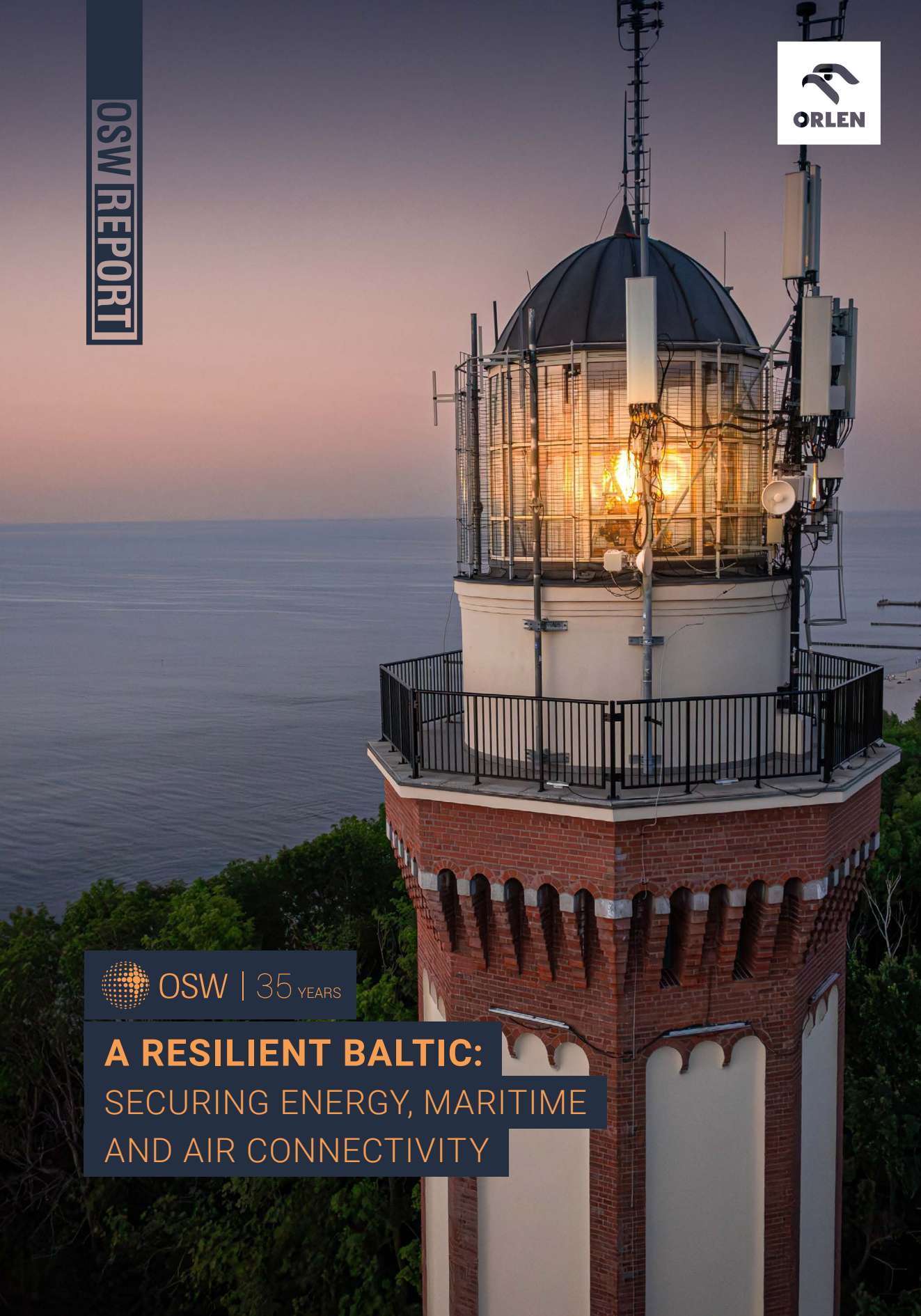
OSW REPORT



OSW | 35 YEARS

A RESILIENT BALTIC:
SECURING ENERGY, MARITIME AND AIR CONNECTIVITY

OSW REPORT

WARSAW
SEPTEMBER 2026

A RESILIENT BALTIC:
SECURING ENERGY, MARITIME AND AIR CONNECTIVITY

OSW | 35 YEARS

AUTHORS
Piotr Szymański, Jacek Tarociński, Filip Rudnik, Sandra Baniak-Stachowiak

COOPERATION
Agata Łoskot-Strachota, Bartosz Chmielewski, Michał Kędzierski

CONTENT EDITOR
Justyna Gotkowska

EDITORS
Katarzyna Kazimierska, Adrianna Stawska-Ostaszewska

COOPERATION
Szymon Sztyk

CHARTS
OSW

MAPS
Wojciech Mańkowski

DTP
Urszula Gumińska-Kurek

PHOTOGRAPH ON COVER
Shaiith / Shutterstock.com

Centre for Eastern Studies
ul. Koszykowa 6a, 00-564 Warsaw, Poland
phone: (+48) 22 525 80 00, info@osw.waw.pl
www.osw.waw.pl

ISBN 978-83-68327-84-7

Contents

Introduction

The Baltic Sea is of steadily growing importance to the coastal states that are members of NATO and the EU, becoming strategically significant for Poland, the Baltic states, Finland and Sweden; the interests of Denmark and Germany – particularly those of its northern federal states – are increasingly bound up with it. The supply of goods and raw materials, the operation of energy systems and the economic development of the region's states depend to a significant extent on the resilience of energy and telecommunications infrastructure in and around the Baltic Sea, and on the security of the Baltic ports and of maritime and air navigation.

The Baltic Sea today serves as a corridor for transporting, producing and storing energy commodities and energy carriers. Energy and telecommunications infrastructure is becoming increasingly concentrated in and around the sea. This includes fixed installations such as production platforms and wind farms; linear infrastructure such as gas pipelines and power and telecommunications cables; and coastal facilities such as LNG, oil and fuel terminals, fuel storage facilities and power plants. Offshore and coastal assets matter to differing degrees for individual states of the region. The Baltic Sea is becoming pivotal to Polish energy policy: Baltic Pipe and the LNG terminal in Świnoujście together provide import capacity approaching Poland's entire annual gas consumption, while Naftoport in Gdańsk handles the entirety of crude oil supplies to Poland's refineries. By the end of the next decade, offshore wind development could, in turn, meet up to one-third of domestic electricity demand.

The Baltic Sea is also growing in importance in terms of economic and military security. Baltic ports guarantee trade and imports of key raw materials for the Baltic states, Finland, Sweden, Denmark and Poland, acting as strategic logistics hubs that bind together European and global supply chains; given their position on NATO's north-eastern flank, they also carry considerable weight in military logistics. The Polish ports of Gdańsk, Gdynia and Szczecin–Świnoujście form part of the European transport corridors. Accounting for more than 40 per cent of the value of Poland's foreign trade, they underpin its economy, the security of energy

commodity supplies and, in part, the country's ability to mount a military response to crises.

Maritime shipping matters in the Baltic because the Baltic states and Finland, and to a degree Poland and Sweden, rely heavily on transport by this sea route. For Finland, Estonia, Latvia and Lithuania, seaports are the principal channels of trade with foreign partners, whereas for Poland and Germany they are an important element of European and global supply chains. The security of maritime transport is therefore becoming pivotal to the economic stability of most coastal states. The airspace over the Baltic Sea, meanwhile, is a crossroads for air routes linking the states of the region, as well as Northern and Central Europe with Western Europe and the Indo-Pacific. The intensity of air traffic means that ensuring the safety and security of air navigation is important not only for the states of the region, but also for the European transport system as a whole.

As Russia's policy towards EU and NATO states grows more aggressive, Baltic energy and telecommunications infrastructure, ports and maritime and air navigation routes are ever more exposed to Russian sabotage and espionage as well as to cyber-attacks. Offshore and coastal gas pipelines, cables, LNG terminals, oil terminals and offshore wind farms are especially at risk: damage to any of them could disrupt energy supplies and the economies of the region's states. A further challenge is posed by action directed against port infrastructure and maritime shipping. Airspace incidents are also being recorded more frequently, among them GNSS jamming and spoofing (which also affect maritime navigation), flights by military aircraft with transponders switched off, and increased reconnaissance activity.

Consequently, the task of securing energy and telecommunications infrastructure, safeguarding freedom of maritime and air navigation as well as building resilience to Russian hybrid activity is becoming one of the foremost challenges for the states of the Baltic Sea region. That, in turn, requires national crisis-response capabilities, resilience to a wide range of threats and closer regional cooperation. This report examines these challenges and threats, outlines the measures being taken at national and multilateral levels, and offers recommendations for strengthening resilience in each of these areas.

Main points

Energy and telecommunications infrastructure

- Physical damage is the greatest challenge facing energy and telecommunications infrastructure in the Baltic Sea. It comes from two directions: the increasingly frequent deliberate actions of hostile actors such as Russia, and accidents and failures, which are becoming more frequent partly as a result of climate change. Between 2023 and 2025 numerous incidents in these waters were caused by vessels dragging their anchors along the seabed and damaging undersea energy and telecommunications infrastructure. Cyber-attacks pose a challenge at least as serious, and one that continues to grow. A further source of risk is the increasingly frequent disruption of Global Navigation Satellite System (GNSS) signals, which, among other things, hampers the implementation of offshore projects, including the construction of wind farms. The growing number of hybrid incidents, cyberattacks and GNSS disruptions is generating tangible costs for operators and developers of energy and telecommunications infrastructure, forcing them to increase spending on physical protection, cybersecurity and measures designed to strengthen infrastructure resilience.

- In response, the states of the Baltic Sea region have taken both immediate and long-term steps to strengthen the protection of maritime infrastructure at national, bilateral and multilateral levels. One example is the 2025 memorandum on the security of critical undersea infrastructure in the Baltic Sea, which provides, among other things, for the establishment of an expert group and a network of contact points, and for the exchange of information and best practice. Since 2025, NATO has intensified its operations in these waters to protect critical undersea infrastructure, under Baltic Sentry. Complementing this, the European Union is developing framework-level legal measures to strengthen the security of critical infrastructure, including at sea.

- The states of the region should give priority to full transposition of the EU CER and NIS2 Directives into their domestic legal orders. A realistic appraisal of the personnel and equipment available to the region's maritime border guard and police units points to the need for wider use of unmanned systems in the monitoring, surveillance and protection of maritime infrastructure. Also crucial is the acquisition of the technical capabilities needed to repair it quickly. Some of the energy infrastructure – including Baltic Pipe, the Klaipėda terminal and Naftoport in Gdańsk – serves more than one coastal state and is critical to the security of supply for other Baltic neighbours. Effective formats for cooperation, both ad hoc and strategic, are therefore important to securing this infrastructure. The Council of the Baltic Sea States (CBSS) could play a coordinating role in strengthening regional cooperation in this area.

Baltic ports

- Among the main challenges now confronting Baltic ports is military and economic espionage. Traffic of vessels linked to Russia in the Baltic Sea has increased: vessels officially engaged in scientific research, fishing vessels and those operated by hydrographic companies. The photographing of ports, key terminals and quays, as well as unauthorised drone flights over ports and fuel terminals, also increased after 2022. Baltic ports face large-scale, even daily, cyber-attacks against their operational systems, including those belonging to terminal operators.

- The ports themselves and the states of the Baltic Sea region are pursuing numerous national measures to reinforce the security of port infrastructure, including bans on photography, filming and drone flights, as well as the roll-out of private 5G networks. Only now have plans for concrete action by the European Commission emerged: in March 2026, the *EU Ports Strategy* was published, with aims including the exchange of best practice, revisions to port-security guidelines and the development of rules on foreign investment in EU ports, particularly those of dual civil-military significance.

- States and port authorities need to strengthen cooperation further in various forums, including within the EU and in the Council of the Baltic Sea States. It would be beneficial to facilitate the mutual exchange of experience and information on incidents, through the creation of task forces bringing together the teams responsible for security at individual ports. Joint efforts by states and ports, pursued in various formats, to secure greater EU funding

for dual-use projects that reinforce ports and linear infrastructure (rail and road) are also important.

