowadzania ataków na ludność cywilną i obiekty. Autorka książek: *Anatomia zamachu. O strategii i taktyce terrorystów*; *Ścieżki radykalizacji dżihadystycznej. Podręcznik dla studentów socjologii, politologii i bezpieczeństwa*. Współautorka publikacji *Polski system antyterrorystyczny a realia zamachów drugiej dekady XXI wieku* oraz wielu innych publikacji związanych z terroryzmem, a także bezpieczeństwem i budowaniem odporności infrastruktury krytycznej. Twórca kanału popularnonaukowego Anatomia zamachu na YouTube.

Kontakt: karolina.wojtasik@rcb.gov.pl

Dr Damian Szlachter

Redaktor naczelny czasopisma naukowego ABW „Terroryzm – studia, analizy, prewencja". Członek komitetu sterującego unijnej grupy doradców ds. budowania odporności na zagrożenia (EU Protective Security Advisors). Ekspert narodowy w Dyrekcji Generalnej ds. Migracji i Spraw Wewnętrznych Komisji Europejskiej (Directorate-General for Migration and Home Affairs) w ramach grupy roboczej ds. ochrony antyterrorystycznej przestrzeni publicznych (Policy Group on Public Spaces Protection). Audytor krajowy kontroli jakości w zakresie ochrony lotnictwa cywilnego (Urzędu Lotnictwa Cywilnego). Uczestnik prac kilkunastu zespołów międzyresortowych oraz grup roboczych administracji państwowej, których zadaniem było budowanie odporności na zagrożenia terrorystyczne i hybrydowe obiektów strategicznych dla bezpieczeństwa państwa oraz infrastruktury krytycznej. Członek zespołu do spraw badania wyzwań inżynierii bezpieczeństwa obiektów budowlanych infrastruktury krytycznej przy Głównym Urzędzie Nadzoru Budowlanego. Autor blisko 40 artykułów naukowych oraz współautor kilku książek i raportów specjalistycznych na temat bezpieczeństwa wewnętrznego.

Kontakt: d.szlachter@abw.gov.pl

MATERIAŁY EKSPERCKIE

Terroryzm – studia, analizy, prewencja, 2025, wydanie specjalne: 291–332

https://doi.org/10.4467/27204383TER.25.011.21514

Materiał ekspercki

Rola standaryzacji i oceny zgodności w zapewnianiu bezpieczeństwa i budowaniu odporności infrastruktury krytycznej na zagrożenia hybrydowe

The role of standardisation and conformity assessment in ensuring security and building resilience of critical infrastructure to hybrid threats

Adam Tatarowski
Zakład Rozwoju Technicznej Ochrony Mienia „TECHOM”
https://orcid.org/0009-0007-5503-6819

Wprowadzenie

Podejście do rozumienia bezpieczeństwa ewoluuje w Polsce od okresu transformacji ustrojowej w 1989 r. Dopiero wtedy zaczęły kształtować się potrzeby rynku i administracji państwowej w zakresie usług ochrony i bezpieczeństwa. Do momentu uchwalenia obowiązującej do dzisiaj *Ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia* sektor ochrony i bezpieczeństwa funkcjonował w Polsce bez dedykowanych ustawowych regulacji. Rozwijał się na zasadach rynkowych i ulegał zarówno pozytywnym, jak i negatywnym wpływom oddolnym – wewnątrzrynkowym, a także odgórnym – ze strony administracji państwowej oraz zewnętrznym.

Przeszkodą w stworzeniu spójnego i przejrzystego systemu prawnego, który zapewniłby sektorowi ochrony i bezpieczeństwa stabilny fundament, był brak jednoznacznej wizji i decyzyjności państwowych instytucji regulacyjnych na poziomie tworzenia szczegółowych wymagań. Wypracowanie spójnych rozwiązań komplikowały ponadto sprzeczne interesy różnych grup wpływu, których działania miały niekorzystny wpływ na przebieg prac legislacyjnych. Potencjał wynikający z dorobku normalizacyjnego nie został wykorzystany. Kolejne inicjatywy legislacyjne, choć niezbędne i często inspirowane europejskimi rozwiązaniami, nie tworzyły spójnej struktury – pozostawiały istotne luki, hamujące wzrost konkurencyjności, transparentności i jakości świadczonych usług oraz dostarczanych rozwiązań organizacyjno-technicznych. Przykładem bardzo potrzebnego aktu normatywnego, który jednak nie uwzględniał rozwiązań systemowych dotyczących zapewnienia jakości i zgodności, było *Rozporządzenie Rady Ministrów z dnia 24 czerwca 2003 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony*, dookreślające zagadnienia ochrony tych obiektów w sytuacji zagrożenia bezpieczeństwa państwa.

Obok „głównego nurtu" prawnego skupionego na ustawie o ochronie osób i mienia zaczęto w Polsce dostrzegać potrzebę utworzenia jednolitego podejścia do ochrony infrastruktury krytycznej (IK) i zapewnienia jej bezpieczeństwa. Choć rozumiano, że pewne systemy i obiekty – takie jak sieci energetyczne, infrastruktura telekomunikacyjna czy systemy transportowe – mają fundamentalne znaczenie dla funkcjonowania państwa, przez długi czas brakowało regulacji, które kompleksowo ujmowałyby ich ochronę. W polskim systemie prawnym brakowało samego pojęcia IK. Jak wskazują Tomasz Szewczyk i Maciej Pyznar[1], polska administracja państwowa spotykała się z tym pojęciem głównie w ramach współpracy międzynarodowej, w strukturach NATO i Unii Europejskiej. Powstające wówczas przepisy koncentrowały się na wybranych sektorach lub odnosiły się do ochrony poszczególnych obiektów, nie tworzyły jednak jednolitego systemu zabezpieczeń. W efekcie działania podejmowane w zakresie ochrony IK były rozproszone, a kwestie odpowiedzialności administracyjnej za jej bezpieczeństwo nie były jasno określone.

[1] T. Szewczyk, M. Pyznar, *Ochrona infrastruktury krytycznej a zagrożenia asymetryczne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2010, nr 2, s. 54.

Dla wielu krajów wzorem w próbie uporządkowania tego zagadnienia stało się podejście amerykańskie, które na przełomie XX i XXI w. kształtowało nowe standardy związane z ochroną IK. Punktem zwrotnym w tym zakresie było wejście w życie dyrektywy Presidential Decision Directive 63 z 22 maja 1998 r.[2], która wprowadziła pojęcie *critical infrastructure* jako systemów niezbędnych do zapewnienia podstawowego funkcjonowania gospodarki i administracji państwowej. Zgodnie z nią są to systemy fizyczne i cyfrowe, których zniszczenie lub zakłócenie mogłoby prowadzić do poważnych konsekwencji społeczno-ekonomicznych i politycznych. Nowością było uznanie, że ochrona tych systemów wymaga skoordynowanego wysiłku zarówno administracji rządowej, jak i sektora prywatnego, który był właścicielem większości zasobów uznawanych za krytyczne dla funkcjonowania państwa. Dyrektywa ta nakładała na poszczególne agencje federalne USA obowiązek opracowania planów ochrony IK oraz stworzenia mechanizmów wymiany informacji między sektorami: publicznym i prywatnym.

Pod wpływem amerykańskich standardów na forum UE rozpoczęto prace nad stworzeniem jednolitych ram ochrony unijnej IK. W Polsce początkowe działania administracji państwowej w tym zakresie koncentrowały się na wybranych sektorach. Wciąż brakowało podejścia, które integrowałoby różne aspekty bezpieczeństwa infrastrukturalnego w jednolitym modelu zarządzania.

Momentem przełomowym w kształtowaniu polskiego systemu ochrony IK było uchwalenie *Ustawy o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 roku*, która w art. 3 pkt 2 po raz pierwszy wprowadziła do polskiego porządku prawnego definicję IK, rozumianej jako:

> (...) systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Infrastruktura krytyczna obejmuje systemy:
> a) zaopatrzenia w energię, surowce energetyczne i paliwa,
> b) łączności,
> c) sieci teleinformatycznych,
> d) finansowe,

[2] *Presidential Decision Directive/Nsc-63*, The White House, 22.05.1998, https://irp.fas.org/offdocs/pdd/pdd-63.htm [dostęp: 5.03.2025].

e) zaopatrzenia w żywność,
f) zaopatrzenia w wodę,
g) ochrony zdrowia,
h) transportowe,
i) ratownicze,
j) zapewniające ciągłość działania administracji publicznej,
k) produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

W tej ustawie zdefiniowano też pojęcie ochrony IK, czyli (...) *działań zmierzających do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie* (art. 3 pkt 3).

Na mocy tej ustawy powstało ponadto Rządowe Centrum Bezpieczeństwa (RCB) – ponadresortowa struktura, podległa bezpośrednio Prezesowi Rady Ministrów, odpowiedzialna za działalność planistyczną i programową z zakresu ochrony IK (art. 10 ust. 1).

Tworzenie europejskich regulacji i ich oddziaływanie na polskie prawodawstwo

Na poziomie unijnym przełom nastąpił po wejściu w życie *Dyrektywy Rady 2008/114/WE z 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony*. W rozumieniu tej dyrektywy IK jest definiowana bardziej ogólnie, jako (...) *składnik, system lub część infrastruktury zlokalizowane na terytorium państw członkowskich, które mają podstawowe znaczenie dla utrzymania niezbędnych funkcji społecznych, zdrowia, bezpieczeństwa, ochrony, dobrobytu materialnego lub społecznego ludności oraz których zakłócenie lub zniszczenie miałoby istotny wpływ na dane państwo członkowskie w wyniku utracenia tych funkcji* (art. 2). Dyrektywa wprowadziła i dookreśliła podejście „obiektowe" do ochrony IK, ponieważ skoncentrowano się w niej na ochronie obiektów i instalacji, których uszkodzenie mogłoby mieć poważne konsekwencje dla funkcjonowania państwa. Polska implementacja dyrektywy uwzględniła ten model bardziej kompleksowo. Wynikało to ze świadomości rosnących zależności między administracją publiczną a sektorem prywatnym oraz dynamicznych zmian w globalnym środowisku bezpieczeństwa. Rozwiązania przyjęte w Polsce nie tylko wzmacniały ochronę obiektów,

lecz także kładły fundament pod pokonywanie przyszłych wyzwań związanych z utrzymaniem ciągłości usług.

Ustawa o zarządzaniu kryzysowym zobowiązywała RCB do utworzenia i systematycznej aktualizacji Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK) – przełomowego dokumentu, w którym szczegółowo zdefiniowano proces wyłaniania IK i jej ochronę. Dodano do niego załącznik pt. *Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje.* Całość stworzyła podbudowę do standaryzacji ochrony IK, opartej na tzw. sześciopaku dotyczącym:

1) ochrony fizycznej,
2) ochrony technicznej,
3) ochrony osobowej,
4) ochrony teleinformatycznej,
5) ochrony prawnej,
6) aspektów związanych z planami odbudowy.

Ustawa i zbiór dokumentów będących jej uzupełnieniem, w tym NPOIK, ewoluowały przez lata. W tym czasie został ugruntowany dość skomplikowany proces identyfikacji IK, składający się z trzech etapów. W pierwszym ustala się, do którego systemu należy potencjalny obiekt IK. Następnie sprawdza się, czy dany obiekt pełni funkcję, o której mowa w definicji ustawowej. Na końcu analizuje się, czy możliwe skutki zniszczenia lub zaprzestania funkcjonowania potencjalnej IK będą spełnieniem kryteriów przekrojowych odnoszących się do społecznych skutków destrukcji bądź zaprzestania funkcjonowania obiektu, urządzenia, instalacji lub usługi. Kryteria te obejmują:

– ofiary w ludziach,
– skutki finansowe,
– konieczność ewakuacji,
– utratę usługi,
– czas odbudowy,
– efekt międzynarodowy,
– unikatowość (w sensie niemożności zastąpienia i odtworzenia zniszczonego obiektu, urządzenia bądź instalacji)[3].

[3] Zob. szerzej: A. Tatarowski, *Budowanie odporności infrastruktury krytycznej w świetle zagrożeń asymetrycznych i terroryzmu. Tendencje legislacyjne w polskiej implementacji dyrektywy CER ze szczególnym uwzględnieniem aspektów standaryzacji i certyfikacji rozwiązań organizacyjno-technicznych*, „Terroryzm – studia, analizy, prewencja" 2024, nr 5, s. 175–194. https://doi.org/10.4467/27204383TER.24.006.19394.

Od momentu zaimplementowania w Polsce dyrektywy NIS[4] *Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* równolegle do podejścia „obiektowego" funkcjonuje „usługowy" system wyłaniania operatorów usług kluczowych, czyli takich, które mają istotne znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej i są wymienione w wykazie usług kluczowych, wydanym na podstawie ustawy. Z kolei decyzję uznającą podmiot za operatora usługi kluczowej wydaje się wtedy, gdy:

- podmiot świadczy usługę kluczową,
- świadczenie tej usługi zależy od systemów informacyjnych,
- incydent miałby istotny skutek zakłócający dla świadczenia usługi kluczowej przez tego operatora[5].

Współistnienie podejścia „obiektowego" i „usługowego" doprowadziło do niespójności w całościowym systemie zarządzania IK. Model „obiektowy", bazujący na klasycznej ochronie infrastruktury, nie obejmował perspektywy systemowej i nie uwzględniał istotnych zależności pomiędzy sektorami. Z kolei podejście „usługowe", rozwijane w ramach regulacji dotyczących cyberbezpieczeństwa, miało ograniczony zakres zastosowania. Dualizm ten był szczególnie widoczny w politykach UE, w których obowiązywały dwie odrębne dyrektywy: dyrektywa Rady 2008/114/WE, nakładająca obowiązek ochrony fizycznej infrastruktury, oraz dyrektywa NIS, koncentrująca się na zapewnieniu odporności systemów informatycznych i usług cyfrowych.

Dojrzewanie do nowego modelu ochrony infrastruktury krytycznej

W ciągu kolejnych lat rosło zrozumienie, że tradycyjny model ochrony IK, skupiony wyłącznie na obiektach fizycznych, jest niewystarczający. Wpływ na to miały zarówno przeprowadzane analizy naukowe, jak i wydarzenia, które ujawniły istotne luki w dotychczasowym systemie zarządzania ryzykiem. Doświadczenia wynikające z ataków terrorystycznych (np. 11 września 2001 r.), pandemii COVID-19, cyberataków oraz katastrof naturalnych (np. huragan Sandy)[6] unaoczniły, że duże znaczenie ma nie tyle ochrona

[4] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii*.

[5] Zob. szerzej: A. Tatarowski, *Budowanie odporności infrastruktury krytycznej…*, s. 178.

[6] M. Wiśniewski, K. Szwarc, W. Skomra, *Continuity of Essential Services as an Emerging Challenge for Societal Resilience*, „IEEE Access" 2023, t. 11, s. 44615. https://doi.org/10.1109/ACCESS.2023.3271751.

pojedynczych obiektów, systemów czy instalacji, ile zapewnienie nieprzerwanego działania usług istotnych dla stabilności państwa i bezpieczeństwa obywateli. Zakłócenie jednej usługi, np. dostaw paliwa, może wywołać efekt domina i prowadzić do problemów w transporcie, niedoborów żywności czy ograniczonej dostępności opieki medycznej. Ciekawą koncepcją, która miała wpływ na kształtowanie się tego podejścia w Polsce i UE, jest „Six Ways to Die"[7]. Jej najważniejszym założeniem jest to, że celem ochrony nie powinna być sama „fizyczna" IK, lecz zapewnienie nieprzerwanego dostępu do usług, od których zależy bezpieczeństwo obywateli na 3 poziomach: indywidualnym, społecznym i państwowym. Identyfikuje ona 6 fundamentalnych zagrożeń, które mogą prowadzić do śmierci jednostek oraz destabilizacji społecznej i gospodarczej: brak żywności, brak wody, choroby, urazy, ekstremalne zimno i ekstremalne ciepło.

Stany Zjednoczone jako pierwsze szeroko zaimplementowały „usługowy" model ochrony. Amerykańska Cybersecurity and Infrastructure Security Agency (CISA) opracowała dokument *National Critical Functions Set* (NCFS)[8], który definiuje funkcje krytyczne jako działania i procesy niezbędne do utrzymania bezpieczeństwa narodowego, stabilności gospodarki oraz podstawowego funkcjonowania społeczeństwa. W dokumencie wyróżniono 4 główne obszary, w których zidentyfikowano 55 funkcji krytycznych:

1) łączność (*connect*) – zapewnienie sprawnego funkcjonowania systemów telekomunikacyjnych, internetu, transmisji danych i usług pocztowych,
2) dystrybucja i transport (*distribute*) – utrzymanie ciągłości ruchu ludzi, towarów oraz zasobów niezbędnych do funkcjonowania gospodarki i infrastruktury,
3) dostawy i infrastruktura fizyczna (*supply*) – zabezpieczenie kluczowych zasobów, w tym energii, wody pitnej, surowców przemysłowych oraz systemów produkcyjnych,
4) zarządzanie i stabilność społeczna (*manage*) – ochrona systemów administracji publicznej (np. istotna w USA ochrona wyborów), stabilności finansowej, rynków kapitałowych oraz zarządzania kryzysowego.

[7] M. Bennett, V. Gupta, *Dealing in Security Understanding Vital Services and How They Keep You Safe*, 2010, http://resiliencemaps.org/files/Dealing_in_Security.July2010.en.pdf [dostęp: 22.06.2022].

[8] *National Critical Functions Set*, CISA, https://www.cisa.gov/national-critical-functions-set [dostęp: 24.06.2022].

Zatem w modelu NCFS nie chroni się pojedynczych obiektów czy systemów, lecz usługi, co implikuje np. konieczność wdrażania kompleksowych rozwiązań zapewniających odporność na awarie oraz redundancji zasobów.

Konsekwencją opisywanych działań stało się przyjęcie (14 grudnia 2022 r.) w UE przełomowej dyrektywy CER (o odporności podmiotów krytycznych)[9]. Dyrektywa CER kończy podział na podejście „obiektowe" i „usługowe". Formalizuje nowoczesne podejście do ochrony infrastruktury, z uwzględnieniem zapewnienia odporności podmiotów świadczących niezbędne usługi dla społeczeństwa. Wprowadza kompleksowy model zarządzania ryzykiem na poziomie systemowym, z uwzględnieniem współzależności między sektorami i z naciskiem na odporność całych łańcuchów dostaw. Co znamienne, w tym samym czasie przyjęto dyrektywę NIS 2[10] dotyczącą cyberbezpieczeństwa. Obie dyrektywy są ze sobą kompatybilne i jako takie powinny być wdrożone w systemach prawnych poszczególnych krajów członkowskich.

Przełomowa rola dyrektywy CER – polska perspektywa

Dla Polski implementacja dyrektywy CER jest nie tylko kolejnym wymogiem legislacyjnym, lecz także naturalnym krokiem w kierunku przyjęcia systemowego podejścia do bezpieczeństwa narodowego. Cenne w tym zakresie są doświadczenia związane z ochroną IK, zdobywane zarówno na poziomie krajowym, jak i we współpracy międzynarodowej (np. w ramach NATO i UE). Polska od lat rozwija własne metody zarządzania ryzykiem i ochrony IK, obejmujące wdrożenie NPOIK, budowanie cyberbezpieczeństwa, wprowadzanie mechanizmów służących ochronie ludności[11] i obronie cywilnej czy zwiększanie potencjału militarnego[12]. Są to solidne fundamenty, na których oprze się nowa architektura odporności podmiotów krytycznych i świadczonych przez nich usług.

[9] *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.*

[10] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2).*

[11] *Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej.*

[12] *Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny.*

Co więcej, Polska ma unikalne kompetencje do kształtowania standardów ochrony IK na poziomie europejskim. Wieloletnie doświadczenie w łączeniu sektorów publicznego i prywatnego w obszarze bezpieczeństwa, uwzględniające świadomość nowych zagrożeń i ich ciągłej ewolucji oraz rozumienie szerokiego kontekstu społeczno-technologicznego, czynią Polskę ważnym uczestnikiem procesu doskonalenia mechanizmów odporności. Polska prezydencja w Radzie UE, trwająca od 1 stycznia do 30 czerwca 2025 r., koncentruje się na wzmacnianiu 7 wymiarów europejskiego bezpieczeństwa. Są to:

- zdolność do obrony,
- ochrona ludzi i granic,
- odporność na obcą ingerencję i dezinformację,
- bezpieczeństwo i swoboda działalności gospodarczej,
- transformacja energetyczna,
- konkurencyjne i odporne rolnictwo,
- bezpieczeństwo zdrowotne[13].

