Journal on Baltic Security, 2026; 12(1): 28-60

Research Article

Open Access
https://doi.org/10.57767/jobs_2026_002

Klaudia Maciata*

Securing Offshore Wind Farms in Poland: Legal Responsibilities, Institutional Gaps, and Hybrid Threat Resilience in the Baltic Sea: Towards an Integrated Model of Protection and Resilience

Received : 1 August 2025.
Accepted : 11 September 2025.

Abstract: Poland's rapid expansion of offshore wind farms (OWFs) in the Baltic Sea elevates them to the status of critical infrastructure central to energy security. This article examines the legal responsibilities, institutional arrangements, and operational challenges in protecting OWFs against hybrid threats such as sabotage, espionage, and cyberattacks. It analyses national frameworks, EU directives (CER and NIS2), and the roles of the Navy, Border Guard, Maritime Offices, Government Centre for Security (RCB), and private operators. This work offers a responsibility matrix which highlights both institutional overlaps as well as gaps. The article concludes with recommendations for legal reforms, capability development, and inter-agency coordination to strengthen Poland's offshore wind infrastructure.

Keywords: Offshore Wind Farms, Critical Infrastructure, Hybrid Threats, Baltic Sea Security, Poland.

* **Corresponding author: Klaudia Maciata**, e-mail: klaudia.maciata@gmail.com, War Studies University and balticseasecurity.pl. **Declaration:** The views expressed are solely those of the author and do not represent the positions of any affiliated institution.

Introduction

Poland's rapid offshore wind energy development has significantly increased the strategic importance of OWFs in the Baltic Sea as part of the country's energy infrastructure. These installations – offshore wind generators, undersea power cables, and offshore substations – are essential for Poland's energy security, thus attracting heightened attention in the current geopolitical climate. The sabotage of the Nord Stream gas pipelines in 2022 starkly demonstrated the vulnerability of undersea infrastructure and underscored the need for robust protections.

Protecting OWFs requires a coordinated, multi-agency effort spanning physical security, cybersecurity, and crisis management. This article assesses how Poland assigns institutional responsibilities for OWF protection by analysing the roles of the Navy, Border Guard, Maritime Offices, the Government Centre for Security (RCB), and OWF operators while detailing institutional gaps and operational challenges through case studies of the Nord Stream sabotage, damage to sea cables, suspicious UAV manoeuvres, and 'shadow fleet' activity, all done in an effort to build resilience against hybrid threats in the Baltic Sea.

This article proceeds as follows: Section 1 outlines the evolving threat landscape for offshore infrastructure in the Baltic Sea. Section 2 examines Poland's national legal and policy framework for critical infrastructure protection. Sections 3 and 4 analyse maritime jurisdiction, safety laws relevant to OWFs, and sectoral statutes that shape security responsibilities. Section 5 maps institutional roles and interdependencies, highlighting gaps via a responsibility matrix. Section 6 assesses the implications of the EU Critical Entities Resilience (CER) Directive and the Network and Information Security Directive (NIS2) on these frameworks. Sections 7 and 8, identify implementation challenges and offers recommendations for legal,

organisational, and capability reforms to strengthen the resilience of Poland's offshore wind infrastructure. Finally, the conclusion synthesises implications for an integrated model of protection and resilience.

Section 1: Threat Landscape for Offshore Infrastructure

Recent incidents in the Baltic region illustrate the escalating threats to offshore energy assets. In May 2025, the Polish Navy intercepted a suspicious vessel from Russia's 'shadow fleet' acting unusually near the undersea power cable connecting Poland to Sweden (Erling and Strzelecki, 2025). This incident is part of a broader pattern targeting Europe's undersea infrastructure since Russia invaded Ukraine. A pivotal moment occurred in September 2022 with the sabotage of the Nord Stream pipeline. Strategically placed explosives were detonated causing an explosion on the Nord Stream 1 and 2 gas pipelines, severely compromising energy security (Kardaś and Łoskot-Strachota, 2022). Security experts indicate that such sabotage, conducted below the threshold of open conflict, constitutes a form of hybrid warfare aimed at disrupting economies (Lorenz and Zaręba, 2022). In the Nord Stream incident, the explosions occurred outside any nation's territorial waters, complicating response and accountability (Lorenz and Zaręba, 2022). Other incidents amplified the cause for concern. Nordic countries have reported unidentified drones near offshore oil and gas platforms (Adomaitis, 2022). In Norway, several Russian nationals were arrested for flying drones near critical infrastructure (Edvardsen, 2022). The clear takeaway is that it is essential to ensure maximum security of critical infrastructure both onshore and offshore.

Poland is responding by implementing to use surveillance drones over the Baltic Sea, especially after spotting a recent 'spy vessel' near its waters (Ledzińska, 2025). In May 2025, Polish Prime Minister Donald Tusk announced a plan to strengthen Baltic Sea surveillance with new drones to enhance intelligence, intelligence reconnaissance surveillance (IRS) activities over the Baltic Sea to protect its vulnerable critical infrastructure (CI) (Ledzińska, 2025). Meanwhile, NATO and regional allies are increasing undersea monitoring efforts, such as the new 'Baltic Sentry' exercises using unmanned surface vessels (USV) (NATO Supreme Headquarters Allied

Powers Europe, 2024). The general agreement is that OWFs, along with pipelines and data cables, face both physical and cyber threats in the tense environment of the Baltic Sea (Baltic Wind EU, 2025).

These incidents highlight that protecting OWFs is not just a technical or corporate issue. It is a matter of national security that requires clear responsibilities and teamwork among Polish stakeholders (Baltic Wind EU, 2025). The following sections will outline Poland's legal framework and the roles of key stakeholders involved in securing OWFs as critical infrastructure.

Section Two: National Legal and Policy Framework

Poland's Crisis Management Act (CMA) (Government of Poland, 2007), often called the Emergency Management Act, provides the foundation for protecting critical infrastructure. It defines 'critical infrastructure' (CI) as systems and assets crucial to the state's and its citizens' security. Under Article 3(2) of this Act, OWFs are classified as critical infrastructure once operational, as they form part of the energy supply. This designation carries essential obligations.

Poland's Council of Ministers has adopted a National Programme for the Protection of Critical Infrastructure (NPOIK) which assigns sectoral responsibilities to various ministries. First, as the Ministers of State Assets and Climate/Energy are responsible for energy, their tasks include conducting risk assessments, coordinating protective measures, supporting training, and approving CIP plans. Next, the RCB (Government Centre for Security) coordinates this programme nationally as a hub for CI-protection. Finally, OWFs Operators must ensure adequate protection by developing and implementing Critical Infrastructure Protection (CIP) plans and emergency procedures that address anticipated threats.

