Przegląd Bezpieczeństwa Wewnętrznego
2026, nr 34, s. 111–131

https://doi.org/10.4467/20801335PBW.26.005.23367

ARTYKUŁ

Morskie farmy wiatrowe jako infrastruktura krytyczna w dobie zagrożeń hybrydowych – nowy wymiar bezpieczeństwa energetycznego Polski

Offshore wind farms as critical infrastructure in the era of hybrid threats – a new dimension of Poland's energy security

KLAUDIA MACIATA

Politechnika Gdańska

https://orcid.org/0000-0001-6227-2851

Abstrakt Morskie farmy wiatrowe (offshore wind farms, OWFs) stają się kluczowym elementem bezpieczeństwa energetycznego Polski. Z uwagi na lokalizację i charakter są one podatne na zagrożenia hybrydowe. Autorka artykułu omówiła OWFs jako nowy komponent infrastruktury krytycznej w kontekście incydentów na Morzu Bałtyckim od 2022 r. oraz przeanalizowała stopień odporności OWFs w aspekcie zagrożeń hybrydowych. Opisała luki prawne i organizacyjne w polskim systemie ochrony infrastruktury, wskazała dobre praktyki stosowane na świecie oraz rekomendacje dla administracji i operatorów w Polsce. Zwróciła uwagę na potrzebę testowania odporności OWFs z wykorzystaniem symulacji digital twin i ćwiczeń red teaming. Postulatem autorki jest złożone podejście do bezpieczeństwa OWFs – integrujące działania legislacyjne, technologiczne i organizacyjne. Artykuł stanowi wkład w dyskurs na temat redefinicji bezpieczeństwa energetycznego Polski w dobie rywalizacji poniżej progu wojny.

Słowa kluczowe morskie farmy wiatrowe, infrastruktura krytyczna, zagrożenia hybrydowe, bezpieczeństwo energetyczne, Morze Bałtyckie, ochrona infrastruktury

Abstract

Offshore wind farms (OWFs) are becoming a key component of Poland's energy security. Due to location and nature, they are vulnerable to hybrid threats. The author of the article discussed OWFs as a new component of critical infrastructure in the context of incidents in the Baltic Sea since 2022 and analysed the degree of OWF resilience in the context of hybrid threats. The author described legal and organisational gaps in the Polish infrastructure protection system, pointed out best practices used around the world, and made recommendations for the administration and operators in Poland. She drew attention to the need to test the resilience of OWFs using digital twin simulations and red teaming exercises. The author advocates a complex approach to OWF security, integrating legislative, technological and organisational measures. The article contributes to the discourse on redefining Poland's energy security in an era of competition below the threshold of war.

Keywords

offshore wind farms, critical infrastructure, hybrid threats, energy security, Baltic Sea, infrastructure protection

Wprowadzenie

Transformacja energetyczna w kierunku niskoemisyjnych źródeł energii czyni morskie farmy wiatrowe (offshore wind farms, OWFs[1]) jednym z najważniejszych elementów nowoczesnego systemu bezpieczeństwa energetycznego Polski. Ich rozwój wpisuje się w cele polityki klimatyczno-energetycznej Unii Europejskiej, w tym w osiągnięcie neutralności klimatycznej do 2050 r. oraz we wzrost udziału odnawialnych źródeł energii (OZE) w miksie energetycznym państw członkowskich[2]. Morskie farmy wiatrowe budowane przez Polskę na Morzu Bałtyckim docelowo mają dostarczać do 2040 r. do 11 GW mocy zainstalowanej, co czyni je największym projektem infrastrukturalnym w historii polskiego sektora OZE[3]. W skali europejskiej prognozuje się wzrost mocy zainstalowanej morskiej energetyki wiatrowej

[1] Wszystkie słowa i zwroty obcojęzyczne użyte w artykule pochodzą z języka angielskiego (przyp. red.).

[2] Komisja Europejska, *Plan REPowerEU*, COM(2022) 230 final, https://eur-lex.europa.eu/resource.html?uri=cellar:fc930f14-d7ae-11ec-a95f-01aa75ed71a1.0010.02/DOC_1&format=PDF [dostęp: 20 VI 2025].

[3] Ministerstwo Klimatu i Środowiska, *Polityka energetyczna Polski do 2040 r. (PEP2040)*, Warszawa 2021.

z ok. 90 GW w połowie dekady do ok. 170 GW do 2030 r. To oznacza niemal dwukrotne zwiększenie potencjału tego sektora[4].

Rosnące znaczenie OWFs jako zasobu energetycznego stwarza nowe wyzwania w obszarze bezpieczeństwa. Infrastruktura ta, zlokalizowana na otwartym morzu, poza strefą wód terytorialnych i rozproszona przestrzennie, jest narażona na zagrożenia hybrydowe. Obejmują one działania poniżej progu wojny takie jak sabotaż, cyberataki, zakłócenia nawigacyjne czy operacje dezinformacyjne oraz inne opisane w literaturze przedmiotu[5]. Działania te mają na celu nie tylko testowanie odporności infrastruktury krytycznej (IK), lecz także wywieranie presji strategicznej i geopolitycznej poniżej progu konfliktu zbrojnego, generowanie kosztów ekonomicznych, osłabianie zdolności reagowania państwa oraz podważanie jego wiarygodności jako podmiotu zdolnego do kontroli i ochrony przestrzeni morskiej.

Na poziomie UE kwestia bezpieczeństwa OWFs została uregulowana w dyrektywie Parlamentu Europejskiego i Rady (UE) 2022/2557 w sprawie odporności podmiotów krytycznych (Critical Entities Resilience, dalej: dyrektywa CER), która zastąpiła wcześniejszą dyrektywę o europejskiej IK[6]. Nowe przepisy zobowiązują państwa członkowskie do identyfikacji i ochrony podmiotów krytycznych w 12 sektorach, w tym w sektorze energetycznym, bez rozróżnienia na infrastrukturę lądową i morską. Morskie farmy wiatrowe, jako element sieci produkcji i przesyłu energii elektrycznej, w oczywisty sposób wpisują się w ten zakres, a operatorzy tych instalacji są zobowiązani do wdrażania środków zwiększających ich odporność fizyczną i cybernetyczną.

W najnowszych analizach think tanku Centrum Studiów Strategicznych i Międzynarodowych (Center for Strategic and International Studies) oraz Centrum Eksperckiego NATO ds. Komunikacji Strategicznej (NATO Strategic Communication Centre of Excellence) OWFs są postrzegane jako tzw. soft targets – cele o wysokiej wartości strategicznej i relatywnie niskim poziomie ochrony[7]. Ich położenie z dala od wybrzeży, zależność od zautomatyzowanych systemów sterowania (SCADA/OT;

---

4 *Energy Transition Outlook 2025*, https://brandcentral.dnv.com/original/gallery/10651/files/original/ec419166-9ecc-40ef-9997-93a6ccb72335.pdf [dostęp: 20 VI 2025].

5 A. Sari, *Protecting maritime infrastructure from hybrid threats: legal options*, https://www.hybridcoe.fi/wp-content/uploads/2025/03/20250306-Hybrid-CoE-Research-Report-14-web.pdf [dostęp: 20 VI 2025]; *Countering hybrid threats*, NATO, 7 V 2024 r., https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats [dostęp: 20 VI 2025].

