Terrorism – Studies, Analyses, Prevention, 2025, special edition: 35–70

https://doi.org/10.4467/27204383TER.25.014.21517

Article

Hybrid threats in the Baltic Sea. The results of analysis of countermeasure options

RAFAŁ MIĘTKIEWICZ

https://orcid.org/0000-0002-3129-7092

Polish Naval Academy
of the Heroes of Westerplatte

Abstract

The maritime areas of the Baltic region, can be considered a space for the conduct of proxy conflict, i.e. of a substitute nature, between the Russian Federation and Western states. Intensifying since 2022 (the start of Russia's full-scale invasion of Ukraine) hybrid actions on the part of Russia have largely targeted the critical infrastructure facilities of coastal states. The article discusses the various forms of subliminal actions against this infrastructure undertaken by Russia, based on available information on events in the period from 2022 to the end of 2024. It also presents the vulnerabilities to hybrid actions that characterise critical infrastructure in the Baltic (possible ways of affecting port facilities and offshore infrastructure, with a particular focus on undersea transmission lines). The publication also presents the author's views on possible responses from NATO countries, in the form of political, military and technological initiatives, to hybrid threats posed by modern maritime autonomous systems.

Keywords

hybrid threats at sea, hybrid conflict, maritime critical infrastructure

Introduction

The situation in the Baltic Sea is under the influence of dynamic processes shaping the security architecture in the region. It can be concluded that the Baltic Sea basin is a space of substitute rivalry between Russia, which strives to change the current order in Europe, and Western countries (the European Union and NATO), which support Ukraine. At the same time, the Baltic Sea is a corridor enabling the countries of the region (NATO's flank) to become independent of hydrocarbon supplies from Russian sources (which the Kremlin uses as a tool of coercion or reward) and to diversify the supply of energy resources (mainly natural gas and oil). The Baltic Sea is also playing an increasingly important role in the production of electricity using renewable energy sources (offshore wind energy with a potential estimated by the European Commission at 93 GW by 2050[1]). In the case of Poland, the energy dependence rate on the Baltic Sea, taking into account the ratio of imports of major energy resources and energy carriers to their total consumption, was 48% in 2024. By 2040, this ratio is expected to reach 60%[2]. At the same time, this basin remains an important area for the implementation of the strategic goals of the Russian Federation (RF). The presence of a heavily militarised exclave of Kaliningrad, the St Petersburg region (anti-access-area denial, A2/AD capabilities) with important ports (oil exports), gas transmission infrastructure (damaged NS1 and NS2 gas pipelines) and the Baltic Fleet of the RF operating in the waters of the Baltic Sea are just the most important elements that make up Russia's Baltic assets. The Russian maritime doctrine introduced in 2022 lowered the rank of the Baltic Sea (the document identifies three levels of importance of the basins, as vital, important and others), indicated the confrontational direction of Russia's policy towards Western countries (total hybrid war) and the desire to remodel the current world order as well as international security architecture[3]. The challenges that the countries of the Baltic region have been facing for years, and which have been intensifying since the beginning of the war in Ukraine, clearly indicate that the RF has not abandoned its efforts

[1] *Study on Baltic offshore wind energy cooperation under BEMIP. Final report*, ENER/C1/2018-456, Luxembourg 2019, Publications Office of the European Union, p. 10.

[2] Z. Nowak, M. Maj, *Bałtyk jako przestrzeń strategicznej aktywności energetycznej* (Eng. The Baltic Sea as a space for strategic energy activities), in: *Czy morze pomoże? Bałtyk a bezpieczeństwo energetyczne Polski*, Z. Nowak (ed.), Warszawa 2024, Institute for Foreign Affairs, pp. 33–46.

[3] *Maritime Doctrine of the Russian Federation*, A. Davis, R. Vest (trans.), Newport 2022, Russia Maritime Studies Institute, United States Naval War College.

to break the unity of the coastal states using the instruments in its resources. Long before Russia's attack on Ukraine, strategic Polish publications pointed to hybrid activities as an important means of achieving the goals of the RF below the threshold of war[4] and the main threats of military and non-military origin in the Baltic region[5].

The reason for increased hybrid threats in the future may be the ineffectiveness of many of the actions taken by Russia against the states on the Baltic Sea[6]. As the situation deteriorates, the anticipated threats of direct nature may include the use of armed forces and threats of their use, as well as indirect forms (in the case of sea basins, we are talking about e.g. maritime blockades, shows of force using fleet, unannounced military exercises, harassment of the enemy, etc.)[7]. A typical state of affairs will be blurring the boundaries between a state of peace and a state of war, asymmetry, the growing importance of non-kinetic activities (especially active operations in cyberspace), or the use of autonomous technologies[8]. The intensification of the conflict and Russia's use of new forms of action is indicated by the events that occurred in the Baltic Sea in 2023–2024. In October 2023, the Balticconnector gas pipeline was damaged by the Hong Kong-flagged vessel Newnew Polar Bear, which was operating a voyage from Kaliningrad to St Petersburg. The Balticconnector was restarted in April 2024[9]. After more than 10 months of investigation into the matter

[4] *National Security Strategy of the Republic of Poland*, Warszawa 2020.

[5] *Poland's Strategic Concept for Maritime Security*, Warszawa–Gdynia 2017, Biuro Bezpieczeństwa Narodowego (Eng. National Security Bureau), p. 11.

[6] P. Mickiewicz, *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, p. 71.

[7] A. Nowakowska-Krystman, *Potencjał obronny Sił Zbrojnych RP w ujęciu relatywnym* (Eng. Defence potential of the Polish Armed Forces in relative terms), Warszawa 2018, Akademia Sztuki Wojennej, p. 73.

[8] R. Kasprzyk, *Sztuczna inteligencja i cyberprzestrzeń a proces złośliwego sterowania ludźmi i maszynami* (Eng. Artificial intelligence and cyberspace and the process of malicious control of humans and machines), in: *GlobState*, vol. 2. *Wyzwania dla Polski w kontekście zmian w środowisku bezpieczeństwa*, Ł. Jureńczyk, R. Reczkowski (sci. ed.), Bydgoszcz 2020, Centrum Doktryn i Szkolenia Sił Zbrojnych – Uniwersytet Kazimierza Wielkiego, pp. 277–298.

[9] J. Hyndle-Hussein, *The Balticconnector gas pipeline damage,* Ośrodek Studiów Wschodnich, 11.10.2023, https://www.osw.waw.pl/en/publikacje/analyses/2023-10-11/balticconnector-gas-pipeline-damage [accessed: 2.01.2025].

by the Finnish side, the explanation from the Chinese side that the damage to the facility was accidental has not been confirmed[10]. Two fibre-optic telecommunications connections Lithuania – Sweden and Finland – Germany were severed in November 2024, and the EstLink 2 submarine power line connecting Finland and Estonia was damaged in December 2024. One of Russia's activities is the use of the so-called *grey fleet* and the so-called *dark fleet* or *shadow fleet*. The term grey fleet refers to a quasi-legal fleet (unclear origin and ownership of the vessel and flag) operating alongside the International Maritime Organization (IMO) positively considered fleet. A dark fleet is one that uses illegal practices (tampering with identifiers and location or deliberately disabling automatic identification systems) to circumvent sanctions on Russia's oil trade[11].

The research problem boils down to answering the question: how to counteract Russian hybrid activities against critical infrastructure (CI) facilities at sea? The aim of this article is to first present possible forms of hybrid activities in the Baltic Sea as a reference basin (partly based on the analysis of past events) that may occur in the next 2 years in relation to offshore CI facilities. Secondly, the vulnerabilities determining the possibility of creating hybrid threats in relation to CI facilities in the Baltic Sea will be specified. In the next step, proposals for actions will be identified to counter this type of threat and increase the level of protection of CI facilities at sea.

A critical analysis of the following sources was carried out in order to develop this paper[12]:

- documents in the form of: doctrines (*Maritime Doctrine of the Russian Federation*, A. Davis, R. Vest, trans.), strategies (*REPowerEU Plan, Communication from the Commission to the European Parliament, the European Council, the Council, The European Economic and Social Committee and the Committee of the Regions*; *Council conclusions on*

[10] *Finlandia: Władze nie potwierdzają informacji o „przypadkowym" uszkodzeniu Balticconnector* (Eng. Finland: Authorities do not confirm information on "accidental" damage to Balticconnector), Portal Morski, 13.08.2024, https://www.portalmorski.pl/offshore/56252-finlandia-wladze-nie-potwierdzaja-informacji-o-przypadkowym-uszkodzeniu-balticconnector [accessed: 29.01.2025].

[11] *Russia's 'shadow fleet': Bringing the threat to light*, European Parliament, https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766242/EPRS_BRI(2024)766242_EN.pdf, p. 3 [accessed: 23.01.2025].