One weakness is that the NPOIK operates on an 'unsanctioned' basis, relying on guidelines and cooperation rather than enforceable laws. Consequently, while most CI operators submit protection plans for RCB review, the state has

limited the ability to audit compliance or sanction negligence. It was noted that as of early 2023, it is challenging to compel entities to draft CIP documents due to the lack of legal instruments; compliance depends on goodwill. This situation is set to change with the new EU CER Directive, which will introduce binding oversight. As noted by Projekt Infrastruktura Krytyczna [Project Critical Infrastructure] (2023), '*The provisions of the CER Directive will be implemented into the Polish legal system through an amendment to the Crisis Management Act. The aim of the amendments is to adapt national regulations to EU requirements for the resilience of critical infrastructure and to ensure consistency of actions at the national and European level*'. As of today, 23 October 2025, the directive is being reviewed by the Standing Committee of the Council of Ministers.

In addition to the CMA, Poland's Anti-Terrorism Law (2016) supplements CI protection in high-threat scenarios. Hypothetically, should the government declare a heightened alert level (e.g. BRAVO or higher) due to a terrorist threat, the Police are mandated to verify critical infrastructure security. The Internal Security Agency (ABW) can also issue recommendations to reinforce certain areas. In such situations, a regulation under this law authorises the Chiefs of Police, Border Guard, or Military Gendarmerie to deploy armed officers to guard potential targets. In practice, if intelligence suggests an imminent threat to OWFs (e.g. a sabotage plot), Polish authorities can elevate the alert level and station armed security (from police or border guard units) to protect the offshore wind turbines. However, as this is a reactive measure tied to officially declared threat levels, it therefore does not substitute for day-to-day protective arrangements.

Section Three: Maritime Areas and Maritime Safety Laws

Poland's jurisdiction over OWFs in the Baltic is established by the Act on Maritime Areas (MAA) of the Republic of Poland (1991). The MAA is a national regulation that implements the provisions of the United Nations Convention on the Law of the Sea (UNCLOS). In line with UNCLOS, this Convention grants Poland exclusive rights in its Exclusive Economic Zone (EEZ) to regulate OWF construction and operation, which must occur beyond its territorial sea, specifically in the adjacent zone/EEZ. Consequently,

Poland's first OWFs are situated in the contiguous zone (12 to 24 NM from shore) or further out (PGE Baltica and Ørsted, 2023). This raises security concerns, as OWFs are situated in areas where Poland exercises only limited sovereignty. Within its EEZ, Poland retains rights related to economic activities, the management and exploitation of natural resources (such as wind and water), scientific research, environmental protection, and the construction and operation of installations. In the case of OWFs, this includes the establishment and use of artificial islands; however, the surrounding waters remain open to international navigation. This legal framework leaves room for intelligence, surveillance, and reconnaissance (ISR) activities by foreign actors – such as those conducted by the so-called 'shadow fleet' – which cannot be fully controlled due to the principle of freedom of navigation in the EEZ.

Polish authorities can establish safety zones around offshore installations within the EEZ. Under Article 24 of MAA, a Maritime Office Director may create a navigational exclusion zone of up to 500 meters around an OWF. This 500m buffer includes the outermost turbines, allowing the Maritime Office to restrict or ban navigation, fishing, diving, and other activities for safety. Unauthorised entry into this zone is an administrative offence subject to a fine (up to 20 times the average monthly salary). If the OWF is damaged, criminal liability under the Penal Code may apply. In summary, Polish law deters intrusions through marked exclusion zones and penalties to protect turbines from collisions or sabotage.

Dangerous activities, such as unidentified vessels loitering, necessitate immediate enforcement. However, a fault in the current system is that establishing safety zones is discretionary. Analysts argue that safety zones should be mandatory for OWFs due to their critical importance. Enforcement at sea depends on the state's surveillance and response capabilities, which will be discussed later.

To ensure OWFs are built and operated safely, Poland updated its Act of Maritime Safety (MSA) of the Republic of Poland in 2022. Initially enacted in

2011, the MSA was amended to introduce strict certification requirements for OWF projects. Developers must obtain certificates from accredited organisations at each stage – design, construction, and operational safety – confirming that the wind farm meets structural integrity, fire safety, environmental, and operational standards. These provisions extend the type of state supervision for vessels and oil rigs to OWFs. While technical, they enhance security by ensuring the OWF is constructed to withstand harsh conditions and prevent accidents.

Crucially, the 2022 amendments to the MSA also introduced new requirements directly related to national security. OWF investors must now commission expert studies on: navigational safety (the OWF's impact on vessel traffic); impacts on marine emergency communication systems, such as the Global Maritime Distress and Safety System (GMDSS) and Search and Rescue (SAR) networks; effects on the National Maritime Safety System (KSBM); and implications on Border Guard radar, monitoring, and radio-communication systems. In other words, an OWF developer must assess how the wind farm might interfere with or be exploited against Poland's maritime surveillance and rescue systems before construction. For instance, large turbines could create radar blind spots or disrupt radio links; these effects must be analysed and mitigated. The law also requires OWF projects to prepare rescue plans for accidents (to protect offshore personnel) and oil spill response plans.

This ensures that agencies like the Navy and Border Guard review OWF plans for any adverse effects on coastal defence or border surveillance. While these measures focus on minimising any adverse side effects of OWFs on security systems, they embody a broader principle of close inter-agency cooperation from the planning stage of OWFs to balance energy objectives with security concerns.

Section 4: Additional National Laws that Shape CI Security Responsibilities

Energy Law

Poland's Energy Law (1997a) governs the energy sector, including licensing electricity generators. Energy enterprises must ensure the continuity of supply and adhere to technical and safety regulations. While it does not detail specific anti-sabotage responsibilities, compliance with this law *implies* OWF operators must operate reliably and could be sanctioned by the Energy Regulatory Office (URE) for failing to secure their facilities adequately (for instance, if a lack of security led to prolonged outages violating supply obligations). The Energy Law also interacts with the Crisis Management Act in that energy infrastructure is part of the state's 'energy security' strategy. In practice, however, the Energy Law's role in OWF protection is indirect and essentially acts as the sectoral backdrop, while the Crisis Management Act and security laws mentioned in a previous subsection impose the concrete protection requirements.

Act on the Protection of People and Property (1997b)

This law regulates security services and mandates, in accordance with the Act on the Protection of Persons and Property (Government of Poland 1997b), that 'facilities of special importance' have physical protection plans. Specific strategic sites (e.g. major power plants, ports, LNG terminals) are classified by the Ministry of Interior as requiring mandatory protection by armed security, often employing either police, military police, or licensed security firms. Post-9/11, airports are a prime example. However, civil aviation security is tightly overseen by state inspectors with enforceable regulations. For OWFs, the analogous requirement in development is their onshore substations and control centres could be designated as mandatory protected facilities. Currently, under this law, an OWF operator must implement a security plan that has been reviewed by the Police and the ABW, and which includes an

anti-terrorism annex. Indeed, Polish CI operators must draft both a physical protection plan (agreed with the police) and an anti-terrorism plan (agreed with ABW) for each task. These plans detail measures against intruders, sabotage devices, and response procedures under various alert levels. Unfortunately, for offshore wind, implementing this is challenging as a guard cannot be posted on every turbine. However, the onshore interface and any service vessels can follow these regulations. Ensuring maritime assets are covered via the Border Guard or Navy instead of static guards is part of ongoing policy development.