6 *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*, s. 164–186.

7 A. Ávila-Zúñiga-Nordfjeld, *Coping with Sabotage and Seabed Security Threats in the Baltic Sea: a Regional Maritime Security Policy*, https://hcss.nl/report/coping-with-sabotage-seabed-security-threats-baltic-sea/, s. 5–8 [dostęp: 20 VI 2025].

supervisory control and data acquisition/operational technology), a także skomplikowana struktura własnościowa i regulacyjna – m.in. prawo morza, które przez gwarantowanie swobód żeglugowych ułatwia agresorom kreowanie zagrożeń – czynią je podatnymi na działania przeciwnika w szarej strefie (gray zone). Przykładami tych zagrożeń mogą być rozwijane od lat przez Chiny i Rosję (Główny Zarząd Badań Głębinowych, GUGI) zdolności podwodne czy flota cieni (shadow fleet)[8].

Celem artykułu jest przedstawienie OWFs jako nowego komponentu IK w Polsce oraz przeanalizowanie stopnia ich odporności w obliczu rosnących zagrożeń hybrydowych. Szczególną uwagę poświęcono trzem obszarom: lukom prawnym i organizacyjnym w polskim systemie ochrony IK, dobrym praktykom na poziomach krajowym i międzynarodowym w zakresie ochrony OWFs oraz rekomendacjom dla decydentów i operatorów w Polsce. Artykuł stanowi wkład w dyskusję o konieczności redefinicji bezpieczeństwa energetycznego w kontekście rywalizacji poniżej progu wojny oraz ochrony zasobów energetycznych w przyszłości.

Ewolucja zagrożeń hybrydowych od 2022 roku – opis przypadków

Wraz z rozpoczęciem pełnoskalowej agresji Federacji Rosyjskiej na Ukrainę w lutym 2022 r. zaobserwowano wzrost liczby incydentów o charakterze hybrydowym, skierowanych przeciwko państwom UE i Sojuszu Północnoatlantyckiego. Obiektem tych działań coraz częściej staje się infrastruktura podmorska, w tym systemy energetyczne i komunikacyjne w regionie Morza Bałtyckiego. Działania te cechuje niska wykrywalność, trudność w jednoznacznym przypisaniu odpowiedzialności oraz prowadzenie ich poniżej progu otwartego konfliktu zbrojnego. W tym kontekście OWFs, stanowiące strategiczne źródło energii, jawią się jako nowa przestrzeń rywalizacji w szarej strefie[9].

Punktem zwrotnym w postrzeganiu zagrożeń wobec infrastruktury morskiej był sabotaż gazociągów Nord Stream 1 i Nord Stream 2 we wrześniu 2022 r. Do eksplozji doszło na wodach terytorialnych Szwecji i Danii, a ich skutkiem było trwałe wyłączenie obu nitek przesyłowych. Szwedzkie służby stwierdziły obecność śladów

[8] T. Szubrycht, *Sojusznicza odpowiedź na zagrożenia na Morzu Bałtyckim*, „Bezpieczeństwo Narodowe" 2025, t. 46, nr 1, s. 49–75. https://doi.org/10.59800/bn/207646.

[9] M. Cavcic, *Hybrid warfare paints 'gray zone' targets on shipping and offshore energy infrastructure*, Offshore Energy, 11 XII 2024 r., https://www.offshore-energy.biz/hybrid-warfare-paints-gray-zone-targets-on-shipping-and-offshore-energy-infrastructure/ [dostęp: 19 VI 2025].

materiałów wybuchowych i uznały zdarzenie za sabotaż[10]. Mimo że sprawca nie został jednoznacznie wskazany, zdarzenie to uświadomiło opinii publicznej, że infrastruktura podmorska może zostać zaatakowana za pomocą środków poniżej progu wojny.

W październiku 2023 r. doszło do poważnego incydentu dotyczącego gazociągu Balticconnector, łączącego Finlandię i Estonię. Śledztwo wykazało, że rurociąg został przecięty przez kotwicę kontenerowca Newnew Polar Bear, która naruszyła również biegnący równolegle kabel telekomunikacyjny[11]. Premier Finlandii Petteri Orpo poinformował opinię publiczną, że uszkodzenie było celowe i można je uznać za działania hybrydowe[12].

W grudniu 2024 r. został naruszony podmorski kabel energetyczno-telekomunikacyjny EstLink 2, który łączy Estonię i Finlandię. Jak podała fińska policja, doszło do tego w wyniku przeciągnięcia kotwicy przez statek Eagle S należący do rosyjskiej floty cieni. Incydent był przedmiotem dochodzenia z udziałem służb wywiadowczych i został zakwalifikowany jako działanie mogące zagrażać bezpieczeństwu IK[13].

Coraz częściej w rejonie Bałtyku obserwuje się również zakłócenia sygnału GPS i AIS (automatic identification system – system automatycznej identyfikacji jednostek), zwłaszcza w okolicach Gotlandii, norweskiego Finnmarku oraz Zatoki Fińskiej[14]. Zakłócenia te, wywoływane najprawdopodobniej przez systemy walki radioelektronicznej, mają bezpośredni wpływ na bezpieczeństwo nawigacji cywilnej i wojskowej.

W literaturze przedmiotu dotyczącej bezpieczeństwa morskiego oraz ochrony morskiej IK do klasyfikacji zagrożeń coraz częściej stosuje się podejście domenowe[15]. Pozwala to na precyzyjniejsze powiązanie charakteru zagrożenia z adekwatnymi środkami detekcji, ochrony i reagowania. W odniesieniu do OWFs zagrożenia

---

[10] J. Henley, *'Gross sabotage': traces of explosives found at sites of Nord Stream gas leaks*, The Guardian, 18 XI 2022 r., https://www.theguardian.com/world/2022/nov/18/gross-sabotage-traces-of-explosives-found-at-sites-of-nord-stream-gas-leaks [dostęp: 19 VI 2025].

[11] *Finnish media: Balticconnector pipeline leak 'does not appear to be an accident'*, ERR News, 10 X 2023 r., https://news.err.ee/1609127993/finnish-media-balticconnector-pipeline-leak-does-not-appear-to-be-an-accident [dostęp: 19 VI 2025].

[12] *Finland blames Chinese ship for Baltic Sea gas pipeline damage*, Euronews, 25 X 2023 r., https://www.euronews.com/2023/10/25/finland-blames-chinese-ship-for-baltic-sea-gas-pipeline-damage [dostęp: 19 VI 2025].

[13] C. Smith, *Finland investigates Russia's 'shadow fleet' ship after cable damage*, BBC, 26 XII 2024 r., https://www.bbc.com/news/articles/cr56l7prj2mo [dostęp: 19 VI 2025].

[14] *Zakłócenia systemu GPS na Bałtyku utrzymują się od ponad 60 dni*, Portal Morski, 18 I 2025 r., https://www.portalmorski.pl/bezpieczenstwo/57341-zaklocenia-systemu-gps-na-baltyku-utrzymuja-sie-od-ponad-60-dni [dostęp: 19 VI 2025].

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

hybrydowe należy analizować nie jako jednorodne „formy", ale jako działania realizowane w odrębnych, lecz przenikających się domenach operacyjnych.