[12] The source materials analysed are only listed here. Their full bibliographic description is given in the appendix bibliography (editor's note).

the Revised EU Maritime Security Strategy (EUMSS) and its Action Plan; *National Security Strategy of the Republic of Poland 2020*; *Poland's Strategic Concept for Maritime Security*; *Energy Policy of Poland until 2040*), official government information (*Joint Declaration on cooperation to secure critical subsea infrastructure*), report of state institution – Supreme Audit Office (*Information on the results of the audit. Preparation of the state for threats related to hybrid actions; Information on the results of the audit. Implementation of measures to improve fuel security in the oil sector*) and publications of international organisations: European Parliament (*P9_TA(2024)0079 – Russiagate: allegations of Russian interference in the democratic processes of the European Union – European Parliament resolution of 8 February 2024 on Russiagate: allegations of Russian interference in the democratic processes of the European Union (2024/2548(RSP))*), European Commission (*Joint Statement by the European Commission and the High Representative on the Investigation into Damaged Electricity and Data Cables in the Baltic Sea*), Baltic Marine Environment Protection Commission (*HELCOM, ensuring safe shipping in the Baltic*), NATO (N. Fridbertsson, *General Report – Protecting Critical Maritime Infrastructure – The Role of Technology*; A. Hagelstam, *Cooperating to counter hybrid threats*), Atlantic Council (E. Braw, *Russia's growing dark fleet: Risks for the global maritime order*);

- available (non-confidential) materials, including press releases (*Finland-Estonia power cable hit in latest Baltic Sea incident*, "The Guardian"; C. Chiappa, *6 countries move to protect the North Sea from Russians*, "Politico"), announcements of the ministries of the Baltic states, post-conference studies by GlobState (K. Kasprzyk, *Artificial intelligence and cyberspace and the process of malicious control of humans and machines*);
- studies of renowned centres dealing with the issue of hybrid threats, such as: Hybrid Centre of Excellence (*Handbook on maritime hybrid threats: 15 scenarios and legal scans*), Maritime Security Centre of Excellence (D. Doğan, D. Çetikli, *Maritime Critical Infrastructure Protection (MCIP) in a Changing Security Environment*) and international relations, such as: the International Centre for Defence and Security (N. Aliyev, *Does Russia want to revise its water border with the Nordic and Baltic states?*), U.S. Helsinki Commission (S. McGrath, *Spotlight on the Shadow War: Inside Russia's Attacks*

on NATO Territory), Ośrodek Studiów Wschodnich (J. Hyndle-Hussein, *The Balticconnector gas pipeline damage*), as well as industry portals Baltic Wind EU dealing with international aspects of maritime development wind energy in the Baltic Sea (K. Bulski, *The Role of the New European Commission and Regional Cooperation in Accelerating Offshore Wind in the Baltic Sea*);

- publications of well-established think tanks, such as: The Polish Institute of International Affairs (K. Dudzińska, *Sweden Takes a Nuclear Turn in Energy Policy*), Center for International Maritime Security (O. Chiriac, *The 2022 Maritime Doctrine of the Russian Federation: Mobilization, Maritime Law, and Socio-Economic Warfare*), The Opportunity Institute for Foreign Affairs (R. Miętkiewicz, *The Baltic Sea as a special protection area*), Warsaw Institute (B. Fraszka, *Baltic States and Russian Hybrid Threats*), Polish Society for National Security (K. Wojtasik, *Results of the survey on the perception of terrorist threats among EU PSA participants*), I. Łukasiewicz Institute of Energy Policy (M. Ruszel, P. Ogarek, *Poland's fuel security in the context of ownership changes in the petroleum products logistics market and the European Commission's remedies on the merger between PKN ORLEN and LOTOS Group. Poland at the threshold of the embargo on petroleum products from Russia – opening analysis 2023*);
- cyber threat analyses published by the European Union Agency for Cybersecurity (*ENISA Threat Landscape 2024*), and American Cybersecurity and Infrastructure Security Agency (*Russian Military Cyber Actors Target US and Global Critical Infrastructure*);
- previous research work devoted to the issues of contemporary threats at sea (R. Miętkiewicz, *Dumped conventional warfare (munition) catalog of the Baltic Sea*; R. Miętkiewicz, *High explosive unexploded ordnance neutralization – Tallboy air bomb case study*), including those created in relation to offshore energy infrastructure facilities (R. Miętkiewicz, *Offshore wind farms and national maritime security;* R. Miętkiewicz, *The Baltic Sea as a special protection area*) and works on the use of modern technologies (R. Miętkiewicz, *Autonomous systems in maritime operations*; R. Miętkiewicz, *Offshore energy infrastructure facilities – an attempt to determine vulnerability to attacks by unmanned platforms*). The results of the EU Protective Security Advisors expert survey were also taken into account

(K. Wojtasik, *Results of the survey on the perception of terrorist threats among EU PSA participants*)[13].

Hybrid threats

Hybrid threats are harmful and intentional activities that are planned and carried out used by authoritarian states and regimes including non-state actors that often act as proxies to undermine a target (state or an institution), through a variety of means, often combined[14]. The use of multiple actors and activities promotes synergies that amplify the effectiveness of the attack. Hybrid threats are constantly changing and the tools used cover the full spectrum of activities, including: advanced cyberattacks[15], information manipulation (including by means of fake social media profiles), economic influence as well as behind-the-scenes political maneuvering, coercive diplomacy (influence and interference operations), or threats of military force. The characteristic features of hybrid conflicts are constant change and the problem with defining all its aspects. It combines conventional and unconventional actions, symmetry and asymmetry, state and non-state actors (sometimes difficult to identify operating below the detection and identification threshold). The attacker's objective is to launch coordinated strikes at points of key importance to the opponent (e.g. systemic weaknesses of democratic states)[16].

[13] A new survey of EU PSA participants was conducted in February 2025, the results of which are presented in the article: K. Wojtasik, D. Szlachter, *Results of the survey on the perception of terrorist and sabotage threats among the experts of the EU Protective Security Advisors*, "Terrorism – Studies, Analyses, Prevention", special issue: *Terrorist and sabotage threats to critical infrastructure*, pp. 249–270. https://doi.org/10.4467/27204383TER.25.022.21525 (editor's note).

[14] *Hybrid threats as a concept, Frequently asked questions on hybrid threats*, The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ [accessed: 2.12.2024].

[15] A. Hagelstam, *Cooperating to counter hybrid threats*, NATO Review, 23.11.2018, https://www.nato.int/docu/review/articles/2018/11/23/cooperating-to-counter-hybrid-threats/index.html [accessed: 2.12.2024].

[16] B. Fraszka, *Państwa bałtyckie a rosyjskie zagrożenia hybrydowe* (Eng. Baltic States vs. Russian Hybrid Threats), Warsaw Institute, 26.10.2020, https://warsawinstitute.org/wp-content/uploads/2020/10/Pa%C5%84stwa-ba%C5%82tyckie-a-rosyjskie-zagro%C5%BCenia-hybrydowe-Bartosz-Fraszka.pdf, p. 4 [accessed: 29.12.2024].

The RF is considered to be the most likely source of hybrid threats, due to the current geopolitical situation. The main purpose of such actions is to discredit the position of attacked state internationally (inter alia, by demonstrating the ineffectiveness of the state's efforts in response to crisis situations), to weaken the cohesion of Western alliances and to force it to meet Russia's politic, economic and military demands. An expert from the Polish Association for National Security points out that due to the shortcomings in the equipment of regular units of the Russian armed forces and the level of losses suffered in Ukraine, the emphasis in terms of impact will shift to hybrid operations. The sea area appears to be particularly advantageous due to the inability to exercise full control over it[17].

The results of the terrorist threat perception survey conducted in early 2023 with EU Protective Security Advisors (EU PSA) experts indicated the highest ranking of CI facilities as primary, secondary and tertiary potential targets for terrorist attacks in the EU (63.63% of all indications). Public transport systems came second (60% of responses). Among the facilities most vulnerable to terrorist attack (the choices were: military bases used within NATO, CI facilities, public transport system, commercial goods transport system, headquarters of constitutional state bodies, tourism infrastructure, sports and entertainment facilities, places of worship, headquarters of EU institutions and agencies), most (40%) respondents indicated energy infrastructure facilities[18]. In turn, among many means of carrying out attacks (unmanned aerial vehicles, 3D printing, vehicles used to ram, improvised explosive devices, melee weapons made of composites, CBRN agents, incendiary agents), according to EU PSA experts, it is the autonomous systems that will be most willingly used by terrorists to carry out attacks (49.09%). The vast majority of respondents (81.82%) believed that in the next 3 years, terrorist activity will be used as part of hybrid activities undertaken on the territory of the EU by a foreign country.

[17] 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), Polskie Towarzystwo Bezpieczeństwa Narodowego (Eng. Polish Association for National Security) 2023.

[18] K. Wojtasik, *Analiza wyników badań na temat percepcji zagrożeń o charakterze terrorystycznym wśród uczestników EU PSA* (Eng. Results of the survey on the perception of terrorist threats among EU PSA participants), PTBN Analyses no. 1, Polskie Towarzystwo Bezpieczeństwa Narodowego (Eng. Polish Association for National Security) 2023, p. 5.

The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), having conducted research on contemporary hybrid threats occurring in sea basins, indicated that the scope of activities of this type is very wide. Their forms may include: illegal fishing and the use of fishing vessels to conduct aggressive activities, cyberattacks, attacks by fast motorboats, or the use of unfavourable hydro-meteorological conditions as a means of authentication, e.g. dropping anchor in the immediate vicinity of submarine cables. Several scenarios included unlawfully declaring and closing maritime zones under the guise of military exercises, introducing zones of control of passing vessels[19]. Between the start of the Russian invasion of Ukraine in February 2022 and September 2024, the U.S. Helsinki Commission Staff identified about 150 hybrid attacks carried out on the territories of NATO countries by Russia or entities associated with it. Among the four separate directions of hybrid operations, attacks on CI facilities were in second place (33%), behind election interference and information campaigns (35%) and ahead of violence campaigns (20%) and the use of migrants as weapons (12%)[20].

The importance of the Baltic Sea for the Russian Federation

In 2022, after the full-scale invasion of Ukraine began, the Russian Maritime Doctrine was published, replacing the previous document in force since 2015. Russia's maritime and energy assets are primarily instruments of power, used to achieve strategic goals. Economic and social aspects remain in the background[21]. The most important priorities formulated in relation to the Baltic Sea include the development of port infrastructure and installations responsible for the transit of hydrocarbons (export reorientation), logistics centres, and the system of offshore export pipelines. The aspect of further strengthening the military capabilities

[19] *Hybrid CoE Paper 16: Handbook on maritime hybrid threats: 15 scenarios and legal scans*, The European Centre of Excellence for Countering Hybrid Threats 2023, p. 5.

[20] S. McGrath, *Spotlight on the Shadow War: Inside Russia's Attacks on NATO Territory. A Report by the U.S. Helsinki Commission Staff*, 2024, p. 2.

