Internal Security Review
2026, no. 34, pp. 331–350

https://doi.org/10.4467/20801335PBW.26.015.23377

ARTICLE

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

KLAUDIA MACIATA

Gdańsk University of Technology
https://orcid.org/0000-0001-6227-2851

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 terms of hybrid threats. She 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

Introduction

The energy transition towards low-carbon energy sources makes offshore wind farms (OWFs) one of the most important elements of Poland's modern energy security system. Their development is in line with the European Union's climate and energy policy objectives, including achieving climate neutrality by 2050 and increasing the share of renewable energy sources (RES) in the energy mix of Member States[1]. The offshore wind farms being built by Poland in the Baltic Sea are expected to deliver up to 11 GW of installed capacity by 2040, making them the largest infrastructure project in the history of the Polish RES sector[2]. On a European scale, offshore wind energy capacity is projected to grow from around 90 GW in the middle of the decade to around 170 GW by 2030. This means almost doubling the potential of this sector[3].

The growing importance of OWFs as an energy resource poses new challenges in the area of security. This infrastructure, located on the open sea, outside territorial waters and spatially dispersed, is vulnerable to hybrid threats. They include below-the-threshold warfare activities such as sabotage, cyber attacks, navigation disruptions, disinformation operations and others described in the literature on the subject[4]. These actions are aimed not only at testing the resilience of critical infrastructure (CI), but also at exerting strategic and geopolitical pressure below the threshold of armed conflict, generating economic costs, weakening the state's response capabilities, and undermining its credibility as an entity capable of controlling and protecting maritime space.

At EU level, the issue of OWF safety has been regulated in Directive (EU) 2022/2557 of the European Parliament and of the Council on the resilience of critical entities (hereinafter: the CER Directive) that replaced the earlier directive on European CI[5]. The new regulations oblige Member States to identify and protect

---

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

2 Ministerstwo Klimatu i Środowiska (Ministry of Climate and Environment), *Polityka energetyczna Polski do 2040 r. (PEP2040)* (Eng. Poland's energy policy until 2040 (PEP2040)), Warszawa 2021.

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

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

5 *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC*, pp. 164–186.

critical entities in 12 sectors, including in the energy sector, without distinguishing between onshore and offshore infrastructure. The offshore wind farms, as part of the electricity production and transmission network, clearly fall within this scope, and the operators of these installations are required to implement measures to increase their physical and cyber resilience.

In the latest analyses by the Center for Strategic and International Studies think tank and the NATO Strategic Communication Centre of Excellence, OWFs are perceived as so-called soft targets – objectives of high strategic value and relatively low level of protection[6]. Their location far from the coast, dependence on automated control systems (SCADA/OT; supervisory control and data acquisition/operational technology), as well as complex ownership and regulatory structures – including maritime law, which by guaranteeing freedom of navigation facilitates threats by aggressors – make them vulnerable to enemy action in the grey zone. Examples of these threats include the submarine capabilities developed over many years by China and Russia (the Main Directorate of Deep-Sea Research, GUGI) or shadow fleet[7].

The aim of the article is to present OWFs as a new component of CI in Poland and to analyse their resilience in the face of growing hybrid threats. Particular attention is paid to three areas: legal and organisational gaps in the Polish CI protection system, good practices in the protection of OWFs at national and international levels, and recommendations for decision-makers and operators in Poland. The article contributes to the discussion on the need to redefine energy security in the context of competition below the threshold of war as well as the protection of energy resources in the future.

The evolution of hybrid threats since 2022 – case studies

With the start of the Russian Federation's full-scale aggression against Ukraine in February 2022, there has been an increase in the number of hybrid incidents targeting EU and North Atlantic Treaty Organisation countries. Submarine infrastructure, including energy and communication systems in the Baltic Sea region, is increasingly becoming the target of such activities. These activities are

[6] 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/, pp. 5–8 [accessed: 20 VI 2025].

[7] T. Szubrycht, *Sojusznicza odpowiedź na zagrożenia na Morzu Bałtyckim* (Eng. Allied response to threat in the Baltic Sea), "Bezpieczeństwo Narodowe" 2025, vol. 46, no. 1, pp. 49–75. https://doi.org/10.59800/bn/207646.

characterised by low detectability, difficulty in clearly assigning responsibility, and being conducted below the threshold of open armed conflict. In this context, OWFs, which are a strategic source of energy, appear to be a new area of competition in the grey zone[8].