Maritime Border Protection and Law Enforcement: The Act on the Border Guard (1990) and the Maritime Code (2001)

These two legal frameworks outline enforcement powers at sea, empowering Border Guard officers to stop, search, and detain vessels violating Polish laws. According to the *Act on the Border Guard* (Government of Poland 1990), these powers are explicitly granted to the 'commander of a Border Guard watercraft in territorial waters, raising questions about officers' authority on piers or aircraft. Within the 12 NM territorial sea, Border Guard patrol boats can enforce security zones, order vessels to stop or change course, inspect them, and even divert them into port if they refuse compliance. They address threats such as unauthorised entry into OWF zones, pollution, smuggling, and other violations like anchoring in restricted areas. In the contiguous zone and EEZ beyond 12 NM, the Border Guard's role includes protecting Poland's rights, though the law is unclear.

Article 14(3) of the BG Act allows Border Guard vessels to act in the EEZ to protect Poland's rights, which is interpreted to cover fisheries enforcement, customs, and environmental laws, potentially including OWF protections (Government of Poland, 1990). However, legal experts note that the wording regarding security incidents around OWFs is ambiguous, detailing that 'the scope of competences of the Border Guard does not cover the sea area in which projects of Polish OWFs are planned or with already existing critical infrastructure facilities' (Romowicz and Niewiński, 2023). They suggest explicitly mentioning the contiguous zone in the Border Guard's authority to

clarify that patrols can intervene, for instance, 15 NM offshore at a wind farm, without overstepping their bounds (see Romowicz and Niewiński, 2021; Romowicz and Niewiński, 2023).

In sum, Poland's legal framework has many necessary components to secure OWFs: critical infrastructure designation with protection planning; maritime regulations for exclusion zones; law enforcement powers at sea; and contingency provisions for high threats. However, as the following sections convey, the practical enforcement of these laws hinges on clearly defined institutional roles and sufficient capabilities. Gaps between legal authority and real-world capacity pose challenges that Poland is now urgently addressing.

Section Five: Roles and Responsibilities of Key Institutions and the Responsibility Matrix

Protecting OWFs involves a number of institutions with distinct duties. The major players include the Polish Navy, the Border Guard (particularly its Maritime Branch), the Maritime Offices, the RCB, and the OWF operators. The following responsibility matrix highlights both how roles of the various institutions complement one another but also reveals fragmentation and potential challenges. After which is a series of paragraphs offering further details for each specific institutions' responsibilities.

Table 1. Responsibility Matrix: Key Actors in OWF Protection in Poland. Institutions in first column.

	Responsibilities for OWF Protection	**Gaps / Challenges**
Polish Navy	Deter and defend against high-end or state-sponsored threats (e.g., sabotage by hostile military or 'grey zone' actors). Conduct surveillance of Poland's EEZ for suspicious vessels or activities: intercept intruders beyond civilian capability. Deploy specialised units (divers, mine countermeasures, naval Special Operations Forces) to respond to OWFs attacks. Provide visible presence to deter adversaries through naval patrols during heightened tensions.	Limited resources for constant patrolling of OWFs areas; few Navy ships available. Peacetime rules restrict use of force on civilian intruders, requiring clear law-enforcement protocols. Risk of over-reliance on Navy for tasks suited to a Coast Guard, potentially diverting them from core defence missions.
Border Guard (MOSG)	Monitor and patrol OWFs sites and surrounding waters on a routine basis. Enforce exclusion zones by stopping, inspecting, and removing unauthorised vessels. Act as first responder to incidents (detaining suspects, securing the area until specialised forces arrive). Coordinate with Navy and Police for joint operations and alerts (e.g., BRAVO alerts).	Legal authority in the EEZ not clearly defined; jurisdiction gap beyond 12 NM. Significant asset shortages (ageing patrol fleet, insufficient coverage during adverse conditions or prolonged operations). Fragmented operations and parallel reporting chains slow integration with Navy and Maritime Offices.

Maritime Offices	Issue permits for OWFs and cables with security conditions; establish 500m safety zones. Monitor traffic via coastal radar/AIS and alert enforcement agencies of violations. Enforce regulations administratively (fines, corrective orders). Coordinate maritime SAR in case of OWFs accidents.	Safety zones are discretionary, not mandatory; potential delays in issuance leave OWFs vulnerable. No patrol assets; rely entirely on Border Guard/Navy for physical enforcement. Separate surveillance systems reduce unified situational awareness. Overlapping authority with other agencies risks confusion in OWFs incidents.
RCB (Government Centre for Security)	Identify OWFs as critical infrastructure and integrate operator protection plans into national strategy. Coordinate inter-agency crisis response and advise leadership during threats/incidents. Update the National CIP Programme with OWF-specific risks (e.g., drones, cyber-physical threats). Liaise internationally with EU/NATO on CI protection and threat intelligence.	Lack of enforcement powers; relies on cooperation rather than sanctions (gap to be closed by CER Directive). Future uncertain due to possible restructuring of civil protection law. Coordination challenges bridging civil-military and public-private divides; fast information flow from operators to Navy/BG still under development.

OWF Operators	Implement physical security (surveillance, access control, tracking systems, and private security during construction). Maintain monitoring & reporting systems (CCTV, radar, SCADA alarms). Train staff in emergency procedures; coordinate drills with state security services. Ensure cybersecurity compliance under NIS2 and national law (risk assessments, incident reporting, and ICS protection).	Cannot counter armed threats; rely on state services for active defence. Limited experience with maritime security among Polish operators; need to build strong security culture. High cost of advanced security technology (anti-drone, underwater sensors) discourages investment without regulatory push. Preparedness gap: few offshore facilities equipped with counter-drone systems as of 2023.

While the Navy provides high-end deterrence and specialised response, it cannot substitute for the day-to-day presence that the Border Guard should deliver. Maritime Offices establish regulatory frameworks but depend on others for enforcement, creating delays and vulnerabilities. The RCB integrates policy and crisis management but still lacks enforcement authority, leaving oversight dependent on voluntary compliance. Finally, operators contribute crucial monitoring and first-layer security, yet they lack coercive powers and face financial and technical limits. Taken together, these findings confirm that Poland's protection model remains fragmented, overly reliant on informal coordination, and exposed to jurisdictional gaps – especially in the EEZ. Effective resilience therefore requires stronger integration of institutional mandates and clearer lines of authority to prevent duplication, delay, or neglect in moments of crisis.

Polish Navy

The Polish Navy defends Poland's maritime territory and contributes to NATO's collective defence. In the context of OWFs, its role is strategic:

deterring and responding to high-end, state-sponsored threats such as sabotage by submarines, hostile divers, or underwater drones.

Key contributions include:

- Military-grade response: The Navy is the only force capable of handling advanced maritime threats. It can deploy sonar-equipped vessels, mine countermeasure units, and special forces (e.g., Formoza) to secure OWFs against sophisticated attacks.

