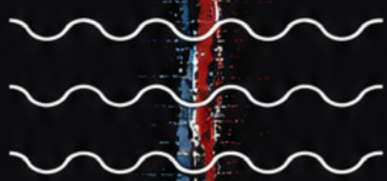
WHITE PAPER

ON RUSSIAN ACTS OF SABOTAGE AND SUBVERSION AGAINST MEMBERS OF THE COUNCIL OF THE BALTIC SEA STATES

FILIP BRYJKA
ANNA MARIA DYNER
ALEKSANDRA KOZIOŁ



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

WHITE PAPER
on Russian Acts of Sabotage and Subversion against Members of the Council of the Baltic Sea States

Filip Bryjka, Anna Maria Dyner, Aleksandra Kozioł

Warsaw, May 2026
The Polish Institute of International Affairs

Editor: **Rob Brooks**

Technical editing and cover design: **Dorota Dołęgowska**

Photocover: **Aleksandra Kozioł**

ISBN 978-83-68555-33-2

E-ISBN 978-83-68555-34-9

The Polish Institute of International Affairs
Warecka 1a, 00-950 Warsaw
tel. (+48) 22 556 80 00
pism@pism.pl, www.pism.pl

This material is distributed by the Polish Institute of International Affairs - Washington, DC Office LLC on behalf of the Polish Institute of International Affairs. Additional information is available at the Department of Justice, Washington, DC.

Printing:
Mazowieckie Centrum Poligrafii
ul. Lisi Jar 29
05-270 Marki

Contents

Introduction and Main Conclusions

Since the start of its full-scale invasion of Ukraine, Russia has stepped up its hybrid activities[1] against NATO member states, especially those most active in supporting the Ukrainian resistance. Those targeted include members of the Council of the Baltic Sea States (CBSS), against whom Russia has employed a full range of tools, such as acts of diversion and sabotage targeting critical infrastructure, incidents involving the violation of airspace and maritime borders, and the jamming of GNSS (satellite radio transmissions), which have caused a range of problems for maritime and air navigation. The aim of the Russian operations was not only to inflict tangible damage and/or test the reactions and responses of the CBSS states, but also to exert a cognitive influence on their societies, so that they would operate under a growing sense of threat. The actions taken against CBSS members were notable in their scale, and the vast majority of acts of sabotage and subversion recorded in European countries since February 2022 were directed against them.

With this strategic reality in mind, the CBSS states should expand and strengthen their cooperation with a focus on preventing and countering these threats. The offensive nature of Russian diversionary and sabotage activities identified since 2022, marked by an intensification in 2024, demonstrates Russia's willingness to take increasingly risky actions, including lethal ones, in order to destabilise NATO and EU countries.

Effectively countering further attacks, therefore, will require a high level of situational awareness, developed through close cooperation (at national and international levels) between military and civilian intelligence and counter-intelligence services, border guards, and police. In this regard, CBSS members have significant potential, based on their geographical proximity and their experience in combating similar threats. Therefore, they could consider establishing a dedicated information exchange mechanism for hybrid threats, where clear identification of the perpetrators of sabotage and subversion plays an essential role. Without definitive attribution, undertaking coordinated actions to prevent and respond to threats becomes significantly more challenging.

[1] "Hybrid threats as a concept," European Centre of Excellence for Countering Hybrid Threats, www.hybridcoe.fi.

Given Russia's well-known and predictable modus operandi, a catalogue of best practices should be drawn up on this basis, setting out common rules for monitoring, reporting on, and responding to hybrid operations. The Baltic Sea region states should commit to consistent application of these countermeasures, as only a coherent regional response will be strong enough to deter Russian aggression. Consequently, mitigating the risk of future hybrid incidents requires NATO and EU member states to deploy a full spectrum of defensive and retaliatory measures.

Methodology

The aim of this report is to identify acts of sabotage and subversion that have occurred within the countries of the CBSS since the outbreak of Russia's full-scale invasion of Ukraine on 24 February 2022 until 13 April 2026. The authors' intention is not only to highlight incidents that can be directly or indirectly attributed to Russia, but also to analyse the dynamics of the ongoing diversion and sabotage campaign, its objectives and strategic context. The practical aim of the report is to formulate conclusions and practical recommendations that can be implemented by the CBSS states (as well as other allies within NATO and the EU) to enhance resilience and the effectiveness of responses to subversion and sabotage.