The turning point in the perception of threats to maritime infrastructure was the sabotage of the Nord Stream 1 and Nord Stream 2 gas pipelines in September 2022. The explosions occurred in the territorial waters of Sweden and Denmark, resulting in the permanent shutdown of both pipelines. The Swedish services found traces of explosives and classified the incident as sabotage[9]. Although the perpetrator was not clearly identified, this incident made the public aware that undersea infrastructure could be attacked using means below the threshold of war.

In October 2023, a serious incident occurred involving the Balticconnector gas pipeline connecting Finland and Estonia. The investigation revealed that the pipeline had been cut by the anchor of the Newnew Polar Bear container ship, which also damaged a parallel telecommunications cable[10]. Finnish Prime Minister Petteri Orpo informed the public that the damage was deliberate and could be considered hybrid activities[11].

In December 2024, the EstLink 2 submarine power and telecommunications cable which links Estonia and Finland was damaged. According to the Finnish police, this was caused by the dragging of an anchor by the Eagle S ship belonging to the Russian shadow fleet. The incident was investigated by the intelligence services and classified as an act that could threaten the security of CI[12].

GPS and AIS (automatic identification system) signal interference is also increasingly being observed in the Baltic Sea region, especially around Gotland,

---

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

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

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

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

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

Finnmark in Norway and the Gulf of Finland[13]. These disruptions, most likely caused by radio-electronic warfare systems, have a direct impact on the safety of civil and military navigation.

In the literature on maritime security and protection of maritime CI, a domain-based approach is increasingly being used to classify threats[14]. This allows for a more precise correlation between the nature of the threat and the appropriate detection, protection and response measures. With regard to OWFs, hybrid threats should be analysed not as homogeneous 'forms', but as activities carried out in separate but overlapping operational domains.

The surface domain concerns physical threats, including sabotage of service vessels, deliberate collisions of ships with OWF infrastructure elements, unauthorised presence of vessels in safety zones, and activities carried out using shadow fleets[15]. From an operational safety perspective, this domain is particularly important during the operation of the OWFs.

The underwater domain covers activities targeting infrastructure hidden beneath the sea surface, especially export cables used to transmit energy and array cables as well as telecommunications fibre optics. The literature indicates that activities in this domain are characterised by a high threshold of detectability, asymmetry of costs and difficulty in clearly attributing responsibility. It is therefore a particularly useful tool for hybrid operations[16].

In the cyber domain, threats mainly concern attacks on SCADA/OT systems, energy management systems and the IT infrastructure of OWF operators. Cyber attacks can lead to both operational disruptions and breaches of physical security of farms by interfering with monitoring, positioning or wind turbine control systems.

The information domain includes disinformation activities and influence operations aimed at reducing the level of public acceptance of OWFs, questioning their safety and profitability, as well as highlighting their negative impact on the marine environment. These activities may indirectly influence regulatory and

---

[13] *Zakłócenia systemu GPS na Bałtyku utrzymują się od ponad 60 dni* (Eng. GPS interference in the Baltic Sea has persisted for over 60 days), Portal Morski, 18 I 2025, https://www.portalmorski.pl/bezpieczenstwo/57341-zaklocenia-systemu-gps-na-baltyku-utrzymuja-sie-od-ponad-60-dni [accessed: 19 VI 2025].

[14] R. Miętkiewicz, *Morskie farmy wiatrowe a bezpieczeństwo morskie państwa* (Eng. Offshore wind farms, new elements of maritime security), "Sprawy Międzynarodowe" 2019, vol. 72, no. 1. https://doi.org/10.35757/SM.2019.72.1.06.

[15] M. Piekarski, *Ochrona infrastruktury krytycznej na polskich obszarach morskich w kontekście zagrożeń hybrydowych* (Eng. Protection of critical infrastructure in Polish maritime areas in the context of hybrid threats), "Ekspertyzy PTBN" 2023, no. 1.

[16] Ibid.

investment decisions and the pace of development of the offshore wind energy sector[17].

In the radio-electronic domain, threats are identified that involve interference with GNSS (global navigation satellite system) signals, maritime communications and navigation systems used by service units and autonomous systems[18]. Such interference may be part of the preparation for or support of physical and undersea activities.

The domain-based approach to threats, present in more recent analyses of maritime and energy security, allows us to move away from a simplified division into 'forms of threats' in favour of a systemic multi-domain analysis that better reflects the nature of hybrid threats to OWFs.