Maritime navigation

- The most serious threat to navigation and the ecosystem in the Baltic Sea is posed by hazardous materials lying on its seabed, in particular German chemical weapons and explosives, including naval mines, coming from the First and Second World Wars. They may not only endanger the natural environment but also be used in acts of sabotage and subversion. Another common threat to navigation in the Baltic Sea is Russia's regular jamming of GPS and other GNSS signals, mainly from the areas of Kaliningrad Oblast and St Petersburg.

- At national level, wrecks regarded as particularly hazardous are monitored. At multilateral level, a key role is played by cooperation among the region's states within the Baltic Marine Environment Protection Commission (HELCOM), which has for years coordinated the collection of data on sites where chemical weapons and ammunition were dumped. Hazardous materials on the Baltic Sea floor have also attracted the attention of the European Union. For three decades, NATO has worked to clear the Baltic seabed of unexploded ordnance dating from the First and Second World Wars.

- Deepening cooperation between maritime administrations, ports, rescue services and navies appears to be the quickest way to improve the safety of navigation and crisis management in this area. The Council of the Baltic Sea States could serve as a platform integrating various activities to strengthen the safety of maritime navigation.

The 'shadow fleet' in the Baltic Sea

- The risky navigation practices of the 'shadow fleet', which operates at the margins of the law, are a response to the Western sanctions regime imposed on Russia since 2022. The threats posed by such vessels operating in the Baltic Sea arise, among other things, from manipulation of the Automatic Identification System (AIS), ship-to-ship transfers at sea, the employment of inexperienced crews and reluctance to cooperate with navigators from EU member states. Incidents in the Baltic's narrow shipping corridors could paralyse navigation, cause collisions and inflict costly environmental damage.

'Shadow fleet' vessels are also suspected of hybrid activity intended to damage critical infrastructure and of espionage.

- G7 countries add to their sanctions lists of specific tankers, together with the natural and legal persons involved in servicing Russian exports in breach of the sanctions regime; those imposed by the United States are the most effective, owing to the threat of secondary sanctions, while EU sanctions mainly target the capacity of 'shadow fleet' vessels to draw on services supplied by EU entities. Several multilateral formats in the Baltic Sea region address this issue. Coastal states have also begun requiring the crews of ships entering their exclusive economic zones to present documentation of the vessel's insurance and registration. Several coastal states conduct occasional inspections in the Baltic. Strengthening these controls, however, carries the risk of Russian countermeasures, which makes states markedly less willing to take such steps without military support within NATO.

- The use of 'shadow fleet' vessels to conduct activities that threaten the security of critical infrastructure in the Baltic Sea provides an important reason for coastal states to persist in efforts to limit the navigation of these vessels and increase maritime security. It is important to exert pressure on flag states and on the jurisdictions in which the companies chartering these vessels are registered. The states of the region could also initiate talks on developing a maritime convention for the Baltic Sea that would make it possible to detain vessels in exclusive economic zones if they fail to comply with environmental standards.

Air navigation

- Russia's jamming of satellite navigation signals is a significant risk factor for air traffic in the Baltic Sea region: between January and April 2025 alone, some 122,000 flights reported GNSS interference. Russian military aircraft flying without their transponders switched on and without filing flight plans are an additional factor adversely affecting the safety of civil air traffic. Moreover, they force NATO to scramble quick-reaction alert fighter pairs for identification, which temporarily reduces the predictability of local air traffic.

- The approach of the region's states to GNSS interference has evolved: initially, instances of interference were treated as technical incidents; today, the phenomenon is viewed as a permanent feature of the Baltic Sea security

environment. The priority is not only to detect the sources of interference, but also to create a resilient air traffic management system capable of operating safely even during prolonged degradation or loss of the satellite signal. An example of a multi-layered architecture combining satellite, terrestrial and inertial technologies is the 'Polish PNT Shield'. In the military dimension, NATO conducts radar surveillance, identifies aircraft moving near Alliance borders and provides coordination and command for air operations under the NATO Integrated Air Defence System (NATINADS).

- Two things are needed: the development of regional cooperation to facilitate information-sharing and threat identification, and the coordinated construction of a multi-layered air navigation architecture. Sharing experience and knowledge, developing common standards for resilience to interference and coordinating action could significantly improve the safety and security of air navigation across the Baltic Sea region. In the military dimension, NATO and the states of the region should seek to further strengthen the NATINADS in response to the multi-faceted aggressive actions of the Russian Federation. The growing threat posed by unmanned aerial vehicles requires an expansion of capabilities to detect and neutralise them.

1

Security of energy and telecommunications infrastructure

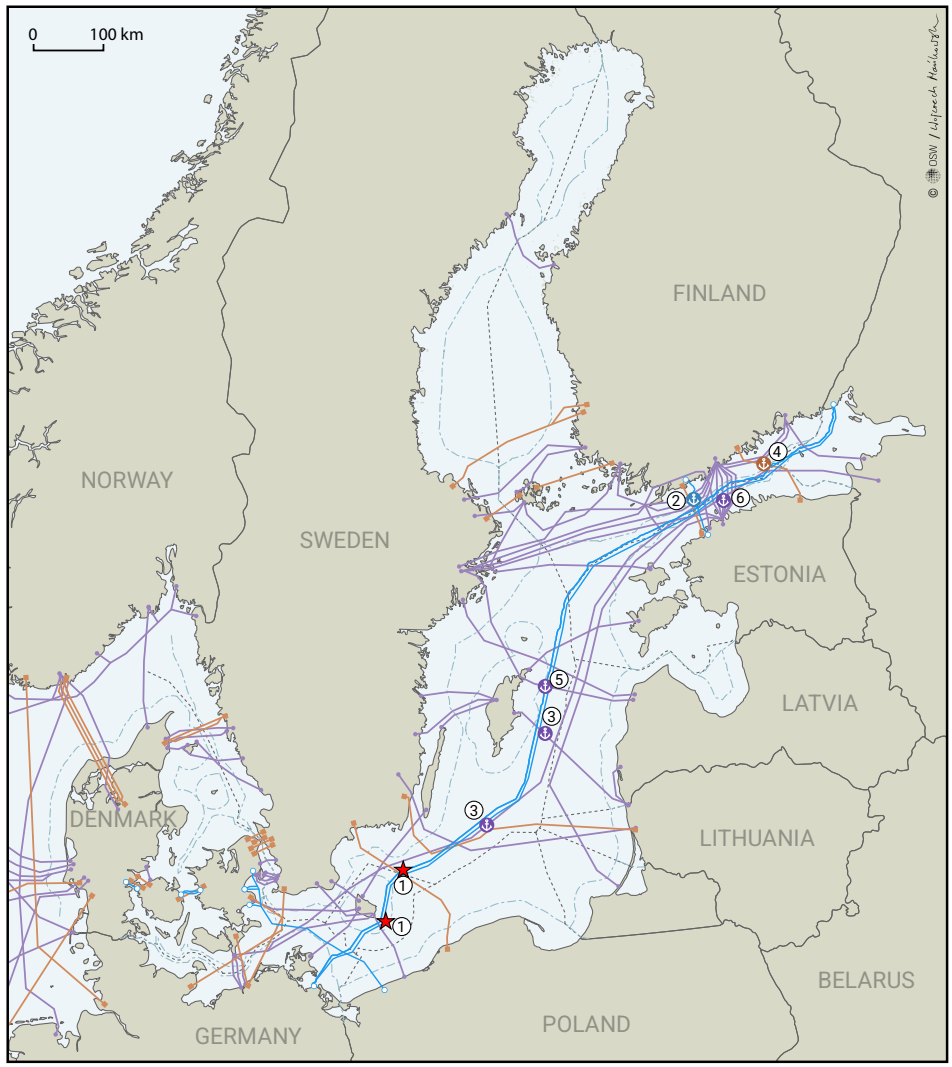
1. Existing and planned energy and telecommunications infrastructure

Offshore energy infrastructure in and around the Baltic Sea is of two types: point-based (drilling platforms and wind farms) and linear (gas pipelines and cables). The coast is also home to numerous significant energy assets, including LNG, oil and fuel import terminals, as well as crude oil and fuel storage facilities. Over the coming years, the sea will be put to steadily greater energy and telecommunications use, driven by decarbonisation and by the growing use of artificial intelligence and data centres. That will entail building further offshore and coastal infrastructure. Planned projects include new subsea power cables (e.g. Estlink 3 between Estonia and Finland) and telecommunications cables (e.g. a link between Sweden, Finland and Estonia), hydrogen pipelines (e.g. the Nordic-Baltic Hydrogen Corridor), nuclear power plants (in Poland and Sweden), LNG terminals (e.g. in Poland), wind farms (the largest are being built by Poland and jointly by Denmark and Germany), transformer stations and service ports.

Energy infrastructure in and around the Baltic Sea is in many cases of strategic importance for individual coastal states. For example, Lithuania imports more than 80 per cent of the gas it consumes through the LNG terminal in Klaipėda (2025). In Poland, Baltic Pipe carries almost half of imported gas (around 45 per cent in 2025), and with the Świnoujście terminal added the two account for almost 90 per cent (88 per cent in 2025). Virtually all of Poland's crude oil imports pass through Naftoport in Gdańsk. In Finland, by contrast, the nuclear power plants located on the coast are pivotal to the energy system, accounting for 26 per cent of national energy consumption (2024). Certain energy infrastructure assets in individual countries also carry strategic weight for their neighbours' security of supply. This is the case with the LNG terminal in Klaipėda, which is important for gas supplies to Latvia and Estonia as well as Lithuania; the Danish section of Baltic Pipe, whose operation is crucial to stable supplies to Poland; and Poland's Naftoport, which currently also delivers to German refineries. That weight will grow as the region's states and companies work more closely together on Baltic offshore wind projects, as the planned hydrogen corridors are built and as the European energy market becomes further integrated.

Smaller states and markets (e.g. Lithuania, Latvia and Estonia) rely far more heavily on energy infrastructure in the Baltic Sea or on its coast than do large ones (Germany) or those bordering other seas or countries (Germany, Denmark). Gas infrastructure assets (pipelines and full-scale LNG terminals) are, moreover, plainly far more significant relative to domestic demand than electricity infrastructure (wind farms and cables).

Map 1. Offshore linear energy and telecommunications infrastructure in the Baltic Sea and incidents of damage to it



gas pipelines
telecommunications cables
power cables
limits of the territorial sea
exclusive economic zone (EEZ) boundaries

Damage to subsea gas pipelines and cables, 2022–2025: ★ by explosion ⚓ by a ship's anchor

1 – September 2022 – Nord Stream 1 and 2 gas pipelines (RU–DE)
2 – October 2023 – Balticconnector gas pipeline (FI–EE), telecommunications cable FET-2 (FI–EE), telecommunications cable EES 1 (EE–SE)
3 – November 2024 – two telecommunications cables (SE–LT and FI–DE)
4 – December 2024 – Estlink 2 power cable (FI–EE) and four telecommunications cables (3 FI–EE and 1 FI–DE)
5 – January 2025 – telecommunications cable (SE–LV)
6 – December 2025 – two telecommunications cables (FI–EE)

Source: Baltic Marine Environment Protection Commission (HELCOM), maps.helcom.fi/website/mapservice.

Map 2. Selected point-based offshore and coastal energy infrastructure in the Baltic Sea

- full-scale LNG terminals
- small-scale LNG terminals
- oil and fuel terminals and fuel storage facilities
- refineries
- ORLEN Petrobaltic drilling platforms
- MFW Baltic Power (Orlen + Northland Power)
- limits of the territorial sea
- exclusive economic zone (EEZ) boundaries
- nuclear power plants
- operating offshore wind farms

Source: Baltic Marine Environment Protection Commission (HELCOM), maps.helcom.fi/website/mapservice.

2. Challenges and threats

Accidents and failures, including those caused by extreme weather events and changes in water levels, remain the greatest challenge for energy and telecommunications infrastructure in the Baltic Sea in peacetime. At the same time, the ongoing war is increasing the threat – from the actions of Russia and of actors linked to it, and the risk of sabotage intended to damage or destroy energy and telecommunications infrastructure (LNG and oil terminals, pipelines and cables, offshore wind farms). **Such operations could make use of 'shadow fleet' vessels, for example, or of hazardous materials lying on the seabed.** Russia routinely deploys hydrographic vessels to map the region's critical infrastructure.