The authors of the report define diversionary and sabotage activities as organised operations aimed at weakening a state by disrupting its functioning in the political, social, economic and military spheres. In doing so, they distinguish—in accordance with the terminology used in Russia—between the concepts of diversion and sabotage. Sabotage refers to actions aimed at disrupting the functioning of a system from within, e.g., by employees of a given institution. This may involve deliberate negligence or dereliction of duty, falsification of documents, discrediting colleagues, or the deliberate infliction of material or financial damage. Diversion, on the other hand, involves the physical destruction of facilities, such as warehouses, communication lines or infrastructure, for example, using explosives or flammable materials to divert the enemy's attention from other activities. It also has a significant psychological dimension, involving, amongst other things, the intimidation of the targeted population, and thus requires strategic planning and the deployment of greater resources by the targeted party.[2]

The authors have also chosen to highlight the role and significance of hybrid tools in Russian foreign and security policy. The concept of "modern warfare," presented by General Valery Gerasimov, Chief of the General Staff of the Russian Armed Forces, in his 2013 and 2019 speeches, can be traced at least as far back as the early days of the Soviet Union, and is still actively developing, thanks to increasingly modern tools and methods of hostile influence.

[2] E. Ferris, "Russian Sabotage of NATO Infrastructure: Identifying Alliance Vulnerabilities," **RUSI**, 26 March 2026, www.rusi.org.

The methodology adopted is based on the premise that effective analysis requires both a structured classification of cases and the use of a set of analytical variables to capture their evolution over time and space. The analysis is based on the division of acts of sabotage and subversion into the following operational domains:

- **maritime**—covering acts of sabotage against subsea energy infrastructure (pipelines and cables), surface energy infrastructure, as well as ports and naval bases;
- **land-based**—including, amongst other things, acts of sabotage and subversion targeting railway lines, soft targets (e.g. large retail outlets, warehouses), military bases, the defence industry and critical infrastructure;
- **airborne**—primarily involving airspace violations, including the use of drones, as well as GNSS signal jamming.

The authors have deliberately chosen not to identify or analyse incidents in cyberspace, limiting themselves to those of a physical (kinetic) nature. Space domain issues, such as GNSS jamming, have been included in the chapter on hostile activities in airspace. Meanwhile, the chapter on diversion and sabotage on land has been expanded to include elements of analysis of the information (cognitive) domain, which is increasingly identified by NATO as the sixth operational domain.

The use of such a structure enables the empirical data to be organised into coherent categories and analysed comparatively, as well as supporting the identification of sectors that are particularly vulnerable to sabotage. The authors of the report also analysed the techniques, tactics and procedures (TTPs) employed by Russia in these specific operational domains, which allows for an understanding of both the context and the mechanism of operation, an analysis of the repetition and adaptation of methods by the perpetrators, and the identification of operational patterns within and across domains.

In compiling the report, the authors drew primarily on information from open sources, including publicly available versions of reports by the intelligence services of CBSS member states and press articles. Materials provided to PISM analysts by the Internal Security Agency, the Intelligence Agency, the Military Counterintelligence Service, the Armed Forces Operational Command, the Government Centre for Security, the Central Investigation Bureau of Police, as well as Polish diplomatic missions in the CBSS countries. Due to the sensitive nature of the information, which is often classified, as well as the difficulties in some cases of identifying the perpetrators and attributing responsibility to the instigator, this White Paper does not aim to create a single comprehensive database containing all acts of sabotage identified to date that can be unequivocally linked to Russia. This would be an impossible task as governments are currently unwilling to disclose and exchange all the information they hold in this regard.

In-depth knowledge of the subject matter, particularly regarding the methodology for analysing threats of this kind, has also been gained through numerous study visits abroad, participation in conferences, workshops and simulation exercises, as well as

through closed-door expert seminars and research projects. Among these, it is worth mentioning, among others, the seminar entitled "Workshop on the Financing of Russian Sabotage," which took place in November 2025 in Warsaw. Organised by PISM in co-operation with the British think tank The Royal United Services Institute (RUSI), it focused primarily on the methods used by Russia to finance sabotage operations in Europe.[3] The participation of one of the authors in a research project carried out by The George C. Marshall Center for European Security Studies (GCMC) and Doctrine and Training Centre of the Polish Armed Forces, entitled "Deterrence and Defence in the Baltic Sea Region Against the Russian Threat," also made a significant contribution to the preparation of this report.[4]

The authors would also like to thank two interns from the International Security Programme—Mr Grzegorz Bator and Mr Jan Starosta—for their assistance in sourcing and compiling some of the data.