According to V Adm. Didier Malaterre from NATO Allied Maritime Command, the Baltic Sea region has become a new arena for destabilising activities, targeting not only equipment but also the entire capacity of states to respond effectively[19]. The scale, frequency and complexity of these incidents demonstrate the need to adapt national infrastructure protection strategies to the realities of the grey zone and to consider OWFs as potential targets.

Analysis of vulnerabilities in the critical infrastructure protection system in Poland

Despite legislative developments, the Polish CI protection system is not keeping pace with the specific nature of hybrid threats to offshore facilities, including OWFs. The *Act of 26 April 2007 on crisis management* and the *Act of 5 July 2018 on the national cybersecurity system* establish a formal framework for the protection of CI, but OWFs have not been explicitly classified as CI of strategic importance. The *Poland's energy policy until 2040* (PEP2040) identifies OWFs as a key element of energy transition and security of supply, but the document does not describe the procedures and protection mechanisms intended for offshore infrastructure[20].

---

[17] R. Miętkiewicz, *Morskie farmy wiatrowe. Architektura ochrony z wykorzystaniem technologii bezzałogowych* (Eng. Offshore wind farms. Security architecture using unmanned technologies), "Gospodarka Materiałowa i Logistyka" 2017, no. 12, pp. 688–702.

[18] Ibid.

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

[20] Ministry of Climate and Environment, *Polityka energetyczna Polski do 2040 r…*

The lack of precise regulations results in an unclear division of responsibilities between ministries. It is not clearly indicated which institutions are responsible for prevention, monitoring and responding to threats to OWFs. Formally, tasks related to CI protection are carried out by the Internal Security Agency, the Border Guard, the Polish Navy and the Operational Centre of the Ministry of National Defence, but there is no integrated coordination mechanism between these entities. The situation is further complicated by the lack of clear guidelines for OWF operators regarding their information obligations and cooperation with state crisis management centres (the Government Centre for Security, CERT Polska, CSIRT MON)[21].

The report prepared by the European Centre of Excellence for Countering Hybrid Threats identified serious gaps in testing the resilience of offshore infrastructure to hybrid activities. National regulations do not require regular exercises involving OWF operators, law enforcement agencies and military structures. Tools such as red teaming or realistic digital twin simulations, which would allow for the assessment of the technical and organisational resilience of OWFs in conditions of physical and cyber disruptions or disinformation activities, are also not used[22].

Another problem area is the insufficient adaptation of regulations concerning the physical protection of CI to maritime conditions. The regulations in force are based on the model of land infrastructure protection, which causes difficulties in implementing security systems in the maritime environment (e.g. patrolling of water areas, installation of acoustic detectors, radar integration)[23]. There is also a lack of harmonised procedures for protecting power cables and the foundations of CI facilities. However, there are rules for creating protection systems for transformer stations and cable lines contained in the *Regulation of the Minister of Climate and Environment of 25 May 2022 on specific requirements for components of power transmission equipment and for components of offshore power stations*.

There is a lack of consistency in the area of cybersecurity. According to the findings of the Supreme Audit Office, many local government units and energy operators do not have updated cyber incident response plans in place, nor do they implement standards similar to those contained in Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common

[21] *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities...*

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

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

level of cybersecurity across the Union (hereinafter: NIS 2 Directive)[24] and in PN-EN ISO/IEC 27001 standard concerning Information Security Management System[25]. Although some OWF operators operating in Poland (e.g. Ørsted, Equinor) implement good practices drawn from Scandinavian markets, there is no national cybersecurity standard for offshore infrastructure.

From a strategic point of view, the main gap is the lack of a comprehensive, inter-ministerial strategy for the protection of maritime infrastructure as a whole. Current strategic documents, including the *National Crisis Management Plan*[26] or the *Cybersecurity doctrine of the Republic of Poland*[27], do not take into account the specific nature of OWFs as objects with dual sensitivity – energy and maritime. The protection of OWFs requires a multi-domain approach, including military (sabotage protection), IT (cyber protection), institutional (coordination) and engineering (technical advancement) components. It should be noted that the National Critical Infrastructure Protection Programme 2023 includes technical measures, carried out mainly by the Government Centre for Security and CI operators (in this case – OWFs). These include: establishing working groups and developing CI security standards, identifying and verifying their effectiveness, creating a database of incidents that have occurred at CI facilities, and training platforms for CI operators and administration[28].

The changes in EU law resulting from the CER Directive and its relation with the NIS 2 Directive are an important context for assessing the effectiveness of the national system for protecting OWFs as CI.

---

[24] *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*, pp. 80–152.