[21] O. Chiriac, *The 2022 Maritime Doctrine of the Russian Federation: Mobilization, Maritime Law, and Socio-Economic Warfare*, Center for International Maritime Security, 28.11.2022, https://cimsec.org/the-2022-maritime-doctrine-of-the-russian-federation-mobilization-maritime-law-and-socio-economic-warfare/ [accessed: 7.12.2024].

and base network of the Baltic Fleet (protection of Russian interests in the Baltic Sea) is also important[22]. The Baltic Sea is important for Russia due to the practice of circumventing Western sanctions (embargo and price caps) imposed on Russian oil exports, in response to the invasion of Ukraine. Russian ports in the Baltic Sea, in September 2023 alone, accounted for 57% of Russia's total oil exports[23]. According to data from 2023, the total turnover of the three Russian ports accounted for almost half (46%) of the total volume of transhipments of the ten largest Baltic ports. This value has remained at a similar level since 2021[24].

Russian *grey fleet* and *shadow fleet* vessels use disorderly ownership and insurance issues to violate sanctions imposed on Russian oil. This in itself is a source of threat to the countries on the Baltic Sea, due to the age of these ships, their technical condition, their use in reconnaissance operations, crew qualifications, oil transhipments on the high sea[25]. *Grey fleet* and *shadow fleet*, as the 2024 events mentioned in *the Introduction* show, are also tools for creating hybrid and asymmetric threats.

In the context of security in the Baltic Sea basins, Russia is expected to introduce a whole package of pressure mechanisms calculated to maximise the involvement of NATO forces and resources in monitoring CI facilities. Such activities are to generate costs related to ensuring the security of the Alliance[26]. Sabotage activities against CI may have consequences for transmission networks, affect the availability of raw materials and energy carriers, and cause perturbations in energy markets. It should be noted that NATO's actions, which will lead to a restriction of Russia's freedom to use *grey fleet* or *shadow fleet* (inspections of Russians ships

[22] *Maritime Doctrine of the Russian Federation*, A. Davis, R. Vest (trans.)...

[23] K. Westgaard, *The Baltic Sea Region: A Laboratory for Overcoming European Security Challenges*, Carnegie Endowment FOR International Peace, 21.12.2023, https://carnegieendowment.org/research/2023/12/the-baltic-sea-region-a-laboratory-for-overcoming-european-security-challenges?lang=en [accessed: 7.12.2024].

[24] P. Frankowski, *Bałtyckie TOP10* (Eng. Baltic TOP10), Namiary na Morze i Handel, 9.05.2024, https://www.namiary.pl/2024/05/09/baltyckie-top10/ [accessed: 3.01.2025].

[25] E. Braw, *Russia's growing dark fleet: Risks for the global maritime order*, Atlantic Council, 11.01.2024, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/russias-growing-dark-fleet-risks-for-the-global-maritime-order/ [accessed: 29.04.2024].

[26] Ł. Wyszyński, *Wyszyński: Wejście Szwecji do NATO rodzi korzyści, ale i wyzwania (rozmowa)* (Eng. Wyszyński: Sweden's entry into NATO brings benefits but also challenges (interview)), Biznes Alert, 5.03.2024, https://biznesalert.pl/szwecja-nato-zalety-wady-rosja-morze-baltyckie-bezpieczenstwo/ [accessed: 7.10.2024].

announced in December 2024 by the United Kingdom, Denmark, Sweden, Finland, Poland and Estonia), may be met with reaction from the RF and cause escalation of security threats. Russia may use its available military capabilities (mainly warships) to escort ships suspected of being used to circumvent sanctions[27].

Baltic critical infrastructure

Ensuring the energy security of the countries on the Baltic Sea requires the development of CI in the form of seaports, specialised terminals (oil, gas, floating storage regasification units – FSRUs), submarine power lines (connecting the energy systems of individual countries), pipelines (responsible mainly for the transmission of natural gas, and in the future also hydrogen), as well as communication lines (fibre optics), to drilling platforms leading offshore oil and gas production from offshore fields (the only country conducting oil and gas exploration and production in the Baltic Sea is Poland). The Baltic states have a high level of ambition in the development of both offshore wind energy and nuclear energy (as an element stabilising renewable energy sources) and the hydrogen economy. The submarine electricity interconnections linking Lithuania, Latvia and Estonia with the energy systems of Sweden (NordBalt), Finland (EstLink) and Poland (LitPol Link onshore connection) will enable the desynchronisation of these countries with the post-Soviet BRELL electricity system (February 2025). Thanks to the centralised system, Russia has so far had the ability to manage the frequency and stability of the grid, while dependent states have not had the ability to operate in isolated island mode[28].

The countries of the Baltic region are undergoing a process of fundamental change in the production of electricity. Sweden's nuclear energy turnaround (10 reactors are to be launched by 2045) has an impact on the energy security situation of countries on the Baltic Sea. For Norway, this means the possibility of temporarily stabilising its own system (based

[27] *Russia's Shadow Fleet Tankers Could Get Naval Escorts*, The Maritime Executive, 18.12.2024, https://maritime-executive.com/article/russia-s-shadow-fleet-tankers-could-get-naval-escorts [accessed: 9.01.2025].

[28] M. Paszkowski, *Litwa, Łotwa oraz Estonia planują stworzenie bałtyckiego hubu energetycznego* (Eng. Lithuania, Latvia and Estonia plan to create a Baltic Energy Hub), „Komentarze IEŚ" 2024, no. 1259, p. 1.

on hydroelectric power plants). Sweden's actions are an incentive for other countries in the region to take similar steps (Estonia and Finland are planning a joint project of Small Modular Reactors – SMRs)[29]. Sweden also plays a specific role in the process of building the Baltic Energy Ring, for whose members it is the guarantor of access to electricity in the event of a crisis situation. The capacities produced by the Swedish system can be supplied to the HVDC (high-voltage direct current) transmission systems with Lithuania (NordBalt), Finland (Fenno-Skan), Germany (Baltic Cable) and Poland (SwePol Link), if necessary. During the operation of the undersea line with Poland, there have already been at least a dozen incidents, including physical damage (fishing activities and ship anchors)[30].

Another country pursuing a nuclear programme is Poland, which intends to obtain a stable source of electricity with a total installed capacity of between 6 GW and 9 GW thanks to the commissioning of 6 units (each with the capacity of between 1 GW and 1.6 GW). The first nuclear power plant will be located on the Baltic coast. Such a location will enable the use of seawater to cool the reactors, as well as ensure the availability of the construction area for the transport of large-size elements, creating the basis for a stable and secure supply chain[31].

The Scandinavia and Baltic Sea region has a significant potential for hydrogen production from renewable sources (green hydrogen), identified at around 27.1 million tons (including offshore and onshore wind and solar power) by 2040. Also by 2040, the Nordic-Baltic Hydrogen Corridor is expected to enable the cross-border transport of up to 2.7 million tons of renewable hydrogen from Finland through Estonia, Latvia, Lithuania and Poland to Germany to meet the REPowerEU targets. The offshore part of the corridor, with a total length of approx. 2500 km, is to run along the bottom of the Gulf of Finland[32], a body of water with a high level of hybrid threats, as evidenced in particular by the events of 2024 previously

[29] K. Dudzińska, *Jądrowy zwrot w szwedzkiej polityce energetycznej* (Eng. Sweden Takes a Nuclear Turn in Energy Policy), „Biuletyn PISM" 2024, no. 58.

[30] R. Miętkiewicz, *Bałtyk jako obszar szczególnej ochrony* (Eng. The Baltic Sea as a special protection area), in: *Czy morze pomoże? Bałtyk a bezpieczeństwo energetyczne Polski*, Z. Nowak (ed.), Warszawa 2024, pp. 33–46.

[31] Ibid.

[32] *Nordycko-Bałtycki Korytarz Wodorowy* (Eng. Nordic-Baltic Hydrogen Corridor), Gaz-System 2024, https://www.gaz-system.pl/pl/rynek-wodoru/projekty/nordycko-baltycki-korytarz-wodorowy.html [accessed: 3.01.2025].

mentioned. Taking into account the implementation of European plans for the development of the hydrogen economy, the strategic goals outlined by the Finnish government assume that the country will become the European leader of this technology in the entire value chain. Production in Finland is expected to reach 10% emission-free hydrogen in the EU by 2030[33].

Offshore gas pipelines are of strategic importance for the energy security of the Baltic states. The first of them is the Baltic Pipe, which enables the transit of 10 billion m^3 of gas per year from the Norwegian Continental Shelf to Polish (transit through Germany and Denmark). The Balticconnector gas pipeline is responsible for the supply of natural gas to customers on the Finnish-Estonian-Latvian gas market. In the Polish exclusive economic zone, there is also a gas pipeline (2 lines) connecting Polish drilling platforms (gas extraction and discharge of gas associated with oil fields) with the coastal heat and power plant. Finland has the ability to obtain gas through its LNG terminals in the Gulf of Finland – Inkoo and Hamina (the country has 2 more terminals servicing industrial facilities), from where the raw material is further transported via an offshore gas pipeline to customers on the other side of the Gulf of Finland. In 2024, Germany launched the largest FSRU terminal in the Baltic Sea in Mukran (Rügen Island), enabling the receipt of gas from two cryogenic tankers at the same time (annual capacity of 13.5 billion m^3 of gas). German plans include the construction of stationary terminals as well as FSRUs with a total regasification capacity of up to 54 billion m^3 in 2027[34].