Domeny nawodnej dotyczą zagrożenia o charakterze fizycznym, obejmujące m.in. sabotaż jednostek serwisowych, celowe kolizje statków z elementami infrastruktury OWFs, nieautoryzowaną obecność jednostek w strefach bezpieczeństwa czy działania realizowane z wykorzystaniem floty cieni[16]. Z perspektywy bezpieczeństwa operacyjnego domena ta jest szczególnie istotna w czasie eksploatacji OWFs.

Domena podwodna obejmuje działania skierowane przeciwko infrastrukturze ukrytej pod powierzchnią morza, zwłaszcza kablom eksportowym służącym do przesyłu energii (export cables) i kablom wewnętrznym (array cables) oraz światłowodom telekomunikacyjnym. W literaturze wskazuje się, że działania w tej domenie charakteryzują się wysokim progiem wykrywalności, asymetrią kosztów oraz trudnością z jednoznacznym przypisaniem sprawstwa. Jest to zatem szczególnie użyteczne narzędzie oddziaływań hybrydowych[17].

W domenie cybernetycznej zagrożenia dotyczą przede wszystkim ataków na systemy SCADA/OT, systemy zarządzania energią oraz infrastrukturę IT operatorów OWFs. Cyberataki mogą prowadzić zarówno do zakłóceń operacyjnych, jak i do naruszenia bezpieczeństwa fizycznego farm przez ingerencję w systemy monitoringu, pozycjonowania czy sterowania turbinami wiatrowymi.

Domena informacyjna obejmuje działania dezinformacyjne i operacje wpływu, których celem jest zmniejszenie poziomu społecznej akceptacji dla OWFs, kwestionowanie ich bezpieczeństwa i opłacalności oraz eksponowanie negatywnego wpływu tych farm na środowisko morskie. Działania te mogą pośrednio wpływać na decyzje regulacyjne, inwestycyjne oraz tempo rozwoju sektora morskiej energetyki wiatrowej[18].

W domenie radioelektronicznej są identyfikowane zagrożenia polegające na zakłócaniu sygnałów GNSS (global navigation satellite system), łączności morskiej oraz systemów nawigacyjnych wykorzystywanych przez jednostki serwisowe i systemy autonomiczne[19]. Zakłócenia te mogą stanowić element przygotowania lub wsparcia działań fizycznych i podmorskich.

Domenowe ujęcie zagrożeń, obecne w nowszych analizach dotyczących bezpieczeństwa morskiego i energetycznego, pozwala na odejście od uproszczonego

[16] M. Piekarski, *Ochrona infrastruktury krytycznej na polskich obszarach morskich w kontekście zagrożeń hybrydowych*, „Ekspertyzy PTBN" 2023, nr 1.

[17] Tamże.

[18] R. Miętkiewicz, *Morskie farmy wiatrowe. Architektura ochrony z wykorzystaniem technologii bezzałogowych*, „Gospodarka Materiałowa i Logistyka" 2017, nr 12, s. 688–702.

[19] Tamże.

podziału na „formy zagrożeń" na rzecz systemowej analizy wielodomenowej, lepiej odpowiadającej charakterowi zagrożeń hybrydowych wobec OWFs.

Zdaniem wiceadmirała Didiera Maleterre'a z NATO Allied Maritime Command przestrzeń Morza Bałtyckiego stała się nową areną działań destabilizacyjnych, w której celem jest nie tylko sprzęt, lecz także cała zdolność państw do skutecznego reagowania[20]. Skala, częstotliwość i złożoność tych incydentów świadczą o konieczności adaptacji narodowych strategii ochrony infrastruktury do realiów szarej strefy i uwzględnienia OWFs jako potencjalnych celów.

Analiza luk w systemie ochrony infrastruktury krytycznej w Polsce

Polski system ochrony IK, mimo rozwoju legislacyjnego, nie nadąża za specyfiką zagrożeń hybrydowych wobec obiektów offshore, w tym OWFs. *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym* oraz *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* tworzą ramy formalne dla ochrony IK, ale OWFs nie zostały jednoznacznie sklasyfikowane jako IK o znaczeniu strategicznym. W *Polityce energetycznej Polski do 2040 roku* (PEP2040) wskazano OWFs jako kluczowy element transformacji energetycznej i bezpieczeństwa dostaw, ale dokument nie zawiera opisu procedur i mechanizmów ochrony przeznaczonych dla infrastruktury offshore[21].

Brak precyzyjnych przepisów skutkuje niejasnym podziałem kompetencji międzyresortowych. Nie wskazano wyraźnie, które instytucje odpowiadają za prewencję, monitoring i reagowanie na zagrożenia wobec OWFs. Formalnie zadania z zakresu ochrony IK realizują Agencja Bezpieczeństwa Wewnętrznego, Straż Graniczna, Marynarka Wojenna RP oraz Centrum Operacyjne Ministra Obrony Narodowej, ale nie istnieje zintegrowany mechanizm koordynacji między tymi podmiotami. Sytuację dodatkowo komplikuje brak jednoznacznych wytycznych dla operatorów OWFs co do obowiązków informacyjnych i współpracy z państwowymi centrami zarządzania kryzysowego (Rządowym Centrum Bezpieczeństwa, CERT Polska, CSIRT MON)[22].

---

[20] M. Bryant, *Undersea 'hybrid warfare' threatens security of 1bn, NATO commander warns*, The Guardian, 16 IV 2024 r., https://www.theguardian.com/world/2024/apr/16/undersea-hybrid-warfare-threatens-security-of-1bn-nato-commander-warns [dostęp: 19 VI 2025].

[21] Ministerstwo Klimatu i Środowiska, *Polityka energetyczna Polski do 2040 r…*

[22] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych…*

W raporcie przygotowanym przez Europejskie Centrum Doskonałości ds. Przeciwdziałania Zagrożeniom Hybrydowym (European Centre of Excellence for Countering Hybrid Threats) zostały wskazane poważne luki w zakresie testowania odporności infrastruktury offshore na działania hybrydowe. Przepisy krajowe nie przewidują obowiązku prowadzenia regularnych ćwiczeń z udziałem operatorów OWFs, służb porządkowych i struktur wojskowych. Nie stosuje się również narzędzi takich jak red teaming czy realistyczne symulacje digital twin, które pozwoliłyby na ocenę odporności technicznej i organizacyjnej OWFs w warunkach zakłóceń fizycznych, cybernetycznych czy działań dezinformacyjnych[23].

Kolejnym obszarem problemowym jest niewystarczające dostosowanie do warunków morskich przepisów dotyczących fizycznej ochrony IK. Obowiązujące regulacje opierają się na modelu ochrony infrastruktury lądowej, co powoduje trudności we wdrażaniu systemów zabezpieczeń w środowisku morskim (np. patrolowanie akwenów, instalacja detektorów akustycznych, integracja radarowa)[24]. Brakuje również zharmonizowanych procedur ochrony kabli energetycznych i fundamentów obiektów IK. Istnieją jednak zasady tworzenia systemów ochrony stacji transformatorowych i linii kablowych zawarte w *Rozporządzeniu Ministra Klimatu i Środowiska z dnia 25 maja 2022 r. w sprawie szczegółowych wymagań dla elementów zespołu urządzeń służących do wyprowadzenia mocy oraz dla elementów stacji elektroenergetycznych zlokalizowanych na morzu*.