- Hybrid threat deterrence: While typically not involved in civilian policing, the Navy has become more active in maritime security amid rising hybrid threats, as seen in recent operations intercepting suspicious vessels near critical infrastructure.

- Maritime domain awareness: The Navy's Maritime Operations Centre in Gdynia coordinates with the Border Guard and NATO to monitor activity near OWFs. Planned acquisitions (e.g., surveillance drones, AI systems) aim to enhance persistent situational awareness.

- Coordination with civilian actors: While the Navy operates under the Ministry of Defence, adequate OWFs protection requires protocols for cooperation with civilian agencies. The Navy steps in when threats surpass Border Guard capacity, ensuring a layered defence.

Resource constraints mean the Navy cannot routinely patrol OWFs, but its presence – when deployed – is a strong deterrent. It is the ultimate backstop for offshore infrastructure security, bringing advanced capabilities and strategic weight when the threat environment escalates.

Border Guard (Maritime Regional Unit)

Under the Ministry of Interior, the Polish Border Guard (*Straż Graniczna*) is the frontline maritime law enforcement agency through its Maritime Regional Unit (MOSG) based in Gdańsk. Acting as Poland's de facto coast guard, it

patrols the Baltic Sea – including the EEZ – to uphold maritime law, monitor sea traffic, and respond to emergencies.

In the context of OWFs, the Border Guard is the primary operational force for daily security. Its patrol vessels and aircraft can monitor safety zones, intercept intruding vessels, conduct onboard inspections, and respond to suspicious or hostile activity (e.g., reconnaissance or sabotage attempts). In territorial waters, they have strong legal authority to stop, inspect, and redirect vessels; however, their jurisdiction in the EEZ is currently more limited and needs clarification – especially for protecting critical infrastructure.

Key challenges include:

- Legal gaps: Existing law does not explicitly empower the Border Guard to protect OWFs beyond 12 NM. Amendments are needed to extend authority into the contiguous zone and EEZ.

- Limited resources: The fleet is small and ageing, with limited endurance in harsh conditions. New patrol vessels and modern surveillance systems are needed.

- Protocol development: Clear procedures must define how the Border Guard should respond to emerging threats at OWFs, especially beyond visual line of sight or involving divers or drones.

Despite these constraints, the Border Guard remains Poland's key asset for persistent maritime presence, enforcement, and first response around OWFs. With legal reform, fleet modernisation, and integration into a future Coast Guard structure, it can become the backbone of OWF operational security.

Maritime Offices (Maritime Administration)

Poland's Maritime Offices (in Gdynia and Szczecin) are civil authorities under the Ministry of Infrastructure responsible for maritime administration, safety, and environmental protection. Regarding OWFs, they serve as the key regulatory body – not an operational force – ensuring secure and lawful integration of these installations into maritime space.

Their roles include:

- Permitting and Zoning: They vet and approve OWFs sites and cable routes to avoid conflicts with navigation and enforce expert safety standards early in the planning process.

- Safety Zones: Maritime Offices issue ordinances establishing exclusion zones around OWFs and defining permitted vessel movements. They also publish navigational warnings and enforce rules through fines.

- Inspections and Sanctions: Through their inspectorates, they can investigate maritime violations, order safety improvements, and impose penalties or halt operations if legal standards are breached.

- Traffic Monitoring and Surveillance: They operate radar, AIS, and VTS systems that track maritime traffic and detect suspicious activity, sharing intelligence with the Border Guard and Navy.

However, maritime offices lack patrol assets and depend on security forces for physical enforcement, creating a risk of fragmented response during incidents. Clear inter-agency protocols and real-time information sharing ensure that threats – such as collisions, intrusions, or sabotage – are promptly acted upon. Effectiveness of the maritime offices in maritime domain awareness hinges on seamless cooperation with operational actors and unified maritime command structures, otherwise they are not effective.

Government Centre for Security (RCB)

The Government Centre for Security (RCB) is Poland's central civilian body for strategic crisis management and critical infrastructure (CI) protection, reporting directly to the Prime Minister. Its core functions include national risk assessments, inter-agency coordination, and oversight of CI protection plans under the National Program for CI Protection (NPOIK). Once connected and power is supplied, OWFs will fall under RCB's oversight.

For OWFs, RCB focuses on policy and preparedness rather than operations. It maintains the CI registry, ensures operators submit and align their protection plans with national standards (covering physical, cyber, and emergency risks), and coordinates with military and civilian agencies to ensure coherence across sectors.

In crisis scenarios, RCB activates national crisis teams, consolidates intelligence from various services, advises top leadership, and can issue alerts (e.g., via the 'Alert RCB' system). It also conducts training, updates standards (e.g., counter-drone measures), and raises awareness among new CI sectors like offshore wind.

Though influential, the RCB lacks enforcement powers, relying on cooperation rather than sanctions. The EU CER Directive will likely require empowering the RCB or a successor body with supervisory and enforcement authority. Experts stress that a single, empowered national coordinator like the RCB is vital to avoid fragmented responsibilities and ensure adequate protection of offshore and other critical infrastructure (Loba, 2025).

Offshore Wind Farm Operators

The operators and owners of OWFs (e.g. joint ventures involving Polish utilities and international energy firms) are the infrastructure proprietors and thus bear direct responsibility for protecting their assets at the operational level. Under Polish law and EU regulations, OWFs operators are considered 'critical infrastructure operators' and (with NIS2) 'essential entities' in the energy sector. Their responsibilities are fourfold: implementing physical security measures; developing critical infrastructure protection plans; cybersecurity; as well as collaboration and information sharing.

Implementing Physical Security Measures: Operators must secure the OWF's onshore facilities (control centres, grid connection points) with fences, surveillance, and guards according to the Protection of Property Act. While the offshore turbines cannot be fenced, operators can deploy technological security (e.g. accessing control systems on the turbines/substation, CCTV cameras, motion or vibration sensors on subsea cables, etc.). They often

maintain a marine surveillance system as part of the farm, with radar and camera units mounted on some turbines to detect approaching vessels. Any such data can be shared live with the Border Guard. Operators also equip their maintenance vessels with AIS and communications, to ensure the authorities are aware of which means of transportation around OWF's are legitimate. Essentially, the operator provides the site's first layer of security monitoring. They are also obligated to comply with any conditions set by authorities. For example, if the Maritime Office says all maintenance trips must be reported 24 hours in advance for security, the operator must do so.

Critical Infrastructure Protection Plan: As discussed, the OWFs operator must develop a comprehensive CIP plan and submit it to the authorities. This plan assesses all risks (sabotage, natural disaster, technical failure) and lays out prevention, response, and recovery strategies. For sabotage scenarios, it would detail coordination with naval forces, redundancy in case a substation is knocked out, etc. Operators must include business continuity plans (e.g., spare parts and contingency arrangements) to restore power if a turbine or cable is RCB. Sectoral ministries review these plans to ensure quality. However, until CER's influence, these were essentially recommendations. Leading OWFs developers, especially international ones, will likely follow global best practices (many have experience securing North Sea wind farms, which have faced similar concerns).