Between 2023 and 2025 a series of incidents in the Baltic Sea caused damage to undersea energy and telecommunications infrastructure – the Balticconnector gas pipeline, the Estlink 2 power cable and telecommunications cables – when vessels dragged their anchors along the seabed (see Map 1). However, investigations to date show that attributing intent to those responsible in such cases is extremely difficult, particularly given the coastal state's lack of jurisdiction beyond the territorial sea, i.e. in the Exclusive Economic Zone (EEZ). The ability to detain a vessel depends to a significant extent on the cooperation of the vessel's captain with the coastal state's law enforcement authorities, i.e. on the captain's willingness to leave the EEZ and enter that country's territorial sea.

Additionally, **operators of energy and telecommunications infrastructure routinely face disruptions to the operation of infrastructure components caused by cyberattacks, as well as the jamming and spoofing of Global Navigation Satellite System (GNSS) signals**. These disruptions create a real risk of collisions and can hinder port operations, particularly for LNG carriers and tankers entering terminals. GNSS disruptions also pose a challenge to the development of offshore infrastructure. For offshore wind farms, the installation of foundations requires centimetre-level accuracy. Given that these operations are carried out by specialised vessels with very high operating costs, even intermittent GNSS disruptions can incur additional costs amounting to tens of thousands of euros.

The 'shadow fleet' is also suspected of carrying out espionage operations using various types of sensors on vessels, and of serving as a launch platform for unmanned systems. The Baltic Sea also sees hazardous activity by the Armed Forces of the Russian Federation, which may be aimed at intimidation (such as dangerous fly-pasts near Poland's Petrobaltic production platform in 2025) or at delaying investments and driving up their costs (such as forcing halts in the

laying of the NordBalt power cable between Sweden and Lithuania by staging naval exercises in 2015).

With the exception of the Gulf of Finland and the Danish Straits, the Baltic Sea's undersea infrastructure is dispersed, which makes it easier to select individual targets for hostile sabotage operations and therefore requires greater military and civilian resources for its protection and monitoring. Attached to the Russian Baltic Fleet is a GRU special unit trained for undersea operations of this type: the 561st Special Purpose Naval Reconnaissance Point at Parusnoye (Kaliningrad Oblast). The states of the region do not have sufficient crewed and uncrewed assets to ensure continuous protection of the Baltic Sea's maritime energy infrastructure. Nor do they command the capabilities needed to repair it swiftly or to investigate incidents.

3. National and multilateral measures

Faced with a series of incidents involving damage to maritime infrastructure in recent years, the states of the Baltic Sea region have taken both immediate and long-term measures to strengthen its protection. These included legal and regulatory changes to improve prevention and make responses to incidents more effective, closer cooperation between military and civilian actors (ministries and agencies, operators, state-owned companies and private firms), investment in capabilities, and operational involvement by uniformed services and law enforcement authorities.

However, these efforts remain insufficient in relation to the threats and the scale of investment in maritime infrastructure. Achieving a sound and effective division of responsibilities, along with information exchange and cooperation between different types of entity both within individual states and across borders, can prove complicated and requires improvement. Protecting maritime infrastructure in exclusive economic zones, that is, in areas beyond states' sovereign jurisdiction, remains a challenge, as does acquiring suitable unmanned assets to raise the level of surveillance and monitoring.

Table 1. Selected measures taken by the states of the region to strengthen the protection of the Baltic Sea's maritime energy and telecommunications infrastructure

State	Measures
Poland	• stronger military surveillance of Polish maritime areas by the navy (Operation Zatoka, since 2022) • creation of the Maritime Security Centre in Gdynia within the Maritime Division of the Border Guard (monitoring Poland's territorial sea and EEZ, and streamlining information exchange between military institutions, law enforcement agencies and the civilian bodies responsible for the maritime dimension of security) • modernisation of the Radar Surveillance System for the maritime border • improvement of civil–military cooperation (e.g. an agreement between the General Staff and Polish power transmission operator Polskie Sieci Elektroenergetyczne on the security of the national energy system's critical infrastructure), and between the legislative and executive authorities and the private sector and state entities (e.g. within the National Chamber of Electronics and Telecommunications) • establishment of special security zones for maritime critical infrastructure • amendment of the legislation on the security of maritime navigation and seaports (2023), adoption of the Safe Baltic Act in 2025 (permitting the rapid use of force in peacetime, on the order of the commander of a naval vessel or military aircraft, to avert an imminent threat to infrastructure outside state territory, that is, in Poland's EEZ), and amendment of the Crisis Management Act (2026)
Germany	• initiation of amendments to the Federal Police Act and the Aviation Security Act to improve the countering of drone threats; creation of a special Federal Police unit dedicated to these tasks, and a plan for a counter-drone defence centre (coordinating the work of the Federal Police, the Länder police and the armed forces) • decision to deploy the special counter-terrorism unit of the Federal Police, GSG 9, to the port of Neustadt (Schleswig-Holstein) to counter threats to critical infrastructure in the Baltic Sea (2024) • adoption by the National Security Council of the *Action Plan for Defence against Hybrid Threats* (2025) and establishment of the Centre for Defence against Hybrid Threats at the Federal Chancellery • a stronger coordinating role for the interministerial Maritime Security Centre in Cuxhaven

Denmark	• introduction of consultation with the defence ministry on offshore wind farm investments at every stage of a project • adoption by Danish Defence of an underwater warfare concept (2024) • conversion of a civilian offshore wind-farm repair vessel into a naval ship for monitoring critical undersea infrastructure by the end of 2026 (to be assigned to the base in Frederikshavn)
Sweden	• intensified inspections of 'shadow fleet' vessels (2025/2026) by extending vessel insurance checks to the territorial sea and the EEZ (previously conducted only in ports) • support for other states with the rescue vessel HSwMS Belos
Finland	• creation of the Regional Cable Hub (2026) by the Finnish Border Guard, together with other Baltic Sea coastal states and the European Commission, to monitor the security of submarine cables in real time • legislative work to extend the security clearance requirement to selected categories of port workers (2025) • installation by the telecommunications company Elisa of acoustic sensors on submarine cables in the Gulf of Finland
Estonia	• drafting of legislation to reinforce counter-drone protection of critical infrastructure in peacetime (including allowing specialised armed security formations to neutralise drones) • strengthening of bilateral cooperation with Finland on maritime infrastructure in the Gulf of Finland • roll-out since 2023 of a smart buoy system for monitoring maritime areas
Latvia	• enhanced patrols of the Latvia–Sweden power cable
Lithuania	• re-establishment of a coast guard unit within the border guard service (VSAT) (2024) • strengthening of cooperation between the armed forces and the electricity transmission system operator Litgrid in protecting critical maritime infrastructure (2025) • development of incident-response protocols concerning undersea infrastructure between the defence and interior ministries (2025) • stronger armed-forces protection of the LNG terminal in Klaipėda (2026)

The region's states are also pursuing bilateral and multilateral initiatives to protect maritime energy and telecommunications infrastructure. One example is the 2025 memorandum of understanding on critical undersea infrastructure in the Baltic Sea. Its parties are the Baltic and Nordic states, Poland, Germany and the EU. Cooperation is to take a number of forms: an expert group; a network of contact points (involving transmission system operators and energy

and telecommunications network operators); the exchange of information and best practice; and the development of technologies for better surveillance and repair of undersea infrastructure.

NATO has given greater attention to the security of critical undersea infrastructure since 2022. In 2024, the **Maritime Centre for the Security of Critical Undersea Infrastructure** was established at Allied Maritime Command (MARCOM). It is a centre of expertise and operational coordination that supports decision-making and the deployment of forces. Work is under way to implement the concept of regional NATO hubs for the protection of critical undersea infrastructure in the Baltic, North, Mediterranean and Black Seas and the Atlantic. Since January 2025, in response to damage to Baltic cables, NATO has been conducting enhanced operations in the Baltic Sea to protect critical undersea infrastructure, under **Baltic Sentry**, which brings together allied naval activity (surface, subsurface and air, including the use of unmanned systems).

The European Union, complementing NATO's activities, is developing framework-level solutions for protecting critical maritime infrastructure. In 2022, the EU adopted two directives: NIS2, on measures for a high common level of cybersecurity, and CER, on the resilience of critical entities. The European Commission has not limited itself to setting general standards; in subsequent years it has developed a series of documents addressing challenges for maritime energy and telecommunications infrastructure.

Table 2. EU documents concerning the protection of maritime energy and telecommunications infrastructure

Document (year)	Maritime energy and telecommunications infrastructure
Revised *EU Maritime Security Strategy and accompanying action plan* (2023)	objective: to protect critical infrastructure in maritime areas (gas pipelines, undersea internet cables, offshore wind farms), including by supporting the development of innovative uncrewed technologies and preparing regional plans for its surveillance
Recommendation on the security and resilience of submarine cable infrastructures (2024)	establishing better coordination in the management and protection of submarine cables, together with adequate funding for that purpose – strengthening the structures managing their security and resilience – creating an expert group to devise a set of risk mitigation measures (Submarine Cable Security Toolbox)

Action Plan on Cable Security (2025)	stricter security requirements for submarine cables – priority for the deployment of new smart cables – greater real-time threat-monitoring capability for early warning and response – creating EU material stockpiles for cable vessels to shorten repair times for damaged infrastructure – establishing cable security surveillance centres (Cable Integrated Surveillance Mechanisms) enabling information exchange, data aggregation and automated analysis, the creation of an alert system and joint repairs
European Internal Security Strategy (2025)	cooperation of the European Commission and the High Representative with Member States, EU agencies and partners (including NATO) to protect submarine cables – cooperation of the European Commission with Member States to devise and roll out an integrated surveillance mechanism for submarine cables in all sea basins, beginning with the Nordic-Baltic region

4. Recommendations

The states of the region should give priority to the full transposition of the CER and NIS2 Directives into their domestic legal orders, particularly as regards the protection of newly emerging maritime infrastructure such as wind farms. Offshore power generation systems are complex ones vulnerable to cyber and physical targeting of its individual elements (offshore substations, cables and points of entry to the national power system). The entities developing wind farm projects, and their operators, must also cooperate closely with the armed forces and law-enforcement authorities, within an orderly legal environment that takes account of both security and investor interests (for example in calculating the costs of different types of radars and sonars, or redundancy). In many countries the rules as they stand remain inconsistent and fragmented. An important task is to integrate state-owned and private companies involved in safeguarding coastal and maritime infrastructure more fully into the uniformed services' information-sharing channels.

A realistic appraisal of the personnel and equipment available to maritime border guard and police units in the region clearly indicates the need for wider use of unmanned systems in the monitoring, surveillance and protection of maritime infrastructure, as well as in the control of shipping. The Baltic coastal states have insufficient resources to mount effective operations of this kind across such extensive sea areas, a shortfall stemming from shortages of personnel and

equipment and from the general overstretch of the uniformed services. Putting unmanned systems to effective use in peacetime, however, calls not only for the requisite investment but also the adaptation of the relevant legal framework. Operational coordination and the division of responsibilities between the military, border and coast guards and the police, on the one hand, and specialised armed security formations, on the other, also often need improvement – for example, in counter-drone operations.

The key requirement, in addition to investment in prevention and crisis response, is to acquire the appropriate capabilities to repair maritime infrastructure rapidly. A regional capability gap is the absence of vessels for laying and servicing cables. In May 2026, the Industrial Development Agency, TFK Group, PGE Baltica and ORLEN Neptun signed a letter of intent on acquiring a Polish cable-laying vessel. Vessels of this kind should be backed by a Baltic network of depots holding pipes, cables and spare parts to shorten repair times. Every state in the region should consider joining the cable hub being built under Finland's aegis, which is meant not merely to keep infrastructure under surveillance but also to establish a regional repair capability. It is also important to build redundancy and resilience into new projects at the design stage.

There is a case for seeking out areas of stronger regional cooperation, because threats to maritime energy and telecommunications infrastructure are cross-border in nature. Some of the energy infrastructure – including Baltic Pipe, the Klaipėda terminal and Naftoport in Gdańsk – serves more than one coastal state and is critical to the security of supply of other Baltic neighbours. The Council of the Baltic Sea States could take on a coordinating role in this process. Through the CBSS, the states of the region could explore the possibility of networking specialised bodies responsible for the security of maritime areas and developing a uniform model for responding to threats and for mutual assistance in their EEZs (common protocols and standards). Also worth considering is a stronger role for the CBSS as a regional hub for cooperation with the private sector and for public-private partnership initiatives, including by involving operators of maritime energy and telecommunications infrastructure.

