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