In compiling the report, the authors also drew on existing research into Russian subversion and sabotage, verifying the data contained therein and supplementing it with their own research. Several comprehensive studies are particularly noteworthy. First, the report published in September 2024 by the US Helsinki Commission, which details 150 Russian hybrid operations carried out on NATO territory since the start of the Russian invasion of Ukraine. These were divided into four categories:

1) attacks on critical infrastructure (33% of cases),
2) campaigns of violence (20%),
3) the exploitation of migration (12%),
4) information manipulation and interference in elections (35%).[5]

Although this provides a good illustration of the scale of Russian subversive activities directed against NATO countries, it covers a wider range of incidents than those classified as subversion or sabotage in this white paper.

More precise data can be found in a report by the Centre for Strategic and International Studies (CSIS), which identified 52 confirmed instances of such activities carried

[3] For further information, see: K. Redlowska, M. Popyk, T. Keatinge, "Responding to Russian Sabotage Financing," RUSI, 14 January 2026, www.rusi.org.

[4] Some of the findings included in this report are taken from the publications of the aforementioned project; see: F. Bryjka, "Russian Sabotage Targeting NATO," in: F. Rademacher, A. Lis (eds.), *Deterrence and Defence in the Baltic Sea Region Against the Russian Threat*, Doctrine and Training Centre of the Polish Armed Forces, Bydgoszcz 2026, pp. 7–32.

[5] *Spotlight on the Shadow War: Inside Russia's Attacks on NATO Territory*, U.S. Helsinki Commission, 2024, www.csce.gov.

out on Russia's behalf between January 2022 and March 2025.[6] Similar figures are presented in a report by the International Institute for Strategic Studies (IISS), which additionally recorded 11 hybrid attacks in Europe between January and May 2025.[7] The CSIS report indicated that Russian diversionary and sabotage activities were directed mainly against transport infrastructure (27%), government and military targets (27%), energy infrastructure (21%) and the defence industry (21%). The authors of the study also analysed attack tactics, showing that Russian agents most frequently (in 35% of cases) used incendiary and explosive materials. In 27% of cases, blunt or sharp tools were used, such as anchors designed to cut undersea cables. In 15% of cases, the attacks were electronic, and in 8% of cases, illegal migrants were exploited as tools.[8]

Researchers at Leiden University in the Netherlands have identified 63 Russian hybrid operations between 2022 and 2024, including sabotage (36), vandalism (10), influence operations (8), assassinations (4), terrorism (4) and the exploitation of migration (1).[9] Research conducted by the International Centre for Countering Terrorism (ICCT) and GLOBSEC also makes a significant contribution to the analysis of Russian diversionary and sabotage activities. The authors of the report identified 151 acts of sabotage carried out on EU territory on Russia's behalf between January 2022 and the end of February 2026. More than half of these (83 incidents) took place in the CBSS countries, with the highest number (31) in Poland, 15 each in Germany and Lithuania, 11 in Estonia, 5 in Latvia, 2 each in Sweden and Finland, and 1 each in Denmark and Norway.[10]

[6] For each attack included in the database, CSIS identified at least three credible sources confirming the direct or indirect involvement of the Russian government and conducted interviews with government and non-governmental experts. Several experts were also asked to review the data and analyses, and the level of certainty for each incident was assessed.

[7] C. Edwards, N. Seidenstein, "The scale of Russian sabotage operations against Europe's critical infrastructure," The International Institute for Strategic Studies, 19 August 2025, www.iiss.org.

[8] S.G. Jones, *Russia's shadow war against the West*, Center for Strategic & International Studies, 18 March 2025, www.csis.org.

[9] B. Schuurman, "Russian operations against Europe since the 2022 invasion of Ukraine," Haga: University of Leiden, 2025.