2

Security of Baltic ports

Baltic Sea ports are of strategic importance to the economies of the region's states, underpinning trade and supplies of key commodities, as well as – increasingly over the past decade – **energy security, given the growing volumes of crude oil and gas handled by these ports.** In 2025, taken together and leaving Russian ports aside, they achieved record throughput in both bulk cargo (641 million tonnes) and containerised cargo (over 10 million TEU).

Baltic ports also play a key role in military logistics – especially Gdańsk, Gdynia and Klaipėda, given their location on NATO's eastern flank. They handle shipments of military equipment, including supplies to Ukraine, and play an important part in moving troops. Since Russia's full-scale invasion, however, Baltic ports have faced mounting challenges to their security. At issue are the risks of military and economic espionage, acts of sabotage and subversion, and cyber-attacks. It is the last of these in particular that ports contend with daily.

1. The main Baltic ports and their specialisations

The largest ports on the Baltic Sea have long been Gdańsk, Klaipėda, Gdynia, Gothenburg, Aarhus, the Szczecin–Świnoujście port complex and Rostock. Container handling is important to almost all of them, the last two excepted; the market leader in this cargo segment is Baltic Hub in Gdańsk, which together with Gdynia handles over 90 per cent of the Polish container market. Beyond containers, Gdańsk also specialises in liquid fuels, handled chiefly by the Naftoport terminal, which currently meets all of the requirements of ORLEN Group's Polish refineries and supplies crude oil to the refinery in Schwedt, Germany. Klaipėda, for its part, also specialises in ro-ro cargo, grain, petroleum products and LNG. Ferry and ro-ro traffic, as well as grain and liquid fuel handling, have also traditionally been important for Gdynia. Among the port's key projects is the expansion of its liquid fuel handling berth, which is due for completion in 2028 and will double the terminal's capacity, reinforcing Poland's energy security.

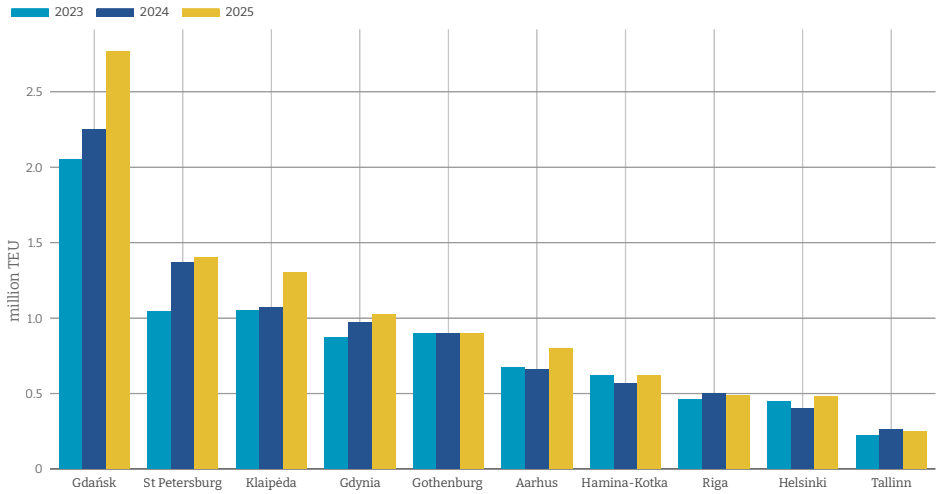
Map 3. Largest seaports on the Baltic Sea

Source: Baltic Marine Environment Protection Commission (HELCOM), maps.helcom.fi/website/mapservice.

In container handling, Gothenburg and Aarhus serve mainly their own countries. The Swedish port, Rostock and Świnoujście are among the largest ferry ports in the Baltic Sea and also play a key role in ensuring their countries' energy security. In 2025 Gothenburg handled some 22 million tonnes of energy commodities, predominantly crude oil; Świnoujście 6 million tonnes of LNG; and Rostock 6 million tonnes of crude bound for Schwedt.

Gdańsk is the undisputed leader in container handling on the Baltic Sea

Container throughput at Baltic Sea ports, 2023–2025

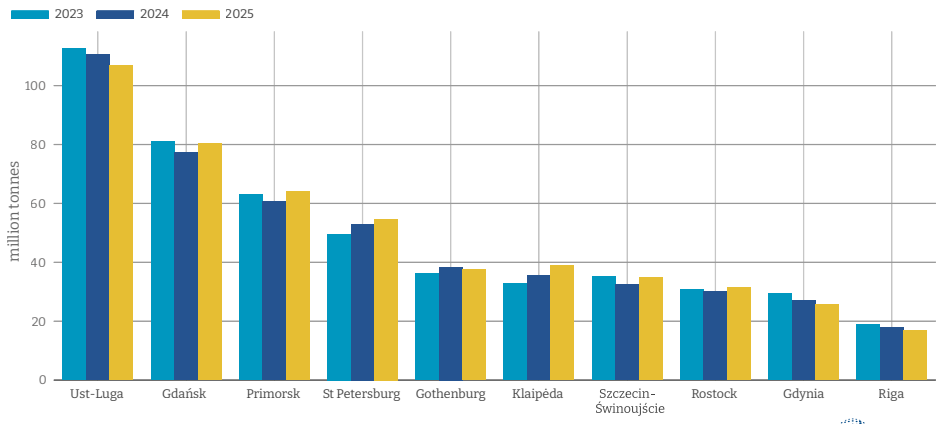


Source: authors' own compilation based on official data from the individual ports.

OSW

Russian ports still lead in bulk cargo handling on the Baltic Sea

Bulk cargo throughput at Baltic Sea ports, 2023–2025



Source: authors' own compilation based on official data from the individual ports.

OSW

2. Key challenges and threats facing ports

Among the principal challenges now confronting Baltic ports is military and economic espionage. In recent years Russia has stepped up its reconnaissance of key port infrastructure – including LNG and oil terminals – along with its intelligence work and its probing of security arrangements. One of its aims is likewise to gather information on deliveries of military equipment to Ukraine. These activities are carried out through observation from land and sea as well as from the air.

Traffic in the Baltic Sea has increased: including vessels linked to Russia that are officially engaged in scientific research, as well as fishing vessels and those operated by hydrographic companies, which map the seabed and critical infrastructure – pipelines and energy and telecommunications cables. The photographing of ports, key terminals and quays has grown more frequent as well. Although such information was often not made public, it is known that individuals documenting port facilities were detained in Latvia, Norway, Sweden and Poland, among other countries, on suspicion of espionage. Unimpeded landward access to parts of Baltic ports likewise remains a problem. Because port land is dispersed across different parts of the host city, fencing it off entirely would, in many cases, be impossible, creating a risk of acts of sabotage and subversion.

Unauthorised drone flights over ports and fuel terminals in the Baltic Sea region also became more frequent after 2022. In addition to the risks associated with espionage, this may lead to damage within port areas, disruptions to port operations, risks to the health and lives of employees, or damage to cargo. In the case of bulk and dangerous cargo, a drone crash may also cause a fire or even environmental contamination.

Another challenge is espionage conducted by Russian sailors serving on ships that fly other states' flags and are not on the list of vessels banned from calling at EU ports. Under international law, ships' crews may as a rule go ashore. A report by the Norwegian Police Security Service (PST) from early 2026 finds that Russian seafarers pose a serious cyber and sabotage threat to Norway. Their espionage is said to centre on the Svalbard archipelago and on Finnmark, the Norwegian region bordering Russia.

Baltic ports also face large-scale, even daily, cyber-attacks against their operational systems, including those belonging to terminal operators. They include attacks on electric cranes, for example, which in turn hamper port operations, and on vessel traffic management systems, as well as attacks designed to steal commercial information. Most frequent are Distributed Denial of Service (DDoS) attacks, which block websites and IT systems, and ransomware, intended to encrypt systems on terminal premises and bring port operations to a standstill.

Threats to Baltic port security have wide-ranging consequences for trade and for the energy security of the state or states concerned. A successful attack on a fuel terminal may lead to the suspension of supplies of a specific feedstock. Actions of this kind entail not only a prolonged halt to port operations but also the expense of repairing damaged infrastructure. Large-scale cyber-attacks on

port infrastructure in the states of the Baltic Sea region may also weaken their position to the advantage of competing ports – attacks on cranes, for instance, which impede port operations and delay deliveries of goods.

3. National and multilateral measures

At present, seaports must increasingly focus on implementing solutions that enhance their security, yet they lack adequate EU rules on which to draw. For the most part, such solutions are introduced either by ports on their own initiative or by individual EU states.

The states of the Baltic Sea region are taking numerous steps at national level to ensure port security. In April 2025 Poland brought in new rules prohibiting the photographing and filming of critical infrastructure facilities, among them the ports of Gdańsk, Gdynia, Szczecin and Świnoujście. In addition, the first of these is located in a Drone Restricted Area (DRA), which means that any unauthorised flight by an unmanned aerial vehicle over the site is treated as a potential security threat and may even result in imprisonment. Klaipėda has adopted similarly restrictive measures. Restrictions on drone flights are in force at the other large Baltic ports too, namely Gdynia, Riga and Tallinn. A further measure, which keeps communications continuously protected, is the use by ports of private 5G networks, capable of connecting cranes and autonomous vehicles. Klaipėda and Riga introduced them in 2025. The Mussalo container terminal at the Finnish port of Hamina-Kotka also has a private 5G network.

Although port security issues have been growing since 2022, concrete plans for action by the European Commission (EC) are only now becoming visible. In March 2026, the EC published its *EU Ports Strategy*, in which it stressed that it would 'strengthen port security by updating and revising existing guidelines, including on new threats'. It is also to convene a forum of EU state representatives and port authorities on cybersecurity for the exchange of best practice, to revise the port security guidelines and to draw up rules on foreign investment in EU ports, particularly those of dual civil-military significance. The intention is better coordination and a common set of guidelines in place of fragmented national rules. One instrument the EU already has in place to improve port cybersecurity is the NIS2 Directive, which covers all sectors deemed critical by EU Member States, with each state defining those sectors at national level, and requires, among other things, mandatory cybersecurity audits, incident reporting and vetting of technology suppliers.

Organisations representing ports – the European Sea Ports Organisation (ESPO) and the Baltic Ports Organization (BPO) – regularly raise the need to create coherent regulations to strengthen port security. They also stress that ports require more EU funding to modernise their infrastructure, for example to meet *dual-use* requirements, and see the new EU financial perspective for 2028–2034 as an opportunity to secure it. Although funds from CEF Military Mobility (Connecting Europe Facility – Military Mobility) are allocated to *dual-use* infrastructure in seaports, they remain insufficient given the scale of needs. Some Baltic ports, Gdańsk among them, are pressing for changes to the EU parameters governing infrastructure that improves military mobility. The EU sets a minimum depth of 14 metres as a condition of funding for quay investments. Although in practice no warship needs quays of that depth, ports without them cannot apply for EU funding.