The largest LNG terminal in the Baltic Sea (specialist port) remains the terminal in Świnoujście, where work is still underway to increase import (8.3 billion m^3 of gas per year) and storage capacity. In the next few years, another terminal (FSRU) is to be launched on the Polish Baltic coast, enabling exports of approx. 6 billion m^3 (one vessel), taking into account the possibility of mooring a second regasification vessel[35]. It should be recalled that as recently as 2018, Poland imported almost 80% of its oil from Russia, and in February 2023 stopped supplying it

[33] *Government adopts resolution on hydrogen – Finland could produce 10% of EU's green hydrogen in 2030*, Ministry of Economic Affairs and Employment, 9.02.2023, https://valtioneuvosto.fi/en/-/1410877/government-adopts-resolution-on-hydrogen-finland-could-produce-10-of-eu-s-green-hydrogen-in-2030 [accessed: 9.11.2024].

[34] M. Kędzierski, *Za wszelką cenę. Niemiecki zwrot ku LNG* (Eng. At all costs. Germany shifts to LNG), „Komentarze OSW" 2023, no. 510.

[35] R. Miętkiewicz, *Bałtyk jako obszar szczególnej ochrony*..., p. 47.

from that country altogether, due to Russia's attack on Ukraine and the expiry of long-term contracts. This situation was possible thanks to the maximisation of Naftoport's turnover (it supplies 4 refineries), one of the strategic facilities of this type in the Baltic Sea (another 2 are located in Lithuania). In addition, since 2022, none of the directions of oil supplies has exceeded 50% of imports[36]. Naftoport is part of the logistics chain of oil supplies in Poland and Germany. Given the geopolitical situation, with the limitations of the Rostock terminal, Naftoport plays an important role in meeting the demand for German refineries (Schwedt and Leuna). It is worth mentioning that the Polish oil infrastructure supports the process of fuel supplies to fighting Ukraine. The West remained the only direction of imports of petroleum products (previously estimated at 5–10%). As of 2022, more than 90% of the supply of crude oil and its products comes from this direction, with Poland and Romania being the main suppliers[37].

The Baltic Sea, after the North Sea, is the basin with the most favourable conditions (due to wind conditions and sea depths) for the development of offshore wind energy in Europe. However, the reorientation towards renewable energy sources from the Baltic and North Seas will result in a significant dependence on the sea as an energy production area. Forecasts assume the possibility of using the wind potential in the Baltic Sea of up to 45 GW by 2050[38]. Projects implemented by individual states on the Baltic Sea (Table 1), as is the case with Poland, change the current shape of the power system.

---

[36] Najwyższa Izba Kontroli (Eng. Supreme Audit Office), *Informacja o wynikach kontroli. Realizacja działań w zakresie poprawy bezpieczeństwa paliwowego w sektorze naftowym* (Eng. Information on the results of the audit. Implementation of measures to improve fuel security in the oil sector), KGP.430.7.2023, Warszawa 2023, p. 69.

[37] M. Ruszel, P. Ogarek, *Bezpieczeństwo paliwowe Polski w kontekście zmian właścicielskich na rynku logistyki produktów naftowych oraz remedies Komisji Europejskiej w sprawie fuzji PKN ORLEN i Grupy LOTOS. Polska u progu embargo na produkty naftowe z Rosji – analiza otwierająca 2023 rok* (Eng. Poland's fuel security in the context of ownership changes in the petroleum products logistics market and the European Commission's remedies on the merger between PKN ORLEN and LOTOS Group. Poland at the threshold of the embargo on petroleum products from Russia – opening analysis 2023), IPE Analysis no. 1/2023, Instytut Polityki Energetycznej (Eng. Institute for Energy Policy) 2023, p. 14.

[38] K. Bulski, *The Role of the New European Commission and Regional Cooperation in Accelerating Offshore Wind in the Baltic Sea*, BalticWind.EU, 11.09.2024, https://balticwind.eu/the-role-of-the-new-european-commission-and-regional-cooperation-in-accelerating-offshore-wind-in-the-baltic-sea/ [accessed: 7.11.2024].

Table 1. Targets of the Baltic Region countries in the field of electricity production from offshore wind farms (including the North Sea).

A country of the region	Targets declared by countries according to national plans			Area of water bodies under WOFs [km²]	Potential [GW]
	2030 [GW]	2040 [GW]	2050 [GW]		
Denmark	7.9	7.9	7.9	11 000	42.3
Germany	4.1	4.1	4.1	8400	70
Estonia	1	3.5	7	1850	9
Latvia	0.4	0.4	0.4	300	4
Lithuania	1.4	2.8	4.5	664	2.4 (may be increased to 3.3)
Poland	5.9	10.9	10.9	3600	17.2
Finland	1	5	12	3500	15.7
Sweden	0.7	-	-	1400 (may be increased to 4400)	6–7 (may be increased to 22)
Together for the region	22.5	34.6	46.8	30 714 (may be increased to 33 714) (the entire UE – 52 000)	167.6 (may be increased to 183.5)

Source: own elaboration. The data in the table is taken from the Baltic Energy Market Interconnection Plan (BEMIP) and *the WindEurope Offshore* report entitled *Wind in EU Maritime Spatial Plans* published on 19.10.2022. Quoted after: P. Wróbel, *Analiza: Inicjatywy UE wzmacniające współpracę regionalną na rzecz morskiej energetyki wiatrowej na Bałtyku* (Eng. Analysis: Review of EU initiatives to strengthen regional cooperation for offshore wind in the Baltic Sea), BalticWind.EU, 4.06.2024, https://balticwind.eu/analysis-review-of-eu-initiatives-to-strengthen-regional-cooperation-for-offshore-wind-in-the-baltic-sea/ [accessed: 9.11.2024].

Projects such as the Balticconnector between Estonia and Finland, the expansion of the interconnection between Latvia and Estonia, the LNG terminal in Klaipeda and the LNG terminal in Świnoujście (long-term contracts for gas supplies from the US and Qatar) have affected market integration and reduced dependence on Russian gas in the region[39]. What is particularly important, selected Baltic islands (Gotland, Åland

[39] *REPowerEU Plan. Communication from the Commission to the European Parliament, the European Council, the Council, The European Economic and Social Committee and the Committee of the Regions*, COM(2022) 230 final, Brussels 2022.

Islands, Bornholm), in addition to their strategic importance for NATO (the possibility of exercising control over the Baltic Sea waters and airspace), are to play the role of energy islands (places of energy production and distribution). For example, Bornholm Energy Island is expected to significantly contribute to the ecological transformation of both Denmark and the rest of Europe (construction of offshore wind farms with a total capacity of at least 3 GW and an area of about 650 km^2). The submarine power lines will connect the offshore wind farms to installations on the island of Bornholm and to the electricity transmission grid in Zealand and Germany[40]. This will require a significant expansion of the transmission infrastructure on the bottom of the Baltic Sea, crossing the most important (the highest traffic volume) sea communication routes leading from the Baltic Straits, to Russian ports among others.

Seaports play an important role in the functioning of the economies of the Baltic Region countries. According to data for 2023, the Russian Ust-Luga (volume of transhipments – 112 million tons) remained the largest port, followed by the Polish Gdańsk (81 million tons), ahead of the Russian ports of Primorsk (63 million tons) and St Petersburg (49.6 million tons). Further down the list are the Swedish Gothenburg (36.3 million tons), the Polish Szczecin-Świnoujście port complex (35.3 million tonnes), the Lithuanian Klaipeda (32.7 million tons)[41]. Military equipment is also transhipped in the ports as part of the replacement of military equipment of NATO units (permanent contingents) or exercises and manoeuvers. Seaports also secure the handling of orders for military equipment (in the case of Poland, it is about armament in the form of tanks and artillery systems from the USA and South Korea).

Threats to critical infrastructure facilities in the Baltic Sea

Among the actions taken by the RF in the last 10 years and bearing the hallmarks of hybrid actions in relation to the countries of the Baltic region, the following can be indicated (selected):

[40] Plan for Program Energy Island Bornholm, Danish Energy Agency 2023, ID: ENØ-FOR-115, p. 9.

[41] P. Frankowski, *Bałtyckie TOP10*...

- attempts to undermine the existing provisions of international law on the delimitation of maritime areas (the course of state borders), as exemplified by the events of 21 May 2024. Russia proposed the establishment of a system of straight baselines in the eastern part of the Gulf of Finland and part of the Kaliningrad Oblast, thus undermining the regulations in force since 1985 (which were revoked by a military-diplomatic source the following day). These activities also included physical attempts to interfere with the course of the border on the Narva River (Estonia) by moving border buoys to the Estonian side[42]. One such activity was also to conduct military exercises in the areas of the exclusive economic zones of Lithuania and Latvia;
- disrupting the operation of satellite navigation systems (especially in the Gulf of Gdańsk, the Gulf of Finland, the Gulf of Riga) and hacking attacks on websites providing information on the current location of maritime facilities[43], an activity observed by the intelligence services of Norway, Denmark and the Netherlands since the beginning of 2023;
- increased activity aimed at reconnaissance of seaports, pipelines, fibre optic cables, oil platforms and wind farms[44];
- low-altitude flights of Russian military aircraft near CI facilities (drilling platforms) or attempts to disrupt military exercises (overflight of USS Donald Cook in 2016);
- the probable violation of the Swedish border by Russian midget submarines[45].

Actions taken against the infrastructure of ports and specialised terminals may include (generalised):

- the use of the so-called insiders recruited among employees of CI facilities in order to identify protection systems, detect

[42] N. Aliyev, *Does Russia want to revise its water border with the Nordic and Baltic states?*, International Centre for Defence and Security, 15.08.2024, https://icds.ee/en/does-russia-want-to-revise-its-water-border-with-the-nordic-and-baltic-states/ [accessed: 16.12.2024].

[43] R. Miętkiewicz, *Systemy autonomiczne w działaniach na morzu* (Eng. Autonomous systems in maritime operations), Gdynia 2023, Wydawnictwo AMW, p. 228.

[44] F. Bryjka, T. Zając, *Wzmocnienie ochrony infrastruktury krytycznej państw UE i NATO* (Eng. EU and NATO countries strengthen the protection of critical infrastructure), „Biuletyn PISM" 2023, no. 79, p. 2.

