DOI https://doi.org/10.30525/978-9934-26-645-4-55

SABOTAGE ACTS OF SHADOW SHIP FLEETS SUPPORTED BY THE RUSSIAN FEDERATION ON SUBMARINE INFRASTRUCTURE IN THE BALTIC SEA IN 2023–2025

Prof. Bernard Wiśniewski
Director of Center for Research Methodology
in Security Sciences WSB University

Assoc. Prof. Tomasz Safjański
Deputy Director of Center for Research
into Cross-Border Security WSB University

Security studies are characterized by a so-called holistic approach to security, which also takes into account its non-military aspects. Security is currently considered a fundamental need. It is expected that for most humans, the threat of chaos will cause a regression from all higher-order needs to the more powerful need for security. Subversion has always been used when armed confrontation between opposing sides occurs.

It falls within the group of asymmetric operations, defined as those in which there is a disproportion between the warring parties. It encompasses land, air, sea, and cyberspace. Contemporary subversive threats are undergoing changes. These indicate a clear blurring of the lines between classic means of warfare and those that do not fit into the catalog of military methods. This means that effectively countering them and minimizing their effects requires scientific research that also utilizes open sources of information. Due to the benefits of its use, subversion and all its manifestations are being systematically refined.

The Russian aggression on Ukraine has generated a number of new threats not only within Ukraine but also in neighboring countries. Among these is the threat of sabotage of underwater infrastructure in the Baltic Sea. Security issues in the Baltic Sea region are a significant part of the defense doctrine of the Republic of Poland.

A historical and contemporary review of influence operations allows us to conclude that acts of sabotage and diversion against underwater infrastructure in the Baltic Sea are part of the philosophy of operations of the Russian Federation's military and special services, referred to as active measures "aktivka" (rus. активка)[1].

[1] More: M. Galeotti, Chapter 14. Active Measures: Russia's Covert Global Reach [in:] G. P. Herd (ed.) Russia's Global Reach. A Security and Statecraft Assessment, https://www.marshallcenter.org/sites/default/files/files/2021-04/Russia%27s_Global_Reach_A_Security_and_Statecraft_Assessment_0.pdf , access 20.09.2025

This concept denotes a set of diverse operational methods and tools used in the past by the Committee for State Security under the Council of Ministers of the USSR, and today primarily by the Federal Security Service of the Russian Federation (FSB), the Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU), and the Foreign Intelligence Service of the Russian Federation (SVR) to conduct influence operations. Active measures are used to destabilize societies, sow chaos and disinformation, support pro-Russian elements, or provoke unrest. Russian military doctrine assumes the use of active measures to attack the West, including sabotage and diversionary acts targeting underwater infrastructure in the Baltic Sea, which are intended to cause panic and social unrest, incite radical sentiment, undermine the professionalism of services (fire brigade, police, counterintelligence), suggest the existence of an internal enemy, and divert attention from other events (e.g., elections, reforms, military operations)[2].

We can therefore speak of the continuity of sabotage practices from the Soviet era and their adaptation to contemporary operational needs and available tools (cybertechnology, artificial intelligence).

Think-tank analyses[3] and pilot research results[4] indicate an increased number of sabotage and diversion incidents in Europe after 2022 (e.g. arson, cyberattacks, attacks on resources intended for aid to Ukraine, disruption of airport operations by commercial drones).

During VI International Scientific Conference “Maritime Security of the Baltic-Black Sea Region: Challenges and Threats” we present the results of diagnostic research on acts of sabotage using a "shadow fleet" on underwater infrastructure in the Baltic Sea in 2023–2025 as part of the implementation of the Russian Federation's influence operations, which complement the Russian strategy of sabotage and diversion activities conducted on land, in cyberspace and in airspace.

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[5].

[2] More: J. Darczewska J., P. Żochowski. Środki aktywne. Rosyjski towar eksportowy. Punkt Widzenia nr 64/2017, Ośrodek Studiów Wschodnich, Warsaw 2017.

[3] More: M. F. Bukowski. Agents of Chaos: The Shadow Campaign Against the West Cognitive Warfare and Covert Action by Russian and Belarusian Intelligence Service. Casimir Pulaski Foundation, Warsaw 2025; K. Rękawek, J. Lanchès, M. Zotova, D. Bowser, *Russia’s Crime–Terror Nexus : Criminality as a Tool of Hybrid Warfare in Europe*, GLOBSEC Centre for Democracy & Resilience and International Center for Counter-Terrorism, 2025.

[4] More: T. Safjański, *Podpalenia w ramach operacji wpływu Federacji Rosyjskiej jako zagrożenie dla bezpieczeństwa powszechnego*, Zeszyty Naukowe Pro Publico Bono 2025, Fire University in Warsaw, pp. 259–278. DOI:10.5604/01.3001.0055.4383

[5] F. Bryjka, NATO and the EU Respond to Russian Maritime Sabotage, Bulletin No. 108 (2609), 9 OCTOBER 2025. The Polish Institut of International Affairs.

According to the definition developed by B. Wiśniewski and P. Lubiewski, sabotage is a form of combat against an enemy aimed at hindering the execution of their plans. Sabotage most often involves destroying or damaging important facilities, disrupting economic or political processes, and disrupting the goals of a government or socio-political organization. Sabotage is also used as an element of sabotage. Potential targets for sabotage include critical infrastructure systems and strategic sectors of the economy (e.g., energy and transportation). Military facilities constitute a special group. Sabotage usually takes a disorganized form, making it difficult to identify the perpetrator. It does not require the use of specialized tools to carry out the attack, such as firearms or explosives. A key advantage of this type of activity is extensive knowledge of the target or organization being attacked, often including easy access to them. Access to the facility and good orientation allow for precise planning of actions that take into account the specific nature of the facility and its technical security. Sabotage often involves the creation of pretenses, intended to draw the enemy's attention to random events, if necessary, thereby creating the impression that the sabotage was accidental. Sabotage can be carried out individually or by several people simultaneously. Furthermore, parallel subversion actions can be conducted to achieve a single, shared goal[6].

The need for diagnosis stems from the difficulties associated with finding points of contact between theory and reality. With all due respect to security organizers, all their actions, even those based on experience, are theoretical in nature, while the solutions implemented and applied can be described as real. This difference creates the need to rationalize existing solutions in order to optimize them. The diagnosis process is carried out to obtain information about (...) the state of the system in terms of its ability to perform required tasks[7].

Security sciences "have a strong tendency to build their theory on the basis of experience from wars, combat, battles, or exercises – using the method of inductive generalizations. At the same time, due to their praxeological nature, they are relatively flexible and sensitive to scientific and technological progress and socio-political changes"[8].

https://www.pism.pl/publications/nato-and-the-eu-respond-to-russian-maritime-sabotage, access: 01.1.2025.

[6] Encyklopedia Bezpieczeństwa Narodowego. https://encyklopedia.revite.pl/articles/view/491, access: 15.07.2025.

[7] T. M. Dąbrowski, Diagnozowanie systemów antropotechnicznych w ujęciu potencjałowo-efektowym, rozprawa habilitacyjna, Wojskowa Akademia Techniczna, Warsaw 2001. 150 s.

[8] J. Świniarski, W. Chojnacki, Bezpieczeństwo jako przedmiot badań wybranych dyscyplin naukowych [w:] Współczesne postrzeganie bezpieczeństwa, Bielsko-Biała 2006. 278 s.