PISM | POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

NO. 108 (2609), 9 OCTOBER 2025 © PISM

BULLETIN

NATO and the EU Respond to Russian Maritime Sabotage

Filip Bryjka

Since October 2023, Russia has damaged 11 undersea cables and pipelines in the Baltic Sea. In response, NATO launched the *Baltic Sentry* mission, allies began inspecting tankers belonging to the "shadow fleet", and the EU imposed sanctions on some of them. As a result, further incidents have been prevented since the beginning of 2025, but Russia is escalating the situation by using drones for provocations. NATO and EU countries should take more decisive action against the "shadow fleet" and strengthen cooperation with private operators of critical infrastructure.

The European Union has imposed sanctions on a total of 444 vessels from the "shadow fleet", which consists of more than 800 vessels. It accounts for 70% of Russia's total maritime oil exports, 60% of which pass through the Baltic Sea. The sanctions include a ban on entry into ports and the provision of shipping services by countries and companies registered in the EU. Their aim is to reduce Russian profits from oil trade: in 2024, according to official data, they accounted for as much as a third of Russia's entire budget (€113 billion), which was equivalent to 83% of military spending. However, the restrictions do not sufficiently extend to countries granting them flags or to non-EU insurance companies. In addition to circumventing sanctions, Russia uses its "shadow fleet" for maritime sabotage, illegal arms trafficking, and as platforms for drones, which in September 2025 conducted reconnaissance of military facilities and critical infrastructure in Denmark, Germany, and Norway. By signalling its readiness to carry out further acts of sabotage, Russia is trying to discourage the EU from adopting the 19th package of sanctions, which is targeting the Russian energy sector (including another 118 ships in the "shadow fleet").

NATO's Response. In reaction to Russia's hostile actions, NATO launched the *Baltic Sentry* mission in January 2025. Its aim is to deter Russia and protect maritime critical infrastructure by increasing monitoring capabilities and reducing time of response to potential incidents. The mission involves destroyers, frigates, and ships for mine countermeasures and underwater infrastructure protection, which are part of NATO's SNMG1 and SNMCMG1 maritime groups. Patrol aircraft, underwater drones, and other maritime surveillance assets are also used. Since September this year, the mission has also been supported by a Danish frigate deployed as part of the NATO mission to counter Russia's violations of Alliance airspace.

In order to better coordinate operations in the Baltic Sea, in October 2024 the Alliance established the Commander Task Force Baltic HQ in Rostock, Germany, and set up the special Task Force X, which uses autonomous systems for detecting and combating underwater threats. To support decision-making and coordination of activities, the Maritime Centre for Critical Underwater Infrastructure Protection was established at Allied Maritime Command in Northwood, England. In addition, as part of the British Joint Expeditionary Force (JEF) initiative, a system for exchanging information on threats to maritime critical infrastructure (Nordic Warden) was launched.

Due to the fact that many elements of critical infrastructure are owned or operated by private companies, a Submarine Critical Infrastructure Coordination Cell was established at NATO Headquarters in early 2023. Its task is to assess vulnerabilities and improve cooperation between states and the private sector, including in the exchange of information and technical data. The Digital Ocean initiative is a platform for cooperation with business in the use of new technologies for underwater observation and surveillance. In order to improve cooperation between NATO and the EU, a joint Task Force on Resilience and Critical Infrastructure has been set up to provide consultation and advice. The EU has also adopted a directive on the resilience of critical infrastructure (CER), which sets out the responsibilities of the public and state sectors.

National Activities and Their Legal Basis. In addition to the *Baltic Sentry* mission, preventive maritime activities have been intensified by navies (e.g., the Polish operation *Zatoka*) and the maritime border guard units of individual Member States. These mainly consist of monitoring the situation in territorial waters and exclusive economic zones. The presence of ships is intended to deter the enemy and shorten the response time in case of suspicious activity. In addition to reconnaissance and patrol activities, NATO countries also conduct exercises in cooperation with border guards and private maritime critical infrastructure operators. A turning point in countering sabotage by the Russian “shadow fleet” was Finland’s detention of the tanker *Eagle S*, which in December 2024 destroyed the Eastlink-2 power cable and damaged four telecommunications cables in the Gulf of Finland. The Georgian captain of the ship was detained and charged with criminal offences. Following Finland’s lead, Estonia, Sweden, Denmark, and Norway, and more recently France, have also begun inspecting “shadow fleet” vessels, but these inspections almost never lead to the detention of ships.