W Polsce za całość prac merytorycznych związanych z implementacją dyrektywy CER do ustawy o zarządzaniu kryzysowym odpowiada RCB.

Nowy etap w ochronie infrastruktury krytycznej dla Unii Europejskiej i krajów członkowskich

Wdrażanie dyrektywy CER stanowi jedno z największych wyzwań legislacyjnych i operacyjnych dla państw członkowskich UE. Jest to kamień milowy w budowaniu europejskiej odporności na zagrożenia o charakterze systemowym – od cyberataków, przez sabotaż infrastruktury, aż po kryzysy energetyczne, zdrowotne i inne, związane z nieznanymi rodzajami ryzyka. To także wyraźny sygnał, że kraje członkowskie dostrzegają konieczność ewolucji modelu ochrony IK w ujednoliconym, nowoczesnym kierunku. Nowe regulacje pozwolą skuteczniej przeciwdziałać obecnym i przyszłym zagrożeniom i zwiększą odporność zarówno na poziomie państw, jak i całej UE. Jako termin jej pełnego wdrożenia Komisja Europejska wyznaczyła październik 2024 r., jednak do marca 2025 r. jedynie 9 państw ukończyło proces transpozycji przepisów do prawa krajowego, a pozostałe – w tym Polska – prowadzą intensywne prace nad ich finalizacją. Warto dodać, że wspólne wysiłki krajów członkowskich w zakresie wdrażania dyrektywy

[13] *Prezydencja w Radzie UE*, Rada Europejska, Rada Unii Europejskiej, https://www.consilium.europa.eu/pl/council-eu/presidency-council-eu/ [dostęp: 28.02.2025].

CER to przejście na nowy poziom integracji i solidarności w zakresie bezpieczeństwa. Dzięki temu UE zyskuje bardziej odporny, elastyczny i skoordynowany system ochrony, który pozwala skutecznie reagować na dynamicznie zmieniające się zagrożenia XXI w.

Źródła założeń polskiej implementacji dyrektywy CER

Prace koncepcyjne nad polską ustawą implementującą dyrektywę CER rozpoczęły się w ramach RCB w pierwszej połowie 2023 r.[14] Ich efekty zostały omówione podczas X Krajowego Forum Ochrony Infrastruktury Krytycznej (2023), a aspekty dotyczące standaryzacji i oceny zgodności przedstawił autor tego artykułu[15]. W I kwartale 2024 r. zapadły formalne decyzje dotyczące zobowiązania RCB jako wykonawcy projektu nowelizacji. W marcu 2024 r. został rozesłany do konsultacji pierwszy projekt, którego nowatorskie rozwiązania zyskały uznanie zarówno administracji państwowej, jak i interesariuszy z rynku, zwłaszcza operatorów IK. Na obecnym etapie prac legislacyjnych (marzec 2025) większość rozwiązań jest już dopracowana, a sama ustawa czeka na wejście do sejmu.

Jednym z najważniejszych obszarów w procesie implementacji dyrektywy CER jest zapewnienie spójnych i skutecznych mechanizmów standaryzacji i oceny zgodności, które umożliwią jednolite podejście do wymagań dotyczących odporności podmiotów krytycznych i ciągłości działania usług kluczowych.

Założeniem niniejszego artykułu jest wkład w dyskusję prowadzoną w ramach polskiej prezydencji w Radzie UE, szczególnie w kontekście prac Grupy Roboczej ds. Ochrony Ludności – Odporność Podmiotów Krytycznych (Working Party on Civil Protection – Critical Entities Resilience, PROCIV CER), Horyzontalnej Grupy Roboczej ds. Wzmacniania Odporności i Przeciwdziałania Zagrożeniom Hybrydowym (Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats) oraz Grupy

[14] 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: 6.04.2025].

[15] A. Tatarowski, *Standaryzacja i certyfikacja rozwiązań wynikających z Dyrektywy CER*, X Krajowe Forum Ochrony Infrastruktury Krytycznej, Warszawa 2023, https://www.gov.pl/web/rcb/x-krajowe-forum-ochrony-infrastruktury-krytycznej-za-nami [dostęp: 28.02.2025].

Roboczej ds. Terroryzmu (Working Party on Terrorism, TWP). W artykule przedstawiono, w jaki sposób w projekcie polskiej ustawy przełożono europejskie regulacje na konkretne rozwiązania w zakresie oceny ryzyka, standaryzacji rozwiązań organizacyjno-technicznych i usług świadczonych na rzecz podmiotów krytycznych, a także oceny zgodności (audytowania i certyfikacji). Autor niniejszego opracowania, jako współtwórca koncepcji systemu standaryzacji w polskiej implementacji CER, przedstawił genezę i uzasadnienie przyjętych rozwiązań oraz ich praktyczne konsekwencje dla operatorów IK i administracji publicznej.

Narodowy Program Ochrony Infrastruktury Krytycznej jako fundament zapewniania bezpieczeństwa infrastruktury krytycznej i źródło inspiracji

W ewoluującym przez lata NPOIK system ochrony IK jest oparty na wspomnianym tzw. sześciopaku. Dla porządku zostanie przytoczony aktualny (z 2023 r.)[16] opis tych założeń, które obejmują:

1) zapewnienie bezpieczeństwa fizycznego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie działań osób, które w sposób nieautoryzowany podjęły próbę dostania się lub znalazły się na terenie IK;
2) zapewnienie bezpieczeństwa technicznego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie zaburzenia realizowanych procesów technologicznych;
3) zapewnienie bezpieczeństwa osobowego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie działań osób, które posiadają uprawniony dostęp do infrastruktury krytycznej;
4) zapewnienie bezpieczeństwa teleinformatycznego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie nieautoryzowanego oddziaływania na aparaturę kontrolną oraz systemy i sieci teleinformatyczne;
5) zapewnienie bezpieczeństwa prawnego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie prawnych działań podmiotów zewnętrznych;

[16] *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.

6) plany ciągłości działania i odtwarzania, rozumiane jako zespół działań organizacyjnych i technicznych prowadzących do utrzymania i odtworzenia funkcji realizowanych przez IK[17].

System ten koresponduje z art. 13 dyrektywy CER, dotyczącym środków w zakresie odporności, które powinny zostać wprowadzone przez podmioty krytyczne. Warto przywołać pierwszy ustęp tego przepisu:

1) Państwa członkowskie zapewniają, aby podmioty krytyczne wprowadzały odpowiednie i proporcjonalne środki techniczne, środki bezpieczeństwa i środki organizacyjne służące zapewnieniu ich odporności, w oparciu o odpowiednie informacje dostarczone przez państwa członkowskie dotyczące oceny ryzyka państwa członkowskiego oraz wyników oceny ryzyka podmiotu krytycznego, w tym środki niezbędne w celu:
   a) zapobiegania incydentom, z należytym uwzględnieniem środków zmniejszania ryzyka związanego z katastrofami i przystosowania się do zmiany klimatu;
   b) zapewnienia odpowiedniej fizycznej ochrony ich budynków i terenów oraz infrastruktury krytycznej, z należytym uwzględnieniem na przykład zainstalowania ogrodzeń, budowy barier, narzędzi i procedur monitorowania terenu podlegającego ochronie, sprzętu do wykrywania i kontroli dostępu;
   c) odpowiedzi na incydenty, stawiania im oporu i łagodzenia ich skutków, z należytym uwzględnieniem wdrażania procedur i protokołów zarządzania ryzykiem i zarządzania kryzysowego, a także procedur ostrzegawczych;
   d) odtworzenia po incydentach, z należytym uwzględnieniem środków na rzecz ciągłości działania oraz identyfikacji alternatywnych łańcuchów dostaw w celu przywrócenia świadczenia usługi kluczowej;
   e) zapewnienia odpowiedniego zarządzania bezpieczeństwem pracowników, z należytym uwzględnieniem środków takich jak ustanowienie kategorii personelu wykonującego funkcje krytyczne, ustanowienie praw dostępu do budynków i terenów, infrastruktury krytycznej i informacji szczególnie chronionych, ustanowienie procedur sprawdzenia przeszłości zgodnie z art. 14, wyznaczenie kategorii osób podlegających takim procedurom sprawdzenia przeszłości oraz określenie odpowiednich wymogów szkoleniowych i kwalifikacji;
   f) zwiększania świadomości odpowiedniego personelu na temat środków, o których mowa w lit. a)–e), z należytym uwzględnieniem szkoleń, materiałów informacyjnych i ćwiczeń.

[17] *Narodowy Program Ochrony Infrastruktury Krytycznej*..., s. 30–31.

> Do celów akapitu pierwszego lit. e) państwa członkowskie zapewniają, aby podmioty krytyczne uwzględniały personel zewnętrznych dostawców usług przy określaniu kategorii personelu, który wykonuje funkcje krytyczne.

Powyższe zapisy stanowiły punkt wyjścia do prac nad nową strukturą dotyczącą standaryzacji w zakresie zapewnienia bezpieczeństwa i budowania odporności IK w Polsce. Dyrektywa CER, zgodnie z art. 3, opiera się na zasadzie minimalnej harmonizacji, co oznacza, że wyznacza jedynie podstawowe ramy regulacyjne i pozostawia państwom członkowskim możliwość wprowadzenia rozwiązań dostosowanych do krajowych realiów, w tym bardziej rygorystycznych. Takie podejście zapewnia elastyczność i możliwość uwzględnienia specyficznych uwarunkowań krajowych oraz pozwala na stworzenie systemu ochrony IK odpowiadającego rzeczywistym zagrożeniom i wymaganiom operacyjnym. W polskiej implementacji wykorzystano ten margines swobody i zaprojektowano rozwiązania, które nie tylko w pełni realizują unijne wytyczne, lecz także integrują krajowe doświadczenia oraz wnioski płynące z dotychczasowych regulacji i praktyk w zakresie bezpieczeństwa IK.

Normalizacja jako podstawa do wdrożenia optymalnej standaryzacji

Normalizacja, rozumiana jako działalność mająca na celu uzyskanie optymalnego stopnia uporządkowania w określonej dziedzinie przez ustalenie postanowień przeznaczonych do powszechnego wielokrotnego stosowania[18], jest fundamentem sprawnego funkcjonowania społeczeństw i gospodarek, a jej znaczenie sięga początków cywilizacji[19].

[18] J. Łunarski, *Normalizacja i standaryzacja*, Rzeszów 2014, Oficyna Wydawnicza Politechniki Rzeszowskiej.

[19] Już w świecie starożytnym dążono do ujednolicenia jednostek miar, systemów wag, standardów budowlanych i organizacyjnych, co było ważne nie tylko dla rozwoju handlu i administracji, lecz także dla zapewnienia skuteczności działań militarnych i bezpieczeństwa publicznego. Starożytny Egipt stosował precyzyjne miary przy wznoszeniu monumentalnych konstrukcji, takich jak piramidy, a w Mezopotamii jednolite systemy wag pozwalały na sprawne funkcjonowanie gospodarki i wymiany towarowej. Starożytny Rzym natomiast rozwinął system normalizacji w sposób, który na wiele stuleci ukształtował organizację społeczną i militarną. Standaryzacja uzbrojenia i wyposażenia legionistów zapewniała przewagę operacyjną na polu bitwy i zwiększała efektywność logistyki wojskowej. Rzymianie stosowali również normy w budownictwie – ujednolicone metody wznoszenia dróg, akweduktów i fortów wojskowych umożliwiały sprawną ekspansję i utrzymanie imperium. Rzymianie rozwinęli także pierwsze ustandaryzowane formy straży miejskiej oraz systemy kanalizacyjne, które minimalizowały zagrożenia zdrowotne w miastach.

Normy organizują rzeczywistość, zapewniają przewidywalność i koordynację działań w skali globalnej. Od systemów produkcji i dystrybucji energii, przez transport i telekomunikację, aż po cyberbezpieczeństwo i zarządzanie ryzykiem – normalizacja stanowi fundament interoperacyjności i stabilności. W dobie dynamicznych zmian technologicznych oraz rosnących zagrożeń bezpieczeństwa jej rola jest jeszcze bardziej istotna, ponieważ tworzy spójne ramy dla funkcjonowania państw, gospodarek i instytucji w coraz bardziej złożonym świecie.

Obecnie normalizacja w istotny sposób wspiera unijną legislację. Przełomowym momentem w umocowaniu normalizacji w unijnym ekosystemie społeczno-gospodarczym było przyjęcie i opublikowanie 7 maja 1985 r. Rezolucji Rady WE[20] w sprawie nowego podejścia do harmonizacji technicznej i normalizacji. Jak twierdzą Teresa Idzikowska i Krzysztof Banaszek, (...) *nadanie szczególnie wysokiej rangi normom i specyfikacjom technicznym będącym produktem działalności normalizacyjnej, przy tworzeniu zasad swobodnego przepływu towarów i likwidowaniu barier w handlu, oznaczało radykalną zmianę statusu norm zarówno na szczeblu krajowym, jak i międzynarodowym*[21]. Przyjęty model zakładał, że przepisy prawne powinny określać jedynie podstawowe wymagania dotyczące bezpieczeństwa i jakości, szczegółowe wytyczne techniczne zaś – być opracowywane w ramach dobrowolnych norm europejskich. W praktyce pozwoliło to na elastyczne dostosowanie wymogów do zmieniających się warunków rynkowych i technologicznych, z jednoczesnym ujednoliceniem najważniejszych standardów na poziomie całej Wspólnoty Europejskiej.

Od 1 stycznia 2004 r. Polski Komitet Normalizacyjny (PKN) jest członkiem europejskich organizacji normalizacyjnych: Europejskiego Komitetu Normalizacyjnego i Europejskiego Komitetu Normalizacyjnego Elektrotechniki. Są to stowarzyszenia prywatne, nienakierowane na osiąganie zysku, działające na podstawie belgijskiego prawa. Nie są organami KE. Europejski system normalizacyjny wyróżnia się tym, że Normy Europejskie są uzgadniane przez wszystkie kraje członkowskie, a każdy z nich, niezależnie od zaangażowania w ich opracowanie, ma obowiązek ich oceny i implementacji. W efekcie w Europie istnieje jedna Norma Europejska, dostępna tylko

[20] *Council Resolution of 7 May 1985 on a new approach to technical harmonization and standards.*

[21] T. Idzikowska, K. Banaszek, *Rola i znaczenie normalizacji w bezpieczeństwie transportu*, „Logistyka" 2010, t. 4.

jako implementacja norm krajowych[22]. Dla porządku należy wspomnieć, że norma ma wiele zbieżnych ze sobą definicji[23]. Dość przystępna jest ta ujęta w *Ustawie z dnia 12 września 2002 r. o normalizacji*, zgodnie z którą jest to (...) *dokument przyjęty na zasadzie konsensu i zatwierdzony przez upoważnioną jednostkę organizacyjną, ustalający – do powszechnego i wielokrotnego stosowania – zasady, wytyczne lub charakterystyki odnoszące się do różnych rodzajów działalności lub ich wyników i zmierzający do uzyskania optymalnego stopnia uporządkowania w określonym zakresie* (art. 2 ust. 4).

Świadomość roli, jaką odgrywa normalizacja jako instrument wspierający zarządzanie ryzykiem i bezpieczeństwem, znalazła odzwierciedlenie w dyrektywie CER, która umożliwiła państwom członkowskim uwzględnianie norm mających zastosowanie do podmiotów krytycznych. Zgodnie z motywem 34 dyrektywy (...) *proces normalizacji powinien pozostać procesem uzależnionym głównie od czynników rynkowych. Nadal mogą jednak zaistnieć sytuacje, w których należy wymagać przestrzegania określonych norm.* Z kolei art. 16 wskazuje, że (...) *aby wspierać spójne wdrażanie niniejszej dyrektywy, państwa członkowskie zachęcają, w przypadkach gdy może to być przydatne i nie narzucając ani nie faworyzując stosowania określonego rodzaju technologii, do stosowania europejskich i międzynarodowych norm i specyfikacji technicznych istotnych dla środków w zakresie bezpieczeństwa i w zakresie odporności mających zastosowanie do podmiotów krytycznych.*

Propozycja polskiej implementacji dyrektywy CER w pełni realizuje te założenia. Uwzględnia zarówno europejski dorobek normalizacyjny, jak i krajowe doświadczenia w zakresie standaryzacji systemów bezpieczeństwa w IK (NPOIK wraz z załącznikami).

Wprowadzanie norm do przepisów prawa – polska specyfika

Możliwość powoływania norm w przepisach prawa wynika ze wspomnianej ustawy o normalizacji. Zgodnie z art. 5 ust. 4: *Polskie Normy mogą być powoływane w przepisach prawnych po ich opublikowaniu w języku polskim*, a sposób powoływania uwzględniający dokładność (powołanie datowane, niedatowane, ogólne) i moc (wyłączne lub wskazujące) określa norma PN-EN 45020:2009 *Normalizacja i dziedziny związane. Terminologia ogólna*. Prace legislacyjne związane z osiągnięciem celów wyznaczonych przez

[22] T. Schweitzer, E. Zielińska, *Działalność normalizacyjna*, w: *Normalizacja*, T. Schweitzer (red.), Warszawa 2013, Polski Komitet Normalizacyjny, s. 15–18.

[23] *A World Built on Standards: A Textbook for Higher Education*, S.A. Bøgh (red.), Nordhavn 2015, Danish Standards Foundation.

dyrektywę CER musiały oczywiście uwzględniać również szeroko rozumianą dobrowolność stosowania norm, wynikającą nie tyle z samej ustawy, ile z przyjętego systemu normalizacji europejskiej. Zgodnie ze stanowiskiem PKN powoływanie się na Polskie Normy w przepisie prawnym nie zmienia jej dobrowolnego statusu, chyba że ustawodawca chce ten status zmienić, co jest możliwe przez wyraźne wskazanie tylko w postanowieniach innej ustawy[24]. Stanowisko to wykorzystano w pierwszym projekcie implementacji, w którym zostały przywołane normy. W toku pierwszej fazy uzgodnień międzyresortowych, opiniowania i konsultacji społecznych RCB przyjęło argumentację Rządowego Centrum Legislacji (RCL), że normy, jako standardy odpłatne, nie powinny być powoływane w ustawie jako obligatoryjne do stosowania. Co więcej, pomimo jasnego stanowiska PKN względem zmiany statusu normy z dobrowolnej na obligatoryjną w rozumieniu ustawy, w której jest powoływana, zasada dobrowolności stosowania norm mogłaby zostać naruszona. W związku z tym zdecydowano się na alternatywne rozwiązanie – normy będą bezpośrednio przywoływane nie w ustawie, lecz w aktach wykonawczych lub w oficjalnych wykazach publikowanych w Biuletynie Informacji Publicznej (BIP) odpowiednich instytucji. Takie podejście pozwala na zachowanie równowagi między zapewnieniem dostępu do standardów a poszanowaniem zasad normalizacji i regulacji prawnych. Co więcej, w porozumieniu z RCL opracowano konstrukcję przepisów, która uwzględnia dotychczasowe ustalenia z zachowaniem pełnej zgodności z obowiązującymi regulacjami dotyczącymi normalizacji oraz zasadami funkcjonowania systemu normalizacyjnego. W projekcie ustawy dookreślono, że rozwiązania, o których mowa w kolejnych akapitach, (...) *powinny spełniać wymagania określone w normach, wskazanych w akcie wykonawczym*. Ten sposób zapisu wskazuje na konieczność spełnienia wymagań określonych w normie, ale nie narzuca normy jako dokumentu obligatoryjnego do stosowania.

Mentalność i bariery systemowe – geneza problemów. Konieczność twardego podejścia do wykorzystania norm

Doświadczenia państwowych instytucji regulacyjnych, zwłaszcza RCB, operatorów IK oraz całego rynku (w tym innych zamawiających – inwestorów, usługodawców, dostawców rozmaitych rozwiązań organizacyjnych

[24] *Dobrowolność stosowania norm*, Polski Komitet Normalizacyjny, https://wiedza.pkn.pl/web/wiedza-normalizacyjna/stanowisko-pkn-w-sprawie-dobrowolnosci-pn [dostęp: 28.02.2025].

i technicznych itp.) jednoznacznie wskazują, że ochrona IK w Polsce przez lata była ograniczana przez bariery systemowe, których źródła sięgają początku transformacji ustrojowej. Doprowadziły one do sytuacji, w której zapewnienie odpowiednio wysokich standardów bezpieczeństwa było utrudnione, a w niektórych przypadkach – wręcz niemożliwe.