[25] Najwyższa Izba Kontroli (Supreme Audit Office), *Informacja o wynikach kontroli. Zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w jednostkach samorządu terytorialnego* (Eng. Information on audit results. Ensuring information security and continuity of IT systems in local government units), https://www.nik.gov.pl/plik/id,30641,vp,33700.pdf [accessed: 20 VI 2025].

[26] Rządowe Centrum Bezpieczeństwa (Government Centre for Security), *Krajowy Plan Zarządzania Kryzysowego 2025* (Eng. The National Crisis Management Plan 2025), https://www.gov.pl/attachment/144aa524-8499-4bfb-9a25-0093184aa889 [accessed: 20 VII 2025].

[27] Biuro Bezpieczeństwa Narodowego (National Security Bureau), *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej* (Eng. The Cybersecurity doctrine of the Republic of Poland), https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf [accessed: 20 VI 2025].

[28] Rządowe Centrum Bezpieczeństwa (Government Centre for Security), *Narodowy Program Ochrony Infrastruktury Krytycznej 2023 – tekst jednolity* (Eng. The National Critical Infrastructure Protection Programme 2023 – consolidated text), Warszawa 2023.

The CER Directive introduces a fundamental change in the approach to CI protection, moving away from the model of protecting 'facilities' towards identifying and regulating critical entities, including those of particular importance for Europe. It imposes a number of public law obligations on these entities, including: conducting regular risk assessments, implementing technical and organisational measures to ensure resilience, reporting incidents, and submitting to supervision by competent authorities equipped with sanctioning instruments.

The NIS 2 Directive stipulates that entities identified under the CER Directive as being of critical importance should also be considered key entities within the meaning of cybersecurity regulations, as follows from Article 2(3) of the NIS 2 Directive.

The mechanism of 'automatic' subjection of OWFs to a dual regulatory regime creates a risk of normative conflicts and dispersion of institutional responsibility in the process of implementing both directives into the Polish legal system. In this context, it seems reasonable to consider a coherent model of supervision and response, including the establishment of specialised sectoral structures, such as CSIRT ENERGY (Computer Security Incident Response Team for the Energy Sector), capable of handling the specific nature of offshore energy infrastructure.

An additional problem is the time needed to implement the regulations. The deadline for transposing the CER Directive expired on 17 October 2024, and the amendment to the Act on crisis management and the issuance of implementing acts are still pending. The operation of the first OWFs in Polish areas of the Baltic Sea is to commence in 2026. During the transition period, this infrastructure may therefore operate in a state of regulatory limbo and be subject to protection instruments that are unsuitable to the realities of the offshore sector. It is therefore reasonable to ask whether the proposed legislative solutions will constitute an effective and coherent instrument for building resilience to hybrid threats, or whether further systemic gaps will emerge when OWFs are launched.

Examples of good practices at national and international levels

In response to growing hybrid threats to maritime infrastructure, NATO and EU countries are developing multifaceted protection models that combine military, civil and technical measures. The experiences of countries with developed offshore sectors – the United Kingdom, the Netherlands and the Nordic countries – are particularly important, as they have developed modern response and prevention instruments.

At the NATO alliance level, the Baltic Sentry[29] concept is being developed – a joint system for patrolling and surveying critical infrastructure for the Baltic Sea. This programme involves the integration of coastal states' forces and the sharing of data between NATO structures, private operators and civil institutions responsible for CI protection. An important element of the Baltic Sentry is the use of advanced analytical tools, including AI-based systems, to detect anomalies in maritime traffic, identify unusual patterns of behaviour by vessels, and provide early warning of potential hybrid activities. These solutions are developed and utilised, among others, within the structures of NATO's Allied Maritime Command (MARCOM) and cover also the Baltic Sea in their operational scope. Within the framework of the Baltic Sentry, joint exercises are conducted as well as underwater and unmanned capabilities are developed. These activities are complemented by the launch of a specialised Maritime Centre for Security of Critical Undersea Infrastructure[30], whose task is to coordinate analyses, exchange information and support allied countries in the field of undersea CI protection.

The European Union, complementing military activities, is developing the CISE (Common Information Sharing Environment) platform. This system enables data sharing between border guards, environmental protection services, search and rescue (SAR) units, and private maritime infrastructure operators. Ultimately, CISE aims to increase so-called maritime situational awareness in times of peace, crisis and conflict[31].