[45] R. Miętkiewicz, *Systemy autonomiczne w działaniach na morzu...*, p. 230.

vulnerabilities or indicate specific objectives of activities (control elements, etc.);

- direct sabotage activities aimed at causing large-scale fires (ports, refineries, specialist terminals) or electrocution of selected infrastructure elements (important from the point of view of maintaining continuity of operation);
- terrorist attacks in various forms and by various means;
- criminal activities against facilities (sensitive elements of the installation) in the form of theft, devastation;
- deliberately causing environmental disasters resulting in large losses in the ecosystem and making it necessary to interrupt or reduce the work of port terminals[46];
- actions aimed at blocking access to infrastructure from land (carried out against railway lines, traffic control systems, etc.) and from the sea (e.g. by deliberately sinking or grounding a ship with the intention of blocking deep-water fairways, laying sea mines);
- cyber attacks aimed at paralysing systems responsible for the operation of terminals, operation and service centres (offshore wind farms), security systems, etc. This type of activity also includes disrupting the operation of navigation systems and generating avatars of units and aircraft. According to US assessments, cyber actors affiliated with the Russian General Staff Main Intelligence Directorate 161st Specialist Training Center (Unit 29155) and other units (26165 and 74455) have been responsible for operations in cyberspace against global targets (espionage, sabotage, and discrediting activities) since at least 2020[47]. Russian funds are also used to fund hacking groups, such as UNC1151/Ghostwriter or Digital Shadows/Conti, in third countries[48]. The second half of 2023 and the first half of 2024 saw a significant escalation of cyber-attacks. This showed that the scale of the problem has definitely increased,

[46] D. Doğan , D. Çetikli, *Maritime Critical Infrastructure Protection (MCIP) in a Changing Security Environment*, Istanbul 2023, Maritime Security Centre of Excellence (MARSEC COE), p. 35.

[47] *Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure*, Cybersecurity and Infrastructure Security Agency 2024, ID: AA24-249A, p. 1.

[48] A.M. Dyner, *Działania hybrydowe Rosji przeciw państwom NATO i UE* (Eng. Preparing for Russian hybrid activities against NATO and EU countries), „Biuletyn PISM" 2022, no. 183, p. 1.

both in terms of the variety and number of such incidents and their consequences[49];

- attacks from multiple directions involving the use of autonomous systems (the possibility of occurring in all domains).

Actions taken against offshore infrastructure (offshore wind farms, submarine cables, submarine pipelines) may include (generalised):

- interference with offshore construction work in the form of dangerous manoeuvres carried out in the vicinity of installation fleet vessels (without escort), these risks can be generated by platforms posing as state service vessels;
- violation of protection zones established around the installations, carried out under various pretences (failure of navigation, propulsion equipment, etc.) and the use of legal freedoms and the freedom to conduct scientific activity at sea to penetrate undersea transmission lines and the surroundings of infrastructure facilities[50];
- attempts to disrupt undersea power connections and gas pipelines by dragging anchors and intentionally manoeuvring ships, sabotage actions carried out by specialised sabotage groups;
- operations with the use of autonomous underwater platforms (autonomous underwater vehicles, AUV), surface platforms (unmanned surface vehicles, USV) and air platforms (autonomous aerial vehicles, AAV) and all derivatives, including those using the latest developments in the field of artificial intelligence, and using swarms (underwater shoals). Threats of this type, as indicated by the naval phase of the war in Ukraine and previous actions by terrorists (e.g. Houthi fighters in the Red Sea), may also be generated by ad hoc improvised measures based on dual-use technologies. A factor that intensifies this type of threat is the progressive process of proliferation of unmanned technologies[51];

[49] *ENISA Threat Landscape 2024, July 2023 to June 2024*, European Union Agency For Cybersecurity 2024, p. 11. https://doi.org/10.2824/0710888.

[50] P. Mickiewicz, *Bezpieczeństwo energetyczne czy bezpieczeństwo morskie?...*, p. 73.

[51] R. Miętkiewicz, *Systemy autonomiczne (bezzałogowe) jako nowe narzędzie w rękach terrorystów* (Eng. Autonomous (unmanned) systems as a new tool in the hands of terrorists), in: *XX-lecie wojny z terroryzmem: bilans i konsekwencje.* Vol. 2. *Infrastruktura krytyczna – analizy – case study*, B. Wiśniewska-Paź, D. Szlachter (eds.), Toruń 2022, Wydawnictwo Adam Marszałek, pp. 69–98.

- the use of sea mines and water borne improvised explosive devices (WBIED), both in the form of modern, quasi-intelligent sea mines (ensuring selective choice of targets or enabling the delay of action and prolonging the occurrence of threats) and in the form of mines constituting war remains. The fact that there is a huge deposit of chemical and conventional munitions in the Baltic Sea, including between 16 000 and 61 000 sea mines, can be used as an element of camouflage these activities[52].

Vulnerabilities of critical infrastructure facilities in the Baltic Sea

The analysis of CI facilities, with particular emphasis on those responsible for energy production, storage and transmission, indicates that in relation to many of them (specialised terminals, offshore wind farms) we are dealing with facilities operating at the interface of land, sea and air environments. Another domain that has a very strong impact on the level of security of facilities of this type is cyberspace. Thus, when considering the maintenance of the security of maritime CI, a whole range of factors determining the possibility of intentional threats should be taken into account. In the case of the intended impact using methods typical of hybrid activities, it should be noted that[53]:

- the threat will be multi-domain, synchronised and combined with a strong disinformation impact in the media;
- subliminal threats will, for political reasons, take the form of sabotage or diversionary actions created against Poland and other countries on the Baltic Sea[54];
- threats in the maritime domain (underwater and air) may concern both infrastructure facilities and units responsible for the supply of hydrocarbons (cryogenic tankers and tankers for the transport

[52] R. Miętkiewicz, *Dumped conventional warfare (munition) catalog of the Baltic Sea*, "Marine Environmental Research" 2020, vol. 161, p. 105057. https://doi.org/10.1016/j.marenvres.2020.105057.

[53] R. Miętkiewicz, *Obiekty morskiej infrastruktury energetycznej – próba określenia podatności na ataki platform bezzałogowych* (Eng. Offshore energy infrastructure facilities – an attempt to determine vulnerability to attacks by unmanned platforms), „Alcumena. Pismo Interdyscyplinarne" 2023, no. 3(15), p. 217. https://doi.org/10.34813/psc.3.2023.11.

[54] P. Mickiewicz, *Bezpieczeństwo energetyczne czy bezpieczeństwo morskie?...*, p. 72.

of crude oil and petroleum products), and in the case of offshore facilities (offshore wind farms and drilling platforms, pipelines and underwater cables for various purposes) – also installation and maintenance fleets;

- location of facilities of strategic importance for the security of the countries of NATO's eastern flank in the immediate vicinity of the borders with Russia (the exclave of Kaliningrad in the case of Poland and Lithuania, the area of St Petersburg in relation to Finland and Estonia) and routes leading from the Gulf of Finland to Kaliningrad. The facilities in the form of the refinery and Naftoport and the planned FSRU terminal in Gdańsk (Poland) or the FSRU terminal in Klaipeda (Lithuania) are located several dozen kilometres from the borders with Russia, which increases vulnerability to hybrid threats;
- the offshore gas and energy infrastructure facilities of the countries on the Baltic Sea are located along the so-called submarine depths and troughs, the depths of which are conducive to sabotage activities. Both submarines and special groups operating from the decks of surface vessels (e.g. research vessels adapted for such activities) can be used to carry out such actions;
- facilities in the form of offshore wind farms, drilling platforms, as well as offshore pipelines and cable connections for various purposes are located outside the territorial sea, in the waters of the exclusive economic zone of the coastal states. The large distance from the shore (the selected investments of the second phase of offshore wind energy development in Poland are adjacent to the outer limits of this zone, with a distance of nearly 80 km from the coastline) and the legal status of international waters (freedom of navigation) increase their vulnerability to hybrid threats[55];
- many of the infrastructure facilities are cross-border (gas pipelines, power cables, telecommunications connections, etc.) and are exploited by numerous operators from different countries. This aspect requires cooperation and coordination of activities to ensure continuity of operations (in the case of the Baltic Pipe gas pipeline,

[55] 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, p. 110. https://doi.org/10.35757/SM.2019.72.1.06.

from the place of extraction of raw material on the Norwegian Continental Shelf to the end point of receipt in Poland);

- very intensive shipping traffic (according to HELCOM reports, the Baltic Sea is one of the most crowded waters in the world)[56], in the vicinity of gas, electricity and telecommunications lines facilitates the generation of dangerous situations (mapping the bottom, dragging anchors, laying sea mines and marine improvised explosive devices - MIED). Such activities can be masked, for example, by switching off AIS (automatic identification system) transponders or manoeuvring suggesting technical problems;
- in the case of specialist terminals (Naftoport in Gdańsk, Gas Terminal in Świnoujście, FSRU terminals), it is necessary to maintain deep-water fairways (artificially deepened) in order to ensure continuity of supply. A potential action enabling a long-term blocking of imports may be the deliberate sinking of the vessel on the axis of the fairway (e.g. under the guise of an accident);
- according to the provisions of strategic documents showing the directions of development of the power system, offshore wind energy is to be one of the pillars (along with nuclear energy and gas as a transitional fuel)[57]. Thus, the disruption of the electricity production chain becomes the main objective of the opponent of Poland and other countries on the Baltic Sea (introducing serious disruptions to the economies and societies of coastal states);
- The RF may attempt to intercept CI-related investments or block them at various stages of project implementation. In resolution P9_TA(2024)0079, the European Parliament pointed to Russian actions and operations aimed at infiltrating European democracies and EU institutions, the presence of a network of agents of influence who affect electoral processes and policies on key strategic issues such as energy infrastructure[58];

[56] *HELCOM, ensuring safe shipping in the Baltic*, Helsinki Commission – Baltic Marine Environment Protection Commission 2009, p. 3.