Jednym z najważniejszych problemów stała się niewłaściwa interpretacja przepisów prawnych regulujących kwestie zamówień publicznych (unijnych i polskich) – najniższa cena była dominującym i czasami jedynym uwzględnianym kryterium. W wielu przypadkach formułowanie wymagań dotyczących jakości sprzętu lub usług napotykało trudności zarówno na poziomie zamawiających, jak i instytucji kontrolujących. Komórki merytoryczne działające u operatorów IK, odpowiedzialne za definiowanie potrzeb w zakresie bezpieczeństwa, często formułowały wymagania odpowiadające rzeczywistym zagrożeniom i wykorzystujące sprawdzone standardy (np. NPOIK) oraz normy. Jednak na kolejnym etapie, na poziomie formalnym, wymagania te były redukowane przez działy zajmujące się zamówieniami (lub zarządy!), które powołując się na przepisy oraz niepisane zasady eliminowania zbędnych kosztów, usuwały dodatkowe wymagania techniczne lub organizacyjne, a pozostawiały wyłącznie te ujęte jednoznacznie w przepisach prawa.

Sytuację dodatkowo komplikowały instytucje kontrolujące, które często utożsamiały wymagania wykraczające poza absolutne minimum prawne z naruszeniem zasad gospodarności. Niejednokrotnie podejmowano działania kontrolne wobec jednostek, które wprowadzały bardziej restrykcyjne wymagania dotyczące bezpieczeństwa. W efekcie osoby odpowiedzialne za zamówienia nie formułowały wysokich standardów z obawy przed oskarżeniami o niegospodarność, a nawet korupcję. W przypadkach, gdy udało się przeforsować wyższe wymagania, kontrole zewnętrzne mogły uznać je za wydatki niezasadne, wzbudzające podejrzenia. Taki układ systemowy doprowadził do błędnego koła:

- operatorzy IK formułują wysokie wymagania dla bezpieczeństwa IK, bazujące na normach i dobrych praktykach,
- komórki zamówień (lub zarządy) odrzucają te wymagania, powołując się na konieczność ograniczenia kosztów i uniknięcia potencjalnych zarzutów o niegospodarność,
- instytucje kontrolujące działają w sposób, który de facto premiuje najniższą cenę, i ignorują realne potrzeby związane z bezpieczeństwem,

– dostawcy wysokiej jakości usług, sprzętu i innych rozwiązań nie mogą skutecznie konkurować, ponieważ nie mają innych argumentów poza ceną,
– dostawcy niskiej jakości usług i sprzętu zdobywają kontrakty przez oferowanie rozwiązań o wątpliwej skuteczności i pochodzeniu.

W tej sytuacji konieczne stało się wprowadzenie regulacji, które uczynią wymagania dotyczące jakości i bezpieczeństwa IK niemożliwymi do ominięcia. Dyrektywa CER w art. 16 oraz motywie 34 jasno wskazuje, że państwa członkowskie powinny zachęcać do stosowania norm, co w przypadku Polski wymagało bardziej stanowczego podejścia. Przyjęcie modelu minimalnej harmonizacji pozwoliło na opracowanie mechanizmów eliminujących możliwość obchodzenia wymagań jakościowych i tym samym na usunięcie luk systemowych, które przez lata utrudniały stosowanie wysokich standardów ochrony.

Co więcej, w projekcie implementacji dyrektywy CER uwzględniono przepisy *Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* jako najważniejsze dla zapewnienia odpowiedniego poziomu ochrony wytwarzanej dokumentacji i stosowanych rozwiązań. Dodatkowo zastosowanie tych przepisów pozwala na skorzystanie z regulacji przewidzianych w art. 12 *Ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych*, co w określonych przypadkach umożliwia realizację zamówień w trybie innym niż przewidziany w ustawie. To rozwiązanie, wynikające z potrzeby dostosowania procedur do specyfiki IK, wpisuje się w koncepcję podnoszenia standardów bezpieczeństwa oraz kształtowania wymagań względem usług i rozwiązań organizacyjno-technicznych.

Standaryzacja rozwiązań organizacyjno-technicznych oraz wymagań względem usług i osób w polskiej propozycji implementacji dyrektywy CER

Standaryzacja bezpieczeństwa IK to proces systemowego ujednolicania wymagań dotyczących ochrony IK, który bazuje zarówno na normach międzynarodowych, europejskich, jak i na standardach, wytycznych lub rekomendacjach krajowych, takich jak NPOIK. Jest to proces, który czerpie z normalizacji, ale też precyzyjnie określa wymagania, unifikuje je i dostosowuje do specyfiki IK, z uwzględnieniem specyficznych zagrożeń i rosnących współzależności sektorowych. Obejmuje on cały ekosystem interesariuszy:

operatorów IK, podmioty krytyczne, usługodawców, jednostki administracji publicznej, organy nadzoru i kontroli, a także podmioty lub osoby prowadzące walidację (audyty i certyfikacje) zastosowanych rozwiązań.

Proces standaryzacji uwzględnia dynamicznie zmieniające się wyzwania w obszarze bezpieczeństwa. Wymaga elastycznego podejścia do aktualizacji i doskonalenia środków ochrony. Wprowadzenie jednolitych standardów pozwala na skuteczniejsze działanie systemu zarządzania ryzykiem, eliminację jego słabych punktów oraz wzmocnienie interoperacyjności pomiędzy podmiotami odpowiedzialnymi za bezpieczeństwo IK. W konsekwencji standaryzacja zapewnia nie tylko wyższy poziom ochrony, lecz także transparentność i przewidywalność w zakresie wymagań i mechanizmów ich realizacji.

Operatorzy IK a podmioty krytyczne

Polska propozycja implementacji dyrektywy CER opisuje wymagania względem operatorów IK i podmiotów krytycznych. Operator IK to zgodnie z projektem ustawy (...) *właściciel lub posiadacz obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług wpisanych do wykazu infrastruktury krytycznej*, z kolei podmiot krytyczny (czyli podmiot wskazany w dyrektywie CER) to (...) *operator IK wpisany do wykazu podmiotów krytycznych, realizujący co najmniej jedną usługę kluczową, prowadzący działalność w sektorze lub podsektorze wymienionym w załączniku do ustawy i prowadzący działalność na terytorium Rzeczypospolitej Polskiej lub na obszarach morskich Rzeczypospolitej Polskiej, o których mowa w ustawie z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej*. Infrastrukturę krytyczną zaś zdefiniowano jako:

> (...) obiekt, urządzenie, instalację, sieć, system oraz usługę lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi niezbędne do:
> a) realizacji ważnych interesów państwa, w tym zapewnienia funkcjonowania organów administracji publicznej,
> b) zapewnienia funkcjonowania przedsiębiorstw,
> c) zaspokajania oraz utrzymania potrzeb obywateli, w tym potrzeb o charakterze lokalnym,
> d) zapewnienia świadczenia usług kluczowych.

Podmiot krytyczny to operator IK, który świadczy co najmniej 1 usługę kluczową, a wystąpienie tzw. incydentu istotnego mogłoby spowodować poważne zakłócenia w jej świadczeniu. Wpis do wykazu podmiotów

krytycznych następuje na podstawie analizy progów istotności skutku zakłócającego, które będą określone w akcie wykonawczym Rady Ministrów. Ocena istotności skutków zakłócających uwzględnia m.in.: liczbę użytkowników zależnych od danej usługi, powiązania między sektorami, wpływ incydentu na gospodarkę, społeczeństwo, bezpieczeństwo publiczne oraz środowisko, udział danego podmiotu w rynku, obszar geograficzny dotknięty ewentualnym incydentem oraz dostępność alternatywnych sposobów świadczenia tej usługi.

Standaryzacja wymagań dla operatorów IK. Wymagania ustawowe i minimalne standardy bezpieczeństwa

W projekcie implementacji dyrektywy CER wprowadzono nowe obowiązki dla operatorów IK, obejmujące systematyczną analizę zagrożeń oraz wdrażanie odpowiednich rozwiązań dostosowanych do jej wyników, zgodnie z tzw. sześciopakiem NPOIK.

W toku prac legislacyjnych udało się wypracować podejście, które będzie obligować operatorów IK do wdrażania minimalnych wymagań we wskazanym zakresie. To *game changer* wychodzący naprzeciw opisywanym w poprzednim rozdziale problemom systemowo-operacyjnym, które dotychczas uniemożliwiały wdrażanie odpowiednich rozwiązań pomimo istnienia NPOIK, norm i wielu innych standardów. Minimalne standardy zostaną określone w drodze rozporządzenia i będą dotyczyły całego tzw. sześciopaku. Powstają z uwzględnieniem rekomendacji o charakterze specjalistycznym w zakresie ochrony IK, niezbędnych do wdrażania rozwiązań w zakresie bezpieczeństwa IK, jej lokalizacji i charakterystyki oraz potrzeby podejmowania działań zapewniających jej bezpieczeństwo. Autor niniejszego artykułu jest współautorem tych standardów (są one na etapie uzgodnień). Stanowią one narzędzie do zapewnienia spójnego i jednolitego podejścia do ochrony IK, zgodnego z wymaganiami określonymi w projekcie ustawy. Dokument ten może mocno oddziaływać na całą branżę bezpieczeństwa w Polsce i w Europie oraz stanowić źródło wiedzy i inspiracji nie tylko dla operatorów IK. Warto go zatem szerzej opisać, ze szczególnym uwzględnieniem bezpieczeństwa fizycznego, tak bardzo podkreślanego w dyrektywie CER.

Standardy dookreślają pojęcie ochrony IK jako procesu podzielonego na następujące etapy:

1) wskazanie zakresu działań, celów do osiągnięcia w ramach ochrony IK oraz adresatów tych działań,

2) identyfikacja krytycznych zasobów, funkcji oraz określenie sieci powiązań (zależności) z innymi sektorami IK, w tym podmiotami i organami,
3) określenie ról i odpowiedzialności uczestników procesu ochrony IK,
4) szacowanie ryzyka,
5) wskazanie priorytetów działania i dokonanie ich hierarchizacji w zależności od wyników oceny ryzyka,
6) rozwój i wdrażanie systemu ochrony IK, w tym:
   – określenie kryteriów projektowych oraz instalacja systemów zabezpieczeń technicznych w obiektach IK,
   – opracowanie, stosowanie i bieżąca aktualizacja dokumentacji ochrony IK,
7) testowanie (przez ćwiczenia) i przegląd (przez samoocenę i audyt lub certyfikację) systemu ochrony IK oraz pomiar postępów na drodze do osiągnięcia celu,
8) doskonalenie rozumiane jako wprowadzanie modyfikacji i korekt w wyniku testów, przeglądów, pomiarów i wykorzystanie inteligentnych rozwiązań, które powinny obejmować chronione zasoby, zagrożenia dla tych zasobów oraz poziomy ich ochrony przed zidentyfikowanymi zagrożeniami.

Etapami wymagającymi szczególnej uwagi i staranności są: szacowanie ryzyka oraz rozwój i wdrażanie systemu ochrony IK. System ten powinien mieć zastosowanie do wszystkich typów zidentyfikowanych zagrożeń, tak naturalnych, jak i intencjonalnych oraz technicznych, a także być przygotowany do możliwie szybkiego przywrócenia funkcji pełnionych przez daną IK. W związku z tym działania podejmowane na rzecz zapewnienia bezpieczeństwa mają na celu minimalizację ryzyka zakłócenia funkcjonowania IK przez:

– zmniejszanie prawdopodobieństwa wystąpienia zagrożenia,
– zmniejszanie podatności na zagrożenia,
– minimalizowanie skutków wystąpienia zagrożenia.

Standardy wprowadzają ujednolicone definicje pojęć istotnych przy wdrażaniu wszystkich zakresów z tzw. sześciopaku. Przykładowo pojęcia związane z ryzykiem zostały zdefiniowane następująco:

– ryzyko – prawdopodobieństwo wystąpienia zagrożenia wraz z jego skutkami,
– źródła ryzyka – elementy lub czynniki, które mogą prowadzić do wystąpienia ryzyka, mogą wynikać z zagrożeń, podatności,

charakterystyki i rodzaju aktywów, otoczenia organizacyjnego lub technicznego, zachowań, działań lub błędów osób,
- kryteria ryzyka – zestaw zasad i poziomów odniesienia określających akceptowalność ryzyka, ustalanych z uwzględnieniem celów organizacji, kontekstu wewnętrznego i zewnętrznego oraz obowiązujących przepisów prawa, regulacji i norm,
- identyfikacja ryzyka – proces wyszukiwania, rozpoznawania i opisywania ryzyka, obejmujący określenie zasobów podlegających ryzyku, rozpoznanie jego źródeł oraz potencjalnych skutków,
- analiza ryzyka – proces określania poziomu ryzyka przez ocenę prawdopodobieństwa wystąpienia zdarzeń wynikających z zagrożeń oraz ich potencjalnych skutków, z uwzględnieniem istniejących podatności i zabezpieczeń,
- ocena ryzyka – proces porównania wyników analizy ryzyka z przyjętymi kryteriami ryzyka w celu określenia jego akceptowalności oraz potrzeby podjęcia działań zaradczych,
- szacowanie ryzyka – całościowy proces identyfikacji, analizy i oceny ryzyka.

Definicje zostały opracowane z uwzględnieniem wielu norm z dziedziny ryzyka i kontekstu ich zastosowania w opracowywanych standardach[25]. Warto przypomnieć, że podejście oparte na ryzyku stanowi filozofię zapewnienia bezpieczeństwa IK w Polsce od wielu lat i zostało wzmocnione celami wyznaczonymi przez dyrektywę CER. To podejście umożliwia operatorom IK stosowanie wielu rozwiązań, w zależności od samodzielnie dokonanej oceny ryzyka. Na przykład systemy zabezpieczeń technicznych (czyli systemy sygnalizacji włamania i napadu, systemy kontroli dostępu i systemy telewizji dozorowej) powinny po zainstalowaniu spełnić wymagania Polskiej Normy odpowiedniej dla danego systemu zabezpieczeń technicznych w stopniu zabezpieczenia adekwatnym do oceny ryzyka, przy czym zaleca się stosowanie stopnia nie niższego niż trzeci[26].

[25] PN-ISO 31000:2018-08 *Zarządzanie ryzykiem – Wytyczne*; PN-ISO 31000:2012 *Zarządzanie ryzykiem – Zasady i wytyczne*; PN-EN ISO/IEC 27005:2025-01 *Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Wytyczne do zarządzania ryzykami w bezpieczeństwie informacji*; PN-ISO/IEC 27005:2014-01 *Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji*; PN-EN IEC 31010:2020-01 *Zarządzanie ryzykiem – Techniki oceny ryzyka*; PKN-ISO Guide 73:2012 *Zarządzanie ryzykiem – Terminologia*.

[26] Według: PN-EN 50131-1 *Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Część 1: Wymagania systemowe*; PN-EN 60839-11-1 *Systemy alarmowe i elektroniczne systemy zabezpieczeń – Część 11-1: Elektroniczne systemy kontroli dostępu – Wymagania dotyczące*

W standardach bardzo szczegółowo są opisane minimalne parametry techniczne, które powinny być stosowane dla sprzętu przeznaczonego do ochrony IK.

W projekcie ustawy zawarto również przepis, który wymusza na operatorach żądanie od usługodawców certyfikatów (przy opracowywaniu i zawieraniu umów zapewniających wdrażanie tzw. sześciopaku). W przypadku ich braku są także uwzględniane, zgodnie z zasadami wzajemnego uznawania w UE, inne dokumenty właściwe dla poszczególnych rozwiązań, potwierdzające posiadanie przez usługodawców odpowiednich kompetencji i uprawnień niezbędnych do realizacji tych rozwiązań. W aspekcie bezpieczeństwa fizycznego, w kontekście projektowania, instalowania i konserwacji systemów zabezpieczeń technicznych, można się spodziewać, że będzie to certyfikat zgodności z przywołaną w projekcie standardów PN-EN 16763 *Usługi w zakresie systemów ochrony przeciwpożarowej i systemów zabezpieczeń technicznych*.

Pierwotna idea standaryzacji wymagań dla podmiotów krytycznych – system zarządzania bezpieczeństwem, audytowanie i certyfikacja

Pierwotną ideą implementacji art. 13 dyrektywy CER było stworzenie dla podmiotów krytycznych systemu zarządzania bezpieczeństwem, który w komplementarny sposób obejmowałby aspekty dotyczące oceny ryzyka, jakości usług, stosowanych rozwiązań organizacyjno-technicznych oraz oceny ich zgodności, a także dotyczące np. wdrażania innych wymagań wynikających z sektorowych aktów prawnych UE. Rozwiązania organizacyjno-techniczne zostały oparte na systemie zarządzania bezpieczeństwem informacji zgodnym z PN-EN ISO/IEC 27001, z uwzględnieniem twardych wymogów w zakresie systemów zabezpieczeń technicznych, które miały być instalowane zgodnie z PN-EN 50131 i/lub PN-EN 60839 i/lub PN-EN 62676. Najbardziej istotnym elementem stało się również utworzenie systemu zarządzania ciągłością działania zgodnego z PN-EN ISO 22301 w zakresie niezbędnym do utrzymania świadczenia usługi kluczowej.

Zwieńczeniem tej idei było sformalizowanie audytów systemu zarządzania bezpieczeństwem podmiotów krytycznych oraz zapewnienie możliwości skorzystania z certyfikacji jako alternatywy dla audytu. Podstawą do tego był art. 21 dyrektywy CER, który umożliwia państwom członkowskim

systemów i komponentów; PN-EN 62676-1-1 *Systemy dozoru wizyjnego stosowane w zabezpieczeniach – Część 1-1: Wymagania systemowe – Postanowienia ogólne*.

określenie wymagań dotyczących oceny zgodności wdrażanych rozwiązań organizacyjno-technicznych oraz zobowiązanie podmiotów krytycznych do stosowania odpowiednich środków bezpieczeństwa. W ten sposób system zarządzania bezpieczeństwem zaproponowany w projekcie implementacji miał stanowić spójną, ustandaryzowaną całość i wychodzić naprzeciw zarówno problemom związanym z brakiem jednolitych wymagań, jak i wieloletnim trudnościom z zapewnieniem wysokiej jakości zabezpieczeń w IK.

Zobowiązanie do prowadzenia audytów objęło 3 filary: system zarządzania bezpieczeństwem informacji, system zarządzania ciągłością działania oraz systemy zabezpieczeń technicznych. Podmioty krytyczne mogły realizować te audyty w sposób elastyczny, dostosowany do swojej specyfiki i struktury organizacyjnej. Proponowane rozwiązanie pozwalało na przeprowadzanie audytów w zintegrowany sposób, obejmowało wówczas jednocześnie wszystkie 3 filary, bądź w sposób rozłączny, np. przez certyfikację systemu zarządzania bezpieczeństwem informacji, równoczesne audytowanie zabezpieczeń technicznych oraz przeprowadzenie odrębnego audytu ciągłości działania. Model ten pozwalał na większą swobodę w doborze audytorów lub jednostek certyfikujących, a także dawał w określonym zakresie możliwość zaangażowania audytorów wewnętrznych. Doprecyzowując, część rozwiązań organizacyjno-technicznych mogła podlegać audytowi wewnętrznemu, realizowanemu przez wykwalifikowanych audytorów będących pracownikami podmiotu, podczas gdy część mogła być certyfikowana przez zewnętrzne jednostki certyfikujące. Wprowadzenie obowiązku audytów i możliwości certyfikacji na zgodność z Polskimi Normami miało zapewnić ujednolicenie wymagań i ich egzekwowanie, a także zwiększyć przejrzystość oraz przewidywalność w zakresie stosowanych mechanizmów kontrolnych. Co więcej, bardzo istotnym elementem systemu stało się zobowiązanie podmiotu krytycznego do żądania od usługodawców, mających realizować na rzecz tego podmiotu różne rozwiązania organizacyjno-techniczne, odpowiednich kompetencji potwierdzonych certyfikatem. Zatem już wstępny etap całego procesu wdrażania systemu zarządzania bezpieczeństwem został zabezpieczony pod względem jakości i zgodności z opisywanymi wymaganiami. Zastosowanie takich narzędzi w polskiej implementacji dyrektywy CER miało na celu nie tylko ułatwienie podmiotom krytycznym wdrażania skutecznych środków zarządzania bezpieczeństwem, lecz także przerwanie błędnego koła, które przez lata utrudniało podnoszenie standardów ochrony IK. Opisana koncepcja w toku uzgodnień

międzyresortowych, opiniowania i konsultacji społecznych zyskała uznanie i ewoluowała w dobrym kierunku.