W zakresie cyberbezpieczeństwa brakuje spójności. Według ustaleń Najwyższej Izby Kontroli wiele jednostek samorządowych i operatorów energetycznych nie posiada zaktualizowanych planów reagowania na cyberincydenty ani nie wdraża standardów pokrewnych do tych zawartych w dyrektywie Parlamentu Europejskiego i Rady (UE) 2022/2555 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa (dalej: dyrektywa NIS 2)[25] oraz w normie PN-EN ISO/IEC 27001 dotyczącej Systemu Zarządzania Bezpieczeństwem Informacji[26]. Chociaż niektórzy operatorzy OWFs działający w Polsce (np. Ørsted, Equinor) implementują dobre praktyki zaczerpnięte ze skandynawskich rynków, to nie istnieje narodowy standard cyberbezpieczeństwa przeznaczony dla infrastruktury offshore.

---

[23] A. Sari, *Protecting maritime infrastructure from hybrid threats*…

[24] A. Ávila-Zúñiga-Nordfjeld, *Coping with Sabotage and Seabed Security Threats*…

[25] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2)*, s. 80–152.

[26] Najwyższa Izba Kontroli, *Informacja o wynikach kontroli. Zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w jednostkach samorządu terytorialnego*, https://www.nik.gov.pl/plik/id,30641,vp,33700.pdf [dostęp: 20 VI 2025].

Ze strategicznego punktu widzenia główną lukę stanowi brak kompleksowej, międzyresortowej strategii ochrony infrastruktury morskiej jako całości. Obecne dokumenty strategiczne, w tym *Krajowy Plan Zarządzania Kryzysowego* (KPZK)[27] czy *Doktryna cyberbezpieczeństwa RP*[28], nie uwzględniają specyfiki OWFs jako obiektów o podwójnej wrażliwości – energetycznej i morskiej. Ochrona OWFs wymaga podejścia multidomenowego, obejmującego komponenty militarne (ochrona przed sabotażem), informatyczne (ochrona cyber), instytucjonalne (koordynacja) i inżynieryjne (zaawansowanie techniczne). Należy nadmienić, że w Narodowym Programie Ochrony Infrastruktury Krytycznej 2023 uwzględniono działania techniczne, prowadzone głównie przez Rządowe Centrum Bezpieczeństwa i operatorów IK (w tym przypadku OWFs). Obejmują one: tworzenie grup roboczych i opracowanie standardów bezpieczeństwa IK, identyfikację i weryfikację skuteczności tychże, stworzenie bazy incydentów, do których doszło na obiektach IK, oraz platform szkoleniowych dla operatorów IK i administracji[29].

Istotnym kontekstem dla oceny skuteczności krajowego systemu ochrony OWFs jako IK są zmiany w prawie UE wynikające z dyrektywy CER oraz jej relacji z dyrektywą NIS 2.

Dyrektywa CER wprowadza fundamentalną zmianę w podejściu do ochrony IK polegającą na odejściu od modelu ochrony „obiektów" na rzecz identyfikacji i regulacji podmiotów krytycznych, w tym podmiotów o szczególnym znaczeniu dla Europy. Nakłada ona na te podmioty szereg publicznoprawnych obowiązków, obejmujących m.in.: przeprowadzanie regularnych ocen ryzyka, wdrażanie środków technicznych i organizacyjnych służących zapewnieniu odporności, obowiązek zgłaszania incydentów oraz poddanie się nadzorowi właściwych organów, które są wyposażone w instrumenty sankcyjne.

Dyrektywa NIS 2 przewiduje, że podmioty zidentyfikowane na gruncie dyrektywy CER jako mające charakter krytyczny powinny być uznane za podmioty kluczowe również w rozumieniu przepisów o cyberbezpieczeństwie, co wynika z art. 2 ust. 3 dyrektywy NIS 2.

Mechanizm „automatycznego" objęcia OWFs podwójnym reżimem regulacyjnym rodzi ryzyko kolizji normatywnych oraz rozproszenia odpowiedzialności instytucjonalnej w procesie implementacji obu dyrektyw do polskiego porządku

---

[27] Rządowe Centrum Bezpieczeństwa, *Krajowy Plan Zarządzania Kryzysowego 2025*, https://www.gov.pl/attachment/144aa524-8499-4bfb-9a25-0093184aa889 [dostęp: 20 VII 2025].

[28] Biuro Bezpieczeństwa Narodowego, *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf [dostęp: 20 VI 2025].

[29] Rządowe Centrum Bezpieczeństwa, *Narodowy Program Ochrony Infrastruktury Krytycznej 2023 – tekst jednolity*, Warszawa 2023.

prawnego. W tym kontekście zasadne wydaje się rozważenie spójnego modelu nadzoru i reagowania, w tym ustanowienia wyspecjalizowanych struktur sektorowych, takich jak CSIRT ENERGY (Computer Security Incident Response Team for the Energy Sector), zdolnych do obsługi specyfiki energetycznej infrastruktury offshore.

Dodatkowym problemem jest czas implementacji przepisów. Termin transpozycji dyrektywy CER upłynął 17 października 2024 r., a nowelizacja ustawy o zarządzaniu kryzysowym oraz wydania aktów wykonawczych nadal jest w toku. Eksploatacja pierwszych OWFs na polskich obszarach Morza Bałtyckiego ma się rozpocząć w 2026 r. W okresie przejściowym infrastruktura ta może zatem funkcjonować w stanie regulacyjnego zawieszenia i być objęta instrumentami ochrony niedostosowanymi do realiów sektora offshore. Uzasadnione jest zatem pytanie, czy projektowane rozwiązania legislacyjne będą stanowiły skuteczny i koherentny instrument budowania odporności na zagrożenia hybrydowe, czy też ujawnią się kolejne luki systemowe w momencie uruchamiania OWFs.

Przykłady dobrych praktyk na poziomach krajowym i międzynarodowym

W odpowiedzi na rosnące zagrożenia hybrydowe wobec infrastruktury morskiej państwa NATO i UE rozwijają wieloaspektowe modele ochrony, łączące działania wojskowe, cywilne i techniczne. Szczególne znaczenie mają doświadczenia państw o rozwiniętym sektorze offshore – Wielkiej Brytanii, Holandii oraz państw nordyckich, które wypracowały nowoczesne instrumenty reagowania i prewencji.

Na poziomie sojuszniczym NATO rozwija koncepcję Baltic Sentry[30] – wspólnego systemu patrolowania i rozpoznania IK na Morzu Bałtyckim. Program ten zakłada integrację działań sił państw nadmorskich oraz współdzielenie danych pomiędzy strukturami NATO, operatorami prywatnymi oraz cywilnymi instytucjami odpowiedzialnymi za ochronę IK. Istotnym elementem Baltic Sentry jest wykorzystanie zaawansowanych narzędzi analitycznych, w tym systemów opartych na sztucznej inteligencji, służących do wykrywania anomalii w ruchu morskim, identyfikacji nietypowych wzorców zachowań jednostek oraz wczesnego ostrzegania przed potencjalnymi działaniami hybrydowymi. Rozwiązania te są rozwijane i wykorzystywane m.in. w ramach struktur NATO Allied Maritime Command (MARCOM) i obejmują swoim zakresem operacyjnym również Morze Bałtyckie.