The public-private partnership model used in the Netherlands and Norway is a good practice. OWF operators cooperate with the armed forces and government agencies to develop joint procedures for risk management, incident response, and testing the physical and cyber resilience of farms. Specialists from the British non-profit organisation Carbon Trust and the consultancy company ABPmer have developed a series of technical standards and guidelines for operators, including in the area of cable protection, foundations and SCADA systems[32].

---

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

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

[31] *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 [accessed: 20 VI 2025].

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

Another distinctive approach is the implementation of the *defence by design* principle, i.e. designing offshore infrastructure with resistance to hybrid activities in mind. This means, for example, installing redundant power supply and data transmission systems, locating vulnerable points below sea level and physically separating critical systems.

The United Kingdom was one of the first countries to launch a special unit for the protection of undersea infrastructure. In 2023, the Royal Navy commissioned the Proteus ship into the Royal Fleet Auxiliary as part of the MROSS (Multi-Role Ocean Surveillance Ship) programme. This ship is equipped with sonar systems, underwater drones and a data analysis centre, which enable real-time monitoring of cables and OWFs[33].

Denmark, in turn, is implementing innovative systems based on autonomous technology. The Saildrone Voyager platforms are being tested – unmanned sailing vessels capable of monitoring selected objects in the Baltic Sea for several weeks. These devices are equipped with meteorological sensors, radar, thermal imaging cameras and AIS kits[34].

International experience shows that effective protection of OWFs cannot be limited to physical and digital security measures, but must be part of an integrated, cross-sectoral response system. Some countries of the Baltic region (Estonia, Finland and Sweden) are currently implementing national models that integrate coast guards, intelligence services, energy network operators and the military. This model could serve as inspiration for Poland, especially in the context of a lack of clear coordination processes.

At the operational level, initiatives are also being developed in Poland aimed at providing digital support for the monitoring and protection of maritime infrastructure in the Baltic Sea region, including programmes provisionally referred to as Digital Baltic[35]. Their aim is to integrate data from maritime surveillance systems, technical sensors and operator sources in order to increase situational awareness at sea. These initiatives are part of a broader trend towards the use of digital and analytical tools for early detection of anomalies and to support decision-making processes in times of peace and crisis[36]. An important role in the maritime infrastructure protection

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

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

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

[36] P. Mickiewicz, *Bezpieczeństwo energetyczne czy bezpieczeństwo morskie? Dylemat oceny potencjalnych zagrożeń bezpieczeństwa Polski na akwenie Morza Bałtyckiego w trzeciej dekadzie XXI wieku*

system is played by the Maritime Border Guard Regional Unit[37] whose tasks include protecting Poland's maritime border, ensuring the safety of navigation and responding to incidents in the territorial sea, where critical infrastructure elements are located, including sections of OWF export lines. The inclusion of the Maritime Border Guard Regional Unit in the OWF protection model is a key element of the non-military security component, complementing the activities of the armed forces and allied structures, especially in the area of ongoing monitoring, control of maritime traffic and cooperation with CI operators.

Strategic, organisational and technological recommendations

In Poland, decisive action is needed at the legislative and operational levels to ensure effective protection for OWFs. The experience of coastal states shows that this requires cooperation between public institutions, the private sector (operators) and the armed forces. The proposed strategic, organisational and technological recommendations are based on such an integrated approach to security of CI.

Strategic recommendations

1. Statutory recognition of OWFs as CI – it is necessary to clarify the status of OWFs in Polish legal system by including them in the list of CI sectors, in accordance with the CER Directive and the updated PEP2040.
2. Development of a national strategy for the protection of offshore infrastructure – this strategy should integrate military and non-military components, including the Maritime Border Guard Regional Unit, Police (including water police), maritime administration and CI operators. A special role in this system should be assigned to OWF operators located in exclusive economic zone (EEZ), who, due to their constant operational presence, are the first link in CI monitoring, early detection of anomalies and reporting of hybrid incidents. The role of the CI operators in EEZ should primarily consist of: a) maintaining technical and environmental monitoring systems (SCADA, sensors, positioning and observation systems), b) ensuring data interoperability with national

(Eng. Energy security or maritime security? The dilemma of assessing potential threats to Poland's security in the Baltic Sea area in the third decade of 21st century), "Nautologia" 2024, no. 161, pp. 71–76.