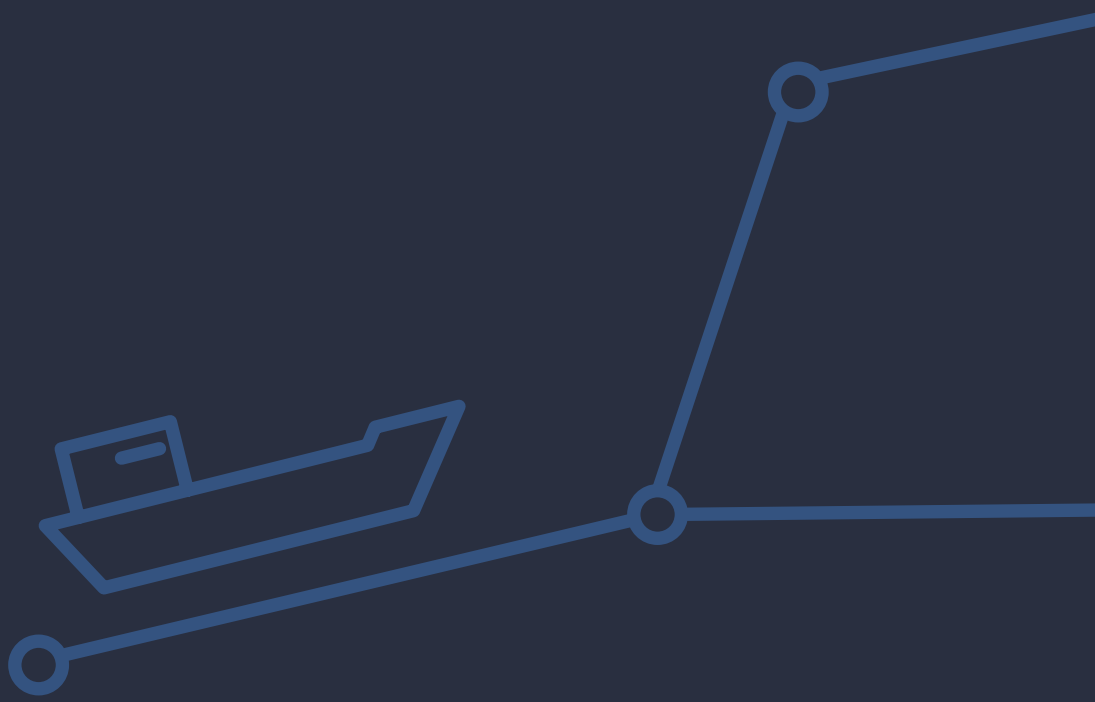
4. Recommendations

States and port authorities need to strengthen cooperation further in various forums, including within the EU and in the Council of the Baltic Sea States. There would be value in a mutual exchange of experience and incident information, achieved by setting up task forces bringing together the teams responsible for security at individual ports. The North Sea ports, themselves regular targets of cyber-attacks, are interested in cooperating with their Baltic counterparts. Structured exchange of experience and information between ports is therefore necessary, as are joint actions by states and ports to strengthen EU regulations on port security.

Also important are joint actions by states and ports, undertaken in various formats, to increase funding for dual-use projects **from EU funds**, strengthening ports and linear infrastructure (rail and road).

3

Security of maritime shipping routes

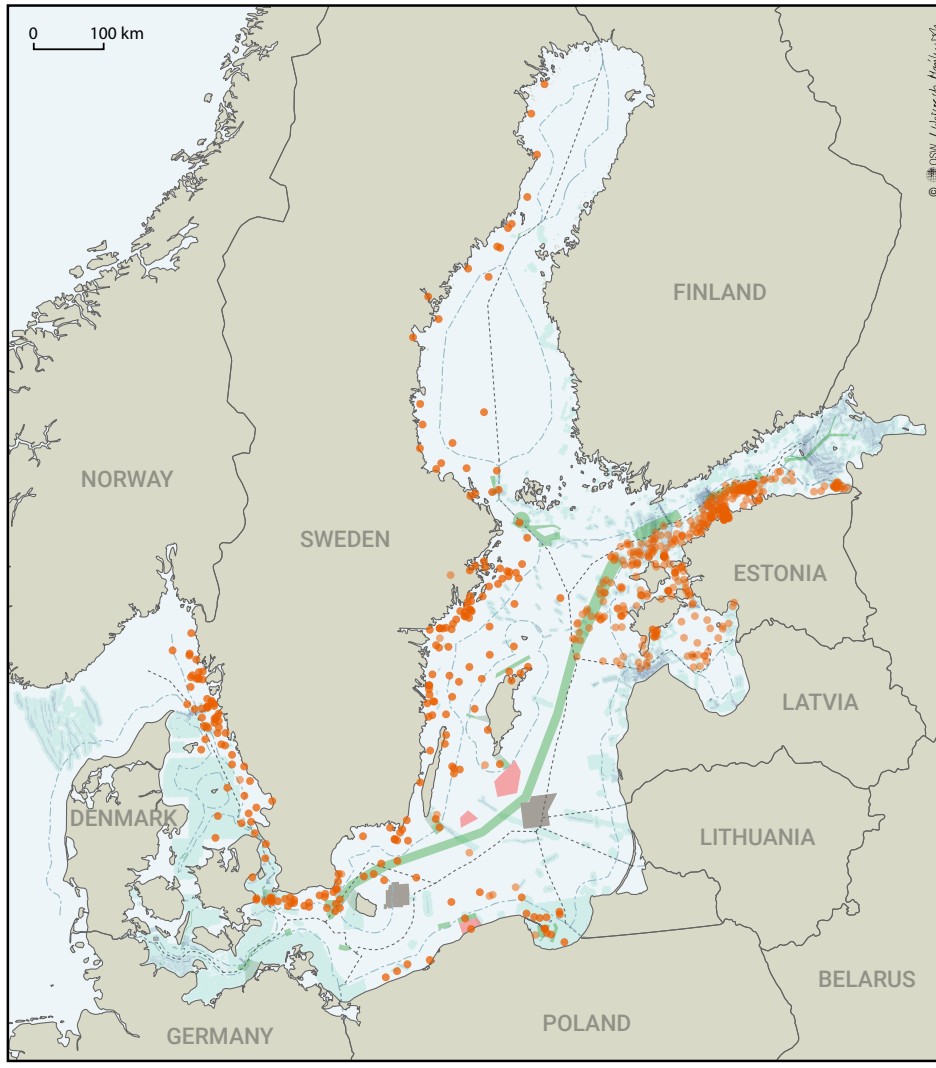


1. Maritime shipping in the Baltic Sea

Maritime transit in the Baltic Sea is highly channelled, a consequence of the basin's geography, hazardous remnants on the seabed and the density of infrastructure, training areas and navigation exclusion zones. The Baltic is a semi-enclosed and relatively shallow sea, with vessel traffic concentrated in a few main corridors leading to the largest ports and through the narrow Danish Straits. Most vessel traffic follows designated shipping routes (*Traffic Separation Schemes*, TSS). Traffic is at its densest around the Sound and Great Belt straits, along the route between southern Sweden and Poland, and in the Gulf of Finland between Helsinki and Tallinn. This channelling of traffic applies to large merchant vessels; outside the designated shipping routes, fishing boats, yachts, wind farm service craft and local vessels operate freely across Baltic waters.

Relative to its size, the Baltic is among the busiest seas in the world: more than 2,000 large merchant vessels are at sea there at any one time, and some 1,500–2,000 vessels of all kinds pass through the Danish Straits each day. The Baltic's geography places considerable constraints on navigation: its average depth is a mere 52 metres, while the many banks, shoals and archipelagos, particularly off the Swedish and Finnish coasts, demand exceptionally precise navigation; in winter, the northern reaches of the Baltic, above all the Gulf of Bothnia and parts of the Gulf of Finland, are also covered in ice, calling for icebreakers and vessels of the appropriate ice class.

Map 4. Traffic Separation Schemes, hazardous materials and wrecks in the Baltic Sea



Source: Baltic Marine Environment Protection Commission (HELCOM), maps.helcom.fi/website/mapservice.

In peacetime, military activity in the Baltic Sea affects civilian traffic through two types of navigation exclusion zone: permanent and temporary. The former comprise national maritime training ranges and military exercise areas, which are recorded in national maritime spatial plans and in the databases of the Baltic Marine Environment Protection Commission (HELCOM) as areas set aside for military training; the latter are local, temporary zones declared solely for the duration of a given exercise. Military exclusion zones have a noticeable effect on Baltic navigation, though in peacetime that effect is primarily local and temporary.

The extensive regulation and channelling of commercial traffic in the Baltic Sea through designated shipping routes **are driven by the desire to reduce risk and prevent possible accidents**. The entire body of water is divided among the territorial seas and exclusive economic zones of the coastal states. At the same time, because of the critical infrastructure, naval training ranges and ecological protection areas located in these waters, individual states have imposed restrictions and traffic bans in many places.

2. Challenges and threats to Baltic Sea navigation

The Baltic Sea is one of the world's largest underwater graveyards of wrecks. According to HELCOM estimates, its seabed contains between 8,000 and 10,000 shipwrecks, naval vessels and other watercraft from various historical periods, from the Middle Ages to the 20th century. A significant proportion of these wrecks have not yet been precisely located or examined and pose a potential risk to navigation.

The most serious threat to navigation and the ecosystem in the Baltic Sea is posed by hazardous materials lying on its seabed, in particular German chemical weapons and explosives, including naval mines. The estimated totals are some 40,000 tonnes of chemical munitions, including 13,000–15,000 tonnes of chemical warfare agents, and over 200,000 tonnes of conventional munitions and explosives dumped during and after the First and Second World Wars. The principal dumping grounds are the Bornholm Deep and the Gotland Deep, but smaller deposits of hazardous material and remnants of the world wars are still being found across the basin, including close to major ports and designated shipping routes. Countering this threat is costly and time-consuming; as a result, despite the passage of 81 years since the end of the Second World War, a significant proportion of the dumped hazardous materials has still not been located.

Hazardous materials lying on the Baltic Sea seabed may not only become a threat to the Baltic ecosystem but also be used in acts of sabotage and subversion. As chemical and conventional munitions and wrecks containing fuel and toxic substances continue to age and corrode, their contents may be released. Chemical warfare agents escaping into the water and the atmosphere would amount to an ecological disaster. Hazardous materials may also be used, directly or indirectly, to disguise acts of sabotage and subversion, by shifting responsibility for deliberate action onto long-standing problems with the munitions lying on the seabed. A further challenge is psychological and information pressure. Even a minor incident involving the discovery of chemical munitions, a fuel leak from a wreck or the detonation of unexploded ordnance may be used to restrict vessel traffic or undermine trust in state institutions. In this sense, sunken hazardous materials may heighten public fear. Deposits of sunken munitions and wrecks hinder seabed monitoring, complicate inspections and may limit the ability to protect critical infrastructure properly.

Another common threat to navigation in the Baltic Sea is Russia's regular jamming of GPS and other GNSS signals, mainly from Kaliningrad Oblast and the St Petersburg area. Because traffic in these waters is dense and channelled, jamming and spoofing of vessels' satellite positioning can produce position-fixing errors, impede traffic and disrupt ports and critical infrastructure, as well as raising the risk of collision and of marine casualties. Given the risk of collision, many ports have had to introduce alternative vessel guidance systems. In March 2025, Poland, Lithuania, Latvia, Estonia, Finland, France, the Netherlands and Ukraine filed a complaint with the International Telecommunication Union (ITU), a UN specialised agency, calling for action in response to these activities.

3. National and multilateral measures

At national level, wrecks regarded as particularly hazardous are monitored. In Poland's case these are the tanker Franken and the wreck of the SS Stuttgart. Hydrographic surveys of the seabed are also being conducted, and when planning offshore investments it is mandatory to identify sources of pollution and hazardous objects lying on the Baltic seabed. Research projects carried out by scientific institutes, the maritime administration and the Polish Navy, aimed at identifying threats associated with munitions and wartime wrecks, are also becoming increasingly important. At the same time, these measures largely involve reconnaissance and monitoring activities, rather than neutralisation.

At the multilateral level, a key role is played by cooperation among the states of the Baltic Sea region under the auspices of the Baltic Marine Environment Protection Commission, which has for years coordinated the collection of data on chemical weapons and munitions dumping sites and developed common standards for assessing environmental risks. In 1993, the ad hoc Working Group on Dumped Chemical Munitions (HELCOM CHEMU) was established and prepared a report on sites where chemical weapons had been dumped in the marine environment. An expert group (HELCOM MUNI) was formed in 2010 to gather and review the existing information on dumped weapons, and in 2013 the HELCOM group on environmental risks from hazardous submerged objects (EG SUBMERGED) followed. In 2021, the updated HELCOM Baltic Sea Action Plan was adopted, setting out measures to neutralise submerged hazardous materials.

Hazardous materials on the Baltic Sea floor have also attracted the attention of the European Union. Council conclusions on the revised *EU Maritime Security Strategy* (2023) provide for the implementation of an action plan to eliminate unexploded ordnance, chemical munitions and potential oil leaks from shipwrecks in the Baltic Sea. The document provides for a mechanism bringing together the European Commission, the CBSS and HELCOM to coordinate scientific work, operations and data exchange in this field. The European Union funds projects such as CHEMSEA, DAIMON, MUNI-RISK, BALTWRECK and MUNIMAP, which aim to develop technologies for locating, identifying, monitoring and neutralising underwater threats.