[30] *NATO launches 'Baltic Sentry' to increase critical infrastructure security*, NATO, 14 I 2025 r., https://www.nato.int/en/news-and-events/articles/news/2025/01/14/nato-launches-baltic-sentry-to-increase-critical-infrastructure-security [dostęp: 6 I 2026].

W ramach Baltic Sentry są prowadzone wspólne ćwiczenia oraz rozwijane zdolności podwodne i bezzałogowe. Uzupełnieniem tych działań jest uruchomienie wyspecjalizowanego Morskiego Centrum Bezpieczeństwa ds. Krytycznej Infrastruktury Podwodnej (Maritime Centre for Security of Critical Undersea Infrastructure)[31], którego zadaniem jest koordynacja analiz, wymiana informacji oraz wsparcie państw sojuszniczych w zakresie ochrony podmorskiej IK.

Unia Europejska, uzupełniając działania wojskowe, rozwija platformę CISE (Common Information Sharing Environment). System ten umożliwia współdzielenie danych między strażami granicznymi, służbami ochrony środowiska, jednostkami służb ratownictwa morskiego (search and rescue, SAR), a także prywatnymi operatorami infrastruktury morskiej. Docelowo CISE ma zwiększyć tzw. świadomość sytuacyjną na morzu (maritime situational awareness) w czasie pokoju, kryzysu i konfliktu[32].

Dobrą praktyką jest również model partnerstwa publiczno-prywatnego stosowany w Holandii i Norwegii. Operatorzy OWFs współpracują z siłami zbrojnymi i agencjami rządowymi przy tworzeniu wspólnych procedur zarządzania ryzykiem, reagowania na incydenty oraz testowania odporności fizycznej i cybernetycznej farm. Specjaliści z brytyjskiej organizacji non profit Carbon Trust oraz z firmy konsultingowej ABPmer opracowali szereg standardów technicznych i wytycznych dla operatorów, m.in. w zakresie zabezpieczeń kabli, fundamentów i systemów SCADA[33].

Wyróżniającym się podejściem jest również implementacja zasady „defence by design", czyli projektowania infrastruktury offshore z uwzględnieniem odporności na działania hybrydowe. Oznacza to np. instalowanie redundantnych systemów zasilania i transmisji danych, lokalizowanie punktów wrażliwych pod poziomem dna morskiego oraz fizyczne separowanie systemów krytycznych.

Wielka Brytania, jako jedno z pierwszych państw, uruchomiła specjalną jednostkę do ochrony infrastruktury podmorskiej. W 2023 r. Marynarka Królewska wprowadziła do służby w Królewskiej Flocie Pomocniczej (Royal Fleet Auxiliary) okręt Proteus w ramach programu MROSS (Multi-Role Ocean Surveillance Ship). Jednostka ta została wyposażona w systemy sonarowe, podwodne drony oraz

[31] *NATO officially launches new Maritime Centre for Security of Critical Undersea Infrastructure*, MARCOM NATO, 28 V 2024 r., https://mc.nato.int/media-centre/news/2024/nato-officially-launches-new-nmcscui [dostęp: 6 I 2026].

[32] *Common information sharing environment (CISE)*, European Commission – Oceans and Fisheries, https://oceans-and-fisheries.ec.europa.eu/ocean/blue-economy/other-sectors/common-information-sharing-environment-cise_en [dostęp: 20 VI 2025].

[33] *Industry leaders agree best practice for protecting offshore wind cables*, Carbon Trust, 13 XI 2024 r., https://www.carbontrust.com/news-and-insights/news/industry-leaders-agree-best-practice-for-protecting-offshore-wind-cables [dostęp: 20 VI 2025].

centrum analiz danych, które umożliwiają monitorowanie kabli i OWFs w czasie rzeczywistym[34].

Dania wdraża z kolei innowacyjne systemy opierające się na technologii autonomicznej. Testowane są platformy Saildrone Voyager – bezzałogowe jednostki pływające z napędem żaglowym, zdolne do wielotygodniowego monitorowania wybranych obiektów na Bałtyku. Urządzenia te są wyposażone w sensory meteorologiczne, radar, kamery termowizyjne i zestawy do AIS[35].

Z międzynarodowych doświadczeń wynika, że skuteczna ochrona OWFs nie może ograniczać się do zabezpieczeń fizycznych i cyfrowych, ale musi być częścią zintegrowanego, międzysektorowego systemu reagowania. Niektóre państwa nadbałtyckie (Estonia, Finlandia i Szwecja) wdrażają aktualnie modele narodowe, które integrują straż przybrzeżną, służby wywiadowcze, operatorów sieci energetycznej oraz wojsko. Model ten może stanowić inspirację dla Polski, zwłaszcza w kontekście braku klarownych procesów koordynacyjnych.

W wymiarze operacyjnym w Polsce są rozwijane również inicjatywy ukierunkowane na cyfrowe wsparcie monitoringu i ochrony infrastruktury morskiej w regionie Morza Bałtyckiego, w tym programy określane roboczo jako Digital Baltic[36]. Ich celem jest integracja danych pochodzących z systemów nadzoru morskiego, sensorów technicznych oraz źródeł operatorów w celu zwiększenia świadomości sytuacyjnej na morzu. Inicjatywy te wpisują się w szerszy trend wykorzystania narzędzi cyfrowych i analitycznych do wczesnego wykrywania anomalii oraz wspierania procesów decyzyjnych w czasie pokoju i kryzysu[37]. Istotną rolę w systemie ochrony infrastruktury morskiej odgrywa Morski Oddział Straży Granicznej (MOSG)[38], którego zadania obejmują m.in. ochronę polskiej granicy morskiej, zapewnienie bezpieczeństwa żeglugi oraz reagowanie na incydenty w pasie morza terytorialnego, gdzie są zlokalizowane newralgiczne elementy infrastruktury, w tym odcinki linii eksportowych OWFs. Włączenie MOSG w model ochrony OWFs stanowi

[34] *RFA Proteus (K60)*, Royal Navy, https://www.royalnavy.mod.uk/organisation/units-and-squadrons/support-ships/rfa-proteus [dostęp: 20 VI 2025].

[35] *Saildrone Launches the Future of Maritime Surveillance in the Baltic Sea*, Saildrone, 16 VI 2025 r., https://www.saildrone.com/news/saildrone-launches-the-future-of-maritime-surveillance-in-the-baltic-sea [dostęp: 20 VI 2025].

[36] Digital Baltic, https://digitalbaltic.pl [dostęp: 7 I 2026].

[37] 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. 71–76.

[38] *Zadania Morskiego Oddziału Straży Granicznej*, Straż Graniczna – Morski Oddział Straży Granicznej, 5 X 2012 r., https://www.morski.strazgraniczna.pl/mor/komenda/zadania/1636,Zadania.html [dostęp: 7 I 2026].

kluczowy element pozamilitarnego komponentu bezpieczeństwa, uzupełniającego działania sił zbrojnych i struktur sojuszniczych, zwłaszcza w zakresie bieżącego monitoringu, kontroli ruchu morskiego oraz współpracy z operatorami IK.