[37] *Zadania Morskiego Oddziału Straży Granicznej* (Eng. Tasks of the Maritime Border Guard Regional Unit), Straż Graniczna – Morski Oddział Straży Granicznej, 5 X 2012, https://www.morski.strazgraniczna.pl/mor/komenda/zadania/1636,Zadania.html [accessed: 7 I 2026].

and allied systems, c) implementing incident response procedures in accordance with the National Crisis Management Plan, d) participating in exercises and resilience tests conducted with the involvement of public administration and armed forces. This definition of the role of operators allows the limited physical presence of the state in EEZ to be supplemented by a model of shared responsibility and public-private partnership, in line with solutions adopted in the Nordic countries and within NATO.

3. Inclusion of OWFs in regular defence and crisis management exercises – OWFs should become an integral part of national exercises such as IGNIS[38], as part of testing resilience to physical sabotage and cyber attacks[39].

Organisational recommendations

1. Establishment of an interministerial team for offshore infrastructure safety – the team should include representatives of the Ministry of National Defence, the Internal Security Agency, the Government Centre for Security, the Ministry of the Interior and Administration, the maritime administration (maritime authorities), the Maritime Border Guard Regional Unit, Police (including water police), and OWF operators as entities directly responsible for infrastructure operation. The role of the maritime administration should include, in particular, the coordination of maritime traffic management activities, the designation and enforcement of security zones, and the integration of threat information with VTS (vessel traffic service) service systems and national maritime situational awareness. OWF operators should be involved in the team's work not only as stakeholders, but also as active participants in the process of planning, testing and improving incident response procedures, including through participation in inter-agency exercises and the provision of operational data to the relevant state authorities.
2. Closer civil-military cooperation – joint patrols, interoperable command centres and data exchange (using platforms such as CISE) will enable faster detection and neutralisation of threats.
3. Mandatory integration of OWF operators with the National Crisis Management Plan system and the national cybersecurity system – this requires a review of executive acts and the incident reporting system.

---

[38] *Krajowe ćwiczenia ratownicze "IGNIS 2025"* (Eng. National rescue exercises 'IGNIS 2025'), Serwis Rzeczypospolitej Polskiej, 15 X 2025, https://www.gov.pl/web/kgpsp/krajowe-cwiczenia-ratownicze-ignis-2025 [accessed: 20 XI 2025].

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

Technological recommendations

1. Investing in unmanned reconnaissance systems[40] (uncrewed surface vehicle, USV; unmanned aerial systems, UAS; unmanned aerial vehicle, UAV) – autonomous patrol platforms (such as Saildrone) should be used to protect OWFs, ensuring round-the-clock surveillance of the maritime area and early detection of unauthorised activity.
2. The use of sensor systems in accordance with national rules governing the operation of OWFs – the installation of radars, acoustic sensors, passive sonars and electro-optical observation systems should be carried out on the basis of analyses conducted in Poland on the impact of OWFs on national security and defence systems, which are part of the planning and consultation process for offshore investments. The need to implement selected sensors has been recognised and is gradually being taken into account in national and allied maritime monitoring systems, while maintaining interoperability with existing state solutions.
3. Building cyber resilience in accordance with the standards of the NIS 2 Directive and PN-EN ISO/IEC 27001 standard – OWF operators should be required to implement auditable incident management procedures as well as regular penetration testing and red teaming, i.e. testing the overall resilience of the organisation to threats, from the level of technology to procedures.

Summary and directions for further research

Offshore wind farms are gaining the status of strategic infrastructure not only from an ecological, economic and business perspective, but also as potential targets for hybrid operations and activities in grey zone. In the face of growing tensions in the Baltic Sea region, they are becoming a new arena for rivalry – involving physical, cyber and information activities conducted below the threshold of open conflict and blurring the line between war and peace.

Poland, aspiring to become a regional leader in the RES sector, is at a very important moment. By adopting an integrated, multi-layered approach – encompassing legal regulations, interoperable civil-military activities, cyber resilience, technical reconnaissance, as well as international and sectoral

[40] R. Miętkiewicz, *Unmanned Surface Vehicles in Maritime Critical Infrastructure Protection Applications – LNG Terminal in Świnoujście*, "Zeszyty Naukowe Akademii Marynarki Wojennej" 2018, vol. 213, no. 2, pp. 43–51. https://doi.org/10.2478/sjpna-2018-0012.

cooperation – Poland can become a model for the effective protection of maritime infrastructure against hybrid threats.