Standaryzacja wymagań dla podmiotów krytycznych – wyewoluowana koncepcja, ujęta w aktualnym projekcie implementacji dyrektywy CER

Podmiot krytyczny zgodnie z projektem ustawy będzie zobowiązany do wdrożenia zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej. Filarem tego systemu jest prowadzenie systematycznej oceny ryzyka z uwzględnieniem:

a) zagrożeń i związanych z tym ryzyk wymienionych w Krajowej Ocenie Ryzyka oraz innych zagrożeń charakterystycznych dla świadczonej usługi kluczowej, w tym zagrożeń antagonistycznych,
b) stopnia zależności innych sektorów lub podsektorów określonych w załączniku do ustawy od usługi kluczowej świadczonej przez podmiot krytyczny oraz stopnia zależności tego podmiotu krytycznego od usług kluczowych świadczonych przez inne podmioty w innych sektorach, w tym w stosownych przypadkach w sąsiadujących państwach członkowskich Unii Europejskiej i w państwach trzecich,
c) identyfikacji alternatywnych łańcuchów dostaw w celu przywrócenia świadczenia usługi kluczowej,
d) ocen ryzyka prowadzonych na podstawie odrębnych przepisów.

Ustandaryzowanie podejścia do oceny ryzyka stanowi jeden z celów dyrektywy CER, który w polskiej propozycji został zrealizowany komplementarnie. Warto wskazać, że Krajowa Ocena Ryzyka – dokument, za którego kształt będzie odpowiedzialne RCB – będzie zawierać:

1) zidentyfikowane istotne zagrożenia, w szczególności:
   a) stanowiące katastrofę naturalną lub awarię techniczną w rozumieniu przepisów ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz. U. z 2017 r. poz. 1897),
   b) hybrydowe,
   c) cyberbezpieczeństwa,
   d) o charakterze terrorystycznym,
   e) mogące spowodować niedostępność usług kluczowych,
   f) inne mogące spowodować znaczące negatywne skutki dla ludności, gospodarki lub dóbr kultury;
2) zagrożenia niezidentyfikowane jednoznacznie, które mogą wystąpić w przyszłości;
3) ocenę ryzyka wystąpienia zidentyfikowanych istotnych zagrożeń.

W przeprowadzaniu oceny ryzyka podmiot krytyczny powinien posiłkować się nie tylko „klasycznymi" normami dotyczącymi ryzyka, o których wcześniej wspomniano, lecz także nową specyfikacją techniczną ISO/TS 31050 *Risk management – Guidelines for managing an emerging risk to enhance resilience*, zgodnie z którą istotne jest wypracowanie podejścia do zarządzania nowymi, nieznanymi dotychczas ryzykami, np. związanymi z rozwojem sztucznej inteligencji[27].

Kolejnym elementem zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej będzie wdrożenie przez podmiot krytyczny odpowiednich i proporcjonalnych do wyników oceny ryzyka rozwiązań organizacyjno-technicznych, zwłaszcza:

a) polityk zarządzania ryzykiem,
b) bezpieczeństwa fizycznego, w tym ochrony fizycznej budynków i terenów należących do podmiotu krytycznego oraz zabezpieczeń technicznych, uwzględniających kontrolę dostępu,
c) ochrony infrastruktury krytycznej niezbędnej do świadczenia usługi kluczowej, zgodnie z wymogami ochrony infrastruktury krytycznej, o których mowa w przepisach rozdziału 7 ustawy,
d) bezpieczeństwa osobowego dotyczącego pracowników i dostawców zewnętrznych,
e) cyberbezpieczeństwa, zgodnie z wymogami dotyczącymi podmiotów kluczowych, o których mowa w przepisach ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa,
f) bezpieczeństwa prawnego świadczenia usługi kluczowej,
g) ciągłości działania i odtwarzania, w tym utrzymywania własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie świadczenia usługi kluczowej do czasu jej pełnego odtworzenia,
h) zdolności do ochrony informacji niejawnych w niezbędnym zakresie do zapewnienia świadczenia usługi kluczowej,
i) szkoleń i ćwiczeń personelu w celu jego przygotowania na różnego rodzaju zagrożenia i incydenty,
j) realizacji okresowych audytów i certyfikacji.

Powyższe zapisy zawarte w formie szczegółowych zadań, przygotowane zgodnie z formalnymi wymogami art. 91 ust. 1 *Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.*, odpowiadają założeniom normatywnym systemu zarządzania bezpieczeństwem informacji i systemu zarządzania ciągłością działania, z uwzględnieniem aspektów dotyczących

[27] Zob. szerzej: A. Tatarowski, *Budowanie odporności infrastruktury krytycznej*...

bezpieczeństwa fizycznego oraz zabezpieczeń technicznych. Z tego względu wymaga się, aby spełniały wymagania określone w normach, które zostaną wskazane w akcie wykonawczym. Koncepcja RCB przewiduje wskazanie co najmniej następujących norm:

1) PN-EN ISO/IEC 27001 *Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności. Systemy zarządzania bezpieczeństwem informacji. Wymagania*,
2) PN-EN ISO 22301 *Bezpieczeństwo i odporność. Systemy zarządzania ciągłością działania. Wymagania*,
3) PN-EN 50131-1 *Systemy alarmowe. Systemy sygnalizacji włamania i napadu. Część 1: Wymagania systemowe*,
4) PN-EN 62676-1-1 *Systemy dozoru wizyjnego stosowane w zabezpieczeniach. Część 1-1: Wymagania systemowe. Postanowienia ogólne*,
5) PN-EN 60839-11-1 *Systemy alarmowe i elektroniczne systemy zabezpieczeń. Część 11-1: Elektroniczne systemy kontroli dostępu. Wymagania dotyczące systemów i komponentów*.

Uzupełnieniem tego aktu wykonawczego będzie możliwość opracowywania i udostępniania przez organ do spraw podmiotów krytycznych (tj. ministra właściwego dla danego sektora lub inny organ, np. Przewodniczącego Komisji Nadzoru Finansowego) dodatkowego wykazu dokumentów normalizacyjnych (czyli norm, specyfikacji technicznych lub innych dokumentów ustalających zasady, wytyczne lub charakterystyki). Wykaz ten, publikowany na stronie podmiotowej BIP, będzie stanowić narzędzie umożliwiające aktualizację i doprecyzowanie niezbędnych wymagań. W konsekwencji podmiot krytyczny przy wdrażaniu odpowiednich rozwiązań organizacyjno-technicznych będzie zobowiązany do uwzględnienia zarówno przepisów aktu wykonawczego, jak i uzupełniającego wykazu, co pozwoli na większą elastyczność w kontekście dynamicznie zmieniającego się otoczenia regulacyjnego i technologicznego. Dobrym przykładem obrazującym zasadność tego rozwiązania są wymagania co do zewnętrznych systemów zabezpieczeń. Obecnie przyjęta przez PKN specyfikacja techniczna[28] funkcjonuje w języku angielskim, co uniemożliwia przywoływanie jej w aktach prawnych. Po przetłumaczeniu na język polski, czego można oczekiwać najwcześniej w 2026 r., łatwiej i zdecydowanie szybciej będzie

[28] PKN-CLC/TS 50661-1:2024-10 *Systemy alarmowe – Zewnętrzne perymetryczne systemy zabezpieczeń – Część 1: Wymagania systemowe*.

można ją uwzględnić w wymaganiach, które będą ponadto ukierunkowane na konkretny sektor lub podsektor.

Sukcesem jest wprowadzenie w projekcie ustawy zobowiązania dla podmiotów krytycznych (przełożonego 1 do 1 z obowiązków określanych dla operatorów IK) do żądania od usługodawców – przy opracowywaniu i zawieraniu umów zapewniających wdrażanie rozwiązań organizacyjno-technicznych – *certyfikatów, uwzględniając równoważne, zgodnie z zasadami wzajemnego uznawania w Unii Europejskiej lub w przypadku ich braku innych dokumentów właściwych dla poszczególnych rozwiązań, potwierdzających posiadanie odpowiednich kompetencji i uprawnień niezbędnych do ich realizacji*. W założeniach koncepcyjnych wykaz certyfikatów miał być ujęty w akcie wykonawczym, jednak w związku z ewolucją rozwiązań organizacyjno-technicznych i sposobów określania kompetencji niemożliwe jest opublikowanie wykazu satysfakcjonującego wszystkich interesariuszy. Uznano, że optymalnym rozwiązaniem będzie opracowywanie i publikowanie takiego zestawienia przez organy do spraw podmiotów krytycznych na podmiotowych stronach BIP. W tym przypadku organ do spraw podmiotów krytycznych jest zobligowany – przed publikacją wykazu – do zasięgnięcia opinii właściwej sektorowej rady do spraw kompetencji, o których mowa w art. 4c ust. 1 pkt 2 *Ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości*. Ten sam mechanizm jest zastosowany w przypadku operatorów IK. W obszarze bezpieczeństwa fizycznego, uwzględniającego systemy zabezpieczeń technicznych, funkcjonują różne możliwości potwierdzania kompetencji i kwalifikacji. Przykładem jest certyfikacja na zgodność z PN-EN 16763, która dotyczy m.in. projektowania, instalowania i konserwacji systemów zabezpieczeń technicznych. Norma ta, opublikowana w języku polskim, była omawiana na wielu konferencjach (w tym tych poświęconych IK, organizowanych przez RCB) i szkoleniach branżowych, a rynek (firmy zajmujące się zabezpieczeniami technicznymi) jest dostosowany do certyfikacji na zgodność z nią. Taki certyfikat mógłby być wskazany w planowanym pierwotnie akcie wykonawczym. Z kolei normy dotyczące prywatnych usług ochrony dla IK[29], dające możliwość certyfikacji, nie mogłyby być wykorzystane w rozporządzeniu jako dokumenty

[29] PN-EN 17483-1:2021-11 *Prywatne usługi ochrony – Zabezpieczenie infrastruktury krytycznej – Część 1: Wymagania ogólne*; PN-EN 17483-2:2024-03 *Prywatne usługi ochrony – Zabezpieczenie infrastruktury krytycznej – Część 2: Usługi ochrony portów lotniczych i lotnictwa*; PN-EN 17483-3:2024-03 *Prywatne usługi ochrony – Zabezpieczenie infrastruktury krytycznej – Część 3: Usługi ochrony morskiej i portowej*.

odniesienia dla oceny kompetencji usługodawców dostarczających usługi ochrony ze względu na brak ich polskiego tłumaczenia.

Wspomniane normy zyskują coraz większe zainteresowanie w UE i krajach członkowskich. Jak wynika z prezentacji Confederation of European Security Services przedłożonej grupie PROCIV CER, normy te powinny odgrywać fundamentalną rolę w przekładaniu zasad bezpieczeństwa wynikających z dyrektywy CER na konkretne wymagania operacyjne. Podkreślono w niej, że prywatne firmy świadczące usługi ochrony stanowią integralną część łańcucha bezpieczeństwa, a jego skuteczność zależy od jakości każdego ogniwa. W tym kontekście normy zostały wskazane jako kluczowe narzędzie do podnoszenia jakości ochrony podmiotów krytycznych oraz zwiększania ich odporności na zagrożenia. Wskazano również, że stosowanie tych norm stanowi rekomendowaną ścieżkę zapewnienia wysokich standardów w obszarze ochrony IK i jest wsparciem realizacji celów dyrektywy CER[30]. Należy zatem podkreślić, że polskie rozwiązania legislacyjne wyróżniają się pragmatyzmem i elastycznością. Umożliwiają sprawne wdrażanie norm jako narzędzia podnoszenia jakości usług. Mechanizm konsultacyjny, uwzględniający opinie sektorowych rad ds. kompetencji, stanowi istotne wsparcie dla organów do spraw podmiotów krytycznych. Rada sektorowa, jako ciało reprezentujące cały sektor (np. sektor ochrony i bezpieczeństwa mienia i osób), zbiera informacje od kluczowych interesariuszy, co pozwala na bieżąco identyfikować potrzeby oraz dostosowywać wymagania kompetencyjne do zmieniających się realiów rynkowych i regulacyjnych.

Dzięki temu mechanizmowi różne dokumenty normalizacyjne mogą zostać włączone do praktyki rynkowej przez publikację zestawień referencyjnych na stronach BIP. To rozwiązanie pozwala na uniknięcie barier formalnych, które mogłyby hamować realizację rozwiązań organizacyjno-technicznych przez kompetentnych usługodawców oraz utrudniać dostosowanie wymagań do ewoluujących wyzwań związanych z bezpieczeństwem. Jednocześnie obowiązek konsultacji z sektorową radą zapewnia, że zestawienia te odzwierciedlają rzeczywiste potrzeby rynku, z uwzględnieniem zarówno praktyki operacyjnej, jak i międzynarodowych trendów w zakresie standaryzacji. Sektorowe rady ds. kompetencji odgrywają rolę w kształtowaniu standardów kwalifikacyjnych i kompetencyjnych w poszczególnych obszarach gospodarki. Są to ciała doradcze, powołane na podstawie

[30] Confederation of European Security Services, *How standards drive quality and resilience in critical entities security*, 5.02.2025, EU Council PROCIV CER Working Party.

ustawy o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości, których zadaniem jest identyfikowanie luk kompetencyjnych, rekomendowanie rozwiązań w zakresie kształcenia oraz wspieranie procesów certyfikacji i walidacji umiejętności zawodowych. Ich szczególną wartością jest szeroka reprezentacja kluczowych interesariuszy – administracji publicznej, instytucji edukacyjnych, organizacji branżowych oraz przedsiębiorstw, co pozwala na efektywne dostosowanie kompetencji do rzeczywistych potrzeb rynkowych.

Przedstawione rozwiązania pokazują, że polska implementacja dyrektywy CER nie tylko realizuje jej cele, lecz także wyznacza nowoczesne rozwiązania legislacyjne, dzięki którym zastosowanie norm staje się rzeczywistym mechanizmem podnoszenia jakości usług świadczonych na rzecz podmiotów krytycznych.

Standaryzację zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej domyka obowiązek przeprowadzania przez podmioty krytyczne, co najmniej raz na 3 lata, audytu tego systemu na własny koszt. Audyt będzie obejmował zakresy:

1) zarządzanie bezpieczeństwem informacji;
2) zarządzanie ciągłością działania usługi kluczowej;
3) zapewnienie bezpieczeństwa fizycznego, w tym ochrony fizycznej budynków i terenów należących do podmiotu krytycznego oraz zabezpieczeń technicznych, uwzględniających kontrolę dostępu.

Audyt będzie mógł być prowadzony przez:

1) jednostkę certyfikującą właściwą dla danego zakresu,
2) co najmniej 2 audytorów, w tym jednego z ukończonym szkoleniem audytora wiodącego, posiadających certyfikaty określone w akcie wykonawczym i spełniających wymagania bezpieczeństwa osobowego i przemysłowego w zakresie dostępu do informacji niejawnych o klauzuli „poufne".

Generalnym założeniem audytu jest ocena zgodności teraz i w przeszłości; audyt może mieć cel prawno-normatywny i powinien realizować potrzeby biznesowe. Opiera się na 7 zasadach, wymienionych we właściwej normie[31]:

1) rzetelności, jako podstawie profesjonalizmu,
2) uczciwości przedstawiania wyników,
3) należytej staranności zawodowej,

[31] PN-EN ISO 19011:2018 *Wytyczne dotyczące audytowania systemów zarządzania*.

4) poufności,
5) niezależności,
6) podejściu opartym na dowodach,
7) podejściu opartym na ryzyku.

Pomysł, aby jednostki certyfikujące prowadziły audyty (które przecież nie muszą się kończyć certyfikatem, tylko raportem z audytu), pojawił się już wcześniej i został zaadaptowany z ustawy o krajowym systemie cyberbezpieczeństwa. Jednostki certyfikujące są bowiem instytucjami, których kompetencje, zasady i etyka działania są określone przepisami wynikającymi z europejskiego systemu oceny zgodności (opisany w kolejnym rozdziale). Alternatywą dla jednostki certyfikującej są audytorzy, którzy będą mieli odpowiednie kompetencje oraz dawali rękojmię zachowania tajemnicy, potwierdzoną stosownym poświadczeniem bezpieczeństwa.

Sposób weryfikacji uprawnień audytorów (w tym ich kompetencji) będzie dookreślony w akcie wykonawczym i uwzględni wykaz certyfikatów uprawniających do realizacji audytów, a także zakres wiedzy specjalistycznej i doświadczenie audytorów. W przypadku systemu zarządzania bezpieczeństwem informacji i systemu zarządzania ciągłością działania można spodziewać się przywołania certyfikatów audytora wiodącego w danym zakresie, zresztą bardzo popularnych na rynku. Można przypuszczać, że dla systemów zabezpieczeń technicznych z kolei będzie wymagany certyfikat audytora wiodącego w zakresie systemu zarządzania bezpieczeństwem informacji w specjalizacji systemów zabezpieczeń technicznych, dlatego że nie ma żadnej normy z dziedziny systemów zabezpieczeń, która umożliwiałaby certyfikację audytorów wiodących. Certyfikacja audytora wiodącego dla tej dziedziny czerpie z utrwalonej na rynku metodyki dotyczącej audytowania systemów zarządzania bezpieczeństwem informacji.

Audyty będą mogły być prowadzone przez audytorów wewnętrznych – pracowników podmiotu krytycznego, którzy nie podlegają obowiązkowi posiadania poświadczenia bezpieczeństwa, ale podmiot krytyczny może przeprowadzić ich sprawdzenie. Uwzględnia w nim zwłaszcza informacje pozyskane z rejestrów karnych (Krajowego Rejestru Karnego oraz analogicznych rejestrów w krajach UE). Zakres kompetencji jest jednolity dla audytorów będących pracownikami podmiotu krytycznego i zewnętrznych, zatem audytor wewnętrzny, aby prowadzić audyt wynikający z ustawy, musi mieć kompetencje audytora wiodącego.

Audyt może być zastąpiony przez certyfikację rozwiązań organizacyjno-technicznych przez uprawnioną jednostkę. W takim przypadku

posiadanie certyfikatu przez podmiot krytyczny w odpowiednim zakresie uznaje się za równoznaczne ze spełnieniem obowiązku audytowego.

Dyrektywa CER wyznacza również cele w zakresie kontroli i karania podmiotów krytycznych, które również zostały zrealizowane w polskiej propozycji. Podmioty krytyczne będą podlegać karom pieniężnym w przypadkach, gdy:

- nie przeprowadzają systematycznej oceny ryzyka,
- nie wdrażają rozwiązań organizacyjno-technicznych,
- nie prowadzą dokumentacji dotyczącej wdrożonych rozwiązań,
- nie wykonują zaleceń pokontrolnych,

i innych.

Inspiracje w zakresie audytowania i certyfikacji w implementacji dyrektywy CER. Obligatoryjna i dobrowolna ocena zgodności

Intencją krajów Wspólnoty Europejskiej było wypracowanie takiego modelu systemu oceny zgodności, który ujednolicałby wymagania dla wyrobów na obszarze wspólnego rynku europejskiego. Temu celowi przyświecała zasada wzajemnego uznawania, znana w literaturze jako Cassis de Dijon[32], zgodnie z którą towar wyprodukowany legalnie i wprowadzony do obrotu w jednym państwie UE powinien być dopuszczony na rynki pozostałych państw członkowskich[33]. Przy uwzględnieniu założeń dotyczących zniesienia barier w handlu, z jednoczesnym zapewnieniem bezpieczeństwa konsumentowi i użytkownikowi, producent wyrobu lub upoważniony przez niego przedstawiciel bądź importer tego wyrobu uczestniczy w systemie oceny zgodności w sposób zróżnicowany (obszar obowiązkowy lub dobrowolny), w zależności od rodzaju danego wyrobu. W uproszczeniu, cały zakres przepisów unijnych dotyczących oceny zgodności odnosi się przede wszystkim do bezpieczeństwa wyrobów i dopuszczania ich do obrotu. W unijnych przepisach wprowadzono ramy dla nadzoru rynku produktów, aby zapewnić, że produkty te spełniają wysokie wymagania w zakresie ochrony interesów publicznych, takich jak ogólne zdrowie

[32] Nazwa nawiązuje do orzeczenia Trybunału Europejskiego w sprawie wprowadzenia na niemiecki rynek likieru o tej nazwie.