Rekomendacje strategiczne, organizacyjne i technologiczne

W Polsce konieczne są zdecydowane działania na poziomie legislacyjnym i operacyjnym, aby zapewnić OWFs skuteczną ochronę. Doświadczenia państw nadmorskich wskazują, że wymaga to współdziałania instytucji publicznych, sektora prywatnego (operatorów) i sił zbrojnych. Proponowane rekomendacje strategiczne, organizacyjne i technologiczne wynikają z takiego zintegrowanego podejścia do bezpieczeństwa IK.

Rekomendacje strategiczne

1. Ustawowe uznanie OWFs za IK – konieczne jest doprecyzowanie statusu OWFs w polskim systemie prawnym przez włączenie ich do wykazu sektorów IK, zgodnie z dyrektywą CER oraz zaktualizowaną PEP2040.
2. Opracowanie narodowej strategii ochrony infrastruktury offshore – strategia ta powinna integrować komponent militarny i pozamilitarny, obejmujący MOSG, Policję (w tym policję wodną), administrację morską oraz operatorów IK. Szczególną rolę w tym systemie należy przypisać operatorom OWFs zlokalizowanym w wyłącznej strefie ekonomicznej (WSE), którzy – ze względu na stałą obecność operacyjną – są pierwszym ogniwem w zakresie monitorowania IK, wczesnego wykrywania anomalii oraz zgłaszania incydentów o charakterze hybrydowym. Rola operatorów IK w WSE powinna polegać przede wszystkim na: a) utrzymywaniu systemów monitoringu technicznego i środowiskowego (SCADA, sensory, systemy pozycjonowania i obserwacji), b) zapewnianiu interoperacyjności danych z systemami państwowymi i sojuszniczymi, c) wdrażaniu procedur reagowania na incydenty zgodnych z KPZK, d) uczestniczeniu w ćwiczeniach i testach odporności prowadzonych z udziałem administracji publicznej i sił zbrojnych. Tak zdefiniowana rola operatorów pozwala na uzupełnienie ograniczonej fizycznej obecności państwa w WSE przez model współodpowiedzialności i partnerstwa publiczno-prywatnego, zgodny z rozwiązaniami przyjmowanymi w państwach nordyckich i w ramach NATO.
3. Włączenie OWFs do cyklicznych ćwiczeń obronnych i z zarządzania kryzysowego – OWFs powinny stać się m.in. integralną częścią ćwiczeń

krajowych takich jak IGNIS[39], w ramach testowania odporności na sabotaż fizyczny i ataki cybernetyczne[40].

Rekomendacje organizacyjne

1. Powołanie międzyresortowego zespołu ds. bezpieczeństwa infrastruktury offshore – w skład zespołu powinni wchodzić przedstawiciele Ministerstwa Obrony Narodowej, Agencji Bezpieczeństwa Wewnętrznego, Rządowego Centrum Bezpieczeństwa, Ministerstwa Spraw Wewnętrznych i Administracji, administracji morskiej (urzędy morskie), MOSG, Policji (w tym policji wodnej), a także operatorzy OWFs jako podmioty bezpośrednio odpowiedzialne za eksploatację infrastruktury. Rola administracji morskiej powinna polegać w szczególności na koordynacji działań w zakresie zarządzania ruchem morskim, wyznaczaniu i egzekwowaniu stref bezpieczeństwa oraz na integracji informacji o zagrożeniach z systemami służby VTS (vessel traffic service) i krajową świadomością sytuacyjną na morzu. Operatorzy OWFs powinni być włączeni w prace zespołu nie tylko w charakterze interesariuszy, lecz także jako aktywni uczestnicy procesu planowania, testowania i doskonalenia procedur reagowania na incydenty, w tym przez udział w ćwiczeniach międzyinstytucjonalnych oraz przekazywanie danych operacyjnych do właściwych organów państwowych.
2. Zacieśnienie współpracy cywilno-wojskowej – wspólne patrole, interoperacyjne centra dowodzenia i wymiana danych (z wykorzystaniem platform takich jak CISE) pozwolą na szybsze wykrywanie i neutralizację zagrożeń.
3. Obowiązkowa integracja operatorów OWFs z systemem KPZK i krajowym systemem cyberbezpieczeństwa – wymaga to rewizji aktów wykonawczych oraz systemu zgłaszania incydentów.

Rekomendacje technologiczne

1. Inwestowanie w bezzałogowe systemy rozpoznawcze[41] (uncrewed surface vehicle, USV; unmanned aerial systems, UAS; unmanned aerial vehicle,

[39] *Krajowe ćwiczenia ratownicze „IGNIS 2025”*, Serwis Rzeczypospolitej Polskiej, 15 X 2025 r., https://www.gov.pl/web/kgpsp/krajowe-cwiczenia-ratownicze-ignis-2025 [dostęp: 20 XI 2025].

[40] Rządowe Centrum Bezpieczeństwa, *Krajowy Plan Zarządzania Kryzysowego 2025*…

[41] R. Miętkiewicz, *Unmanned Surface Vehicles in Maritime Critical Infrastructure Protection Applications – LNG Terminal in Świnoujście*, „Zeszyty Naukowe Akademii Marynarki Wojennej” 2018, t. 213, nr 2, s. 43–51. https://doi.org/10.2478/sjpna-2018-0012.

UAV) – do ochrony OWFs należy wykorzystać autonomiczne platformy patrolowe (takie jak Saildrone), które zapewnią całodobowy nadzór obszaru morskiego i wczesne wykrywanie nieautoryzowanej aktywności.
2. Zastosowanie systemów sensorycznych zgodnie z krajowymi zasadami funkcjonowania OWFs – instalacja radarów, sensorów akustycznych, sonarów pasywnych oraz systemów obserwacji elektrooptycznej powinna być realizowana na podstawie prowadzonych w Polsce analiz oddziaływania OWFs na systemy bezpieczeństwa i obronności państwa, stanowiące element procesu planistycznego i uzgodnieniowego dla inwestycji offshore. Potrzeba implementacji wybranych sensorów została rozpoznana i jest stopniowo uwzględniana w ramach krajowych i sojuszniczych systemów monitoringu przestrzeni morskiej, przy zachowaniu interoperacyjności z istniejącymi rozwiązaniami państwowymi.
3. Budowa odporności cybernetycznej zgodnie ze standardami dyrektywy NIS 2 i normy PN-EN ISO/IEC 27001 – operatorzy OWFs powinni być zobowiązani do wdrażania podlegających kontroli procedur zarządzania incydentami oraz regularnych testów penetracyjnych i red teaming, czyli sprawdzania całościowej odporności organizacji na zagrożenie od poziomu technologii po procedury.

Podsumowanie i kierunki dalszych badań

Morskie farmy wiatrowe zyskują status infrastruktury strategicznej nie tylko z punktu widzenia ekologii, ekonomii i gospodarki, lecz także jako potencjalne cele operacji hybrydowych i aktywności w szarej strefie. W obliczu rosnących napięć w regionie Morza Bałtyckiego stają się one nowym polem rywalizacji – obejmującym działania fizyczne, cybernetyczne i informacyjne prowadzone poniżej progu otwartego konfliktu i zacierające granicę pomiędzy stanem wojny a stanem pokoju.