NATO regularly works to clear the Baltic seabed of unexploded ordnance from the First and Second World Wars through Standing NATO Mine Countermeasures Group 1 (SNMCMG1). One example is the annual Open Spirit naval exercises, held in the territorial seas and exclusive economic zones of the Baltic states: Lithuania hosted them in 2025 and Latvia in 2026.

The 'Polish PNT Shield' (Positioning, Navigation and Timing) concept is under development. Its objective is to build a national, resilient positioning, navigation and timing (PNT) system capable of operating under conditions of electronic interference and ensuring the continuity of positioning, navigation and timing services even when GNSS satellite signals are jammed or spoofed. The project is being developed by the National Institute of Telecommunications – National Research Institute in cooperation with the Ministry of National Defence, the Ministry of Digital Affairs, the Head Office of Geodesy and Cartography, the Polish Space Agency, and academic and industry partners.

4. Recommendations

The efforts of the states of the Baltic Sea region to improve the safety and security of Baltic navigation, and their cooperation to that end, remain insufficient. There is still no complete and uniform database covering all known and potential locations of munitions and hazardous materials. Much of the seabed has yet to be surveyed with modern sonar and magnetometric methods, and the exact position of many objects remains unknown. Nor is there any common regional programme for the systematic removal of the most dangerous wartime remnants. Beyond further intensifying comprehensive seabed mapping, a programme is needed for the gradual neutralisation of the most dangerous objects and remnants of war, whose continued degradation may both lead to environmental disasters and increase vulnerability to sabotage.

Deepening cooperation between maritime administrations, ports, rescue services and navies appears to be the quickest way to improve the safety of navigation and crisis management in this area. Regular joint exercises – addressing scenarios involving critical infrastructure failures, incidents with hazardous materials lying on the seabed and disruptions to vessel traffic on the main transport routes – should form an important element of this.

The CBSS could serve as a platform bringing together efforts on environmental protection, maritime security and critical infrastructure protection, supporting measures leading to the creation of a common regional database, the development of common procedures for responding to incidents involving the discovery of chemical munitions or damage to wrecks containing fuel, and the organisation of regular exercises involving rescue services, navies and maritime administrations. The CBSS and HELCOM should continue to deepen their cooperation and exchange information.

To increase resilience to jamming and spoofing of the navigation system, one option worth exploring is to extend the 'Polish PNT Shield' project to other states in the region. Sharing experience and knowledge, developing common standards for resilience to disruption and coordinating action could significantly improve the safety and security of maritime and air navigation across the Baltic Sea region.

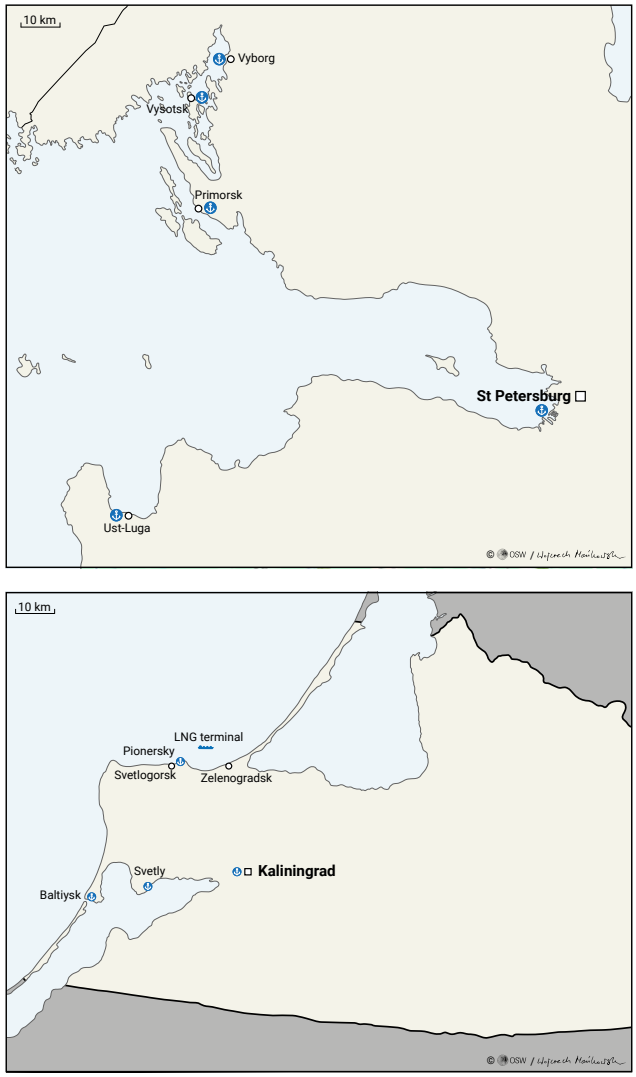
4

Activity of Russia's 'shadow fleet' in the Baltic Sea

1. The importance of the Baltic Sea and the 'shadow fleet' operating there for Russia

The Baltic Sea is a key transport corridor for Russia. A significant share of the country's foreign trade passes through the Baltic, with Russia's ports there handling around one-third of the total cargo throughput of all Russian ports. Moreover, with Kaliningrad Oblast isolated from EU countries, supplies to the exclave – including liquefied natural gas (LNG), which is essential to its energy sector – are shipped across the Baltic.

Map 5. Baltic ports of the Russian Federation in Kaliningrad Oblast and the Gulf of Finland

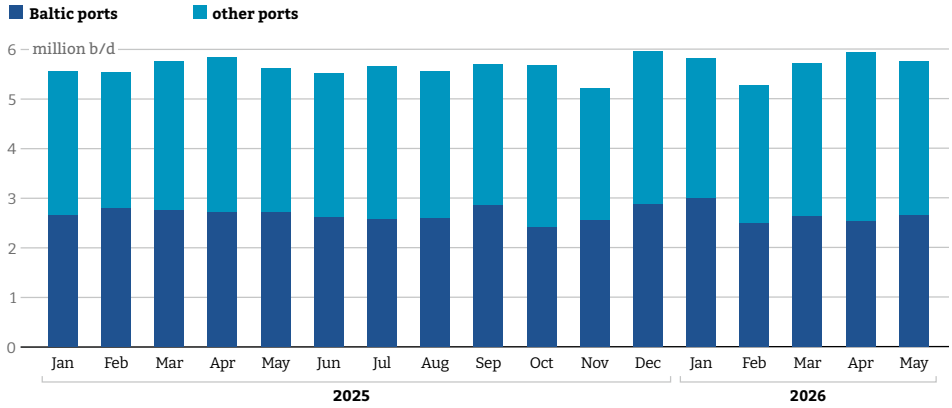


Source: authors' own work.

Transit through the Baltic Sea is particularly important from the perspective of Russian exports, primarily hydrocarbons, but also fertilisers and metal ores. Russian oil terminals in the Baltic Sea account for nearly half of the country's seaborne exports of crude oil and petroleum products, thereby generating substantial economic benefits for Russia's budget. Under the sanctions regime, this trade is largely carried out by tankers from the 'shadow fleet' – vessels outside the jurisdiction of G7 countries whose legal status is ambiguous. These ships carry chiefly crude oil and, to a lesser extent, fuels.

Baltic ports are a key export hub for Russia, accounting for almost half of its seaborne exports of crude oil and fuels

Russian seaborne exports of crude oil and petroleum products, January 2025 – May 2026

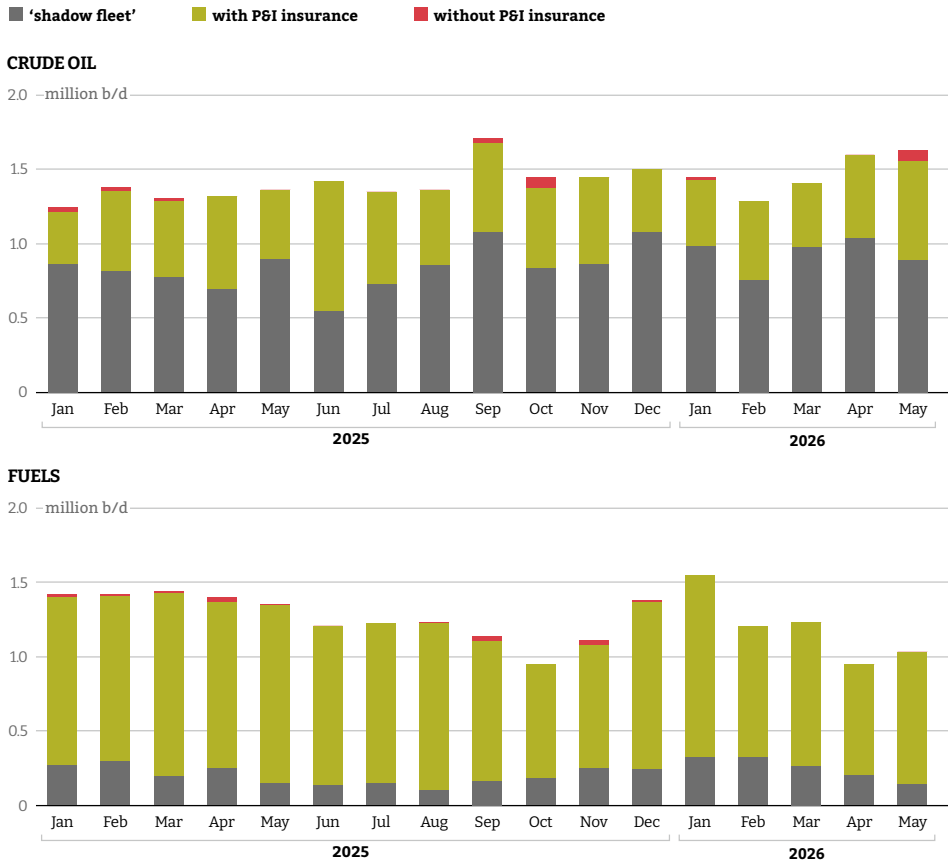


Source: authors' own compilation based on Kyiv School of Economics (KSE) data.

Despite its collective name, the 'shadow fleet' is a heterogeneous group of tankers, whose vessels vary both in their degree of wear and tear and in the transparency of their ownership structures. Nevertheless, sailing under false flags or lack of P&I insurance (covering, among other things, the costs of cargo spills and the resulting environmental damage) these vessels create a risk that compensation will not be paid if a 'shadow fleet' tanker causes a serious maritime incident. In this way, these vessels systemically undermine international standards and rules governing commercial shipping, as confirmed by the International Maritime Organization (IMO) in December 2023.

'Shadow fleet' tankers account for most of Russia's crude oil exports from Baltic ports – though they play a far smaller role in fuel shipments

Share of the 'shadow fleet' in Russian seaborne exports of crude oil and petroleum products from Baltic ports, January 2025 – May 2026



Source: authors' own compilation based on KSE data.

2. Challenges: threats to ecosystems and infrastructure, and the risk of escalation

The threats posed by 'shadow fleet' navigation in the Baltic Sea stem from the way these vessels operate, which is characterised by:

- **manipulation of the Automatic Identification System (AIS)** – tankers switch off transponders that enable them to be located or falsify location data, including by impersonating other vessels;

- **constant changes in ownership structure**, as well as regular re-registration of tankers, including changes of name and flag (use of so-called *flags of convenience* or the absence of a lawful flag), which makes attribution difficult in the event of an incident;

- **ship-to-ship transfers on the open sea** – in order to blend the crude or transfer the entire cargo to another vessel, which significantly increases the risk of environmental damage;

- **employment of inexperienced crews and reluctance to cooperate with navigators from EU countries** when transiting difficult shipping routes (including the Danish Straits), as well as a lack of cooperation with the services of coastal states.

The risky practices of the 'shadow fleet', which operates at the margins of the law, are a response to the Western sanctions regime imposed on Russia since 2022: through them, Russia has made its exports of crude oil and fuels resilient to interference by Western actors.

The specific features of the Baltic Sea – its semi-enclosed nature, weak water exchange and high intensity of shipping – make the operation of the 'shadow fleet' in these waters particularly dangerous. Individual incidents in narrow shipping corridors may not only paralyse navigation and lead to collisions (for example with a ferry or infrastructure), but also cause costly environmental damage. Over the past three years, several incidents have been recorded in which tankers carrying crude from Russia left oil slicks in their wake (including in the waters of the North Sea and Mediterranean Sea, but also the Baltic Sea). In 2024 a vessel serving Russian exports collided with another ship in the Danish Straits (see Table 3). 'Shadow fleet' vessels are at the same time suspected of hybrid activity intended to damage critical infrastructure, or of espionage (see Chapter 1).