[57] *Energy Policy of Poland until 2040* (EPP2040), Warszawa 2022, Ministerstwo Klimatu i Środowiska (Eng. Ministry of Climate and Environment), p. 7.

[58] *P9_TA(2024)0079 – Russiagate: allegations of Russian interference in the democratic processes of the European Union – European Parliament resolution of 8 February 2024 on Russiagate: allegations of Russian interference in the democratic processes of the European Union (2024/2548(RSP))*.

- it can be expected that the military potential will be used more and more as a response to the escalation of the situation and the retaliatory nature of the actions of the antagonised parties, reminiscent of "Cold War" scenarios (attempts to physically push ships back in order to enforce their own interpretation of the regulations, helicopters hovering over enemy ships, blocking communication routes under the guise of exercises);
- non-state entities (organisations and movements of activists of various backgrounds), national minorities, criminal groups, used both for direct actions and attempts to test security procedures, cooperation of services, etc., may be involved in the activities;
- the actions taken will be accompanied by massive media attacks and shaping their own version of events (in the case of the RF, aimed at Russian society, in order to maintain the image of a "besieged fortress" and demonise the image of Russia by the West);
- hybrid threats in the Baltic region can be characterised by the use of modern technologies (autonomous platforms) as well as dual-use systems, to completely improvised means[59];
- with regards to objects of maritime CI, threats can also be created using objects of historical origin. According to the author, data on the location of dangerous chemical and conventional weapons deposits can be used to plan this type of activity. Estimates indicate the presence on the Baltic Sea of between 300 000 and 385 000 tons of conventional and chemical munitions deliberately sunk after World War II. A large number of wrecks with dangerous contents should be added to this [60];
- threats may be generated during holiday periods, as was the case with the intersection of the EstLink 2 power line (Christmas 2024), of which the Chinese ship Yi Peng 3 was initially suspected[61].

[59] R. Miętkiewicz, *Systemy autonomiczne (bezzałogowe) jako nowe narzędzie w rękach terrorystów*..., pp. 69–98.

[60] R. Miętkiewicz, *High explosive unexploded ordnance neutralization – Tallboy air bomb case study*, "Defence Technology" 2022, vol. 18, no. 3, pp. 524–535. https://doi.org/10.1016/j.dt.2021.03.011.

[61] *Finland-Estonia power cable hit in latest Baltic Sea incident*, The Guardian, 25.12.2024, https://www.theguardian.com/world/2024/dec/25/finland-estonia-power-cable-hit-in-latest-baltic-sea-incident [accessed: 27.12.2024].

Measures to counter hybrid threats in the Baltic Sea

The nature of hybrid threats occurring and possible to appear in the Baltic Sea requires far-reaching consolidation of activities and cross-border cooperation between institutions (mainly armed forces, coast guards and intelligence) of coastal states. Secondly, it seems necessary to apply the achievements resulting from the development of modern technologies, with particular emphasis on maritime autonomous systems and elements of artificial intelligence. In order to effectively counteract incidents, it is necessary to take actions of a political nature (strategies, doctrines, common road maps of NATO members), legal (tools and legal regulations enabling the creation of solutions and law enforcement), military (presence of forces, exercises, multinational operations and initiatives), technological (directing scientific research, using available solutions to increase the level of protection) and building common data processing and exchange systems (common situational awareness, efficient command). Projects aimed at minimising hybrid threats to CI facilities at sea should include:

- conducting ongoing analyses of the level of security, taking into account identifying risks, estimating probabilities and impacts (risk matrices) and developing methods to mitigate them. This requires close cooperation between sectors (private investors) and state services, as well as the exchange of information between allies;
- conducting monitoring of communication routes in the Baltic Sea, to enable the detection and tracking of ships despite the AIS transponders being switched off, as well as vessels (mainly up to 20 m in length or displacement up to 150 tons) not covered by VTS (vessel traffic service) reporting systems. Due to the large spaces requiring supervision, it is recommended to use the space component (satellite pictures). In order to minimise costs and increase the efficiency of operations, the use of autonomous systems for monitoring (also hidden in the case of submarine infrastructure) should be indicated as expedient. Cooperation in this area is required at the level of the maritime security systems of the countries on the Baltic Sea;
- implementation of EU standards for the protection of CI (even though the management of CI is mainly the responsibility of the EU Member States). The primary documents in this regard include the Revised EU Maritime Security Strategy, whose selected fundamental aims are: improve the resilience of critical entities

and the security of networks and information systems and ensuring the resilience and protection of maritime CI[62] and The Critical Entities Resilience Directive on reducing the vulnerability of critical entities and strengthening their physical resilience[63];

- the use of artificial intelligence methods enabling the selection of units (based on intelligence data, monitoring data on suspicious behaviour in the form of speed reduction, manoeuvring over CI, etc.), which will reduce the freedom of potential perpetrators to use high traffic volume to mask their activities. This type of action was taken by NATO in January 2025, when Joint Expeditionary Force, formed by 10 countries with the United Kingdom in lead, launched a reaction system (codenamed Nordic Warden) to track potential threats to undersea infrastructure and monitor the Russian shadow fleet. The system covers 22 areas of interest, including the Baltic Sea and the Baltic Straits. The warnings generated by the system will be transmitted to NATO members[64];
- maintaining the capacity of coastal states to respond immediately (within a few hours) to the sabotage and other dangerous events. The above requires the possession of qualified subunits maintained in an appropriate readiness regime, capable of quickly sub-seizing ships and recapturing CI objects at sea and at the interface of environments (seaports);
- support at the international level in the face of emerging events, showing the approval of the EU and uniform line of perception and response to incidents, as was the case with the events of December 2024 and the actions of the Finnish authorities related to the seizure of the vessel Eagle S[65];

[62] *Council conclusions on the Revised EU Maritime Security Strategy (EUMSS) and its Action Plan*, Brussels 2023, Council of the European Union.

[63] *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*.

[64] *Joint Expeditionary Force activates UK-led reaction system to track threats to undersea infrastructure and monitor Russian shadow fleet*, 6.01.2025, https://www.gov.uk/government/news/joint-expeditionary-force-activates-uk-led-reaction-system-to-track-threats-to-undersea-infrastructure-and-monitor-russian-shadow-fleet [accessed: 7.01.2025].

[65] *Joint Statement by the European Commission and the High Representative on the Investigation into Damaged Electricity and Data Cables in the Baltic Sea*, Brussels 2024, European Commission – Statement.

- strengthening cooperation between the armed forces and other entities responsible for maintaining security in sea basins and stakeholders of the energy industry (especially oil and gas as well as wind offshore) in order to build industry awareness of threats, vulnerabilities and increase resilience, as well as to understand the needs (e.g. expenditure on security systems). Sharing sensitive knowledge can be resented by the private sector;
- the adoption by the NATO countries on the Baltic Sea of an initiative similar to the declaration signed in 2024 by Belgium, the Netherlands, Germany, Norway, the United Kingdom and Denmark on the protection of underwater CI against attacks and acts of sabotage[66]. Such activities are aimed at jointly implementing appropriate solutions, exchanging information and best practices to increase the level of protection and prevention[67];
- holistic approach to maritime CI risks, including both preventive and protective actions as well as the development of rapid infrastructure recovery (restoration) of infrastructure (cross-border reparability). Such measures should also take into account the mitigation of the effects of attacks on CI through planning alternative supply chains in advance (it took almost half a year to restore the operational efficiency of the Balticconnector). This means that the onus will continue to shift from protection to building resilience. Whereby it is important not only to prevent the occurrence of an adverse event, but also to be prepared to quickly minimise its impact (also by using the potential of foreign partners). International (EU, NATO) unified standards for assessing the resilience of CI should be used to implement such activities;
- development of *the maritime policing* initiative proposed by the Polish Prime Minister, which is to increase the presence of NATO naval forces and groups operating within the framework of bilateral and multinational initiatives of the countries on the Baltic Sea (e.g. on the basis of rotational command and declaration of forces for joint

[66] C. Chiappa, *6 countries move to protect the North Sea from Russians*, Politico, 9.04.2024, https://www.politico.eu/article/6-european-countries-sign-pact-protect-critical-energy-infrastructure-north-sea-from-russia/ [accessed: 27.12.2024].

[67] *Joint Declaration on cooperation to secure critical subsea infrastructure*, Regjeringen, 9.04.2024, https://www.regjeringen.no/en/aktuelt/joint-declaration-on-cooperation-to-secure-critical-subsea-infrastructure/id3033122/ [accessed: 27.12.2024].

operations). Such a solution will allow to minimise costs and at the same time increase the level of interoperability of forces, as well as build appropriate relationships (trust);
- continuous mapping and analysis of vulnerabilities and shortcomings of CI by its owners (often private entities) and strengthening cooperation between the EU and NATO. Some countries such as Norway or the United Kingdom are members of only one of these organisations;
- taking quick and effective action to minimise the challenges posed by the shadow fleet, which has a great potential to create hybrid threats to maritime CI (destroying undersea lines by dragging anchors, espionage, causing deliberate collisions, the threat of a large-scale environmental disaster and others). To this end, multilateral cooperation between EU countries and the International Maritime Organization, ship owners and insurers is necessary to promote the provisions of international law. These provisions are effective only if the majority of sea users apply to it.