Polska, aspirując do roli regionalnego lidera sektora OZE, znajduje się w bardzo ważnym momencie. Dzięki zastosowaniu zintegrowanego, wielowarstwowego podejścia – obejmującego regulacje prawne, interoperacyjne działania cywilno-wojskowe, cyberodporność, rozpoznanie techniczne oraz współpracę międzynarodową i sektorową – może stać się przykładem skutecznej ochrony infrastruktury morskiej przed zagrożeniami hybrydowymi.

Kierunki dalszych badań powinny obejmować:

1. Modelowanie ryzyka hybrydowego z wykorzystaniem symulacji digital twin[42] – należy je traktować jako narzędzie uzupełniające procesy identyfikacji i szacowania ryzyka realizowane przez operatorów OWFs na etapie planowania, budowy i eksploatacji infrastruktury. Zgodnie z wymogami regulacyjnymi i dobrymi praktykami sektora offshore operatorzy OWFs prowadzą analizy ryzyka obejmujące zagrożenia techniczne, środowiskowe i operacyjne[43]. Zastosowanie digital twin nie zastępuje tych działań, pozwala natomiast na ich pogłębienie oraz analizę zależności pomiędzy różnymi kategoriami zagrożeń, m.in. fizycznych, cybernetycznych i informacyjnych. Stworzenie wirtualnego odpowiednika OWF umożliwia testowanie odporności infrastruktury na złożone, wielodomenowe scenariusze zagrożeń w kontrolowanym środowisku symulacyjnym, bez ingerencji w funkcjonowanie rzeczywistych obiektów. Narzędzie to pozwoli na ocenę skutków skumulowanych oddziaływań, takich jak zakłócenia elektroenergetyczne, ingerencje w systemy SCADA/OT czy działania informacyjne wpływające na procesy decyzyjne. Podejście to znajduje już praktyczne zastosowanie w sektorze offshore, przede wszystkim w państwach nordyckich, jako element wsparcia decyzji operacyjnych i planowania zabezpieczeń infrastruktury morskiej[44].
2. Projektowanie i przeprowadzanie ćwiczeń red teaming – wdrażanie realistycznych scenariuszy ataku (fizycznych, cybernetycznych, socjotechnicznych) umożliwia rzetelną ocenę gotowości operatorów OWFs oraz instytucji państwowych, co jest niezbędne do poprawienia procedur reagowania na naruszenia infrastruktury.
3. Analizę włączenia sektora prywatnego do koordynacji reagowania na zagrożenia – dalsze badania powinny koncentrować się na określeniu miejsca operatorów OWFs w wielopoziomowej architekturze reagowania, w której operator odpowiada za poziomy operacyjny i techniczny (detekcja, wstępna ocena incydentu, zabezpieczenie ciągłości działania), a koordynacja reagowania kryzysowego oraz decyzje o charakterze strategicznym pozostają w gestii właściwych organów państwowych i struktur

[42] G. Faiz, *Leveraging a network of safe, integrated digital twins to address the energy challenge*, DNV, https://www.dnv.com/article/leveraging-a-network-of-safe-integrated-digital-twins/ [dostęp: 7 I 2026].

[43] *Energy Transition Outlook 2025*…

[44] T. Russell, *Carbon Trust launches the next stage of the Offshore Wind Accelerator*, TGS 4C Offshore, 27 X 2020 r., https://www.4coffshore.com/news/carbon-trust-launches-the-next-stage-of-offshore-wind-accelerator-nid19386.html [dostęp: 7 I 2026].

sojuszniczych[45]. Takie przypisanie ról jest spójne z podejściem przyjmowanym w dokumentach NATO i UE oraz z praktyką w sektorze offshore, w ramach której operatorzy pełnią funkcję pierwszej linii monitoringu i raportowania, a nie podmiotów dowodzących reakcją na sytuację kryzysową[46].

4. Rozwój i ocenę krajowych technologii na potrzeby bezpieczeństwa OWFs – należy skupić się na identyfikacji i ocenie potencjału krajowych technologii podwójnego zastosowania (dual-use), które mogą zostać wykorzystane do ochrony OWFs, w szczególności w obszarze systemów sensorowych, bezzałogowych platform morskich i powietrznych, analityki danych oraz cyberbezpieczeństwa infrastruktury offshore[47]. Istotnymi kierunkami badań są: analiza wpływu rozwoju i wdrażania krajowych technologii na zwiększenie odporności systemowej OWFs, ograniczenie zależności technologii od systemów wrażliwych na ataki oraz poprawa kontroli państwa nad kluczowymi elementami systemu bezpieczeństwa[48]. Badania powinny obejmować również ocenę mechanizmów integracji krajowych rozwiązań technologicznych z systemami państwowymi i sojuszniczymi, w tym UE i NATO, a także analizę barier prawnych, organizacyjnych i finansowych ograniczających implementację tych rozwiązań w środowisku offshore[49].

Bibliografia

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

Miętkiewicz R., *Morskie farmy wiatrowe. Architektura ochrony z wykorzystaniem technologii bezzałogowych*, „Gospodarka Materiałowa i Logistyka" 2017, nr 12, s. 688–702.

[45] *Energy Transition Outlook 2025*…

[46] *Industry leaders agree best practice*…; A. Sari, *Protecting maritime infrastructure from hybrid threats*…

[47] Rządowe Centrum Bezpieczeństwa, *Krajowy Plan Zarządzania Kryzysowego 2025*…; P. Mickiewicz, *Bezpieczeństwo energetyczne czy bezpieczeństwo morskie?*…

[48] Tamże.

[49] *Common information sharing environment (CISE)*…

Miętkiewicz R., *Unmanned Surface Vehicles in Maritime Critical Infrastructure Protection Applications – LNG Terminal in Świnoujście*, „Zeszyty Naukowe Akademii Marynarki Wojennej" 2018, t. 213, nr 2, s. 43–51. https://doi.org/10.2478/sjpna-2018-0012.

Piekarski M., *Ochrona infrastruktury krytycznej na polskich obszarach morskich w kontekście zagrożeń hybrydowych*, „Ekspertyzy PTBN" 2023, nr 1.

Szubrycht T., *Sojusznicza odpowiedź na zagrożenia na Morzu Bałtyckim*, „Bezpieczeństwo Narodowe" 2025, t. 46, nr 1, s. 49–75. https://doi.org/10.59800/bn/207646.

Źródła internetowe

Ávila-Zúñiga-Nordfjeld A., *Coping with Sabotage and Seabed Security Threats in the Baltic Sea: a Regional Maritime Security Policy*, https://hcss.nl/report/coping-with-sabotage-seabed-security-threats-baltic-sea/ [dostęp: 20 VI 2025].

Bryant M., *Undersea 'hybrid warfare' threatens security of 1bn, NATO commander warns*, The Guardian, 16 IV 2024 r., https://www.theguardian.com/world/2024/apr/16/undersea-hybrid-warfare-threatens-security-of-1bn-nato-commander-warns [dostęp: 19 VI 2025].

Cavcic M., *Hybrid warfare paints 'gray zone' targets on shipping and offshore energy infrastructure*, Offshore Energy, 11 XII 2024 r., https://www.offshore-energy.biz/hybrid-warfare-paints-gray-zone-targets-on-shipping-and-offshore-energy-infrastructure/ [dostęp: 19 VI 2025].

Common information sharing environment (CISE), European Commission – Oceans and Fisheries, https://oceans-and-fisheries.ec.europa.eu/ocean/blue-economy/other-sectors/common-information-sharing-environment-cise_en [dostęp: 20 VI 2025].