Cybersecurity Responsibilities (NIS/NIS2): OWF installations rely on SCADA control systems and communications that could be cyber targets. Under Poland's National Cybersecurity System Act (implementing the EU NIS directive), large energy operators are 'operators of essential services' and must implement cybersecurity measures and incident reporting. NIS2, coming into force by late 2024, will broaden and tighten these OWF operators will need to conduct cyber risk assessments, apply state-of-the-art security controls, and report any cyber incidents (e.g. hacking attempts on turbine controls) to the national services. They will also have to address supply chain cybersecurity (ensuring contractors like turbine suppliers have good security).

The operator thus has parallel duties: keep the OT (operational technology) systems safe from hacking and keep the physical infrastructure safe from intrusion. In practice, cyber and physical security converge – a cyberattack might aim to cause a turbine malfunction, while a physical intruder might try to insert malware via a USB port. Operators must integrate these aspects into their protection plans.

Collaboration and Information Sharing: Operators must work closely with the government. This includes immediately reporting suspicious activities they observe (e.g., drone sightings around turbines) to the authorities. It also includes participating in joint exercises or drills. For example, Polish authorities may run a simulated OWFs attack exercise; the operator should cooperate by testing their emergency shutdown procedures and communications. Operators also often hire private security or maintain standby contracts for additional protection if threat levels rise. For instance, they could arrange with a private maritime security company to provide an escort vessel, though ultimately, the law enforcement authority remains with the state.

In summary, OWFs operators have a duty of care to protect their infrastructure, comply with the law, and act prudently. They invest in security measures, plan for contingencies, and coordinate with state services. However, they do not have sovereign powers – they cannot engage forcefully with intruders beyond passive measures (private security at sea cannot, say, open fire or arrest a suspect in Polish jurisdiction). Thus, their role is mainly preventative and coordinative: hardening the target, monitoring it, and acting as the first notifier to state authorities if something is amiss. Polish law reinforces this by obligating operators to 'ensure adequate protection' of their CI systems and to maintain backup. Failure to do so could result in penalties under the new CER regime – a significant shift from previous voluntary compliance.

It is worth noting that a glaring practical challenge for operators is the remote location of OWFs. Response times by state services (Navy, BG) could be longer than on land, simply due to the significant distance from shore, limited accessibility, and the reliance on specialized vessels or aircraft to reach the site.

Operators must account for this 'extended reaction period' by having enhanced detection (to give early warning) and resilience (so that even if a turbine is sabotaged, the grid remains stable). Polish analysts have already flagged that OWFs, once feeding the grid, could become attractive targets and that their location far offshore increases the response time of security services, making them more vulnerable if not specially. This calls for innovative solutions, like on-site autonomous surveillance drones or acoustic sensors for underwater threats, which operators might implement in partnership with the government.

Section Six: Impact of EU Directives: CER and NIS2

European Union initiatives significantly influence Poland's approach to critical infrastructure protection by requiring updates in physical security governance and cybersecurity.

Critical Entities Resilience (CER) Directive

The EU CER Directive (2022/2557) requires member states, including Poland, to strengthen the resilience of critical entities across 11 energy sectors against all hazards (European Parliament and Council, 2022b). For OWFs, this marks a significant shift from voluntary protection measures to enforceable obligations.

For Poland, implementing the CER Directive means they must: identify critical entities, such as major OWF operators based on their role in national energy security; appoint a Competent Authority (likely RCB or a successor) with powers to inspect, enforce, and sanction operators failing to meet resilience standards; ensure OWF operators conduct risk assessments and develop resilience plans with an integrated multi-hazard approach which covers both physical and cyber threats; implement incident reporting, obligating entities to notify authorities of major disruptions, such as sabotage or cable damage; and adopt a national CI resilience strategy by 2026, mapping risks, coordination mechanisms, and cross-sectoral dependencies.

The directive also promotes international cooperation, aligning with Poland's regional efforts, such as the June 2025 Baltic MoU on infrastructure protection. CER pushes Poland to empower a central CI authority, close institutional gaps, and harden OWFs against complex hybrid threats. Analytically, the Directive forces Poland to transition from voluntary compliance to enforceable obligations. Its success depends on whether national law creates real supervisory powers, or whether Poland continues to rely on informal cooperation. If implemented robustly, CER could close long-standing accountability gaps; if weakly transposed, it risks remaining trapped within another layer of paper regulation.

NIS2 Directive

The NIS2 Directive (EU 2022/2555) strengthens cybersecurity requirements for critical sectors, including energy (European Parliament and Council, 2022a). EU states must transpose it – Poland included – by October 2024. Offshore wind farm (OWF) operators will fall under NIS2 as 'essential entities', subject to strict obligations.

Key requirements include: cybersecurity measures requiring OWFs operators to implement robust technical and organisational controls, including incident response, supply chain security, and business continuity plans; incident reporting mandating major cyber incidents to be reported to national authorities within 72 hours, and the establishment of governance and oversight bodies accountable for cybersecurity compliance, in cooperation with designated national authorities responsible for enforcement.

Poland could harmonise enforcement under the Ministry of Digital Affairs or a new Cybersecurity Authority. NIS2 also indirectly applies to agencies like the Navy and Border Guard by obliging them to harden their systems and cooperate in joint cyber-physical response scenarios. Poland's legislative update, including a revised Cybersecurity System Act, is underway.

Aligning with the CER Directive, NIS2 advances an integrated resilience model requiring digital and physical safeguards. The challenge lies in implementation, coordination between authorities, and ensuring operator

readiness. Poland's fast-tracked legal reforms and regional cooperation signal a commitment to meeting these high standards. This creates both opportunity and burden. On one hand, NIS2 strengthens resilience by aligning cyber and physical security; on the other, it imposes significant compliance costs on new Polish operators still building expertise. Effective implementation will require state support, sector-wide information-sharing mechanisms (e.g., Information Sharing and Analysis Centre), and coordination between energy and cyber authorities. Together, CER and NIS2 reshape OWFs' protection into a binding legal duty. Their impact, however, hinges on Poland's ability to integrate EU requirements with domestic enforcement and avoid duplication across ministries.

Section Seven: Challenges, Implementation Issues, and Recommendations

Despite significant progress in legal frameworks and strategic awareness, Poland faces multiple implementation challenges in effectively securing OWFs as critical infrastructure.

Fragmented Coordination

Maritime security responsibilities are dispersed among several agencies – the Navy, the Border Guard, the Maritime Offices, the Police, and the SAR services – often operating without a unified command structure. This fragmentation can lead to operational confusion or delayed response. For instance, a suspicious vessel near an OWF could be tracked simultaneously by the Navy, Border Guard, and Maritime Office, with no clear lead agency.