[33] Judgment of the Court of 20 February 1979. – Rewe-Zentral AG v Bundesmonopolverwaltung für Branntwein. – Reference for a preliminary ruling: Hessisches Finanzgericht – Germany. – Measures heaving an effect equivalent to quantitative restrictions. – Case 120/78, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?isOldUri=true&uri=CELEX:61978CJ0120 [dostęp: 28.02.2025].

i bezpieczeństwo, zdrowie i bezpieczeństwo w miejscu pracy, ochrona konsumentów, ochrona środowiska i bezpieczeństwa publicznego[34]. Zdefiniowano ogólne ramy reguł i zasad w odniesieniu do akredytacji i nadzoru rynku:

1) „akredytacja" oznacza poświadczenie przez krajową jednostkę akredytującą, że jednostka oceniająca zgodność spełnia wymagania określone w normach zharmonizowanych oraz – w stosownych przypadkach – wszelkie dodatkowe wymagania, w tym wymagania określone w odpowiednich systemach sektorowych konieczne do realizacji określonych czynności związanych z oceną zgodności;
2) „krajowa jednostka akredytująca" oznacza jedyną autorytatywną jednostkę w państwie członkowskim, udzielającą akredytacji na podstawie upoważnienia udzielonego jej przez państwo;
3) „ocena zgodności" oznacza proces wykazujący, czy zostały spełnione określone wymagania odnoszące się do produktu, procesu, usługi, systemu, osoby lub jednostki;
4) „jednostka oceniająca zgodność" to jednostka, która wykonuje czynności z zakresu oceny zgodności, w tym wzorcowanie, badanie, certyfikację i inspekcję[35].

W polskim prawodawstwie system oceny zgodności jest uregulowany *Ustawą z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku*, która określa przede wszystkim zasady funkcjonowania systemu oceny zgodności w Polsce oraz zasady działania systemu kontroli wyrobów wprowadzanych do obrotu. Jej dwa główne cele to:

– eliminowanie zagrożeń dla życia lub zdrowia użytkowników i konsumentów stwarzanych przez wyroby, a także zagrożeń dla środowiska,

[34] *Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93*.

[35] Tamże. Zob. także: *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/515 z dnia 19 marca 2019 r. w sprawie wzajemnego uznawania towarów zgodnie z prawem wprowadzonych do obrotu w innym państwie członkowskim oraz uchylające rozporządzenie (WE) nr 764/2008*; *Decyzja Parlamentu Europejskiego i Rady nr 768/2008/WE z dnia 9 lipca 2008 r. w sprawie wspólnych ram dotyczących wprowadzania produktów do obrotu, uchylająca decyzję Rady 93/465/EWG*; *Dyrektywa 2001/95/WE Parlamentu Europejskiego i Rady z dnia 3 grudnia 2001 r. w sprawie ogólnego bezpieczeństwa produktów*.

– stworzenie warunków do rzetelnej oceny wyrobów poprzez ich badania, inspekcję i certyfikację przez kompetentne i niezależne podmioty.

Infrastrukturę systemu oceny zgodności tworzą jednostki notyfikowane, certyfikujące, przeprowadzające badania (laboratoria badawcze, wzorcujące), inspekcyjne oraz akredytujące. W Polsce krajową jednostką akredytującą jest Polskie Centrum Akredytacji.

Wspomniana ustawa, tak jak prawodawstwo europejskie, koncentruje się na obligatoryjnej ocenie zgodności, co jest widoczne już w samych definicjach przywołanych w ustawie, w której to np. certyfikat jest rozumiany jako (...) *dokument wydany przez jednostkę notyfikowaną, potwierdzający, że wyrób, projekt wyrobu lub proces jego wytwarzania są zgodne z wymaganiami* (art. 4 pkt 4). Jednostka notyfikowana to z kolei jednostka oceniająca zgodność (czyli, zgodnie z art. 4 pkt. 11, taka, o której mowa w art. 2 pkt 13 rozporządzenia (WE) nr 765/2008), funkcjonująca w obszarze regulowanym – zgodnie z art. 4 pkt 12. Jak piszą Anna Stankowska, Adam Muszyński i Sławomir Wilczyński[36]:

> (...) tam gdzie prawo określa wymagania w odniesieniu do przedmiotu regulacji, ocena zgodności jest obowiązkowa oraz określone są jednostki/organizacje oceniające zgodność, które z mocy prawa zajmują się taką oceną, jeśli przepis prawa tego wymaga. Biorąca udział w ocenie zgodności jednostka oceniająca zgodność (strona trzecia), wyznaczona w dyrektywie do współuczestniczenia w ocenie zgodności, musi być notyfikowana. Notyfikacja służy formalnemu wykazaniu kompetencji tej jednostki do wykonywania określonych zadań w zakresie oceny zgodności.

Wzorce z obligatoryjnego systemu oceny zgodności, wypracowane na poziomie UE i doprecyzowane w Polsce, były istotnym punktem odniesienia przy formułowaniu rozwiązań legislacyjnych dotyczących audytowania i certyfikacji rozwiązań organizacyjno-technicznych wdrażanych przez podmioty krytyczne. Należy podkreślić, że normy mające zastosowanie do tych rozwiązań nie podlegają obowiązkowej certyfikacji, ale można prowadzić ocenę zgodności z nimi na zasadach dobrowolności. Na potrzeby projektu ustawy przyjęto zatem następujące definicje. Jednostkę certyfikującą określono jako (...) *jednostkę oceniającą zgodność, akredytowaną*

[36] A. Stankowska, A. Muszyński, S. Wilczyński, *System oceny zgodności*, w: *Normalizacja*, T. Schweitzer (red.), Warszawa 2013, Polski Komitet Normalizacyjny, s. 169.

zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 1854) lub upoważnioną do certyfikacji zgodnie z przepisami ustawy z dnia 12 września 2002 r. o normalizacji (Dz. U. z 2015 r. poz. 1483), co nie tylko uwzględnia postanowienia rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 765/2008, lecz także daje możliwości działania jednostkom certyfikującym, które nie mają akredytacji. Akredytacja bowiem, co należy podkreślić, jest wymagana dla zakresów określonych we wspomnianym rozporządzeniu i ustawie o systemach zgodności i nadzoru rynku. Z kolei jednostki upoważnione do certyfikacji zgodnie przepisami ustawy o normalizacji nie działają w obszarze regulowanym, lecz dobrowolnym i mają możliwość posługiwania się jedynym w Polsce dobrowolnym znakiem certyfikacyjnym umocowanym prawnie, tj. znakiem PN[37].

Certyfikat opisano jako (...) *dokument wydany przez jednostkę certyfikującą potwierdzający, że wyrób, instalacja, system, proces, usługa lub osoba spełniają odpowiednie wymagania.* To bardzo ważna definicja, ponieważ stosowanie pojęcia certyfikatu ma często charakter potoczny i jest ono nadużywane. Powszechne są również przypadki – intencjonalne lub nie – kierowania zainteresowanych na definicję określoną w ustawie o systemach zgodności i nadzoru rynku, co – gdy nie zostanie uwzględniony kontekst – jest mylące i ma ogromny potencjał manipulacyjny i dezinformacyjny. Było to zauważalne zwłaszcza w branży systemów zabezpieczeń technicznych. Certyfikacja z kolei to (...) *działania jednostki certyfikującej, wykazujące, że wyrób, instalacja, system, proces, usługa lub osoba spełniają odpowiednie wymagania.*

W projekcie implementacji dyrektywy CER zaadaptowano istniejące w europejskim i polskim porządku prawnym mechanizmy akredytacji i upoważnienia jako narzędzi do walidacji kompetencji podmiotów zajmujących się oceną zgodności z normami dotyczącymi systemu zarządzania bezpieczeństwem informacji, systemu zarządzania ciągłością działania oraz systemów zabezpieczeń technicznych. Uwzględnienie tych mechanizmów pozwoliło na sprawne wpisanie systemu audytowania i certyfikacji w ugruntowane ramy prawne, już wcześniej regulujące zasady weryfikacji kompetencji jednostek oceniających zgodność.

[37] *Rozporządzenie Rady Ministrów z dnia 11 października 2010 r. w sprawie sposobu nadawania i wykorzystywania znaku zgodności z Polską Normą.*

Podstawowym celem było zapewnienie wysokiego poziomu rzetelności i wiarygodności procesu oceny zgodności, przy jednoczesnym uniknięciu wprowadzania nadmiernie skomplikowanych, nowatorskich mechanizmów prawnych, które mogłyby generować trudności interpretacyjne i wdrożeniowe. Akredytacja, jako uznana forma formalnego poświadczenia kompetencji jednostek certyfikujących, stanowi gwarancję niezależności, jakości, najwyższego poziomu merytorycznego, organizacyjnego oraz stosowania zasad etyki. Analogicznie jest z upoważnieniem wskazanym w art. 7 ust. 3 ustawy o normalizacji, które otwiera ścieżkę dla podmiotów chcących działać w obszarze certyfikacji na zasadach dobrowolnych. Rozwiązania te korespondują z rynkiem, zapewniają elastyczność systemu i umożliwiają jego sprawne funkcjonowanie. Istotnym elementem, który dopełnia powyższe wyjaśnienia, są funkcjonujące na rynku certyfikaty.

Podsumowanie

Rok 2025 będzie przełomowy dla państw członkowskich UE, które finalizują proces transpozycji dyrektywy CER do krajowych systemów prawnych. Polska, jako jedno z państw najbardziej zaangażowanych w ten proces, wyznacza wysokie standardy w zakresie ochrony IK. Proponowane rozwiązania legislacyjne, oparte na normalizacji, łączące standaryzację i ocenę zgodności, mogą stanowić wzorzec dla pozostałych krajów członkowskich, szczególnie w kontekście narastających zagrożeń antagonistycznych i hybrydowych – a te stanowią dziś jedno z największych wyzwań dla bezpieczeństwa IK. W raporcie dotyczącym sektora ochrony i bezpieczeństwa mienia i osób w Polsce Anna Araminowicz, Piotr Klatta, Tomasz Radochoński i Magda Sierżyńska piszą: *Na poziomie lokalnym udane sabotaże mogą obniżać potencjał gospodarczy, powodując straty osobowe i materialne, jak też stanowić zagrożenie dla życia i zdrowia mieszkańców oraz dla środowiska naturalnego (np. podpalenia wysypisk śmieci). Na poziomie krajowym każdy taki akt, z uwagi na nagłaśnianie go w mediach tradycyjnych i elektronicznych, może wywoływać niepokoje społeczne, panikę i wrażenie chaosu w państwie. Wszystkie te skutki są celami działań w konflikcie hybrydowym*[38].

[38] 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., s. 106.

Polska propozycja implementacji wyróżnia się kompleksowym podejściem do ochrony IK, ponieważ integruje system zarządzania bezpieczeństwem świadczenia usługi kluczowej, wymagania normatywne oraz mechanizmy audytowania i certyfikacji. Najważniejszą rolę odgrywa tu obowiązek weryfikacji kompetencji dostawców i usługodawców przez uznane systemy oceny zgodności, co pozwala na eliminację ryzyka związanego z niską jakością rozwiązań organizacyjno-technicznych.

Położenie geopolityczne i doświadczenia wynikające z bezpośredniego sąsiedztwa z regionem objętym konfliktem wojennym wzmacniają pozycję Polski jako państwa, które kształtuje politykę bezpieczeństwa IK na poziomie europejskim. Przyjęte rozwiązania mogą stać się fundamentem przyszłych inicjatyw wzmacniających odporność strategicznych sektorów gospodarki w UE.

Bibliografia

Araminowicz A., Klatta P., Radochoński T., Sierżyńska M., *Ochrona i Bezpieczeństwo Mienia i Osób – analiza sektora. Raport z badania*, Kraków 2024, MABEA sp. z o.o.

A World Built on Standards: A Textbook for Higher Education, S.A. Bøgh (red.), Nordhavn 2015, Danish Standards Foundation.

Confederation of European Security Services, *How standards drive quality and resilience in critical entities security*, 5.02.2025, EU Council PROCIV CER Working Party.

Idzikowska T., Banaszek K., *Rola i znaczenie normalizacji w bezpieczeństwie transportu*, „Logistyka" 2010, t. 4.

Łunarski J., *Normalizacja i standaryzacja*, Rzeszów 2014, Oficyna Wydawnicza Politechniki Rzeszowskiej.

Schweitzer T., Zielińska E., *Działalność normalizacyjna*, w: *Normalizacja*, T. Schweitzer (red.), Warszawa 2013, Polski Komitet Normalizacyjny.

Stankowska A., Muszyński A., Wilczyński S., *System oceny zgodności*, w: *Normalizacja*, T. Schweitzer (red.), Warszawa 2013, Polski Komitet Normalizacyjny.

Szewczyk T., Pyznar M., *Ochrona infrastruktury krytycznej a zagrożenia asymetryczne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2010, nr 2, s. 53–59.

Tatarowski A., *Budowanie odporności infrastruktury krytycznej w świetle zagrożeń asymetrycznych i terroryzmu. Tendencje legislacyjne w polskiej implementacji dyrektywy CER ze szczególnym uwzględnieniem aspektów standaryzacji i certyfikacji rozwiązań organizacyjno-technicznych,* „Terroryzm – studia, analizy, prewencja" 2024, nr 5, s. 175–194. https://doi.org/10.4467/27204383TER.24.006.19394.

Wiśniewski M., Szwarc K., Skomra W., *Continuity of Essential Services as an Emerging Challenge for Societal Resilience,* „IEEE Access" 2023, t. 11, s. 44614–44635. https://doi.org/10.1109/ACCESS.2023.3271751.

Źródła internetowe

Bennett M., Gupta V., *Dealing in Security Understanding Vital Services and How They Keep You Safe,* http://resiliencemaps.org/files/Dealing_in_Security.July2010.en.pdf [dostęp: 22.06.2022].

Dobrowolność stosowania norm, Polski Komitet Normalizacyjny, https://wiedza.pkn.pl/web/wiedza-normalizacyjna/stanowisko-pkn-w-sprawie-dobrowolnosci-pn [dostęp: 28.02.2025].

Narodowy Program Ochrony Infrastruktury Krytycznej, Rządowe Centrum Bezpieczeństwa, 2023.

National Critical Functions Set, CISA, https://www.cisa.gov/national-critical-functions-set [dostęp: 24.06.2022].

Prezydencja w Radzie UE, Rada Europejska, Rada Unii Europejskiej, https://www.consilium.europa.eu/pl/council-eu/presidency-council-eu/ [dostęp: 28.02.2025].

Akty prawne

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/515 z dnia 19 marca 2019 r. w sprawie wzajemnego uznawania towarów zgodnie z prawem wprowadzonych do obrotu w innym państwie członkowskim oraz uchylające rozporządzenie (WE) nr 764/2008 (Dz. Urz. UE L 91/1 z 29.03.2019).

Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93 (Dz. Urz. UE L 218/30 z 13.08.2008).

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 27.12.2022).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) – (Dz. Urz. UE L 333/80 z 27.12.2022).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194/1 z 19.07.2016).

Dyrektywa Rady 2008/114/WE z 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (Dz. Urz. UE L 345/75 z 23.12.2008).

Dyrektywa 2001/95/WE Parlamentu Europejskiego i Rady z dnia 3 grudnia 2001 r. w sprawie ogólnego bezpieczeństwa produktów (Dz. Urz. UE L 11/4 z 3.12.2002).

Council Resolution of 7 May 1985 on a new approach to technical harmonization and standards (Dz. Urz. UE C 136/1 z 4.06.1985).

Decyzja Parlamentu Europejskiego i Rady nr 768/2008/WE z dnia 9 lipca 2008 r. w sprawie wspólnych ram dotyczących wprowadzania produktów do obrotu, uchylająca decyzję Rady 93/465/EWG (Dz. Urz. UE L 218/82 z 13.08.2008).

Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (DzU z 2024 poz. 1907).

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

Ustawa z dnia 11 września 2019 r. – Prawo zamówień publicznych (t.j. DzU z 2024 poz. 1320).

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. DzU z 2024 poz. 1077, ze zm.).

Ustawa z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (t.j. DzU z 2022 poz. 1854, ze zm.).

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. DzU z 2024 poz. 632, ze zm.).

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. DzU z 2023 poz. 122, ze zm.).

Ustawa z dnia 12 września 2002 r. o normalizacji (t.j. DzU z 2015 poz. 1483).

Ustawa z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (t.j. DzU z 2025 poz. 98).

Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (t.j. DzU z 2021 poz. 1995, ze zm.).

Ustawa z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej (t.j. DzU z 2024 poz. 1125).

Rozporządzenie Rady Ministrów z dnia 11 października 2010 r. w sprawie sposobu nadawania i wykorzystywania znaku zgodności z Polską Normą (DzU z 2010 nr 198 poz. 1316).

Rozporządzenie Rady Ministrów z dnia 24 czerwca 2003 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony (DzU z 2003 nr 116 poz. 1090).

Presidential Decision Directive/Nsc-63, The White House, 22.05.1998, https://irp.fas.org/offdocs/pdd/pdd-63.htm [dostęp: 5.03.2025].

Tatarowski A., *Standaryzacja i certyfikacja rozwiązań wynikających z Dyrektywy CER*, X Krajowe Forum Ochrony Infrastruktury Krytycznej, Warszawa 2023, https://www.gov.pl/web/rcb/x-krajowe-forum-ochrony-infrastruktury-krytycznej-za-nami [dostęp: 28.02.2025].

Orzecznictwo

Judgment of the Court of 20 February 1979. – Rewe-Zentral AG v Bundesmonopolverwaltung für Branntwein. – Reference for a preliminary ruling: Hessisches Finanzgericht – Germany. – Measures heaving an effect equivalent to quantitative restrictions. – Case 120/78, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?isOldUri=true&uri=CELEX:61978CJ0120 [dostęp: 28.02.2025].

Inne dokumenty

ISO/TS 31050 *Risk management – Guidelines for managing an emerging risk to enhance resilience*.

PKN-CLC/TS 50661-1:2024-10 *Systemy alarmowe – Zewnętrzne perymetryczne systemy zabezpieczeń – Część 1: Wymagania systemowe*.

PKN-ISO Guide 73:2012 *Zarządzanie ryzykiem – Terminologia*.

PN-EN 16763 *Usługi w zakresie systemów ochrony przeciwpożarowej i systemów zabezpieczeń technicznych*.

PN-EN 17483-1:2021-11 *Prywatne usługi ochrony – Zabezpieczenie infrastruktury krytycznej – Część 1: Wymagania ogólne*.

PN-EN 17483-2:2024-03 *Prywatne usługi ochrony – Zabezpieczenie infrastruktury krytycznej – Część 2: Usługi ochrony portów lotniczych i lotnictwa.*

PN-EN 17483-3:2024-03 *Prywatne usługi ochrony – Zabezpieczenie infrastruktury krytycznej – Część 3: Usługi ochrony morskiej i portowej*.

PN-EN 45020:2009 *Normalizacja i dziedziny związane. Terminologia ogólna*.

PN-EN 50131-1 *Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Część 1: Wymagania systemowe*.

PN-EN 60839-11-1 *Systemy alarmowe i elektroniczne systemy zabezpieczeń – Część 11-1: Elektroniczne systemy kontroli dostępu – Wymagania dotyczące systemów i komponentów*.

PN-EN 62676-1-1 *Systemy dozoru wizyjnego stosowane w zabezpieczeniach – Część 1-1: Wymagania systemowe – Postanowienia ogólne*.

PN-EN IEC 31010:2020-01 *Zarządzanie ryzykiem – Techniki oceny ryzyka*.

PN-EN ISO 19011:2018 *Wytyczne dotyczące audytowania systemów zarządzania*.

PN-EN ISO 22301 *Bezpieczeństwo i odporność. Systemy zarządzania ciągłością działania. Wymagania*.

PN-EN ISO/IEC 27001 *Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności. Systemy zarządzania bezpieczeństwem informacji. Wymagania*.

PN-EN ISO/IEC 27005:2025-01 *Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Wytyczne do zarządzania ryzykami w bezpieczeństwie informacji*.

PN-ISO 31000:2012 *Zarządzanie ryzykiem – Zasady i wytyczne*.

PN-ISO 31000:2018-08 *Zarządzanie ryzykiem – Wytyczne*.

PN-ISO/IEC 27005:2014-01 *Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji*.

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: 6.04.2025].

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, wydanie specjalne: 333–358

https://doi.org/10.4467/27204383TER.25.012.21515

Materiał ekspercki

Wartość unijnych projektów badawczych w ochronie infrastruktury krytycznej

The value of EU research projects in critical infrastructure protection

Małgorzata Wolbach
Polska Platforma Bezpieczeństwa Wewnętrznego
https://orcid.org/0009-0005-1837-0389

Rashel Talukder
Polska Platforma Bezpieczeństwa Wewnętrznego
https://orcid.org/0000-0003-4743-9355

Ochrona infrastruktury krytycznej (IK) i zapewnianie jej ciągłej odporności, zwłaszcza na zagrożenia hybrydowe, mają fundamentalne znaczenie dla stabilnego funkcjonowania współczesnych społeczeństw. Nieograniczony dostęp do energii, wody, żywności, opieki zdrowotnej i transportu stanowi podstawę bezpiecznego życia.