Conclusions

Hybrid threats are a convergence of activities below the threshold of war carried out in many domains, covertly and directly (less frequently), but planned and coordinated using various means (political, military, economic, legal, social and other). Hybrid activities threaten the security of the functioning of the state and its citizens, and a wide range of means is used to create them, including both classic (disinformation) and modern (cyberattacks) tools. A special feature is the creeping, staggered and difficult to immediately diagnose nature of the threats, which additionally take various forms using the synergy effect[68]. Taking into ccount the considerations contained above, it should be pointed out that the potential package of threats that can be generated by the RF and its related entities in relation to offshore CI facilities in the Baltic Sea is very broad. Taking into account the domain approach and the fact that in the coming

[68] Najwyższa Izba Kontroli (Eng. Supreme Audit Office), *Informacja o wynikach kontroli. Przygotowanie państwa na zagrożenia związane z działaniami hybrydowymi* (Eng. Information on the results of the audit. Preparing the state for the threats of hybrid activities), KPB.430.002.2023, Warszawa 2023, p. 7.

years numerous offshore facilities will be launched (mainly offshore wind farms, which in the case of the most advanced projects in 2025 will enter the physical construction phases on specific investment locations), cyber threats come to the fore (in addition to cyber-attacks, we are also talking about the generation of avatars of units and aircraft violating zones around CI, as well as disruption of satellite navigation systems) and underwater hazards (resulting in disruption of the functioning of CI on the seabed), and subsequently surface hazards. The purpose of such actions will be to directly disrupt the schedules of construction works, or to interrupt logistics chains by generating incidents involving the use of mine warfare elements (covert laying of sea mines, maritime improvised explosive devices), violation of prohibited zones by autonomous submarine units, submarines and sabotage groups (in order to conduct reconnaissance activities, lay sea mines, map the bottom, identify vulnerabilities weaknesses, etc.). Among the surface threats, the probable forms of action include dangerous manoeuvring in relation to installation vessels and service fleets carrying out complex operations, actions of vessels simulating technical problems (dragging anchors, drifting towards CI objects, intentional collisions, to deliberate sinking of vessels, e.g. shadow fleet). Civilian ships carrying out activities on behalf of Russia may be responsible for transporting sabotage groups, conducting reconnaissance activities, and deliberately causing disruptions to navigation and communication systems in the immediate vicinity of the investment in order to disrupt the work. In the event of further escalation of the situation, it should also be taken into account that threats will be generated by vessels disguised as ships of the state services of the countries on the Baltic Sea. It is also possible to use autonomous aerial platforms (according to the author, also operating from the decks of civilian ships) to create threats in relation to oil platforms and transformer stations (an element of the OWF). It should be assumed that autonomous platforms in the near future will range from hybrid systems (capable of changing the environment of operations) to biomimetic platforms resembling marine organisms. The development of artificial intelligence methods currently makes it possible to create swarms (in the case of underwater vehicles, it seems advisable to use the term: shoals) of unmanned platforms, the joint use of which allows for achieving synergy effect.

The analysis of hybrid threats indicate the growing importance of modern technology in the creation of these threats (increasingly perfect

platforms with constantly growing capabilities), especially in the underwater domain. With regard to the increasing capabilities in this domain, in terms of both attack, protection and defence, there is even talk of seabed warfare[69].

Bibliography

Bryjka F., Zając T., *Wzmocnienie ochrony infrastruktury krytycznej państw UE i NATO* (Eng. EU and NATO countries strengthen the protection of critical infrastructure), „Biuletyn PISM" 2023, no. 79.

Doğan D., Çetikli D., *Maritime Critical Infrastructure Protection (MCIP) in a Changing Security Environment,* Istanbul 2023, Maritime Security Centre of Excellence (MARSEC COE).

Dudzińska K., *Jądrowy zwrot w szwedzkiej polityce energetycznej* (Eng. Sweden Takes a Nuclear Turn in Energy Policy), „Biuletyn PISM" 2024, no. 58.

Dyner A.M., *Działania hybrydowe Rosji przeciw państwom NATO i UE* (Eng. Preparing for Russian hybrid activities against NATO and EU countries), „Biuletyn PISM" 2022, no. 183.

ENISA Threat Landscape 2024, July 2023 to June 2024, European Union Agency For Cybersecurity 2024. https://doi.org/10.2824/0710888.

HELCOM, ensuring safe shipping in the Baltic, Helsinki Commission – Baltic Marine Environment Protection Commission 2009.

Hybrid CoE Paper 16: *Handbook on maritime hybrid threats: 15 scenarios and legal scans,* The European Centre of Excellence for Countering Hybrid Threats 2023.

Kasprzyk R., *Sztuczna inteligencja i cyberprzestrzeń a proces złośliwego sterowania ludźmi i maszynami* (Eng. Artificial intelligence and cyberspace and the process of malicious control of humans and machines), in: *GlobState,* vol. 2. *Wyzwania dla Polski w kontekście zmian w środowisku bezpieczeństwa,* Ł. Jureńczyk, R. Reczkowski (sci. eds.), Bydgoszcz 2020, Centrum Doktryn i Szkolenia Sił Zbrojnych – Uniwersytet Kazimierza Wielkiego, pp. 277–298.

[69] N. Fridbertsson, *Protecting Critical Maritime Infrastructure – The Role of Technology. General Report,* NATO Parliamentary Assembly, Science and Technology Committee (STC) 2023, p. 1.

Kędzierski M., *Za wszelką cenę. Niemiecki zwrot ku LNG* (Eng. At all costs. Germany shifts to LNG), „Komentarze OSW" 2023, no. 510.

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, pp. 71–76.

Miętkiewicz R., *Bałtyk jako obszar szczególnej ochrony* (Eng. The Baltic Sea as a special protection area), in: *Czy morze pomoże? Bałtyk a bezpieczeństwo energetyczne Polski*, Z. Nowak (ed.), Warszawa 2024, pp. 33–46.

Miętkiewicz R., *Dumped conventional warfare (munition) catalog of the Baltic Sea*, "Marine Environmental Research" 2020, vol. 161, p.105057. https://doi.org/10.1016/j.marenvres.2020.105057.

Miętkiewicz R., *High explosive unexploded ordnance neutralization – Tallboy air bomb case study*, "Defence Technology" 2022, vol. 18, no. 3, pp. 524–535. https://doi.org/10.1016/j.dt.2021.03.011.

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, pp. 97–112. https://doi.org/10.35757/SM.2019.72.1.06.

Miętkiewicz R., *Obiekty morskiej infrastruktury energetycznej – próba określenia podatności na ataki platform bezzałogowych* (Eng. Offshore energy infrastructure facilities – an attempt to determine vulnerability to attacks by unmanned platforms), „Alcumena. Pismo Interdyscyplinarne" 2023, no. 3(15), pp. 205–225. https://doi.org/10.34813/psc.3.2023.11.

Miętkiewicz R., *Systemy autonomiczne (bezzałogowe) jako nowe narzędzie w rękach terrorystów* (Eng. Autonomous (unmanned) systems as a new tool in the hands of terrorists), in: *XX-lecie wojny z terroryzmem: bilans i konsekwencje.* Vol. 2. *Infrastruktura krytyczna – analizy – case study*, B. Wiśniewska-Paź, D. Szlachter (eds.), Toruń 2022, Wydawnictwo Adam Marszałek, pp. 69–98.

Miętkiewicz R., *Systemy autonomiczne w działaniach na morzu* (Eng. Autonomous systems in maritime operations), Gdynia 2023, Wydawnictwo AMW.

Nowak Z., Maj M., *Bałtyk jako przestrzeń strategicznej aktywności energetycznej* (Eng. The Baltic Sea as a space for strategic energy activities), in: *Czy morze pomoże? Bałtyk a bezpieczeństwo energetyczne Polski*, Z. Nowak (ed.), Warszawa 2024, Institute for Foreign Affairs, pp. 33–46.

Nowakowska-Krystman A., *Potencjał obronny Sił Zbrojnych RP w ujęciu relatywnym* (Eng. Defence potential of the Polish Armed Forces in relative terms), Warszawa 2018, Akademia Sztuki Wojennej.

Paszkowski M., *Litwa, Łotwa oraz Estonia planują stworzenie bałtyckiego hubu energetycznego* (Eng. Lithuania, Latvia and Estonia plan to create a Baltic Energy Hub), „Komentarze IEŚ" 2024, no. 1259.

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), PTBN expert opinions no. 1, Polskie Towarzystwo Bezpieczeństwa Narodowego (Eng. Polish Association for National Security) 2023.

Plan for Program Energy Island Bornholm, Danish Energy Agency, 2023, ID: ENØ-FOR-115.

Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure, Cybersecurity and Infrastructure Security Agency 2024, ID: AA24-249A.

Ruszel M., Ogarek P., *Bezpieczeństwo paliwowe Polski w kontekście zmian właścicielskich na rynku logistyki produktów naftowych oraz remedies Komisji Europejskiej w sprawie fuzji PKN ORLEN i Grupy LOTOS. Polska u progu embargo na produkty naftowe z Rosji - analiza otwierająca 2023 rok* (Eng. Poland's fuel security in the context of ownership changes in the petroleum products logistics market and the European Commission's remedies on the merger between PKN ORLEN and LOTOS Group. Poland at the threshold of the embargo on petroleum products from Russia – opening analysis 2023), IPE analysis no. 1, Instytut Polityki Energetycznej (Eng. Institute for Energy Policy) 2023.

Wojtasik K., *Analiza wyników badań na temat percepcji zagrożeń o charakterze terrorystycznym wśród uczestników EU PSA* (Eng. Results of the survey on the perception of terrorist threats among EU PSA participants), PTBN analyses no. 1, Polskie Towarzystwo Bezpieczeństwa Narodowego (Eng. Polish Association for National Security) 2023.

Internet sources

Aliyev N., *Does Russia want to revise its water border with the Nordic and Baltic states?,* International Centre for Defence and Security, 15.08.2024, https://icds.ee/en/does-russia-want-to-revise-its-water-border-with-the-nordic-and-baltic-states/ [accessed: 16.12.2024].

Braw E., *Russia's growing dark fleet: Risks for the global maritime order*, Atlantic Council, 11.01.2024, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/russias-growing-dark-fleet-risks-for-the-global-maritime-order/ [accessed: 29.04.2024].