To address this, Poland must establish a Maritime Security Coordination Centre, possibly by expanding the Navy's Maritime Operations Centre that operates 24/7, integrating the Navy, Border Guard, Maritime Office, and Police inputs. This centre would fuse radar/AIS feeds from all sources into one picture and have direct communication links to all patrol units. It would function much like a 'coast guard command'. A logical approach is to expand

the Navy's Maritime Operations Centre in Gdynia into a Joint Maritime Security Centre staffed by officers from each agency. This centre would coordinate responses in real-time, eliminating delays from fragmented decision-making. A single watch officer with authority can dispatch the Navy or Border Guard asset closest to an OWF upon detecting a threat. Such integration addresses the current 'fragmentation and incompatible systems' identified. It also ensures no more gaps or overlaps as agencies will act in concert, guided by a unified command. The centre can also be Poland's point of contact for international coordination (linking with NATO's Maritime Security Centre or neighbouring states' ops rooms as needed). This would enable joint situational awareness, real-time decision-making, and seamless civil-military cooperation.

Resource Limitations

In tandem with the above, Poland should strengthen the coast guard function by reorganising and reinforcing the Maritime Border Guard. The current fleet of patrol vessels is ageing and insufficient for long-term offshore presence, especially in harsh Baltic conditions. Many analysts advocate establishing a bona fide Polish Coast. The quickest path is to build on the existing Maritime Branch of the Border Guard, expanding its resources and transferring certain Navy non-combat vessels to it. The Coast Guard would be responsible for day-to-day law enforcement and security in Polish maritime areas, including OWF protection, while the Navy focuses on high-end defence.

Key steps would include procuring new multi-role offshore patrol vessels for the Coast Guard, recruiting and training additional personnel, and explicitly updating the Border Guard Act to cover EEZ infrastructure protection (as previously noted). By adding a clause to Article 14(3) extending BG powers to the contiguous zone/EEZ for critical infrastructure security, Border Guard units will have a clear legal footing to act around. A well-equipped Coast Guard can conduct regular patrols at wind farm sites, provide armed escort to maintenance teams if threat levels are high, and quickly respond to intrusions, relieving the Navy from routine tasks and allowing specialisation. Offshore

Poland's Coast Guard should similarly be multi-mission: safety, security, and environmental protection around OWFs.

Poland must invest in modern offshore patrol vessels (OPVs), drones for wide-area surveillance, and underwater detection systems (e.g., sonar, UUVs). Standing it up will require political will and funding, but it is an investment in long-term maritime security as Poland's blue economy (wind, shipping, pipelines) grows. Innovation from domestic startups and co-financing from OWF operators could accelerate capability development. Funding from EU or NATO programmes, such as those dedicated to Baltic maritime security, should be leveraged where possible.

Legal and Regulatory Gaps

Domestic legislation must catch up with strategic needs. Amendments are needed to extend Border Guard jurisdiction in the EEZ and designate OWFs (and their onshore substations) as facilities requiring mandatory protection. Clear legal frameworks are also needed to govern military support to civilian operations at sea, especially in hybrid threat scenarios.

Poland should also enact a comprehensive Critical Infrastructure Protection Act (or amend existing laws) to implement the CER directive. This act should: designate the Competent Authority by making either RCB or a new 'National Critical Infrastructure Authority' the clear lead, grant it powers to audit and sanction CI operators, and mandate regular resilience assessments by operators. It should reconcile the existing Crisis Management Act with CER by updating definitions by aligning 'critical infrastructure' with 'critical entities' terminology and ensuring no overlap or conflict with the new Protection of People and Property Act. Specifically, it should preserve a central coordination role, as it can also be problematic to scatter CI duties among multiple. The law could explicitly establish an RCB 2.0 with an Inspectorate for Critical Infrastructure Resilience empowered to conduct inspections at OWF facilities (onshore control centres, etc.) and impose fines or orders. This will instil compliance.

Poland must also finalise the NIS2 transposition. The updated National Cybersecurity System Act should clarify that OWF operators are essential entities and fall under energy sector oversight (likely by the energy ministry working with the cybersecurity authority). It should set out penalty frameworks for lapses and encourage information-sharing by formalising an Information Sharing and Analysis Centre (ISAC) for the energy sector, where OWF operators and authorities can exchange cyber threat intelligence. Since CER and NIS2 overlap on aspects like risk assessment, Poland's implementation should create synergies such as a single reporting portal for incidents to both the cyber-CERT and the CI authority, to reduce duplication for operators.

Additionally, Poland should update the Anti-Terrorism Act regulations to explicitly list OWFs as facilities that can receive enhanced protection measures during heightened alerts. This might include authorising the use of military assets (e.g. deployment of Marines or Military Police) to guard OWF infrastructure if an alert level Charlie/Delta is declared for maritime terrorism risk. Given that OWFs are remote, pre-arranging rapid deployment teams (e.g., a helicopter-delivered commando squad that can reach an OWF platform) when an alert is up is prudent.

A final legal recommendation is to revise the list of 'mandatory protected' facilities under the Protection of People and Property Act to include onshore and offshore critical energy infrastructure. For offshore, this could be worded as requiring operators to implement 'adequate physical protection measures' subject to approval by the Police and ABW, analogous to onshore sites, although the enforcement mechanism at sea differs, as direct state supervision and guarding are more complex in a maritime environment and typically rely on coordination with the Border Guard or Navy rather than on-site security personnel. In practice, an OWF operator might have to hire vessel patrols or install specific security systems as part of mandatory protection, all coordinated with state authorities. Coordination with local authorities (e.g., voivodes, maritime governors) must also be codified, as they play critical roles in initial incident response.

Operational Readiness and Training

Security plans must be tested through realistic, multi-agency exercises simulating OWF-specific threats, such as underwater sabotage or coordinated cyber-physical attacks. Poland should implement a regular schedule of multi-agency exercises focused on the security of OWFs and subsea cables. Annual scenario-based drills (e.g., 'Baltic Shield') should simulate diverse hybrid threats – such as sabotage, cyber-physical disruptions, or underwater attacks – engaging OWF operators, naval forces, police, and international partners. These exercises will expose operational gaps and train personnel in complex response tasks.

These should involve *Formoza* [Naval Special Forces], Border Guard units, police bomb squads, and OWF staff. Exercises should stress-test communications, response times, and interagency protocols. The new regional MoU with the Baltic states enables joint drills, which should simulate cross-border sabotage scenarios to enhance interoperability.

Complement this with independent red-teaming, inviting allied experts to conduct controlled cyber and physical penetration tests to assess system resilience. At the strategic level, run tabletop exercises involving ministries and crisis bodies to test decision-making in scenarios like OWF shutdowns, repair prioritisation, and public communication. Together, these drills will strengthen preparedness across operational and policy domains.

Finally, continuously evaluate and update plans. Use the feedback loop from incidents elsewhere (e.g. learn from what happened with the Finnish-Estonian pipeline cut in 2023, or North Sea cable cuts) to adjust Polish plans. The threat landscape evolves, so a yearly review of the OWF security strategy, perhaps coordinated by RCB with all stakeholders, will keep the system resilient and ready. This aligns with CER's requirement for regular risk assessments and supervision.