Under the 1884 Convention for the Protection of Submarine Cables, a state may inspect and detain a vessel suspected of cutting or damaging such infrastructure. Furthermore, under Article 220 of the United Nations Convention on the Law of the Sea, states have the right to inspect and check documents in cases of suspected violations of environmental protection regulations, as well as to detain the vessel and initiate criminal proceedings if it causes or may cause serious damage to the coastline or interests of the coastal state. Tankers in the “shadow fleet” often have no insurance, sail under false or expired flags, and do not meet international safety standards. This carries a serious risk of incidents that could lead, among other things, to an environmental disaster, which, like damage to marine cultural heritage, may constitute grounds for intervention.

Russia’s Potential for Escalating Sabotage. Russia described the Alliance’s actions as “illegal” and provided military escorts for the tankers. To weaken NATO’s resolve, it began to escalate the situation, as seen in the violation of Estonian airspace by a Russian Su-35 fighter jet during an attempt by the Estonian navy to detain the tanker *Jaguar* (flying the Gabonese flag) in May this year. In its attacks on critical underwater infrastructure, the “shadow fleet” mainly uses tactics adopted from China that involve dragging an anchor along the seabed to damage undersea cables and pipelines. In recent weeks, Russia has also demonstrated its ability to attack maritime critical infrastructure (e.g., drilling platforms, wind farms) using drones launched from “shadow fleet” ships and naval vessels.

Russia uses naval ships (especially those of the Northern and Baltic fleets), but also autonomous submarines, research vessels, fishing boats, and even civilian yachts equipped with sonar and other technologies capable of scanning the seabed to map underwater critical infrastructure. The Main Directorate for Deep Sea Research (GUGI), which reports to the Ministry of Defence and has been collecting intelligence on NATO’s maritime activities since the 1960s, is responsible for such activities. Russia may also use marine infantry units (including the 336th Brigade from Baltiysk) and three Spetsnaz naval units, one of which (the 561st Naval Reconnaissance Unit) is based in the Kaliningrad Oblast, for actions against the Alliance. Preparations for maritime sabotage against NATO are indicated by the Baltic and Northern Fleets’ exercises as part of the *Zapad-25* manoeuvres.

Conclusions. By using its “shadow fleet”, Russia retains the ability to avoid legal responsibility for maritime sabotage. Although measures taken by NATO and the EU have to some extent limited its ability to conduct these activities at no cost, they may prove insufficient in the event of an escalation involving the use of drones. In the near future, Russia may carry out further incidents to exert pressure and deter the U.S. from supplying Ukraine with Tomahawk cruise missiles.

Due to its geographical extent and limited resources, protecting maritime critical infrastructure is a serious challenge for NATO and the EU. Member States should therefore maintain increased operational activity to deter the adversary, while strengthening the capabilities of maritime border guard units. An important element in countering sabotage is to strengthen cooperation with the private sector in the exchange of information, ensuring the physical protection of critical infrastructure, and joint response to incidents.

Poland’s priorities should be the efficient implementation of naval modernisation programmes, the strengthening of reconnaissance capabilities using underwater and surface drones and satellite observation, the adaptation of operational procedures, and a clear division of responsibilities for maritime critical infrastructure protection between the military, border guards and the private sector. It would be beneficial for private operators of critical infrastructure facilities in Poland, with the support of the Ministry of National Defence, to implement modern technological solutions for underwater observation and surveillance, which would increase situational awareness and reduce response times to incidents. Investments in anti-drone systems will also be an important element in strengthening the resilience of critical infrastructure facilities at sea.