Countering hybrid threats, NATO, 7 V 2024 r., https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats [dostęp: 20 VI 2025].

Digital Baltic, https://digitalbaltic.pl [dostęp: 7 I 2026].

Energy Transition Outlook 2025, https://brandcentral.dnv.com/original/gallery/10651/files/original/ec419166-9ecc-40ef-9997-93a6ccb72335.pdf [dostęp: 20 VI 2025].

Faiz G., *Leveraging a network of safe, integrated digital twins to address the energy challenge*, DNV, https://www.dnv.com/article/leveraging-a-network-of-safe-integrated-digital-twins/ [dostęp: 7 I 2026].

Finland blames Chinese ship for Baltic Sea gas pipeline damage, Euronews, 25 X 2023 r., https://www.euronews.com/2023/10/25/finland-blames-chinese-ship-for-baltic-sea-gas-pipeline-damage [dostęp: 19 VI 2025].

Finnish media: Balticconnector pipeline leak 'does not appear to be an accident', ERR News, 10 X 2023 r., https://news.err.ee/1609127993/finnish-media-balticconnector-pipeline-leak-does-not-appear-to-be-an-accident [dostęp: 19 VI 2025].

Henley J., '*Gross sabotage': traces of explosives found at sites of Nord Stream gas leaks*, The Guardian, 18 XI 2022 r., https://www.theguardian.com/world/2022/nov/18/gross-sabotage-traces-of-explosives-found-at-sites-of-nord-stream-gas-leaks [dostęp: 19 VI 2025].

Industry leaders agree best practice for protecting offshore wind cables, Carbon Trust, 13 XI 2024 r., https://www.carbontrust.com/news-and-insights/news/industry-leaders-agree-best-practice-for-protecting-offshore-wind-cables [dostęp: 20 VI 2025].

Krajowe ćwiczenia ratownicze „IGNIS 2025", Serwis Rzeczypospolitej Polskiej, 15 X 2025 r., https://www.gov.pl/web/kgpsp/krajowe-cwiczenia-ratownicze-ignis-2025 [dostęp: 20 XI 2025].

NATO launches 'Baltic Sentry' to increase critical infrastructure security, NATO, 14 I 2025 r., https://www.nato.int/en/news-and-events/articles/news/2025/01/14/nato-launches-baltic-sentry-to-increase-critical-infrastructure-security [dostęp: 6 I 2026].

NATO officially launches new Maritime Centre for Security of Critical Undersea Infrastructure, MARCOM NATO, 28 V 2024 r., https://mc.nato.int/media-centre/news/2024/nato-officially-launches-new-nmcscui [dostęp: 6 I 2026].

RFA Proteus (K60), Royal Navy, https://www.royalnavy.mod.uk/organisation/units-and-squadrons/support-ships/rfa-proteus [dostęp: 20 VI 2025].

Russell T., *Carbon Trust launches the next stage of the Offshore Wind Accelerator*, TGS 4C Offshore, 27 X 2020 r., https://www.4coffshore.com/news/carbon-trust-launches-the-next-stage-of-offshore-wind-accelerator-nid19386.html [dostęp: 7 I 2026].

Saildrone Launches the Future of Maritime Surveillance in the Baltic Sea, Saildrone, 16 VI 2025 r., https://www.saildrone.com/news/saildrone-launches-the-future-of-maritime-surveillance-in-the-baltic-sea [dostęp: 20 VI 2025].

Sari A., *Protecting maritime infrastructure from hybrid threats: legal options*, https://www.hybridcoe.fi/wp-content/uploads/2025/03/20250306-Hybrid-CoE-Research-Report-14-web.pdf [dostęp: 20 VI 2025].

Smith C., *Finland investigates Russia's 'shadow fleet' ship after cable damage*, BBC, 26 XII 2024 r., https://www.bbc.com/news/articles/cr56l7prj2mo [dostęp: 19 VI 2025].

Zadania Morskiego Oddziału Straży Granicznej, Straż Graniczna – Morski Oddział Straży Granicznej, 5 X 2012 r., https://www.morski.strazgraniczna.pl/mor/komenda/zadania/1636,Zadania.html [dostęp: 7 I 2026].

Zakłócenia systemu GPS na Bałtyku utrzymują się od ponad 60 dni, Portal Morski, 18 I 2025 r., https://www.portalmorski.pl/bezpieczenstwo/57341-zaklocenia-systemu-gps-na-baltyku--utrzymuja-sie-od-ponad-60-dni [dostęp: 19 VI 2025].

Akty prawne

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Dz. Urz. UE L 333 z 27 XII 2022 r.).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) – (Dz. Urz. UE L 333 z 27 XII 2022 r.).

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. DzU z 2026 r. poz. 20).

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. DzU z 2023 r. poz. 122, ze zm.).

Rozporządzenie Ministra Klimatu i Środowiska z dnia 25 maja 2022 r. w sprawie szczegółowych wymagań dla elementów zespołu urządzeń służących do wyprowadzenia mocy oraz dla elementów stacji elektroenergetycznych zlokalizowanych na morzu (DzU z 2022 r. poz. 1257).

Inne dokumenty

Biuro Bezpieczeństwa Narodowego, *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf [dostęp: 20 VI 2025].

Komisja Europejska, *Plan REPowerEU*, COM(2022) 230 final, https://eur-lex.europa.eu/resource.html?uri=cellar:fc930f14-d7ae-11ec-a95f-01aa75ed71a1.0010.02/DOC_1&format=PDF [dostęp: 20 VI 2025].

Ministerstwo Klimatu i Środowiska, *Polityka energetyczna Polski do 2040 r. (PEP2040)*, Warszawa 2021.

Najwyższa Izba Kontroli, *Informacja o wynikach kontroli. Zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w jednostkach samorządu terytorialnego*, https://www.nik.gov.pl/plik/id,30641,vp,33700.pdf [dostęp: 20 VI 2025].

Norma PN-EN ISO/IEC 27001 – Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Systemy zarządzania bezpieczeństwem informacji – Wymagania.

Rządowe Centrum Bezpieczeństwa, *Krajowy Plan Zarządzania Kryzysowego 2025*, https://www.gov.pl/attachment/144aa524-8499-4bfb-9a25-0093184aa889 [dostęp: 20 VII 2025].

Rządowe Centrum Bezpieczeństwa, *Narodowy Program Ochrony Infrastruktury Krytycznej 2023 – tekst jednolity*, Warszawa 2023.

Klaudia Maciata

Specjalistka ds. operacji offshore w sektorze energetyki wiatrowej. Ambasadorka inicjatywy Women Offshore, członkini międzynarodowych projektów z zakresu bezpieczeństwa morskiego i klimatycznego. Ekspertka zajmująca się tematyką ochrony infrastruktury krytycznej przed zagrożeniami hybrydowymi w regionie Morza Bałtyckiego. Autorka publikacji w „NATO Review". Zawodowo związana m.in. z firmą Ørsted, wcześniej pracowała w sektorze usług przemysłowych, technologii bezzałogowych i doradztwa public affairs. Obecnie fundatorka projektu „Baltic Sea Security" i freelancerka.

Kontakt: klaudia.maciata@gmail.com