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