The operation of these ships in the Baltic Sea also carries a risk of escalation between NATO and Russia. Given the importance of Baltic transit to the Russian economy, Moscow is signalling at the political level that it is prepared to thwart attempts to restrict the navigation of these tankers. To underline that resolve, Russian warships occasionally escort ships leaving Baltic ports, in the English Channel among other places, and in the Baltic itself.

3. Measures targeting the 'shadow fleet' in the Baltic Sea

To counter the threats associated with the 'shadow fleet', G7 countries are taking steps to limit its activities, primarily by adding to their sanctions lists specific tankers, together with the individuals and legal entities involved in handling Russian exports in breach of the Western restrictions. That policy has resulted in the EU, the United Kingdom and the United States imposing sanctions on close to 700 tankers in total, although the effectiveness of these measures varies.

While US restrictions are the most effective thanks to the United States' use of the threat of secondary sanctions (which deters companies from cooperating with sanctioned entities, materially limiting their ability to operate globally), EU restrictions primarily affect these vessels' ability to use services provided by entities from EU countries. According to Kpler data, **activity among vessels subject to US sanctions fell by 70 per cent, compared with around 30 per cent for vessels subject to UK or EU restrictions**. Sanctions on the 'shadow fleet' are most effective when restrictions are imposed in coordinated fashion across every jurisdiction. Since the beginning of 2025, however, Washington has ceased actively adding vessels serving Russian exports to its sanctions list, which has weakened the sanctions regime.

The states of the Baltic Sea region have begun requiring the crews of ships entering their exclusive economic zones to produce documentation of the vessel's insurance and registration, in order to minimise the risk of incidents in their vicinity. If irregularities are found or the crew fails to cooperate, these states reserve the right of carrying out a physical inspection on board, up to and including detaining the vessel. In practice several countries have carried out inspections in the Baltic, a large share of them on grounds of environmental risk or falsified ship documentation, such as a vessel passing itself off under a particular flag.

Calls are emerging in the region for active interdiction of the 'shadow fleet', the creation of zones 'free of shadow fleet tankers' and greater coordination among coastal states, including the development of a common *modus operandi* shared by NATO countries, in order to restrict the navigation of dangerous tankers across the entire Baltic Sea. Three formats should be distinguished as part of efforts to counter this phenomenon:

- the Shadow Fleet Expert Group, which brings together states bordering the Baltic Sea and North Sea, together with Iceland;

- NB8++, i.e. the expanded Nordic-Baltic Eight format, serving as a platform for countering the 'shadow fleet';

- the Shadow Fleet Task Force, which expands NB8++ to include representatives of the G7 countries and constitutes a response to the IMO resolution of December 2023 identifying the threat posed by the 'shadow fleet'.

In its December 2025 conclusions, the European Union declared its intention to make fuller use of the international law of the sea to protect undersea infrastructure and to restrict navigation by those vessels whose activities pose serious risks. That same year an EU special coordinator for the 'shadow fleet' was appointed. These efforts dovetail with NATO's work on monitoring and safeguarding the security of critical infrastructure in the Baltic Sea.

Further restricting the activity of the 'shadow fleet' would require coordinated measures by the G7 countries and the states of the Baltic Sea region; however, awareness of the associated risks is an obstacle to such steps. Subjecting further tankers to sanctions or introducing a complete ban on Western companies handling Russian exports of crude oil and fuels (a so-called *price cap* mechanism currently operates, allowing these goods to be exported from Russia at a specified price) would in practice hit Russia's ability to conduct export sales, but paradoxically could also lead to an intensification of 'shadow fleet' activity in the Baltic Sea.

On the other hand, increasing controls over tankers carries the risk of Russian countermeasures, which significantly reduces the likelihood of such steps being taken without military support within NATO. Notably, the Baltic currently matters to Russia as a transit corridor because of the threats to exports through the Black Sea: since mid-2025 Ukraine has stepped up attacks on tankers carrying crude oil and fuels from Novorossiysk. It can therefore be assumed that Moscow will communicate even more assertively its intention to defend the freedom of navigation of vessels departing from its oil ports. That said, Sweden's detention of several vessels serving Russian ports in 2026 drew no reaction from Moscow.

4. Recommendations

The use of 'shadow fleet' vessels for activities threatening the security of critical infrastructure in the Baltic Sea **provides an important reason for coastal states to persist in efforts to limit the navigation of these tankers and increase**

security in these waters. Inaction in this field makes it more likely that shipping conditions will deteriorate further and that environmental damage will occur, generating costs and paralysing navigation. For this reason, the states of the Baltic Sea region should remain engaged in those formats that can make restrictions on 'shadow fleet' tankers more effective.

In this context, it is particularly important to exert pressure – including through EU diplomacy – on flag states or jurisdictions in which the companies chartering these vessels are registered (in the past, such pressure has led to vessels losing their flag through deregistration as a result of a political decision). **When listing vessels under sanctions and increasing the effectiveness of this instrument, coordination within the G7 appears necessary** – because the impact of US sanctions is significantly greater in this area than that of EU sanctions.

The states of the region could also initiate talks on developing a maritime convention for the Baltic Sea that would make it possible to detain vessels in exclusive economic zones if they fail to comply with environmental protection standards. Developing international-law solutions of this kind, which would interfere with the principle of freedom of navigation, would, however, be a considerable challenge. Some capitals resist more far-reaching measures against the 'shadow fleet' out of concern for the interests of their own shipping industries.

Table 3. Incidents involving 'shadow fleet' vessels in the Baltic Sea, 2023–2026

Legend:

incidents involving critical infrastructure

incidents involving environmental threats

(attempted) detentions of 'shadow fleet' vessels

Date	Type of event	Suspected vessel	Description
Oct 2023	Damage to the Balticconnector gas pipeline	Container ship Newnew Polar Bear	Transmission via the pipeline was halted until April 2024; the parallel telecommunications cable was also damaged
Mar 2024	Maritime collision in the Danish Straits	Tanker Andromeda Star	Risk of a cargo spill, though the tanker Andromeda Star was empty

Date	Type of event	Suspected vessel	Description
Nov 2024	Damage to telecommunications cables BCS East-West Interlink (SE–LT) and C-Lion 1 (FI–DE)	Bulk carrier Yi Peng 3	Transmission through the cables ceased for approx. 10 days
Dec 2024	Damage to the electricity transmission cable Estlink 2 (EE–FI) and four telecommunications cables in the Gulf of Finland (three between Tallinn and Helsinki and one FI–DE – C-Lion 1). Eagle S also most likely damaged two Russian telecommunications cables between St Petersburg and Kaliningrad Oblast	Tanker Eagle S	Reduced transmission between the countries as a result of the damage; repairs ran until June 2025
Jan 2025	Engine failure and drift of the tanker; taken over by Germany	Tanker Eventin	The environmental risk was averted when the German authorities took control of the tanker, which had earlier switched off its transponder
Jan 2025	Damage to a telecommunications cable (LT–LV)	Bulk carrier Vezhen and general cargo vessel Silver Dania	Both ships were detained by the Swedish and Norwegian authorities; the investigations did not substantiate suspicions of sabotage; the Vezhen damaged the cable due to navigational errors and poor weather conditions
Apr 2025	Inspection of a 'shadow fleet' tanker by Estonia	Tanker Kiwala	Environmental risk – Estonian authorities detected technical defects and legal irregularities, as a result of which the vessel was forced to dock in Estonia

Date	Type of event	Suspected vessel	Description
May 2025	Suspicious tanker manoeuvre near the SwePol cable	Tanker Sun	Risk of infrastructure damage – the tanker departed after intervention by the Polish Navy
May 2025	Russian efforts to deter Estonia from inspecting the tanker	Tanker Jaguar	A Russian Su-35 fighter flew close to the tanker and an Estonian Navy patrol vessel, violating Estonian airspace
May 2025	Location spoofing in the Gulf of Finland; drifting near a cable	Tanker Falcon (carrying LPG) and tanker Blint (formerly Jaguar)	Monitoring of tankers by Estonia and Finland
Sep 2025	Detection of drones over the territory of Denmark, Norway, Germany and the Benelux countries – suspected launch from the decks of 'shadow fleet' tankers; the suspect vessel was detained by the French Navy	Including the tanker Boracay (formerly named Kiwala; see the April 2025 incident)	Paralysis of air traffic and drone overflights of military installations
Dec 2025	Swedish inspection of a ro-ro vessel	Russian ro-ro freighter Adler	The Swedish authorities inspected the vessel, which had broken down close to the Swedish coast. The vessel is under sanctions for carrying armaments
Dec 2025	Damage to two telecommunications cables (EE–FI) in the Estonian exclusive economic zone	General cargo ship Fitburg	Finnish police and the Border Guard detained a suspect vessel that had sailed from St Petersburg (it was carrying steel products subject to sanctions)
Jan 2026	Damage to a telecommunications cable (LT–LV) near Liepāja	No data	Latvian police boarded the suspect vessel, which was moored in the port of Liepāja (the investigation did not establish culpability)

Date	Type of event	Suspected vessel	Description
Feb 2026	Launch of a drone by a Russian naval vessel	Russian electronic reconnaissance vessel Zhigulevsk	According to the Swedish military, a drone was launched from the Russian vessel towards the French aircraft carrier Charles de Gaulle, moored in Malmö – the drone was neutralised by a Swedish Navy patrol boat
Mar 2026	Sanctions breaches and sailing under a false flag	General cargo ship Caffa	Detention by the Swedish Coast Guard – an inspection found a number of irregularities (including deviations from safety standards), and the vessel's crew was arrested
Mar 2026	Sanctions breaches and sailing under a false flag	Tanker Sea Owl I	Detention of the tanker by the Swedish Coast Guard – during the investigation, the vessel's captain was arrested; according to the authorities, the vessel was sailing under a false Comoros flag
Apr 2026	Suspected environmental contamination (oil spill) east of Gotland	Tanker Flora	Detention of the tanker by the Swedish Coast Guard
Apr 2026	Suspected environmental pollution (discharge of pollutants)	General cargo ship Hui Yuan	Detention of the tanker by the Swedish Coast Guard
May 2026	Suspected sailing under a false flag and breaches of environmental standards	Tanker Jin Hui	Detention of the tanker by the Swedish Coast Guard and the arrest of the vessel's captain; according to the authorities, the vessel was using false documents

5

Safety and security of air navigation

1. Air traffic in the airspace over the Baltic Sea

The airspace over the Baltic Sea is an important regional transport artery, and its role in passenger flights beyond Europe grew after 2022. The war in Ukraine and the closure of Russian airspace to European air traffic reshaped the route network between Europe and Asia, shifting part of the traffic onto routes running over the Baltic Sea and Northern Europe. Despite this growth in importance, the Baltic Sea region accounts for only a small share of the continent's total air traffic when viewed in a Europe-wide context.

The average daily number of flights over the Baltic Sea in 2025 hovered around 1,000–1,200. Civil aviation made up the bulk of it, and as much as 40 per cent of those flights were regional, that is, they began and ended in a state of the Baltic Sea basin. Cargo flights made up no more than 25 per cent of all air activity over the Baltic Sea. The region combines a relatively high density of flights, the vast majority of them short-haul, with a wide range of challenges stemming from military activity.

Air traffic control over the Baltic Sea is based on a multi-level airspace management system that combines the activities of national air traffic control services, international organisations and military structures. It rests above all on the division of airspace between states. No single institution is responsible for managing the whole area; each state therefore supervises its own Flight Information Region (FIR). These areas are managed by national air navigation service providers. Given the volume of flight operations, the European Organisation for the Safety of Air Navigation (EUROCONTROL) plays a vital role in managing traffic flows, planning the use of air routes and limiting the risk of individual airspace sectors becoming overloaded.