Directions for further research should include:

1. Hybrid risk modelling using digital twin simulation[41] – this should be treated as a tool supplementing the risk identification and assessment processes carried out by OWF operators at the infrastructure planning, construction and operation stages. In accordance with regulatory requirements and good practices in the offshore sector, OWF operators conduct risk analyses covering technical, environmental and operational risks[42]. The use of digital twin does not replace these activities, but allows for their deepening and analysis of the relationships between different categories of threats, including physical, cyber and information threats. The creation of a virtual equivalent of OWF enables testing the resilience of infrastructure to complex, multi-domain threat scenarios in a controlled simulation environment, without interfering with the functioning of real facilities. This tool will allow for the assessment of the effects of cumulative impacts, such as power disruptions, SCADA/OT system interference, or information activities affecting decision-making processes. This approach is already being put to practical use in the offshore sector, primarily in the Nordic countries, as part of operational decision support and maritime infrastructure security planning[43].
2. Designing and conducting red teaming exercises – implementing realistic attack scenarios (physical, cybernetic, social engineering) enables a reliable assessment of the readiness of OWF operators and state institutions, which is necessary to improve procedures for responding to infrastructure violations.
3. Analysis of private sector involvement in coordinating responses to threats – further research should focus on determining the place of OWF operators in a multi-level response architecture, in which the operator is responsible for the operational and technical levels (detection, initial assessment of the incident, securing business continuity), while crisis response coordination and strategic decisions remain the responsibility

[41] 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/ [accessed: 7 I 2026].

[42] *Energy Transition Outlook 2025*…

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

of the relevant state authorities and allied structures[44]. This allocation of roles is consistent with the approach adopted in NATO and EU documents and with practice in the offshore sector, where operators perform a front-line monitoring and reporting function rather than commanding the response to a crisis situation[45].

4. Development and evaluation of national technologies for OWF security – focus should be placed on identifying and evaluating the potential of national dual-use technologies that can be used to protect OWFs, particularly in the areas of sensor systems, unmanned maritime and aerial platforms, data analytics, and offshore infrastructure cybersecurity[46]. Important areas of research include the analysis of the impact of the development and implementation of national technologies on increasing the systemic resilience of OWFs, reducing the dependence of technologies on attack-sensitive systems, and improving state control over the key elements of security system[47]. The research should also include an assessment of the mechanisms for integrating national technological solutions with state and allied systems, including the EU and NATO, as well as an analysis of the legal, organisational and financial barriers limiting implementation of these solutions in offshore environment[48].

Bibliography

Mickiewicz P., *Bezpieczeństwo energetyczne czy bezpieczeństwo morskie? Dylemat oceny potencjalnych zagrożeń bezpieczeństwa Polski na akwenie Morza Bałtyckiego w trzeciej dekadzie XXI wieku* (Eng. Energy security or maritime security? The dilemma of assessing potential threats to Poland's security in the Baltic Sea area in the third decade of 21st century), "Nautologia" 2024, no. 161, s. 71–76.

Miętkiewicz R., *Morskie farmy wiatrowe a bezpieczeństwo morskie państwa* (Eng. Offshore wind farms, new elements of maritime security), "Sprawy Międzynarodowe" 2019, vol. 72, no. 1. https://doi.org/10.35757/SM.2019.72.1.06.

[44] *Energy Transition Outlook 2025*…

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

[46] Rządowe Centrum Bezpieczeństwa, *Krajowy plan zarządzania kryzysowego 2025*…; P. Mickiewicz, *Bezpieczeństwo energetyczne czy bezpieczeństwo morskie*…

[47] Ibid.

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

Miętkiewicz R., *Morskie farmy wiatrowe. Architektura ochrony z wykorzystaniem technologii bezzałogowych* (Eng. Offshore wind farms. Security architecture using unmanned technologies), "Gospodarka Materiałowa i Logistyka" 2017, no. 12, pp. 688–702.

Miętkiewicz R., *Unmanned Surface Vehicles in Maritime Critical Infrastructure Protection Applications – LNG Terminal in Świnoujście*, "Zeszyty Naukowe Akademii Marynarki Wojennej" 2018, vol. 213, no. 2, pp. 43–51. https://doi.org/10.2478/sjpna-2018-0012.

Piekarski M., *Ochrona infrastruktury krytycznej na polskich obszarach morskich w kontekście zagrożeń hybrydowych* (Eng. Protection of critical infrastructure in Polish maritime areas in the context of hybrid threats), "Ekspertyzy PTBN" 2023, no. 1.

Szubrycht T., *Sojusznicza odpowiedź na zagrożenia na Morzu Bałtyckim* (Eng. Allied response to threat in the Baltic Sea), "Bezpieczeństwo Narodowe" 2025, vol. 46, no. 1, pp. 49–75. https://doi.org/10.59800/bn/207646.