Bulski K., *The Role of the New European Commission and Regional Cooperation in Accelerating Offshore Wind in the Baltic Sea*, BalticWind.EU, 11.09.2024, https://balticwind.eu/the-role-of-the-new-european-commission-and-regional-cooperation--in-accelerating-offshore-wind-in-the-baltic-sea/ [accessed: 7.11.2024].

Chiappa C., *6 countries move to protect the North Sea from Russians*, Politico, 9.04.2024, https://www.politico.eu/article/6-european-countries-sign-pact-protect-critical-energy-infrastructure-north-sea-from-russia/ [accessed: 27.12.2024].

Chiriac O., *The 2022 Maritime Doctrine of the Russian Federation: Mobilization, Maritime Law, and Socio-Economic Warfare*, Center for International Maritime Security, 28.11.2022, https://cimsec.org/the-2022-maritime-doctrine-of-the-russian--federation-mobilization-maritime-law-and-socio-economic-warfare/ [accessed: 7.12.2024].

Finland-Estonia power cable hit in latest Baltic Sea incident, The Guardian, 25.12.2024, https://www.theguardian.com/world/2024/dec/25/finland-estonia-power-cable-hit-in-latest-baltic-sea-incident [accessed: 27.12.2024].

Finlandia: Władze nie potwierdzają informacji o „przypadkowym" uszkodzeniu Balticconnector (Eng. Finland: Authorities do not confirm information on "accidental" damage to Balticconnector), Portal Morski, 13.08.2024, https://www.portalmorski.pl/offshore/56252-finlandia-wladze-nie-potwierdzaja-informacji-o-przypadkowym-uszkodzeniu-balticconnector [accessed: 29.01.2025].

Frankowski P., *Bałtyckie TOP10* (Eng. Baltic TOP10), Namiary na Morze i Handel, 9.05.2024, https://www.namiary.pl/2024/05/09/baltyckie-top10/ [accessed: 3.01.2025].

Fraszka B., *Państwa bałtyckie a rosyjskie zagrożenia hybrydowe* (Eng. Baltic States vs. Russian Hybrid Threats), Warsaw Institute, https://warsawinstitute.org/wp-content/uploads/2020/10/Pa%C5%84stwa-ba%C5%82tyckie-a-rosyjskie-zagro%C5%BCenia-hybrydowe-Bartosz-Fraszka.pdf [accessed: 29.12.2024].

Government adopts resolution on hydrogen – Finland could produce 10% of EU's green hydrogen in 2030, Ministry of Economic Affairs and Employment, 9.02.2023, https://valtioneuvosto.fi/en/-/1410877/government-adopts-resolution-on-hydrogen-finland-could-produce-10-of-eu-s-green-hydrogen-in-2030 [accessed: 9.11.2024].

Hagelstam A., *Cooperating to counter hybrid threats*, NATO Review, 23.11.2018, https://www.nato.int/docu/review/articles/2018/11/23/cooperating-to-counter-hybrid-threats/index.html [accessed: 2.12.2024].

Hybrid threats as a concept, Frequently asked questions on hybrid threats, The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ [accessed: 2.12.2024].

Hyndle-Hussein J., *The Balticconnector gas pipeline damage,* Ośrodek Studiów Wschodnich, 11.10.2023, https://www.osw.waw.pl/en/publikacje/analyses/2023-10-11/balticconnector-gas-pipeline-damage [accessed: 2.01.2025].

Joint Expeditionary Force activates UK-led reaction system to track threats to undersea infrastructure and monitor Russian shadow fleet, 6.01.2025, https://www.gov.uk/government/news/joint-expeditionary-force-activates-uk-led-reaction-system-to-track-threats-to-undersea-infrastructure-and-monitor-russian-shadow-fleet [accessed: 7.01.2025].

Nordycko-Bałtycki Korytarz Wodorowy (Eng. Nordic-Baltic Hydrogen Corridor) (2024), https://www.gaz-system.pl/pl/rynek-wodoru/projekty/nordycko-baltycki-korytarz-wodorowy.html [accessed: 3.01.2025].

Russia's 'shadow fleet': Bringing the threat to light, European Parliament, https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766242/EPRS_BRI(2024)766242_EN.pdf [accessed: 23.01.2025].

Russia's Shadow Fleet Tankers Could Get Naval Escorts, The Maritime Executive, 18.12.2024, https://maritime-executive.com/article/russia-s-shadow-fleet-tankers-could-get-naval-escorts [accessed: 9.01.2025].

Westgaard W., *The Baltic Sea Region: A Laboratory for Overcoming European Security Challenges*, Carnegie Endowment for International Peace, 21.12.2023, https://carnegieendowment.org/research/2023/12/the-baltic-sea-region-a-laboratory-for-overcoming-european-security-challenges?lang=en [accessed: 7.12.2024].

Wróbel P., *Analiza: Inicjatywy UE wzmacniające współpracę regionalną na rzecz morskiej energetyki wiatrowej na Bałtyku* (Eng. Analysis: Review of EU initiatives to strengthen regional cooperation for offshore wind in the Baltic Sea), BalticWind.EU, 4.06.2024, https://balticwind.eu/pl/analiza-inicjatywy-ue-wzmacniajace-wspolprace-regionalna-na-rzecz-morskiej-energetyki-wiatrowej-na-baltyku/ [accessed: 9.11.2024].

Wyszyński Ł., *Wyszyński: Wejście Szwecji do NATO rodzi korzyści, ale i wyzwania (rozmowa)* (Eng. Wyszyński: Sweden's entry into NATO brings benefits but also challenges (interview)), Biznes Alert, 5.03.2024, https://biznesalert.pl/szwecja-nato-zalety-wady-rosja-morze-baltyckie-bezpieczenstwo/ [accessed: 7.10.2024].

Legal acts

P9_TA(2024)0079 – Russiagate: allegations of Russian interference in the democratic processes of the European Union – European Parliament resolution of 8 February 2024 on Russiagate: allegations of Russian interference in the democratic processes of the European Union (2024/2548(RSP)) – (Official Journal of the EU C/2024/6343 of 7.11.2024).

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 333/164 of 27.12.2022).

Other documents

Council conclusions on the Revised EU Maritime Security Strategy (EUMSS) and its Action Plan, Brussels 2023, Council of the European Union.

Energy Policy of Poland until 2040 (EPP2040), Warszawa 2022, Ministerstwo Klimatu i Środowiska (Eng. Ministry of Climate and Environment).

Fridbertsson N., *General Report – Protecting Critical Maritime Infrastructure – The Role of Technology*, NATO Parliamentary Assembly 2023, Science and Technology Committee (STC).

Joint Declaration on cooperation to secure critical subsea infrastructure, Regjeringen, 9.04.2024, https://www.regjeringen.no/en/aktuelt/joint-declaration-on-cooperation-to-secure-critical-subsea-infrastructure/id3033122/ [accessed: 27.12.2024].

Joint Statement by the European Commission and the High Representative on the Investigation into Damaged Electricity and Data Cables in the Baltic Sea, Brussels 2024, European Commission – Statement.

Maritime Doctrine of the Russian Federation, A. Davis, R. Vest (trans.), Newport 2022, Russia Maritime Studies Institute, United States Naval War College.

McGrath S., *Spotlight on the Shadow War: Inside Russia's Attacks on NATO Territory. A Report by the U.S. Helsinki Commission Staff*, 2024.

Najwyższa Izba Kontroli (Eng. Supreme Audit Office), *Informacja o wynikach kontroli. Przygotowanie państwa na zagrożenia związane z działaniami hybrydowymi* (Eng. Information on the results of the audit. Preparing the state for the threats of hybrid activities), KPB.430.002.2023, Warszawa 2023.

Najwyższa Izba Kontroli (Eng. Supreme Audit Office), *Informacja o wynikach kontroli. Realizacja działań w zakresie poprawy bezpieczeństwa paliwowego w sektorze naftowym* (Eng. Information on the results of the audit. Implementation of measures to improve fuel security in the oil sector), KGP.430.7.2023, Warszawa 2023.

National Security Strategy of the Republic of Poland, Warszawa 2020.

REPowerEU Plan. Communication from the Commission to the European Parliament, the European Council, the Council, The European Economic and Social Committee and the Committee of the Regions, COM(2022) 230 final, Brussels 2022.

Poland's Strategic Concept for Maritime Security, Warszawa-Gdynia 2017, Biuro Bezpieczeństwa Narodowego (Eng. National Security Bureau).

Study on Baltic offshore wind energy cooperation under BEMIP. Final report, ENER/C1/2018-456, Luxembourg 2019, Publications Office of the European Union.

Commander Rafał Miętkiewicz, Associate Professor

Professor at the Polish Naval Academy of the Heroes of Westerplatte in Gdynia. Associate professor in social sciences in the field of security sciences. Graduate of the Polish Naval Academy and Gdynia Maritime Academy (postgraduate studies in crisis management). Expert of the Ignacy Łukasiewicz Institute for Energy Policy in Rzeszów, member of the Polish National Security Association and the Polish Nautological Society. Line officer with several years of experience on board naval mine warfare ships, former commander of ORP "Śniardwy"(645). Academic lecturer in military studies, courses and postgraduate studies (Gdańsk University of Technology, University of Gdańsk) and MBA (Collegium Civitas in Warsaw). Author and co-author of several monographs, academic textbooks and dozens of articles, reports and analyses. Commentator publishing on industry portals (Portal Stoczniowy, Biznes Alert, Baltic Wind EU, Polon). Member of Erasmus+ Programme, European and national research programmes (DAIMON, EU Interreg South Baltic, SABUVIS,

SWAT-SHOAL). His research interests include the use of modern autonomous (unmanned) technologies in maritime operations. His research addresses, inter alia, national maritime security, energy security, with particular emphasis on the supply of strategic raw materials, and the security of critical infrastructure in Polish maritime areas.

Contact: r.mietkiewicz@amw.gdynia.pl