



Acute Need for Security of Critical Infrastructure in the Baltic Sea Region

Kinga Dudzińska

Incidents of apparently deliberate damage to critical infrastructure in the Baltic Sea are increasing, including the disruption of an undersea link between Estonia and Finland on Christmas Day. Effective protection against such acts is essential in the context of Russia's strengthening military capabilities in the region and intensification of hybrid activities. NATO and the EU have undertaken to create a framework for joint actions, but it is in the interest of its Member States, including Poland, to increase interstate cooperation and, in particular, the development of regional operational protocols.

Russia's full-scale invasion of Ukraine in 2022 changed the security environment in the Baltic Sea Region (BSR) and highlighted the strategic importance of critical infrastructure. The support for Ukraine by EU and partner states and the accession of Finland and Sweden to NATO have led to an increase in hybrid attacks on critical infrastructure, attributed primarily to Russia, but also clearly supported by China. It also stems from the increased importance of the BSR in the energy and logistics dimensions through the redirection of transport routes after the imposition of sanctions on Russia, the need to secure energy supply chains after the abandonment of Russian sources, and the importance of the Baltic in the EU's energy transition due to the development of offshore wind power.

Threats to Critical Infrastructure in the BSR. Since 2022, the scale of the threats from Russia's military potential because of the strengthening of the Baltic Fleet, mainly in the Königsberg region, but also in the Gulf of Finland and the connected Lake Ladoga, has been growing. There is a progressive intensification of hybrid actions against critical infrastructure, [from the explosion of the NordStream 1 and 2 pipelines](#) in the fall of 2022, to the damage to the Balticconnector pipeline in October 2023 and the disruption of fibreoptic cables between Finland and Germany and Lithuania and Sweden in November 2024. The most recent incident was the disruption of EstLink 2, a submarine power cable connecting Estonia and Finland, in late December

2024. There also has been increasing interference with GPS and radar signals, as reported by the Nordic countries, the Baltics, and Germany.

Various elements of critical infrastructure are at risk, including the Baltic Pipe and Balticconnector gas connections synchronised with the onshore pipeline system, and the intensively developed facilities for LNG. There are now 10 terminals in operation and two under construction. Oil terminals, such as those in Gdansk, Butinga, Vindava, Porvoo, and Rostock, are essential for the transportation of crude oil and petroleum products. High-voltage electricity connections also run through the Baltic, including parts of the so-called Baltic Ring (EstLink 1 and 2, SwePol, SwedLink, along with the complementary onshore LitPolLink) and between Finland and Sweden and Germany and Sweden. The network of undersea telecommunications cables is even denser. Expanded wind farms are increasingly important (especially off the coast of Denmark, but also Poland and the Baltic States), as offshore wind is expected to guarantee the achievement of EU climate targets and emissions reductions. The increased role of certain maritime logistics routes following the reduction of trade with Russia has further increased the critical importance of the Baltic Sea port hinterland. In December 2023, during an exercise by the Russian Baltic Fleet, there was a loss of communications in many areas of the BSR, seriously threatening air traffic, among other things. [Russia's "shadow fleet" remains](#)

[a problem](#), as it continues to transport oil despite sanctions and poses a large environmental risk, while also being used for diversionary activities.

Protecting Critical Infrastructure in the Baltic Sea. [The increase in risk in the region has prompted the EU and NATO to act, albeit mostly reactively.](#) The Union has taken steps to update the legal regime requiring critical infrastructure monitoring, then in 2023 it updated its maritime strategy and developed an initial plan for critical infrastructure protection. NATO has, among other things, established a Maritime Centre for the Protection of Underwater Critical Infrastructure, launched additional surveillance and reconnaissance flights, and is strengthening its presence in Baltic waters. Damage to critical infrastructure motivated the Alliance to include a scenario protecting it during the June 2024 *BALTOPS* exercise and to hold the *Freezing Winds* exercise focused on anti-submarine warfare in November 2024.

Following a meeting between the region's representatives and NATO Secretary General Mark Rutte in Helsinki on 14 January this year, the Alliance, on the initiative of Polish Prime Minister Donald Tusk and others, launched the *Baltic Sentry* mission to monitor the Baltic Sea. Multilateral cooperation is also intensifying, with military exercises involving the UK, Finland, and Estonia in 2023. Also, [the countries forming the Joint Expeditionary Force led by the UK](#), have decided to use it to strengthen protection of Baltic waters.

In addition, individual BSR countries have taken initiatives to strengthen the security of critical infrastructure. The Baltic States, most notably Lithuania, already treated it as particularly vulnerable before 2022, including cybersecurity. Estonia in November 2024 called for strengthening regional cooperation to protect critical infrastructure in the Baltics, and in December the Lithuanian government committed the Lithuanian Public Security Service to protecting key facilities, including Klaipėda's port and NordBalt infrastructure. Poland, for example, uses special forces to protect critical infrastructure and has amended its law on the protection of shipping and seaports. Sweden is focusing on the BSR in its updated security strategy, defining it as a contested sphere and potential field of conflict due to Russia's presence. Finland is adapting its legislation, noting an increase in threats to critical infrastructure primarily in the Gulf of Finland. Denmark highlights the increasing activity of the Russian "shadow fleet" and "research" vessels purportedly mapping the seabed, especially in areas such as straits and port roadsteads, and notes the threat of cyberattacks.

Cooperation between these countries is also intensifying. Agreements strengthening security, including energy security, have been made by Germany with Sweden, Sweden

with Estonia and Finland, and Finland with Estonia. In the area of critical infrastructure protection, Germany is becoming more active, having proposed the establishment of a regional centre for protection of such infrastructure in the Baltic Sea. Polish-Swedish cooperation is becoming increasingly important, as confirmed by the strategic partnership concluded at the end of November 2024. Sweden has initiated stronger cooperation with Poland, especially when it comes to training sailors and soldiers, as well as developing an integrated operational concept for the Baltic Sea.

Conclusions and Recommendations. Numerous recent incidents of damage to critical infrastructure in the Baltic Sea Region indicate its high vulnerability to attack. It is proving to be a crucial element in building resilience, not only of the region but also of the EU and NATO. While Union and Alliance initiatives are positively welcomed, in practice they are and will be time-consuming, and in the case of the BSR, so far insufficient—all the more so if the goal is to further strengthen security and preserve the region's economic competitiveness. Advanced bilateral and multilateral cooperation among the BSR states is therefore necessary. In response to this need, Poland has taken the initiative to create joint maritime patrols in the Baltic Sea, as a consequence of which NATO has decided to establish the Baltic Sentry. It would be desirable to develop regional scenarios for incident prevention, rapid detection, and response. These scenarios should take into account interstate civil-military cooperation, especially with the intensification of reconnaissance activities by Russia and probable diversionary acts. There is a growing need to intensify joint exercises of uniformed services, including coast guard training. It is also important to increase the compatibility of equipment (sensors, radar systems, naval vessels) to detect threats and evaluate risks in advance.

The challenge for the region, therefore, is that the operational models for protecting critical infrastructure in the Baltic are insufficiently developed and tested by the EU and NATO.

The effectiveness of prevention against an attack is a product of individual countries' decisions, such as increased military mobility and clear procedures for warning, monitoring, and sharing sensitive information. Past activities in the region are a source of good practice for the EU and NATO and could be the basis for a new protocol of action for the protection of maritime critical infrastructure. It is advisable to involve private actors more strongly (e.g., investors in offshore wind), strengthen civil-military cooperation, and develop new technologies and innovations regarding, for example, seabed monitoring or warning systems.