Instytucje Unii Europejskiej w ostatnich latach położyły nacisk na wzmocnienie ochrony i odporności IK. Wpływ na to miała trwająca wojna w Ukrainie, która spotęgowała obawy o bezpieczeństwo IK w całej Europie.

Do kluczowych obszarów działań UE należą:

- wprowadzenie dyrektywy CER[1] (*The Critical Entities Resilience Directive*) w sprawie odporności podmiotów krytycznych;

[1] *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.*

- wprowadzenie dyrektywy NIS 2[2] (*Network and Information Systems Directive 2*) w sprawie bezpieczeństwa sieci i informacji;
- ustalenie planu UE dotyczącego IK (zalecenia przyjęte przez Radę UE m.in. koordynują reakcje na zakłócenia funkcjonowania IK mające istotne znaczenie transgraniczne)[3];
- współpraca z NATO[4];
- wymiana informacji i dobrych praktyk m.in. przy zaangażowaniu Grupy ds. Odporności Podmiotów Krytycznych (ang. Critical Entities Resilience Group, CERG), która ułatwia współpracę i wymianę informacji między państwami członkowskimi w celu zapewnienia skutecznego wdrożenia dyrektywy CER[5].

Ponadto UE zapewnia znaczne wsparcie finansowe i strategiczne dla badań i innowacji w ochronie IK za pośrednictwem różnych programów finansowania. Pomagają one w rozwoju nowych technologii i wprowadzaniu rozwiązań w celu przeciwdziałania pojawiającym się zagrożeniom i poprawy odporności infrastruktury[6]. Unia Europejska ustanowiła kilka takich programów. Dzięki temu nie tylko wzmacnia ona ochronę swojej IK, lecz także promuje wzrost gospodarczy i zrównoważony rozwój. Jak podkreślono w rocznym sprawozdaniu z postępów we wdrażaniu wspólnych rozwiązań dotyczących przeciwdziałania zagrożeniom hybrydowym[7], finansowane przez UE projekty badawcze w zakresie bezpieczeństwa

[2] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148*.

[3] *Zalecenie Rady z dnia 25 czerwca 2024 r. w sprawie planu skoordynowanego reagowania na szczeblu Unii na zakłócenia w funkcjonowaniu infrastruktury krytycznej mające istotne znaczenie transgraniczne*.

[4] *NATO and European Union release final assessment report on resilience of critical infrastructure*, NATO, 29.06.2023, https://www.nato.int/cps/en/natohq/news_216631.htm [dostęp: 6.01.2025].

[5] *Critical infrastructure resilience at EU-level*, European Commission, 23.09.2024, https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en [dostęp: 6.01.2025].

[6] Tamże.

[7] *Joint Staff Working Document. Eighth progress report on the implementation of the 2016 Joint framework on countering hybrid threats and the 2018 Joint communication on increasing resilience and bolstering capabilities to address hybrid threats*, https://defence-industry-space.ec.europa.eu/system/files/2025-01/SWD_Annual-Progress-Report-2024.PDF [dostęp: 2.01.2025].

odgrywają kluczową rolę w identyfikowaniu istniejących luk oraz zwiększaniu bezpieczeństwa i odporności IK w całej UE.

W artykule przedstawiono wybrane projekty finansowane przez UE w ramach programów Horyzont 2020 i Horyzont Europa, takie jak: EU-HYBNET, EU-CIP, VIGIMARE, TESTUDO, NBSINFRA, ENDURANCE i TRANSCEND. Ponadto omówiono wyzwania związane z realizacją tych projektów, w tym niespójności regulacji (odmienne krajowe regulacje prawne i niespójne interpretacje dyrektyw UE), ograniczenia finansowe i potrzebę współpracy transgranicznej. Przedstawiono zalecenia dotyczące przyszłych kierunków badań oraz podkreślono znaczenie cyberbezpieczeństwa, technologii kwantowej i wymiany w czasie rzeczywistym informacji o zagrożeniach w zwiększeniu zdolności UE do reagowania na zmieniające się zagrożenia bezpieczeństwa.

Finansowanie badań i innowacji w ochronie infrastruktury krytycznej na przykładzie programu Horyzont Europa

Jednym z unijnych programów finansowania, który wyróżnia się istotnym wkładem w badania i rozwój (mającymi na celu wzmocnienie odporności IK), jest Horyzont Europa. To flagowy program UE na lata 2021–2027 poświęcony badaniom naukowym i innowacjom, z przewidzianym budżetem w wysokości 93,5 mld euro. Wspieranie postępów w nauce i technologii staje się coraz pilniejsze, zwłaszcza w kontekście rosnącej niestabilności geopolitycznej. Wydarzenia takie jak pełnoskalowa inwazja Rosji na Ukrainę uwypukliły zagrożenia bezpieczeństwa, demokracji i globalnych łańcuchów dostaw, co uczyniło cele programu w drugiej połowie jego realizacji jeszcze bardziej istotnymi. Program Horyzont Europa wspiera międzynarodową współpracę i zwiększa wpływ badań naukowych i innowacji na kształtowanie polityki UE. Jednocześnie odgrywa ważną rolę w podejmowaniu działań związanych z pilnymi globalnymi wyzwaniami. Zapewnia zróżnicowany zestaw instrumentów – od badań podstawowych, przez przełomowe innowacje, do opracowywania i wdrażania najnowocześniejszych rozwiązań – dla rozwiązań opartych na badaniach naukowych[8].

[8] *Horizon Europe*, https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en [dostęp: 7.01.2025].

Plan strategiczny programu Horyzont Europa na lata 2025–2027[9] wyszczególnia najważniejsze cele strategiczne, działania priorytetowe i obszary tematyczne na ostatnich etapach jego realizacji. Ma na celu dostosowanie końcowej fazy tego programu do pojawiających się wyzwań, ewoluujących polityk UE i zmieniających się potrzeb państw członkowskich. Jest to jak dotąd najbardziej ambitny program UE w zakresie badań naukowych i innowacji, ponieważ odpowiada na globalne uwarunkowania, wspiera przełomowe rozwiązania i ułatwia dostęp do funduszy różnym grupom badawczym i firmom nie tylko z UE, a także ma rekordowy budżet. Plan ten łączy nadrzędne cele polityki UE z działaniami badawczo-rozwojowymi prowadzonymi w ramach programu Horyzont Europa. Oferuje stabilność planowania, która wykracza poza standardowy dwuletni cykl programu prac. Zapewnia społeczności badawczej przewidywalność, przy jednoczesnym zachowaniu elastyczności w celu sprostania nieoczekiwanym zmianom i wyzwaniom[10].

Projekty finansowane w ramach programu Horyzont Europa służą pozyskiwaniu nowej wiedzy, technologii i rozwiązań, spełniających określone wymagania. Są to projekty, w ramach których do współpracy są angażowani użytkownicy końcowi, naukowcy i partnerzy przemysłowi. Ten inkluzywny model zapewnia, że wyniki badań i innowacji są ściśle dostosowane do praktycznych potrzeb tych, którzy ostatecznie je wdrożą, dzięki czemu zwiększa się użyteczność projektów.

Projekty te odgrywają kluczową rolę w działaniach służących rozwiązywaniu aktualnych globalnych problemów, w tym w zwiększaniu odporności IK[11]. Wojna w Ukrainie podkreśliła znaczenie badań i innowacji w takich kwestiach, jak: dostarczanie czystej energii, zrównoważonej żywności, leków, zapewnianie zdolności obronnych i bezpieczeństwa społeczno-gospodarczego. Wysiłki te są niezbędne nie tylko do minimalizowania bezpośrednich zagrożeń, lecz także do zapewnienia długoterminowej odporności i stabilności. Projekty realizowane w ramach programu Horyzont Europa już teraz

[9] *Horizon Europe. Strategic Plan 2025–2027*, European Commission, 2024, https://op.europa.eu/en/web/eu-law-and-publications/publication-detail/-/publication/6abcc8e7-e685-11ee-8b2b-01aa75ed71a1 [dostęp: 7.01.2025].

[10] *Strategic plan*, https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/strategic-plan_en [dostęp: 3.01.2025].

[11] *Horizon Europe. Strategic Plan 2025–2027. Analysis*, European Commission, 2023, https://op.europa.eu/en/publication-detail/-/publication/b3baec75-fdd0-11ed-a05c-01aa75ed71a1/language-en [dostęp: 9.01.2025].

przyczyniają się do pokonywania szybko zmieniających się wyzwań związanych z IK o znaczeniu transgranicznym. W przyszłości będzie to wymagało jeszcze większej innowacyjności i bardziej skoordynowanych wysiłków.

Odporność IK, w tym energetycznej, transportowej i telekomunikacyjnej, jest priorytetem dla UE, szczególnie w obliczu istnienia zagrożeń hybrydowych. Podejmowane działania, np. wdrożenie dyrektywy CER, mają na celu zapewnienie zarówno fizycznej, jak i cybernetycznej odporności IK. Badania nad bezpieczeństwem prowadzone w ramach programu Horyzont Europa wspierają te wysiłki, zapewniają nowatorskie metody planowania scenariuszy służących jako środowisko testowe dla rozwiązań powstających w ramach projektów, testów w warunkach skrajnych (ang. *stress-test*) i minimalizowania zagrożeń. Rada UE zachęciła państwa członkowskie do pełnego wykorzystania wyników badań naukowych i innowacji finansowanych przez UE. Podkreśliła tym samym ich znaczenie dla zwiększenia odporności infrastruktury. W tym kontekście projekty badawczo-rozwojowe stanowią ważny pomost między polityką a praktyką, umożliwiają UE i jej państwom członkowskim skuteczne reagowanie na wyzwania. Przez współpracę, wspieranie innowacji i odporności na zagrożenia projekty te są integralną częścią ochrony infrastruktury, bezpieczeństwa i konkurencyjności UE w coraz bardziej złożonym świecie[12].

Program Horyzont Europa wspiera badania naukowe i innowacje za pomocą programów prac, które określają możliwości finansowania różnych działań. Struktura programu opiera się na 3 zasadniczych filarach. Filar II – Globalne wyzwania i europejska konkurencyjność przemysłowa jest podzielony na 6 klastrów działań badawczo-rozwojowych. Klastry zostały zaprojektowane tak, aby zwiększyć integralność i komplementarność między obszarami tematycznymi, przy jednoczesnym zapewnieniu, że UE osiągnie znaczący i trwały wpływ na wyzwania zidentyfikowane w poszczególnych klastrach programu Horyzont Europa w stosunku do zainwestowanych środków.

Klaster 3 – Bezpieczeństwo cywilne na rzecz społeczeństwa dotyczy zwiększania bezpieczeństwa przez wspieranie wysiłków na rzecz zapobiegania zagrożeniom bezpieczeństwa: wewnętrznego, indywidualnego i społeczeństwa jako całości oraz budowania odporności na nie[13]. Obejmuje również walkę z ewoluującymi zagrożeniami, w tym terroryzmem, korupcją, przestępczością zorganizowaną i atakami hybrydowymi na IK. Celem

[12] Tamże.

[13] *Horizon Europe. Strategic Plan 2025–2027*, European Commission, 2024...

Klastra 3 jest zwiększenie zrozumienia tych zagrożeń i ich społecznych uwarunkowań oraz opracowanie zaawansowanych narzędzi do zapobiegania im, wykrywania ich i badania, a także zwiększenie zdolności UE w zakresie bezpieczeństwa. Działania dotyczące badań i innowacji są skoncentrowane również na zapewnieniu odporności IK, takiej jak systemy energetyczne, wodne, zaopatrzenia w żywność i opieki zdrowotnej, na ataki fizyczne lub cybernetyczne. Na Klaster 3 przeznaczono budżet w wysokości 1,596 mld euro.

Klaster 3 jest podzielony na 6 głównych celów, z których każdy koncentruje się na określonych priorytetach w ramach nadrzędnego tematu bezpieczeństwa cywilnego. Cel 3 – Odporna infrastruktura – jest poświęcony zwiększaniu odporności i autonomii infrastruktury zarówno krytycznej, jak i cyfrowej. Oczekiwane rezultaty opisano w następujący sposób: *Odporność i autonomia infrastruktury fizycznej i cyfrowej są zwiększone, a kluczowe funkcje społeczne są zapewnione dzięki skuteczniejszemu zapobieganiu, gotowości i reagowaniu, głębszemu zrozumieniu powiązanych aspektów ludzkich, społecznych i technologicznych oraz rozwojowi najnowocześniejszych możliwości dla operatorów infrastruktury*[14].

Cel ten jest ściśle powiązany z Celem 6 – Wzmocnione badania i innowacje w zakresie bezpieczeństwa – który zapewnia badania, postęp technologiczny i nowatorskie rozwiązania, stanowiące podstawę i wsparcie Celu 3. Razem tworzą one uzupełniające się ramy dla realizacji priorytetów bezpieczeństwa UE, zwiększają ochronę IK przy jednoczesnym wzmacnianiu odporności społecznej i gospodarczej. Mają one praktyczne zastosowania w związku z wyposażaniem operatorów infrastruktury w zaawansowane narzędzia i możliwości skutecznego reagowania na wyzwania.

Przykładem realizacji założeń Celu 3 było zaproszenie do składania wniosków w ramach programu Odporna infrastruktura (HORIZON-CL3-2024) o finansowanie w 2024 r.[15] badań naukowych i innowacji mających na celu wzmocnienie odporności infrastruktury. Tematy finansowane w ramach HORIZON-CL3-2024 to:

- **INFRA01**: *Lepsza gotowość i reagowanie na zakłócenia na dużą skalę w europejskiej infrastrukturze*;

[14] *Horizon Europe. Work Programme 2023-2025. 6. Civil Security for Society (European Commission Decision C(2024) 2371 of 17 April 2024)*, https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2023-2024/wp-6-civil-security-for-society_horizon-2023-2024_en.pdf, s. 8 [dostęp: 10.01.2025]. Tłumaczenia w artykule pochodzą od redakcji (dop. red.).

[15] Tamże.

• **INFRA02:** *Odporne i bezpieczne obszary miejskie i inteligentne miasta*.

Szczegóły dotyczące tych tematów, w tym rodzaj działań i oczekiwane wyniki, podsumowano w tabeli 1.

Tabela 1. Podtematy programu Odporna infrastruktura (HORIZON-CL3-2024).

Podtemat INFRA01	**HORIZON-CL3-2024-INFRA-01-01: Temat otwarty**
Rodzaj działania	Działania w zakresie innowacji
Oczekiwane wyniki	Oczekuje się, że wyniki projektów przyczynią się do osiągnięcia wszystkich poniższych rezultatów: • zwiększona odporność operatorów IK na zagrożenia naturalne i spowodowane przez człowieka; • ulepszone techniki monitorowania, oceny ryzyka, jego prognozowania, ograniczania i modelowania mające na celu zwiększenie odporności IK, walidację scenariuszy obejmujących wiele zagrożeń, tworzenie interaktywnych map zagrożeń na podstawie obserwacji Ziemi i innych źródeł danych
Podtemat INFRA02	**HORIZON-CL3-2024-INFRA-01-02: Odporne i bezpieczne planowanie urbanistyczne oraz nowe narzędzia dla jednostek terytorialnych UE**
Rodzaj działania	Działania w zakresie innowacji
Oczekiwane wyniki	Oczekuje się, że wyniki projektów przyczynią się do osiągnięcia wszystkich poniższych rezultatów: • ocena odporności środowiska miejskiego i podmiejskiego, identyfikacja słabych punktów i zalecenia dotyczące zmian w procesach organizacyjnych; • tworzenie nowych narzędzi i efektywnych kosztowo ulepszeń bezpieczeństwa infrastruktury miejskiej z możliwością łączenia i współdzielenia złożonych systemów bezpieczeństwa, z uwzględnieniem ograniczonych budżetów władz lokalnych; • większa skuteczność sił bezpieczeństwa i służb ratunkowych (policji, straży pożarnej, ratowników medycznych itp.) z korzyścią dla obywateli i mieszkańców Europy; • promowanie najlepszych praktyk, stworzenie unijnego narzędzia/rozwiązania wspierającego podejmowanie decyzji oraz rozpowszechnianie skutecznych narzędzi i możliwości wśród podmiotów na różnych terytoriach UE, niezależnie od ich wielkości i lokalizacji

Podtemat INFRA02	**HORIZON-CL3-2024-INFRA-01-03: Zaawansowana analiza danych w czasie rzeczywistym wykorzystywana do zapewnienia odporności infrastruktury**
Rodzaj działania	Działania w zakresie badań i innowacji
Oczekiwane wyniki	Oczekuje się, że wyniki projektów przyczynią się do osiągnięcia wszystkich poniższych rezultatów: • ulepszone możliwości identyfikacji ryzyka i zdarzeń awaryjnych w sieciach infrastruktury i inteligentnych miastach przez analizę w czasie rzeczywistym (w tym dużych zbiorów danych) przez podmioty publiczne i prywatne za pośrednictwem zabezpieczonych i zaufanych platform oraz wzajemnie połączonych systemów, w których współpraca opiera się na jasnych ramach prawnych i politycznych; • narzędzia i procesy ułatwiające interesariuszom identyfikację, analizę, ocenę i ciągłe monitorowanie ryzyka oraz zwiększanie zdolności adaptacyjnych do nieoczekiwanych zdarzeń z wyprzedzeniem przez umożliwienie analizy różnych źródeł danych (np. audio, wideo, mediów społecznościowych, treści internetowych, informacji przestrzennych, danych generowanych przez czujniki lub maszyny); • szybka i ciągła identyfikacja, klasyfikacja i śledzenie w czasie rzeczywistym niebezpiecznych czynników, zanieczyszczeń lub anomalii w sieciach infrastruktury i łańcuchach dostaw; • interoperacyjne interfejsy i lepsza współpraca między systemami wykrywania i reagowania na operacje infrastrukturalne, krajowymi/unijnymi centrami zarządzania ryzykiem/koordynacji i sprzętem pierwszej pomocy w celu umożliwienia zdalnych operacji na miejscu zdarzenia z uwzględnieniem wiedzy obywateli; • zwiększona cyberodporność przemysłowych sieci xG i danych w chmurze obejmujących określone domeny infrastruktury; • ulepszona zdolność do mapowania w czasie rzeczywistym źródeł ryzyka, które mogłyby zagrozić infrastrukturze sieciowej wspieranej przez obserwację Ziemi i dane geolokalizacyjne. Jeśli analiza obejmuje przetwarzanie danych osobowych, należy rozważyć uwzględnienie oceny związanego z nim ryzyka lub wpływu na prywatność osób fizycznych i społeczeństwa.

Źródło: *Horizon Europe. Work Programme 2023–2025. 6. Civil Security for Society (European Commission Decision C(2024) 2371 of 17 April 2024)*, https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2023-2024/wp-6-civil-security-for-society_horizon-2023-2024_en.pdf, s. 91–97 [dostęp: 10.01.2025].

Na program Odporna infrastruktura przydzielono w 2024 r. orientacyjny budżet w wysokości 16 mln euro[16]. Termin składania wniosków upłynął 20 listopada 2024 r. Z 79 wniosków, które złożono, tylko 3 zostaną rozpatrzone pozytywnie, a ich realizacja rozpocznie się we wrześniu 2025 r. To pokazuje nie tylko konkurencyjność konkursu, lecz także ograniczenie ogólnego budżetu przeznaczonego na badania i innowacje w dziedzinie ochrony IK.

Przegląd wybranych inicjatyw w zakresie badań naukowych i innowacji finansowanych w ramach programów Horyzont 2020 i Horyzont Europa

W ramach inicjatyw finansowanych przez UE w dziedzinie ochrony IK są rozwijane zarówno rozwiązania technologiczne, jak i nietechnologiczne. Inicjatywy te wzmacniają jednocześnie współpracę europejską. Celem przedstawienia wybranych przez autorów inicjatyw jest pokazanie możliwości, jakie projekty oferują interesariuszom, w tym instytucjom badawczym napędzającym innowacje, przedsiębiorstwom opracowującym najnowocześniejsze rozwiązania w zakresie bezpieczeństwa, organizacjom publicznym wdrażającym polityki oraz właścicielom i operatorom IK odpowiedzialnym za zapewnienie ciągłości usług.