Intelligence and Early Warning

Preventing sabotage requires actionable intelligence shared with operational units in time to act. Intelligence agencies (ABW, The Military Counterintelligence Service (SKW)) must collaborate with maritime forces and OWF operators without compromising sources. Poland should establish clear procedures for threat-level escalation and response (e.g., increasing patrols based on intelligence about possible attacks). EU platforms like the Critical Infrastructure Resilience Group offer opportunities for coordinated threat assessment.

Poland must invest in a state-of-the-art maritime domain awareness (MDA) system covering its OWF areas. This includes deploying additional sensors: high-resolution coastal radars, long-range day/night cameras, and hydro-acoustic sensors to detect underwater vehicles or divers. The aim is to ensure that any approaching surface or subsurface threat is detected as early as possible. Given the difficulty of constant physical presence, force-multiplying technologies like drones (UAVs) and USVs should be rapidly integrated. The government should expedite the purchase of long-endurance drones capable of patrolling OWF as indicated in May 2025. It should also consider unmanned surface or underwater vehicles that can loiter around critical sites. NATO's ongoing experiments with drone boats could be leveraged – Poland can seek to host or contribute to these capabilities for persistent OWF monitoring. Additionally, equipping some wind turbines with monitoring gear (radar or sonar nodes) could create a distributed sensor network. Since turbines have power and height, mounting radar/camera units on a few would greatly extend coverage and help track low-signature threats. The Maritime Offices or the Navy could partner with operators to install these – a form of public-private tech cooperation.

Crucially, all these sensors must feed into the integrated command centre (Recommendation 9.1) to share real-time data. Poland should use intelligence cues (e.g., NATO intel about suspicious vessels, either USV or manned) to dynamically re-task surveillance assets to potential hot spots. Given the concern that 'if a ship turns off AIS, authorities only have a radar blip and

must scramble a patrol to identify it', better sensor coverage and automated anomaly-detection software (possibly with AI) should be implemented as suggested by the Naval Academy. The goal is to shorten reaction times – detect, classify, and intercept a threat before it reaches a turbine or cable. Funding for these upgrades could be drawn from a combination of sources: the national defence budget (particularly for dual-use technologies), EU security and resilience funds, and financial contributions from OWF operators – potentially as a licensing condition requiring developers to co-finance designated security measures.

Public-Private Collaboration

NIS2 and CER formalise the relationship between sectors, but building day-to-day trust remains critical. OWF operators must be treated as security partners, not just regulated entities. They need confidence that reporting anomalies (e.g., suspicious objects on a turbine) will not lead to liability but prompt support. Encourage OWF operators to exceed minimum security requirements through incentives and partnerships. For instance, the government can create a co-financing programme where, if an operator invests in advanced security (like underwater drone detection or extra backup power systems), the state covers part of the cost or gives regulatory credits. This could be framed as part of corporate social responsibility for energy companies – protecting critical infrastructure is protecting customers and the nation.

Operators should also be involved in the early design stage of security measures. Because they know their systems best, their input can ensure that protective measures are practical and do not overly hamper operations (security should enable resilience, not choke the business). A forum or working group between OWF industry representatives and security agencies (Navy, RCB, etc.) can be set up to exchange ideas and best practices regularly.

Poland can also tap into its tech sector and EU research funds to develop custom solutions for Baltic Sea conditions. For example, support Polish tech companies to build robust wind-farm monitoring software using AI, as

suggested by naval experts, which can learn standard patterns of vessel movement and flag anomalies (Miętkiewicz, 2018). Alternatively, create hardening kits for undersea cables (making them less snag-prone or easier to fix). By becoming a testbed for such innovations, Poland could turn security into an exportable expertise, in line with the notion of being a 'leader in the region by developing good practices'

Public Communication and Political Support

Finally, an often overlooked but vital part of resilience is public confidence. The government and operators should maintain a clear communication strategy about OWF security. Without revealing sensitive details, they should inform local communities (e.g. fishermen, port authorities, sailors) about the presence of safety zones and why they matter. Restrictive measures such as exclusion zones or increased patrols must be communicated effectively to maintain public and industry support. Public signage, notices, and even community meetings can foster understanding that these are protected sites akin to an airport or power plant.

Disinformation campaigns targeting wind energy or attempting to delegitimise security responses pose an added challenge. When incidents happen or suspicious activities are noted, timely factual communication can pre-empt rumour and disinformation. For example, if a drone is spotted and investigated, say so publicly (once it is safe) to prevent wild theories. Emphasise positive steps: Poland can highlight that it has increased patrols or caught a suspicious vessel (like in May 2025) – this signals both deterrence to adversaries and reassurance to citizens/investors.

In the event of an actual attack or accident, having a prepared crisis communication plan (who addresses media, what initial info to release) will be essential to maintain order and trust. Strategic communication – transparent, proactive, and coordinated – is key to maintaining legitimacy and resilience. This is part of psychological resilience; it deters adversaries, too, because they see that sabotage will not cause panic or chaos, just a firm and managed response.

Conclusion

In conclusion, Poland's road to safeguarding its OWFs involves organisational reform, capacity building, legal updates, and continuous vigilance. The evolving security landscape – with hybrid threats blending physical and cyber elements – demands a holistic approach. Poland should adopt a defence-in-depth strategy for offshore wind farm (OWF) protection, combining layered measures to deter, detect, and respond to threats.

Increasing Navy and Border Guard presence around OWFs, especially during high-risk periods, will act as a deterrent. Implementing rotational 'Navy policing' patrols with Baltic allies will project a persistent security presence.

Creating a specialised maritime quick-reaction unit (e.g., *Formoza*, sappers, medics) capable of rapid deployment to OWFs by sea or air in combination with regular drills will ensure a swift, coordinated response in the event of sabotage attempts.

Collaborating with OWF operators and the grid to ensure backup systems – extra cables, routing options, spare parts, and emergency power – to minimise disruption from attacks or failures will increase essential resilience and redundancy.

Deploying drone and diver detection systems (RF sensors, sonar, jammers) at OWFs and on patrol assets will increase threat detection in order to better counter unmanned systems. Launching a pilot 'Safe Wind Farm' programme to field-test integrated anti-drone and anti-UUV technologies will continue to develop safety and security measures.

Deepening Baltic-NATO coordination and establishing a regional infrastructure threat hub will support sharing real-time intelligence on maritime threats (e.g., 'ghost fleet'), and aligning patrol areas will foster continued regional and international cooperation while enhancing situational awareness and joint action.

Poland can create a robust shield around its critical offshore energy assets, turning them into a strategic strength rather than a vulnerability. Only through unified, innovative effort can Poland ensure its offshore wind programme thrives safely under even the harshest conditions, whether delivered by nature or man. Together, these steps form a layered, resilient defence architecture for protecting critical offshore energy infrastructure.