To improve the efficiency of air traffic management under the Single European Sky initiative, the airspace over the Baltic Sea has been divided among three functional airspace blocks (FABs): the Baltic FAB, covering Poland and Lithuania; the Danish-Swedish FAB; and the North European FAB (NEFAB), covering Norway, Finland, Estonia and Latvia. The FABs act above all as coordination platforms, not as a unified airspace management system for the Baltic Sea area. While this division facilitates air traffic management by allowing airspace to be organised less rigidly along national borders, the lack of full integration and the division of the Baltic Sea area into three separate organisational zones limit the resulting synergies. In recent years, the concept of Free Route Airspace (FRA) has become increasingly important in Europe, allowing flights to be planned along

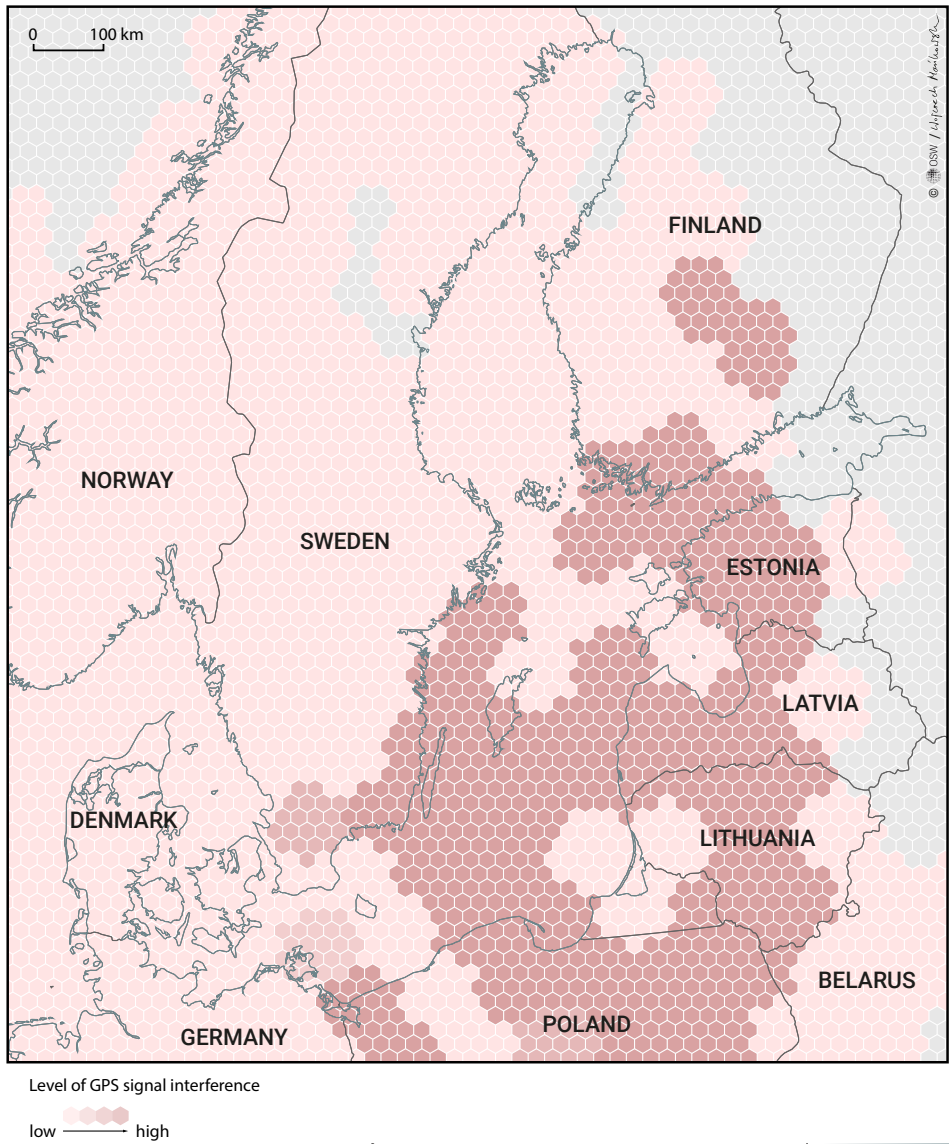
the most direct trajectory and reducing the role of the traditional network of airways. The Russian Federation remains outside the FAB structures and European air traffic management mechanisms, which limits institutional integration in airspace management and the scope for fully optimising air traffic in the region.

The specific characteristics of the Baltic Sea also make close cooperation between civil and military services necessary. Temporary Segregated Areas (TSA) and Temporary Reserved Areas (TRA) are regularly designated over these waters for military exercises and flight training. While they are in force, part of the airspace is closed to civil use and air traffic controllers must reroute traffic accordingly. This model of airspace management allows military tasks to be carried out while maintaining a high level of civil aviation safety.

2. Challenges and threats

Russia's jamming of satellite navigation signals is a significant risk factor for air traffic in the region: between January and April 2025 alone, some 122,000 flights in the Baltic Sea region reported interference with the Global Navigation Satellite System (GNSS). Beyond the difficulties it creates during landing, jamming of the satellite navigation signal can affect actual separation between aircraft, reducing it below the formal safety minima. To counter such a scenario, passenger aircraft must proactively maintain much greater separation from one another, which reduces the capacity of airspace sectors over the Baltic Sea.

Map 6. Satellite navigation system jamming in the Baltic Sea region as of 31 July 2026



Source: GPS jamming map, Flightradar24, flightradar24.com/data/gps-jamming?date=2026-07-31.

Flights by Russian military aircraft without their transponders switched on and without filed flight plans are an additional factor adversely affecting the safety of civil air traffic in the region. They force NATO quick-reaction alert fighter pairs to be scrambled to identify Russian aircraft. This leads to a local and temporary reduction in the predictability of the air traffic system. Civil aircraft must widen their separation to leave a buffer for military activity, cutting sector capacity by as much as 40 per cent. Diminished capacity in the airspace sectors

over the Baltic Sea produces a cascading effect, feeding into flight delays and driving up airline costs. Scrambles of quick-reaction alert fighter pairs to identify Russian military aircraft in international airspace do not amount to violations of the airspace of NATO countries in the region. Since 2025, unmanned aerial vehicles have also accounted for such violations.

Table 4. Violations of the airspace of the states of the Baltic Sea region by Russian and Belarusian assets from 2022 to the end of July 2026

Legend: **aircraft** **helicopters** **missiles** **unmanned aerial vehicles**

Date	Location of violation	Type of asset
29 Jan 2022	Estonia Vaindloo Island, Gulf of Finland	Russian Su-27 aircraft
2 Mar 2022	Sweden east of Gotland	Four Russian fighters (two Su-27s, two Su-24s)
8 Apr 2022	Finland Porvoo, Gulf of Finland	Russian Il-96–300 state aircraft
29 Apr 2022	Denmark east of Bornholm	Russian reconnaissance aircraft
4 May 2022	Finland eastern Gulf of Finland	Russian Mi-17 helicopter
18 Jun 2022	Estonia near the Koidula border crossing point	Russian Border Guard Mi-8 helicopter
9 Aug 2022	Estonia near the Koidula border crossing point	Russian Border Guard Mi-8 helicopter
18 Aug 2022	Finland Porvoo, Gulf of Finland	Two Russian MiG-31 fighter aircraft
16 Dec 2022	Poland object found near Bydgoszcz	Kh-55 cruise missile
1 Aug 2023	Poland Białowieża area	Two Belarusian helicopters, an Mi-8 and an Mi-24

Date	Location of violation	Type of asset
6 Nov 2023	Latvia Latvian-Russian border	Russian aircraft
29 Dec 2023	Poland Polish-Ukrainian border	Russian Kh-101 cruise missile (overflight and return to Ukraine)
24 Mar 2024	Poland Polish-Ukrainian border	Russian Kh-101 cruise missile (overflight and return to Ukraine)
10 Jun 2024	Finland Loviisa, Gulf of Finland	Four Russian aircraft (two fighters and two bombers)
14 Jun 2024	Sweden east of Gotland	Russian Su-24 aircraft
7 Sep 2024	Latvia object crashed near Gaigalava	Russian Shahed/Geran-type unmanned aerial vehicle, entered from Belarus
7 Feb 2025	Finland west of the city of Hanko	Russian state aircraft
11 Feb 2025	Poland eastern Gulf of Gdańsk	Russian Su-24MR reconnaissance aircraft
25 Apr 2025	Poland eastern Gulf of Gdańsk	Russian Baltic Fleet military helicopter
13 May 2025	Estonia Juminda Peninsula	Russian Su-35
23 May 2025	Finland vicinity of Porvoo	Two Russian military aircraft
22 Jun 2025	Estonia Vaindloo Island, Gulf of Finland	Russian Il-76 state aircraft
10 Jul 2025	Lithuania object crashed near the Lithuanian-Belarusian border	Russian Gerbera unmanned aerial vehicle
28 Jul 2025	Lithuania the object crashed at the Gažiūnai training ground	Russian Gerbera unmanned aerial vehicle

Date	Location of violation	Type of asset
9–10 Sep 2025	Poland objects shot down or crashed on Polish territory	19 Russian unmanned aerial vehicles
19 Sep 2025	Estonia Vaindloo Island, Gulf of Finland	Three Russian MiG-31 fighter aircraft
23 Oct 2025	Lithuania Lithuanian-Russian border	Russian Su-30 fighter aircraft and Il-78 tanker aircraft
18 Mar 2026	Estonia Vaindloo Island, Gulf of Finland	Russian Su-30 fighter aircraft
27 May 2026	Finland Porkkala Peninsula	Russian fighter aircraft
30 Jul 2026	Poland the object exploded in the village of Tarnawa-Kolonia	Russian Kh-101 cruise missile

Source: authors' own compilation based on official information.

3. National and multilateral measures

The primary pillar of the safety and security of air navigation over the Baltic Sea is action taken by individual states within their respective areas of responsibility for particular sections of airspace. The approach of the region's states to GNSS interference has evolved: initially, instances of interference were treated as technical incidents; today, the phenomenon is viewed as a permanent feature of the Baltic Sea security environment. The priority is therefore no longer only to detect the sources of interference, but also to build a resilient air traffic management system capable of operating safely even during prolonged degradation or loss of the satellite signal. This is to be achieved by creating a multi-layered architecture combining satellite, ground-based and inertial technologies, examples of which include the 'Polish PNT Shield' and the development of regional cooperation allowing information to be shared more easily and threats to be identified.

In civil air traffic management, the European Union sets the legal framework for the European system, in particular under the Single European Sky initiative, while **EUROCONTROL** is responsible for the operational coordination of air traffic and air traffic flow management at the European level.

In the military dimension, NATO conducts radar surveillance and identifies aircraft moving near Alliance borders, and provides coordination and command for air defence activities under the NATO Integrated Air Defence System (NATINADS). NATINADS combines the national military capabilities of member states: radars, command centres, early warning aircraft, combat aircraft, and ground-based air and missile defence systems. Most NATO countries keep a pair of fighter aircraft on 24-hour quick-reaction alert to protect their own airspace – including by intercepting military and civil aircraft that have lost communications; identifying aircraft with the transponder switched off; or responding to violations of airspace. Lacking national military capabilities of this kind, the Baltic states have their airspace protected on this basis by other allies under the Baltic Air Policing (BAP) mission, flown from bases at Šiauliai in Lithuania and Ämari in Estonia.

4. Recommendations

Developing capabilities to counter interference with GNSS satellite signals remains an important line of effort. The growing number of incidents involving jamming and spoofing of satellite signals requires investment in alternative and multi-layered navigation systems combining satellite, inertial and ground-based technologies. To increase the navigation system's resilience to jamming and spoofing, one option worth exploring is to extend the 'Polish PNT Shield' project to other states in the region. Sharing experience and knowledge, developing common standards for resilience to interference and coordinating action could significantly improve the safety and security of air and maritime navigation across the Baltic Sea region.

NATO and the states of the region should seek to further strengthen the allied air defence system in response to the multi-faceted aggressive actions of the Russian Federation. Monitoring and responding to unreported Russian military flights conducted without an active transponder and without a flight plan mean keeping larger numbers of fighter aircraft on alert in the region and flying reconnaissance and air surveillance missions more frequently. The growing threat posed by unmanned aerial vehicles requires expanded capabilities to detect and, where necessary, neutralise them. Additional radar stations operating in different frequency bands, counter-drone effectors and electronic-warfare systems are all needed; so too is further refinement of the procedures governing cooperation between civil air traffic services and NATO command structures.