EU-HYBNET

(Empowering a Pan-European Network to Counter Hybrid Threats, pol. Wzmocnienie Ogólnoeuropejskiej Sieci Przeciwdziałania Zagrożeniom Hybrydowym)[17]

Projekt finansowany z unijnego programu badań i innowacji Horyzont 2020 (poprzednika programu Horyzont Europa). Jest to pierwsza inicjatywa UE, która łączy praktyków bezpieczeństwa, naukowców, podmioty branżowe oraz organizacje biznesowe i pozarządowe w celu współpracy oraz identyfikacji i analizy wspólnych wyzwań i wymagań w zakresie przeciwdziałania zagrożeniom hybrydowym.

[16] *Resilient Infrastructures*, https://rea.ec.europa.eu/funding-and-grants/horizon-europe-cluster-3-civil-security-society/resilient-infrastructures_en [dostęp: 10.01.2025].

[17] *Empowering a Pan-European Network to Counter Hybrid Threats*, European Commission, https://cordis.europa.eu/project/id/883054 [dostęp: 13.01.2025].

Głównymi celami projektu EU-HYBNET są:

1. Stworzenie i rozwój sieci europejskich organizacji przeciwdziałających zagrożeniom hybrydowym oraz zapewnienie długoterminowej stabilności sieci.
2. Określenie wspólnych wymagań w celu wypełnienia luk w wiedzy, zaspokojenia potrzeb w zakresie wydajności i zwiększenia możliwości badań, innowacji i szkoleń dotyczących zagrożeń hybrydowych.
3. Monitorowanie rozwoju działalności badawczej i innowacyjnej w odniesieniu do zagrożeń hybrydowych.
4. Określenie priorytetów w zakresie wdrażania innowacji i uprzemysłowienia oraz w celu zwiększenia roli europejskiej sieci w skutecznym przeciwdziałaniu zagrożeniom hybrydowym.
5. Ustanowienie warunków dla zwiększonej interakcji między praktykami bezpieczeństwa, przedstawicielami sektora przemysłu i środowiskiem akademickim w celu wspierania rzeczowego dialogu i zwiększenia liczby członków sieci.
6. Wspieranie budowania potencjału i wymiany wiedzy na temat przeciwdziałania zagrożeniom hybrydowym.
7. Stworzenie podstaw do skutecznego współdziałania istniejących europejskich, krajowych i regionalnych sieci praktyków i innych podmiotów przeciwdziałających zagrożeniom hybrydowym.

Projekt obejmuje 4 podstawowe tematy, aby zapewnić spójność jego wyników i ułatwić skupienie się na wszystkich domenach zagrożeń hybrydowych (w tym IK). Są to:

1. Przyszłe trendy zagrożeń hybrydowych.
2. Cyberbezpieczeństwo i technologie przyszłości.
3. Odporna ludność cywilna, administracja lokalna i krajowa.
4. Informacja i komunikacja strategiczna.

W ramach tych tematów szczególny nacisk kładzie się na interfejsy między domenami, zidentyfikowane i zdefiniowane przez Komisję Europejską i Połączone Centrum Badawcze UE (ang. EU Joint Research Centre). Zapewnia to niezbędne wsparcie dla działań badawczych i innowacyjnych w domenach zagrożeń hybrydowych uznanych za kluczowe dla dostarczania rozwiązań w trakcie cykli projektowych.

Pomimo tego, że projekt skończył się w kwietniu 2025 r., sieć stale się rozrasta (obecnie składa się z ponad 150 organizacji z krajów UE, Ukrainy i Wielkiej Brytanii)[18].

EU-CIP

(European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection, pol. Europejskie Centrum Wiedzy i Testowania Polityk w Zakresie Ochrony Infrastruktury Krytycznej)[19]

To inicjatywa również networkingowa, ale skupiająca się wyłącznie na ochronie IK. Trwa od października 2022 r. do września 2025 r.

Głównym celem EU-CIP jest ustanowienie unikalnego ogólnoeuropejskiego centrum wiedzy na temat odpornej infrastruktury, które umożliwi decydentom kształtowanie i tworzenie polityk opartych na danych i dowodach, przy jednoczesnym zwiększaniu zdolności innowacyjnych i konkurencyjności operatorów IK, władz, naukowców i innowatorów. W tym kierunku projekt rozwija utworzony i obsługiwany przez partnerów projektu European Cluster for Securing Critical Infrastructures, ECSCI (pol. Europejski Klaster na rzecz Zabezpieczenia Infrastruktury Krytycznej) – najważniejsze europejskie centrum wiedzy w zakresie badań i innowacji na rzecz bezpieczeństwa i odporności IK. Klaster ECSCI skupia 22 projekty, które współpracują w zakresie zapewniania odporności IK. W celu stworzenia ogólnounijnego centrum wiedzy EU-CIP wykorzystuje potencjał, organizację, społeczność i osiągnięcia klastra ECSCI.

EU-CIP oferuje zaawansowane możliwości analizy informacji w celu kształtowania polityki opartej na dowodach i wsparcia innowacji, by ułatwić wykorzystanie i komercjalizację wyników badań. Aby zmaksymalizować wpływ swoich działań, EU-CIP tworzy i rozwija dynamiczny ekosystem zainteresowanych i zaangażowanych interesariuszy wokół analizy informacji i usług wsparcia innowacji.

Główne cele EU-CIP:

1. Analiza: zwiększenie zdolności analitycznych w Europie w zakresie badań, technologii i polityk – wspieranie rozwoju polityki i innowacji opartego na danych. EU-CIP przyjmuje metodologię gromadzenia danych, monitorowania i analizy informacji, polegającą

[18] *EU-HYBNET*, https://euhybnet.eu/ [dostęp: 13.01.2025].

[19] *European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection*, European Commission, https://cordis.europa.eu/project/id/101073878 [dostęp: 13.01.2025].

na nieustannym gromadzeniu, analizie, selekcji, wyodrębnianiu i prezentowaniu informacji i spostrzeżeń na temat odporności infrastruktury. W ramach tego celu EU-CIP prezentuje prognozy i spostrzeżenia na temat luk w wiedzy, rozwiązań i technologii, a także wyników badań i praktyk.

2. Wzmocnienie: maksymalizacja wpływu działań badawczo-rozwojowych w zakresie ochrony IK (ang. c*ritical infrastructure protection,* CIP) i odporności IK (ang. *critical infrastructure resilience,* CIR) w Europie. Projekt zapewnia usługi wsparcia innowacji i walidacji rozwiązań dla wyników badań w obszarach odpornej infrastruktury (CIP/CIR). Wykorzystuje wyniki analityczne filaru EU-CIP-ANALYSIS w celu zidentyfikowania luk w istniejących rozwiązaniach i obszarach IK o znacznym potencjale innowacyjnym. W związku z tym oferowane przez EU-CIP usługi będą wspierać innowatorów CIP/CIR (w tym małe i średnie przedsiębiorstwa) w ich działaniach związanych z wykorzystywaniem i komercjalizacją wyników badań. Ponadto projekt oferuje zwirtualizowane środowisko testowe do eksperymentowania z opartymi na standardach rozwiązaniami CIP/CIR i systemami certyfikacji, wraz z odpowiednimi procesami walidacji i oceny obejmującymi zaangażowanie zainteresowanych stron.
3. Stworzenie ekosystemu: ustanowienie centrum wiedzy (ang. Knowledge Hub) i stworzenie wokół wyników projektu dynamicznego ekosystemu zainteresowanych i zaangażowanych interesariuszy. EU-CIP ustanawia i rozwija ogólnounijny ekosystem interesariuszy CIP/CIR, obejmujący 27 państw UE i inne kraje Europejskiego Obszaru Gospodarczego. Ekosystem ułatwia dostęp do wiedzy, wyników, usług i infrastruktury opracowanych w poprzednich celach, a także zaangażowanie zainteresowanych stron w rozwój innowacji i kształtowanie polityki w ramach inicjatyw UE (np. projektów badawczych, inicjatyw technologicznych, inicjatyw politycznych). Centrum wiedzy zapewnia dostęp (przez właściwą infrastrukturę cyfrową) do zasobów wiedzy projektu, w tym infrastruktury i wyników opracowanych w poprzednich celach. Pozwala na współpracę między różnymi zainteresowanymi stronami.

Oczekiwane rezultaty EU-CIP są następujące:

- zwiększona odporność IK – projekt przez kompleksową analizę umożliwia identyfikowanie i eliminowanie luk;

- rozwój polityki oparty na dowodach – projekt przez agregację i analizę wielu różnych danych wspiera tworzenie bardziej skutecznych polityk dla CIP/CIR;
- zwiększanie innowacyjności i konkurencyjności – projekt przez zaawansowane możliwości analizy informacji i usług wsparcia innowacji zwiększa możliwości innowatorów, zwłaszcza w zakresie wykorzystywania i komercjalizacji wyników badań;
- wspieranie ekosystemu współpracy – ustanowienie dynamicznego ekosystemu interesariuszy ułatwia dzielenie się wiedzą, współpracę i współtworzenie rozwiązań, co zwiększa zbiorową zdolność do sprostania wyzwaniom CIP/CIR[20].

VIGIMARE

(Vigilant Maritime Surveillance of Critical Submarine Infrastructure, pol. Uważny nadzór morski nad podwodną infrastrukturą krytyczną)[21]

To projekt typu działania innowacyjnego – koncentruje się na opracowywaniu rozwiązań podwyższających poziom gotowości technologicznej (ang. Technology Readiness Level, TRL).

W ramach projektu opracowano innowacyjne rozwiązanie umożliwiające poprawę bezpieczeństwa i ograniczenia ryzyka ataków fizycznych i cyberzagrożeń. Celem projektu jest identyfikacja wczesnych sygnałów ostrzegawczych i wsparcie analizy przez mapowanie systemów podwodnych, ocenę słabych punktów i tworzenie świadomości sytuacyjnej w czasie rzeczywistym, zarówno nawodnej, jak i podwodnej IK. Projekt przyjmuje systematyczne podejście do wzmocnienia europejskiego sektora IK podmorskich kabli telekomunikacyjnych, energetycznych i gazociągów. Analiza, a także system VIGIMARE będą wspierać operatorów IK sieci podwodnej przez zwiększenie jej odporności na ataki i uszkodzenia.

Cele VIGIMARE:

- zapewnienie operatorom IK środowiska wymiany informacji w celu przeciwdziałania zagrożeniom dla IK okrętów podwodnych UE;
- zwiększenie odporności operatorów IK na zagrożenia fizyczne, cybernetyczne i hybrydowe przez wdrożenie środków zapobiegających ryzyku i ograniczających je;

[20] *EU-CIP*, https://www.eucip.eu/ [dostęp: 13.01.2025].

[21] *Vigilant Maritime Surveillance of Critical Submarine Infrastructure*, European Commission, https://cordis.europa.eu/project/id/101168016 [dostęp: 14.01.2025].

- wzmocnienie świadomości sytuacyjnej operatorów IK i państw członkowskich UE w odniesieniu do europejskich obszarów morskich, zarówno wodnych, jak i lądowych, w celu rozpoznawania fizycznych (spowodowanych przez człowieka i naturalnych), cybernetycznych i hybrydowych ataków i incydentów, co umożliwi lepsze planowanie odpowiedzi na atak oraz działań naprawczych;
- wsparcie państw członkowskich UE w wypełnianiu wymogów dyrektyw CER i NIS 2. Wyniki tego projektu wprowadzą również wspólne środowisko wymiany informacji (ang. *common information sharing enviroment*, CISE) Europejskiej Agencji Bezpieczeństwa Morskiego (European Maritime Safety Agency, EMSA) do tego nowego obszaru zainteresowań. Rozwiązanie zaproponowane w ramach projektu VIGIMARE zostanie przetestowane w warunkach skrajnych, z wykorzystaniem danych z rzeczywistych incydentów i zatwierdzone na 3 różnych europejskich obszarach morskich – Morzu Śródziemnym, Morzu Irlandzkim i Morzu Bałtyckim – w celu promowania jego cennych wyników w społeczeństwie europejskim[22].

TESTUDO

(Autonomous Swarm of Heterogeneous resources in infrastructure protection via threat prediction and prevention, pol. Wykorzystanie rojów autonomicznych pojazdów bezzałogowych w celu przewidywania zagrożeń i zapobiegania im)[23]

Ten projekt ma na celu wzmocnienie nadzoru nad europejską IK i jej ochrony przy użyciu autonomicznych systemów i zaawansowanych technologii, aby zapewnić ich solidne działanie.

Cele TESTUDO:

- wykorzystanie zaawansowanych pojazdów bezzałogowych wraz z istniejącym sprzętem do ciągłego monitorowania nawet w trudnych warunkach i na odległych terytoriach;
- włączenie najnowocześniejszych technologii wykrywania niebezpiecznych zdarzeń, zapobiegania im i przewidywania ich, aby zwiększyć możliwości w tym zakresie;

[22] *VIGIMARE,* https://vigimare.eu/ [dostęp: 15.01.2025].

[23] *Autonomous Swarm of Heterogeneous resourcse in infrastructure protection via threat prediction and prevention,* European Commission, https://cordis.europa.eu/project/id/101121258 [dostęp: 15.01.2025].

- identyfikacja zasobów potrzebnych do realizacji działań operacyjnych za pomocą technik optymalizacji, przyczyniająca się do całkowitej autonomii systemu;
- zebranie multidyscyplinarnej grupy składającej się ze specjalistów w zakresie: modeli opartych na sztucznej inteligencji, zagrożeń chemicznych, biologicznych, radiacyjnych, nuklearnych (ang. *chemical, biological, radiological, nuclear*, CBRN), zagrożeń cyberbezpieczeństwa, cyfrowych bliźniaków (cyfrowej repliki fizycznych obiektów, procesów i systemów) oraz IK, w celu opracowania innowacyjnych rozwiązań służących ochronie różnych obiektów IK funkcjonujących w długiej perspektywie czasowej i całkowicie autonomicznie[24].

NBSINFRA

(Citynature-based Solutions Integration to Local Urban Infrastructure Protection for a Climate Resilient Society, pol. Integracja rozwiązań opartych na przyrodzie z lokalną infrastrukturą miejską w celu ochrony społeczeństwa odpornego na zmiany klimatu)[25]

To pionierska europejska inicjatywa, która wspiera wzmocnienie ochrony lokalnej miejskiej IK przed zagrożeniami naturalnymi i spowodowanymi przez człowieka. Polega na współprojektowaniu i współtworzeniu rozwiązań opartych na przyrodzie (ang. *Nature-based Solutions*, NbS) w celu zbudowania społeczeństwa odpornego na zmiany klimatu. NBSINFRA wykazuje, że NbS są: a) technicznie wykonalne w zakresie ochrony IK przed zagrożeniami, b) społecznie akceptowalne i opłacalne w skali lokalnej, c) zdolne do skutecznego wzmocnienia pozycji społeczności przez zwiększenie ich odporności ekologicznej, społecznej i gospodarczej.

NBSINFRA ustanawia 5 reprezentatywnych regionów europejskich z taką samą liczbą tzw. laboratoriów miejskich (ang. City Labs) w: Fingal (Irlandia), Kolonii (Niemcy), Ruse (Bułgaria), Aveiro (Portugalia), Pradze (Czechy). Laboratoria ocenią opłacalność rozwiązań NbS w ochronie lokalnej infrastruktury i zmaksymalizują ich wpływ na nią. Rozwiązania te będą własnością obywateli i będą współtworzone przez użytkowników końcowych i zarządców oraz społeczeństwo obywatelskie.

[24] *TESTUDO*, https://testudo-project.eu/ [dostęp: 15.01.2025].

[25] *Citynature-based Solutions integration to local urban infrastructure protection for a climate resilient society*, https://cordis.europa.eu/project/id/101121210 [dostęp: 17.01.2025].

NBSINFRA zapewnia zestaw narzędzi, które zainteresowane strony i społeczeństwo mogą wykorzystać do porównania i wyboru najbardziej skutecznych NbS dla ochrony lokalnej IK. Głównym celem jest zwiększenie jej ochrony przed zagrożeniami przez współprojektowanie, współmonitorowanie i współtworzenie NbS służących rozwojowi zrównoważonego i odpornego społeczeństwa[26].

ENDURANCE

(Strategies and Services for Enhanced Disruption Resilience and Cooperation in Europe, pol. Strategie i usługi na rzecz zwiększonej odporności na zakłócenia i współpracy w Europie)[27]

Projekt ENDURANCE ma na celu wzmocnienie w Europie sektorów takich jak energetyka, ochrona zdrowia, woda pitna. Zapewnia zgodność z europejskimi regulacjami, zwłaszcza z dyrektywami CER i NIS 2, daje operatorom i organom niezbędne narzędzia, strategie i wiedzę w celu minimalizowania ryzyka i skutecznego usuwania skutków zakłóceń.

Cele ENDURANCE:

- wzmocnienie na wszystkich poziomach strategicznej współpracy między interesariuszami IK z różnych sektorów i krajów;
- opracowanie zbiorów danych, rejestrów, metodologii, technologii i usług (na poziomie TRL 6-7) w celu bezpiecznego udostępniania i przetwarzania danych istotnych dla CER, wspólnej oceny istotnych zagrożeń i odporności oraz testowania gotowości w warunkach skrajnych na dużą skalę;
- zapewnienie zharmonizowanej i pragmatycznej strategii na rzecz ciągłości połączonych podstawowych usług[28].

[26] *NBSINFRA*, https://nbsinfra.eu/ [dostęp: 17.01.2025].

[27] *Strategies and Services for Enhanced Disruption Resilience and Cooperation in Europe*, European Commission, https://cordis.europa.eu/project/id/101168007 [dostęp: 17.01.2025].

[28] *ENDURANCE*, https://endurance-horizon.eu/ [dostęp: 17.01.2025].

TRANSCEND

(Transport resilience against Cyber and Non-Cyber Events to prevent Network Disruption, pol. Odporność transportu na zdarzenia cybernetyczne i niecybernetyczne w celu zapobiegania zakłóceniom sieci)[29]

Projekt TRANSCEND ma na celu:

- zapewnienie operatorom transportu towarowego zintegrowanego zestawu zaawansowanych narzędzi, wytycznych i rozwiązań technologicznych w celu zmniejszenia ryzyka dla sieci i usług transportowych, które może wynikać ze zdarzeń cybernetycznych i niecybernetycznych;
- zwiększenie ochrony i odporności systemów transportowych przed zagrożeniami fizycznymi, cybernetycznymi i hybrydowymi.

Aby zrealizować te cele, w ramach projektu zostanie zapewniona platforma cyfrowa do monitorowania zagrożeń i ryzyka, a także zostanie opracowanych 5 rzeczywistych projektów pilotażowych. Są one podzielone na 3 główne: pilotażowy port lotniczy w Luksemburgu, pilotażowy terminal kolejowo-drogowy w Bolonii we Włoszech i pilotażowe wdrożenie portu trimodalnego w Hiszpanii; oraz na 2 naśladowców: port rzeczny w Budapeszcie i autostrada Egnatia w Grecji.

Wyniki projektu zostaną zintegrowane w Wieżę Kontroli, czyli platformę cyfrową z wbudowaną inteligencją biznesową (ang. *Business Intelligence*), zapewniającą interesariuszom wspólny i ciągły wgląd w zagrożenia i ryzyko przez poprawę przepływu wiedzy w organizacjach i między nimi. Aby przetestować skuteczność tego podejścia, z rozwiązaniami metodologicznymi i technologicznymi będzie eksperymentować 5 różnych obiektów transportowej IK, 3 w roli liderów i 2 naśladowców[30].

Wyzwania i doświadczenia związane z realizacją projektów

Konkurencja o fundusze unijne jest duża, a pozyskanie takich środków stanowi cenną okazję do międzynarodowej współpracy. Wdrażanie kolejnych unijnych projektów badawczych i innowacyjnych cieszy się zatem dużym uznaniem w środowisku naukowym. W porównaniu z grantami krajowymi, które czasami zawierają komponent międzynarodowy, projekty unijne

[29] *Transport resilience against Cyber and Non-Cyber Events to prevent Network Disruption*, European Commission, https://cordis.europa.eu/project/id/101168023 [dostęp: 17.01.2025].

[30] *TRANSCEND*, https://www.transcend-logistics.eu/ [dostęp: 17.01.2025].

zakładają współpracę między uczestnikami z krajów europejskich, reprezentujących różne organizacje, w tym uniwersytety, instytucje badawcze, firmy prywatne, podmioty sektora publicznego i organizacje pozarządowe. Średni budżet projektu w wysokości 3–5 mln euro może wydawać się znaczny, ale w ciągu 3 lat realizacji projektu musi on zostać rozdzielony między konsorcja składające się z 10–15 lub nawet więcej partnerów. Biorąc pod uwagę wysokie – zdaniem autorów – oczekiwania co do wyników projektu, a także poziom inflacji w Europie w ostatnich latach, dostępny obecnie budżet może już nie być tak korzystny.