Internet sources

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/ [accessed: 20 VI 2025].

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

Cavcic M., *Hybrid warfare paints 'gray zone' targets on shipping and offshore energy infrastructure*, OffshoreEnergy, 11 XII 2024, https://www.offshore-energy.biz/hybrid-warfare-paints-gray-zone-targets-on-shipping-and-offshore-energy-infrastructure/ [accessed: 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 [accessed: 20 VI 2025].

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

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

Energy Transition Outlook 2025, https://brandcentral.dnv.com/original/gallery/10651/files/original/ec419166-9ecc-40ef-9997-93a6ccb72335.pdf [accessed: 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/ [accessed: 7 I 2026].

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

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

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

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

Krajowe ćwiczenia ratownicze "IGNIS 2025" (Eng. National rescue exercises 'IGNIS 2025'), Serwis Rzeczypospolitej Polskiej, 15 X 2025, https://www.gov.pl/web/kgpsp/krajowe-cwiczenia-ratownicze-ignis-2025 [accessed: 20 XI 2025].

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

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

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

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

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

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

Zadania Morskiego Oddziału Straży Granicznej (Eng. Tasks of the Maritime Border Guard Regional Unit), Straż Graniczna – Morski Oddział Straży Granicznej, 5 X 2012, https://www.morski.strazgraniczna.pl/mor/komenda/zadania/1636,Zadania.html [accessed: 7 I 2026].

Zakłócenia systemu GPS na Bałtyku utrzymują się od ponad 60 dni (Eng. GPS interference in the Baltic Sea has persisted for over 60 days), Portal Morski, 18 I 2025, https://www.portalmorski.pl/bezpieczenstwo/57341-zaklocenia-systemu-gps-na-baltyku-utrzymuja-sie-od-ponad-60-dni [accessed: 19 VI 2025].

Legal acts

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC – (Official Journal of the EU L 333 of 27 XII 2022).

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 Decem-ber 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) – (Official Journal of the EU L 333 of 27 XII 2022).

Act of 5 July 2018 on the national cybersecurity system (consolidated text, Journal of Laws of 2026, item 20).

Act of 26 April 2007 on crisis management (consolidated text, Journal of Laws of 2023, item 122, as amended).

Regulation of the Minister of Climate and Environment of 25 May 2022 on specific requirements for components of power transmission equipment and for components of offshore power stations (Journal of Laws of 2022, item 1257).

Other documents

Biuro Bezpieczeństwa Narodowego (National Security Bureau), *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej* (Eng. The cybersecurity doctrine of the Republic of Poland), https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf [accessed: 20 VI 2025].

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

Ministerstwo Klimatu i Środowiska (Ministry of Climate and Environment), *Polityka energetyczna Polski do 2040 r. (PEP2040)* (Eng. Poland's energy policy until 2040 (PEP2040)), Warszawa 2021.

Najwyższa Izba Kontroli (Supreme Audit Office), *Informacja o wynikach kontroli. Zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w jednostkach samorządu terytorialnego* (Eng. Information on audit results. Ensuring information security and continuity of IT systems in local government units), https://www.nik.gov.pl/plik/id,30641,vp,33700.pdf [accessed: 20 VI 2025].

PN-EN ISO/IEC 27001 standard – Information security, cybersecurity and privacy protection – Information security management systems – Requirements.

Rządowe Centrum Bezpieczeństwa (Government Centre for Security), *Krajowy Plan Zarządzania Kryzysowego 2025* (Eng. The National Crisis Management Plan 2025), https://www.gov.pl/attachment/144aa524-8499-4bfb-9a25-0093184aa889 [accessed: 20 VII 2025].

Rządowe Centrum Bezpieczeństwa (Government Centre for Security), *Narodowy Program Ochrony Infrastruktury Krytycznej 2023 – tekst jednolity* (Eng. The National Critical Infrastructure Protection Programme 2023 – consolidated text), Warszawa 2023.

Klaudia Maciata

Offshore operations specialist in the wind energy sector. Ambassador for the Women Offshore initiative, member of international projects in the field of maritime and climate security. Expert on the protection of critical infrastructure against hybrid threats in the Baltic Sea region. Author of publications in "NATO Review". Professionally associated with, among others, Ørsted, she previously worked in the industrial services, unmanned technology and public affairs consulting sectors. Currently she is a founder of the "Baltic Sea Security" project and a freelancer.

Contact: klaudia.maciata@gmail.com