AI Statement: No AI was used in writing this article. AI assisted programs were used, specifically Grammarly, Evernote for bibliography, and Safari search engine

Bibliography

Adomaitis, N. (2022) 'Norway oil safety regulator warns of threats from unidentified drones', *Reuters*, [online] 26 September. Available at: https://www.reuters.com/business/energy/norway-oil-safety-regulator-warns-threats-unidentified-drones-2022-09-26/. (Accessed: 17 October 2025).

Baltic Wind EU (2025) 'Baltic Sea Offshore Wind Summit: Security Takes Center Stage Amid Geopolitical Tensions', *Baltic Wind*, [online] 18 March. Available at: https://balticwind.eu/baltic-sea-offshore-wind-summit-security-takes-center-stage-amid-geopolitical-tensions/. (Accessed: 15 July 2025).

Edvardsen, A. (2022) 'Russian citizen arrested in Northern Norway for drone flights on Svalbard', *High North News*, [online] 20 October. Available at: https://www.highnorthnews.com/en/russian-citizen-arrested-northern-norway-drone-flights-svalbard. (Accessed: 17 October 2025).

Erling, B. and Strzelecki, M. (2025) 'Poland intervenes as Russian "shadow fleet" ship spotted near power cable', *Reuters*, [online] 21 May. Updated 22 May. Available at: https://www.reuters.com/world/europe/poland-says-russian-ship-performed-suspicious-manoeuvres-near-cable-sweden-2025-05-21/. (Accessed: 13 July 2025).

European Parliament and Council (2022a) *'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)*'. Official Journal of the European Union, L333/80, [online] 27 December, pp. 80-152. Available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng. (Accessed: 14 July 2025).

European Parliament and Council (2022b) '*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 European Union, L333/164, [online] 27 December, pp.164-198. Available at: https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng (Accessed: 19 March 2026).

Government of Poland (1990) *Ustawa z dnia 12 października 1990 r. o ochronie granicy państwowej* [Act of 12 October 1990 on State Border Protection], Dziennik Ustaw, 1990, 78(461). Available at: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19900780461. (Accessed: 14 July 2025).

Government of Poland (1991) *Ustawa z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej* [Act of 21 March 1991 on the Maritime Areas of the Republic of Poland and Maritime Administration], Dziennik Ustaw, 1991, 32(131), art. 22-24. Available at: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19910320131. (Accessed: 13 July 2025).

Government of Poland (1997a) *Ustawa z dnia 10 kwietnia 1997 r. – Prawo energetyczne* [Act of 10 April 1997 – Law on Energy], Dziennik Ustaw, 1997, 54(348). Available at: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19970540348/U/D19970348Lj.pdf. (Accessed: 14 July 2025).

Government of Poland (1997b) *Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia* [Act of 22 August 1997 on the Protection of Persons and Property], Dziennik Ustaw, 1997, 114(740). Available at: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu19971140740. (Accessed: 14 July 2025).

Government of Poland (2001) *Ustawa z dnia 18 września 2001 r. Kodeks morski* [Act of 18 September 2001 on Maritime Code], Dziennik Ustaw, 2001, 138(1545). Available at: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu20011381545. (Accessed: 14 July 2025).

Government of Poland (2007) *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym* [Act of 26 April 2007 on Crisis Management], Dziennik Ustaw, 2007, 89(590). Available at: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20070890590. (Accessed: 13 July 2025).

Government of Poland (2016) *Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych* [Act of 10 June 2016 on Counter-Terrorism Measures], *Dziennik Ustaw*, 2016, poz. 904. Available at: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000904/T/D20160904L.pdf *(Access: 14 July 2025).*

Kardaś, S. and Łoskot-Strachota, A. (2022) '*Dywersja na gazociągach Nord Stream 1 i Nord Stream 2*' [Sabotage of the Nord Stream 1 and Nord Stream 2 gas pipelines], *Ośrodek Studiów Wschodnich*, [online] 29 September. Available at: https://www.osw.waw.pl/pl/publikacje/analizy/2022-09-29/dywersja-na-gazociagach-nord-stream-1-i-nord-stream-2. (Accessed: 17 October 2025).

Ledzińska, P. (2025) '*Premier: podjęliśmy decyzję o uruchomieniu realizacji zamówienia dronów przez Marynarkę Wojenną*', [Prime Minister: we have decided to launch the implementation of the Navy's drone procurement], *PortalMorski*, [online] 23 May. Available at: https://polskamorska.pl/2025/05/23/premier-podjelismy-decyzje-o-uruchomieniu-realizacji-zamowienia-dronow-przez-marynarke-wojenna/. (Accessed: 17 October 2025).

Loba, N. (2025) 'The role and tasks of the state in the scope of strategic security of offshore energy, including in particular offshore wind energy', *Bezpieczeństwo Narodowe*, 46(1), pp. 173-198. DOI: https://doi.org/10.59800/bn/207650.

Lorenz, W. and Zaręba, S. (2022) 'Consequences of the Nord Stream 1 and 2 Gas Pipeline Explosions', *PISM*, [online] 125-2022, 29 September. Available at: https://pism.pl/publications/consequences-of-the-nord-stream-1-and-2-gas-pipeline-explosions. (Accessed: 14 September 2025).

Miętkiewicz, R. (2018) *Wykorzystanie bezzałogowych jednostek nawodnych w zabezpieczeniu morskich obiektów infrastruktury krytycznej* [Use of unmanned surface vessels in securing maritime critical infrastructure facilities]. Gdynia: Akademia Marynarki Wojennej im. Bohaterów Westerplatte.

NATO Supreme Headquarters Allied Powers Europe (2024) Baltic Sentry, *NATO SHAPE*, [online] Available at: https://shape.nato.int/operations/operations-and-missions/baltic-sentry. (Accessed: 13 July 2025).

PGE Baltica and Ørsted (2023) '*Podsumowanie Nietechniczne Morskiej Farmy Wiatrowej Baltica 2'* [Non-Technical Summary of the Baltica 2 Offshore Wind Farm], *PGE Baltica and Ørsted*, [online] Available at: https://pgebaltica.pl/o-spolce/kluczowe-dane-o-projektach/baltica-2. (Accessed: 13 July 2025).

Projekt Infrastruktura Krytyczna (2023) *Dyrektywa CER* [CER Directive], *Projekt Infrastruktura Krytyczna*, [online] Available at: https://projektik.eu/dyrektywa-cer/ R - Projekt IK. (Accessed: 23 October 2025).

Romowicz, M. and Niewiński, P. (2021) 'Offshore wind farms as critical infrastructure in the security system', *MarinePoland.com*, [online] 5 August. Available at: https://www.marinepoland.com/shipyards-offshore-wind-farms-as-critical-infrastructure-in-the-security-system-1363. (Accessed: 13 July 2025).

Romowicz, M. and Niewiński, P. (2023) 'Poland urgently needs Coast Guard', *MarinePoland.com*, [online] 6 July. Available at: https://www.marinepoland.com/poland-urgently-needs-coast-guard-1910. (Accessed: 13 July 2025).