Po przeanalizowaniu tych wszystkich czynników wyciągnięto wnioski i zidentyfikowano kilka wyzwań. W koordynacji między państwami członkowskimi jednym z wyzwań są odmienne regulacje prawne i interpretacje dyrektyw UE. Mimo że UE zapewnia wspólne dyrektywy dotyczące CIP, cyberbezpieczeństwa i zarządzania danymi, to ich wdrażanie i interpretacja różnią się w poszczególnych państwach członkowskich. Niektóre kraje ściśle dostosowują przepisy krajowe do dyrektyw UE, podczas gdy inne pozostawiają sobie większy margines swobody lub mają opóźnienia w ich transpozycji do prawa krajowego. Na przykład dyrektywy CER i NIS 2 mają na celu stworzenie wspólnych ram bezpieczeństwa, ale ich praktyczne egzekwowanie różni się w poszczególnych krajach[31]. Te niespójności regulacji mogą prowadzić do opóźnień w realizacji projektów i komplikacji we wspólnych inicjatywach państw członkowskich.

Dodatkowym wyzwaniem może być odmienne postrzeganie przez nie zagrożeń i priorytetów krajowych, które również mają wpływ na projekty UE. Przekłada się to na zaangażowanie tych państw w ułatwianie wymiany doświadczeń i pogłębianie wiedzy na temat zagrożeń hybrydowych, a także w prowadzenie międzynarodowych ćwiczeń obejmujących scenariusze hybrydowe[32]. Ta rozbieżność jest szczególnie widoczna w przypadku Rosji i Chin, w odniesieniu do których państwa członkowskie UE zajmują odmienne stanowiska. Na przykład zarówno rządy, jak i społeczeństwa w Polsce i krajach bałtyckich uważają Chiny za zagrożenie cyberbezpieczeństwa, a Rosję za agresora po ataku na Ukrainę i ograniczają z nimi współpracę,

[31] *The Commission calls on 23 Member States to fully transpose the NIS2 Directive*, European Commission, 28.11.2024, https://digital-strategy.ec.europa.eu/en/news/commission-calls-23-member-states-fully-transpose-nis2-directive [dostęp: 29.01.2025].

[32] P. Szymański, *NATO i Unia Europejska wobec zagrożeń hybrydowych*, Ośrodek Studiów Wschodnich, 24.04.2020, https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2020-04-24/nato-i-unia-europejska-wobec-zagrozen-hybrydowych [dostęp: 7.02.2025].

podczas gdy niektóre rządy w państwach członkowskich (np. Węgry i Słowacja) prowadzą intensywną współpracę gospodarczą i infrastrukturalną z Chinami i Rosją, szczególnie w dziedzinie energetyki. Ten brak ujednoliconej oceny ryzyka utrudnia pełne wdrożenie wspólnych środków ochronnych i zapewnienie spójnych standardów bezpieczeństwa infrastruktury w całej UE.

Doświadczenia z realizacji projektów UE, potwierdzone obserwacjami autorów artykułu, wskazują, że kraje członkowskie mają różne możliwości skutecznego wdrażania projektów ochrony IK z powodu odmiennych zasobów finansowych, technologicznych i ludzkich. Na lepszej pozycji są kraje Europy Zachodniej i Północnej. Kraje Europy Wschodniej i Południowej z kolei borykają się z większymi ograniczeniami budżetowymi, co prowadzi do wolniejszego wdrażania nowych technologii bezpieczeństwa i modernizacji infrastruktury.

Problemem w wielu projektach UE w zakresie bezpieczeństwa jest złożoność współpracy transgranicznej, w tym wymiana danych. Należy jednak podkreślić, że zarówno Komisja Europejska, jak i państwa członkowskie wdrażają specjalne mechanizmy i tworzą instytucje (powołują nowe struktury w ramach istniejących instytucji lub nowe instytucje) wspierające ten proces w obszarze ochrony IK. Są to m.in. dyrektywy CER i NIS 2, Europejski Program Ochrony Infrastruktury Krytycznej (European Programme for Critical Infrastructure Protection, EPCIP), Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa (European Cybersecurity Competence Centre, ECCC), a także działania w zakresie cyberbezpieczeństwa prowadzone przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (European Union Agency for Cybersecurity, ENISA). Wszystkie te mechanizmy i instytucje powinny wspierać zarówno realizację projektów, jak i wykorzystanie ich wyników.

Inna grupa wyzwań wiąże się z równoważeniem innowacyjności z praktycznością. Projekty finansowane przez UE koncentrujące się na ochronie IK (zwłaszcza w ramach Klastra 3 programu Horyzont Europa) mają na celu wprowadzenie rozwiązań innowacyjnych, aby zwiększyć bezpieczeństwo, odporność i wydajność. Wdrażanie najnowocześniejszych rozwiązań jest jednak trudne z powodu m.in. wykonalności technologicznej, ograniczeń regulacyjnych, zagrożeń bezpieczeństwa, braku opłacalności i możliwości zastosowania w praktyce.

Duża część projektów badawczych koncentruje się na opracowywaniu zaawansowanych technologicznie rozwiązań, takich jak wykrywanie zagrożeń oparte na sztucznej inteligencji, zaawansowane narzędzia cyberbezpieczeństwa, szyfrowanie kwantowe. Wiele innowacji jednak znajduje się w fazie eksperymentalnej i wymaga miesięcy, a nawet lat testów i kalibracji, zanim będzie można je bezpiecznie zintegrować z istniejącą infrastrukturą. Infrastruktura krytyczna działa przez wiele lat (tzw. długi cykl życia), co oznacza, że nowe technologie muszą być kompatybilne ze starszymi systemami, a to często jest trudne i kosztowne. Niektóre pojawiające się technologie (np. sztuczna inteligencja; blockchain; systemy bezpieczeństwa internetu rzeczy, ang. Internet of Things, IoT) mogą nie być jeszcze wystarczająco dojrzałe do rzeczywistego zastosowania w środowiskach wysokiego ryzyka. Zatem innowacje, chociaż niezbędne, muszą być praktyczne, skalowalne i sprawdzone w rzeczywistych warunkach, zanim zostaną wdrożone.

Nawet jeśli istnieją techniczne możliwości wprowadzenia innowacji, to mogą pojawić się przeszkody prawne i regulacyjne[33]. Unijne i krajowe przepisy dotyczące cyberbezpieczeństwa, ochrony danych i bezpieczeństwa IK mogą spowalniać lub ograniczać wykorzystanie nowych technologii. Różne interpretacje prawne w poszczególnych państwach członkowskich powodują niespójności, co utrudnia wdrożenie jednego innowacyjnego rozwiązania w wielu krajach. Rządy i operatorzy muszą się upewnić, że nowe technologie nie stworzą dodatkowego ryzyka, co w praktyce oznacza długie procesy zatwierdzania, testowania i oceny bezpieczeństwa. W rezultacie nawet najbardziej zaawansowane innowacje mogą potrzebować lat, aby organy regulacyjne wyraziły na nie zgodę.

Dodatkowym wyzwaniem jest to, że innowacje często wiążą się z wysokimi kosztami początkowymi na rozwój, testowanie i wdrażanie nowych technologii. Ponadto IK, taka jak sieci energetyczne, sieci transportowe, systemy wodne i systemy telekomunikacyjne, często opiera się na technologiach sprzed dziesięcioleci. W związku z tym wykonalność technologiczna nie zawsze przekłada się na szybkie praktyczne wdrożenie ze względu na brak kompatybilności i względy operacyjne.

Nowe technologie oprócz tego, że mogą zwiększyć bezpieczeństwo, powodują również luki w zabezpieczeniach. Zaawansowane technologie

[33] *Case Studies on the Regulatory Challenges Raised by Innovation and the Regulatory Responses*, OECD Publishing, Paris 2021. https://doi.org/10.1787/8fa190b5-en.

(np. IoT, sztuczna inteligencja, przetwarzanie w chmurze) są celem cyberprzestępców i podmiotów państwowych i wymagają ciągłych aktualizacji i poprawek bezpieczeństwa[34]. Co więcej, niektóre innowacje mogą opierać się na sprzęcie lub oprogramowaniu pochodzącym z krajów spoza UE, co budzi obawy o bezpieczeństwo danych, backdoory i ingerencję z zagranicy.

Innowacje w zakresie ochrony IK wymagają współpracy między rządami, operatorami z sektora prywatnego i społeczeństwem. Często jednak pojawiają się opory i sceptycyzm wobec nowych technologii, związane z brakiem zaufania do automatyzacji i sztucznej inteligencji oraz obawy o prywatność. Technologie, takie jak zabezpieczenia biometryczne i inteligentny monitoring często spotykają się ze sprzeciwem opinii publicznej ze względu na obawy przed masową inwigilacją i niewłaściwym wykorzystaniem danych. W niektórych krajach, np. w Niemczech, Francji czy Polsce, społeczeństwo sprzeciwia się zaangażowaniu prywatnych firm technologicznych lub podmiotów zagranicznych w projekty IK. Jeśli interesariusze nie ufają technologii, nie będą wspierać jej wdrożenia. Głosy obywateli są istotne, ponieważ bierze się je pod uwagę przy kształtowaniu polityk dotyczących technologii, które mają znaczący wpływ na społeczeństwo[35].

Przyszłe kierunki badań UE nad ochroną infrastruktury krytycznej

Przyszłe kierunki badań UE nad ochroną IK zdecydowanie muszą uwzględniać wyzwania mogące się pojawić w przyszłości. Na podstawie badań i publikacji, w tym wyników projektu EU-HYBNET i raportów Europejskiego Centrum Doskonalenia ds. Przeciwdziałania Zagrożeniom Hybrydowym (European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE), autorzy wskazują następujące obszary jako najbardziej istotne w perspektywie krótko- i średnioterminowej:

- cyberataki (w tym ataki oparte na sztucznej inteligencji i brak zabezpieczeń IoT);

[34] *The cybersecurity challenges of legacy OT and how to manage them*, Control Engineering, 21.03.2024, https://www.controleng.com/the-cybersecurity-challenges-of-legacy-ot-and-how-to-manage-them [dostęp: 7.02.2025].

[35] K. Kieslich, M. Lünich, *Regulating AI-Based Remote Biometric Identification. Investigating the Public Demand for Bans, Audits, and Public Database Registrations*, preprint, https://arxiv.org/abs/2401.13605v3 [dostęp: 7.02.2025]. https://doi.org/10.48550/arXiv.2401.13605.

- technologia kwantowa (zwłaszcza przejście na kryptografię postkwantową i związane z nią luki w zabezpieczeniach);
- surowce krytyczne i bezpieczeństwo łańcucha dostaw (baterie, półprzewodniki, telekomunikacja);
- zagrożenia fizyczne (pożary, drony);
- satelity;
- szczególna dbałość o odporność energetyczną;
- bezpieczna telekomunikacja (5G, ale także 6G).

Ze względu na szybki rozwój technologii, niestabilność geopolityczną i zmieniającą się percepcję społeczną trudno jest dokładnie przewidzieć wszystkie zagrożenia. W przyszłych projektach i innowacyjnych działaniach powinny zostać dodatkowo uwzględnione następujące obszary:

- wzmocnienie wspólnego monitorowania zagrożeń cybernetycznych i fizycznych w czasie rzeczywistym oraz wymiana informacji o nich;
- wspólne ćwiczenia w całej UE;
- współpraca z globalnymi organizacjami normalizacyjnymi w celu zapewnienia, że priorytety UE w zakresie bezpiecznej infrastruktury już na etapie projektowania, etycznej sztucznej inteligencji i cyberbezpieczeństwa opartego na prywatności są odzwierciedlone w globalnych standardach;
- zwiększenie partnerstw publiczno-prywatnych z dostawcami technologii;
- współpraca z zaufanymi partnerami UE, w tym z Wielką Brytanią, USA, Kanadą, Japonią, Koreą Południową i Australią.

Wnioski

Ochrona IK pozostaje fundamentem europejskiej polityki bezpieczeństwa, zwłaszcza w obliczu ewoluujących zagrożeń hybrydowych. Unia Europejska podejmuje istotne działania w zakresie finansowania inicjatyw mających na celu wzmocnienie odporności IK. Projekty takie jak: EU-HYBNET, EU-CIP, VIGIMARE, TESTUDO, TRANSCEND, NBSINFRA i ENDURANCE pokazują zakres wysiłków na rzecz zwiększenia bezpieczeństwa obejmujących rozwój technologii, koordynację polityki i współpracę transgraniczną.

Jednym z wniosków płynących z tej analizy jest rosnąca złożoność zagrożeń stojących przed operatorami IK. Konwergencja cybernetycznych

i fizycznych zagrożeń bezpieczeństwa, trudności wynikające z odmiennych krajowych regulacji prawnych i niespójnych interpretacji dyrektyw UE w państwach członkowskich UE oraz wyzwania dotyczące równoważenia innowacyjnych projektów z ich wdrażaniem wzmacniają potrzebę ciągłych wysiłków badawczo-rozwojowych. Pomimo że program Horyzont Europa i inne mechanizmy finansowania zapewniły duże wsparcie, konieczne są dodatkowe zasoby finansowe i strategiczne, aby utrzymać wiodącą pozycję UE w zakresie odporności infrastruktury.

Kolejnym istotnym spostrzeżeniem jest konieczność wspierania silniejszej współpracy między zainteresowanymi stronami. Omówione projekty pokazują znaczenie integracji perspektyw przemysłu, środowiska akademickiego, władz publicznych i społeczeństwa obywatelskiego. Wzmacnianie bardziej elastycznych i adaptacyjnych partnerstw będzie miało zasadnicze znaczenie w zmieniającym się krajobrazie zagrożeń. Ponadto zapewnienie, że wyniki badań zostaną przełożone na praktyczne zastosowania, będzie wymagało ściślejszej współpracy między decydentami, twórcami technologii i operatorami infrastruktury.

Kolejna faza badań i rozwoju polityki powinna koncentrować się na zwiększaniu odporności przez prognozowanie strategiczne, innowacje technologiczne i współpracę międzysektorową. Dzięki temu unijna IK pozostanie odporna na przyszłe zagrożenia i tym samym będzie chronić bezpieczeństwo i stabilność społeczeństw na kontynencie.

Zdaniem autorów warto monitorować i analizować, czy i w jaki sposób wyniki projektów opisanych w artykule zostały wdrożone w praktyce.

Bibliografia

Case Studies on the Regulatory Challenges Raised by Innovation and the Regulatory Responses, OECD Publishing, Paris 2021. https://doi.org/10.1787/8fa190b5-en.

Źródła internetowe

Autonomous Swarm of Heterogeneous resourcse in infrastructure protection via threat prediction and prevention, European Commission, https://cordis.europa.eu/project/id/101121258 [dostęp: 15.01.2025].

Citynature-based Solutions integration to local urban infrastructure protection for a climate resilient society, https://cordis.europa.eu/project/id/101121210 [dostęp: 17.01.2025].

Critical infrastructure resilience at EU-level, European Commission, 23.09.2024, https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en [dostęp: 6.01.2025].

Empowering a Pan-European Network to Counter Hybrid Threats, European Commission, https://cordis.europa.eu/project/id/883054 [dostęp: 13.01.2025].

ENDURANCE, https://endurance-horizon.eu/ [dostęp: 17.01.2025].

EU-CIP, https://www.eucip.eu/ [dostęp: 13.01.2025].

EU-HYBNET, https://euhybnet.eu/ [dostęp: 13.01.2025].

European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection, European Commission, https://cordis.europa.eu/project/id/101073878 [dostęp: 13.01.2025].

Horizon Europe, https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en [dostęp: 7.01.2025].

Horizon Europe. Strategic Plan 2025–2027, European Commission, 2024, https://op.europa.eu/en/web/eu-law-and-publications/publication-detail/-/publication/6abcc8e7-e685-11ee-8b2b-01aa75ed71a1 [dostęp: 7.01.2025].

Horizon Europe. Strategic Plan 2025–2027. Analysis, European Commission, 2023, https://op.europa.eu/en/publication-detail/-/publication/b3baec75-fdd0-11ed-a05c-01aa75ed71a1/language-en [dostęp: 9.01.2025].

Horizon Europe. Work Programme 2023-2025. 6. Civil Security for Society (European Commission Decision C(2024) 2371 of 17 April 2024), https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2023-2024/wp-6-civil-security-for-society_horizon-2023-2024_en.pdf [dostęp: 10.01.2025].

Joint Staff Working Document. Eighth progress report on the implementation of the 2016 Joint framework on countering hybrid threats and the 2018 Joint communication on increasing resilience and bolstering capabilities to address hybrid threats, https://defence-industry-space.ec.europa.eu/system/files/2025-01/SWD_Annual-Progress-Report-2024.PDF [dostęp: 2.01.2025].

Kieslich K., Lünich M., *Regulating AI-Based Remote Biometric Identification. Investigating the Public Demand for Bans, Audits, and Public Database Registrations*, preprint, https://arxiv.org/abs/2401.13605v3 [dostęp: 7.02.2025]. https://doi.org/10.48550/arXiv.2401.13605.

NATO and European Union release final assessment report on resilience of critical infrastructure, NATO, 29.06.2023, https://www.nato.int/cps/en/natohq/news_216631.htm [dostęp: 6.01.2025].

NBSINFRA, https://nbsinfra.eu/ [dostęp: 17.01.2025].

Resilient Infrastructures, https://rea.ec.europa.eu/funding-and-grants/horizon-europe-cluster-3-civil-security-society/resilient-infrastructures_en [dostęp: 10.01.2025].

Strategic plan, https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/strategic-plan_en [dostęp: 3.01.2025].

Strategies and Services for Enhanced Disruption Resilience and Cooperation in Europe, European Commission, https://cordis.europa.eu/project/id/101168007 [dostęp: 17.01.2025].

Szymański P., *NATO i Unia Europejska wobec zagrożeń hybrydowych,* Ośrodek Studiów Wschodnich, 24.04.2020, https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2020-04-24/nato-i-unia-europejska-wobec-zagrozen-hybrydowych [dostęp: 7.02.2025].

TESTUDO, https://testudo-project.eu/ [dostęp: 15.01.2025].

The Commission calls on 23 Member States to fully transpose the NIS2 Directive, European Commission, 28.11.2024, https://digital-strategy.ec.europa.eu/en/news/commission-calls-23-member-states-fully-transpose-nis2-directive [dostęp: 29.01.2025].

The cybersecurity challenges of legacy OT and how to manage them, Control Engineering, 21.03.2024, https://www.controleng.com/the-cybersecurity-challenges-of-legacy-ot-and-how-to-manage-them [dostęp: 7.02.2025].

TRANSCEND, https://www.transcend-logistics.eu/ [dostęp: 17.01.2025].

Transport resilience against Cyber and Non-Cyber Events to prevent Network Disruption, European Commission, https://cordis.europa.eu/project/id/101168023 [dostęp: 17.01.2025].

Vigilant Maritime Surveillance of Critical Submarine Infrastructure, European Commission, https://cordis.europa.eu/project/id/101168016 [dostęp: 14.01.2025].

VIGIMARE, https://vigimare.eu/ [dostęp: 15.01.2025].

Akty prawne

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. L 333/164 z 27.12.2022).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) – (Dz. Urz. L 333/80 z 27.12.2022).

Zalecenie Rady z dnia 25 czerwca 2024 r. w sprawie planu skoordynowanego reagowania na szczeblu Unii na zakłócenia w funkcjonowaniu infrastruktury krytycznej mające istotne znaczenie transgraniczne (Dz. Urz. UE C 2024/4371 z 5.07.2024).

Małgorzata Wolbach

Starsza specjalistka ds. realizacji projektów w Polskiej Platformie Bezpieczeństwa Wewnętrznego (PPBW). Absolwentka studiów magisterskich na kierunku bezpieczeństwo wewnętrzne oraz licencjackich na kierunku kryminologia w Wyższej Szkole Policji w Szczytnie. W PPBW odpowiada za wdrażanie i realizację projektów finansowanych z programów Unii Europejskiej, ze szczególnym uwzględnieniem projektów dotyczących zagrożeń hybrydowych oraz bezpieczeństwa przestrzeni publicznych.

Kontakt: malgorzata.wolbach@ppbw.pl

Rashel Talukder

Prezes zarządu Polskiej Platformy Bezpieczeństwa Wewnętrznego. Od 2009 r. aktywnie uczestniczy w pracach badawczo-rozwojowych w obszarze bezpieczeństwa w Polsce i Europie, w tym jako koordynator projektów europejskich. Angażował się także w sprawy społeczności lokalnej jako radny gminy Stęszew (2018–2024).

Kontakt: rashel.talukder@ppbw.pl