[10] For further reading, see: J. Lanchès, K. Rękawek, "More of the Same: Russia's Crime-Terror Nexus: Criminality as a Tool of Hybrid Warfare Revisited," International Centre for Counter-Terrorism, 23 February 2026, www.icct.nl. The text supplements the data included in the report: D. Hajdu (ed.), *Russia's Crime–Terror Nexus*: *Criminality as a Tool of Hybrid Warfare in Europe, International Centre for Counter-Terrorism*, Globsec, September 2025, pp. 18–19, www.globsec.org.

Russia's Strategy

Russia views NATO and its member states as its primary threat. It has articulated this position for years in key strategic security documents, including the 2014 military doctrine,[11] the 2021 national security strategy,[12] and, indirectly, in the nuclear doctrine adopted in 2024.[13] Reinforcing this stance, senior Russian officials—notably Dmitry Medvedev and Dmitry Peskov—have repeatedly claimed that since the 24 February 2022 invasion of Ukraine, Russia has been in a *de facto* state of war with the Alliance.[14]

Therefore, Russia aims to take action designed to weaken its main adversary as much as possible, using all means that do not cross the threshold of kinetic warfare and do not expose it to systemic retaliation. Russia seeks to carry out these activities across all areas it considers particularly sensitive—namely the information sphere and cyberspace—while also targeting critical infrastructure. In doing so, it draws on its long experience of confrontation with Western states dating back to the formation of the Soviet state, the interwar period, and the Cold War, whilst expanding its operational scope to weaponise modern technologies.

In 2013, General Valery Gerasimov, Chief of the General Staff of the Russian Armed Forces, presented an outline of the concept of a new generation of warfare, which in Western countries is most commonly referred to as hybrid warfare.[15] This model assumes that hostile activities against adversaries can be of a political, economic, informational and social nature, relying directly on the exploitation of a target state's "potential for protest" or high social polarisation. Gerasimov also indicated that the first phase of military operations should focus on eliminating critical infrastructure,

[11] "Военная доктрина Российской Федерации," Совет Безопасности Российской Федерации, www.scrf.gov.ru/security/military/document129/.

[12] "Указ Президента Российской Федерации от 02.07.2021 г. № 400 о Стратегии национальной безопасности Российской Федерации," Президент России, www.kremlin.ru/acts/bank/47046.

[13] "Указ Президента Российской Федерации от 19.11.2024 г. № 991 об утверждении Основ государственной политики Российской Федерации в области ядерного сдерживания," Президент России, www.kremlin.ru/acts/bank/51312.

[14] "Медведев заявил, что Россия в одиночку сражается с Западом," ТАСС, https://tass.ru/politika/16307167.

[15] В. Герасимов, "Ценность науки в предвидении," „Военно-промышленный курьер", ВПК.name, https://vpk.name.

preventing state structures from functioning and negatively impacting morale in the targeted society.[16]

The concept presented by General Gerasimov grew out of Russia's analysis of the "colour revolutions" that took place both within the former Soviet Union at the start of the 21st century and the events of the "Arab Spring" in Africa and the Middle East. Russia began implementing this model as early as 2013, including targeting Ukraine through economic, political and information operations, aiming to force its authorities to change their pro-Western policy and abandon the signing of an association agreement with the European Union, which was ultimately successful. By leveraging military and information resources, alongside the protest potential of the Russian-speaking population of Crimea, Russia also managed to seize control of Crimea and illegally annex the peninsula. Moscow subsequently tested the effectiveness of these influence tools during the irregular armed operations it conducted in Donbas between 2014 and 2022.

In 2019, General Gerasimov expanded on his earlier arguments,[17] emphasising that, in order to enhance the effectiveness of non-military tools, it is necessary to actively employ not only economic, political, diplomatic and informational leverage, but also demonstrations of military force. He added that the Russian armed forces must be prepared to wage wars and armed conflicts of a new type, using asymmetric methods of operation. In doing so, he clearly outlined the priorities of the Russian state, and particularly its security forces. The concepts presented by General Gerasimov even include the assertion that, for an impact to be effective, a 4:1 ratio is required in the use of non-military and military means.[18]

The modern warfare concept is a direct continuation and evolution of the Soviet concept of "active measures"—disinformation, destabilisation and espionage campaigns, driven by the USSR's strategic priorities to influence foreign governments. After testing these methods in Ukraine between 2013 and 2022, Russia has now deployed them against NATO countries on a massive scale, seeking to manipulate their policies while continuously refining its operational methods.

Russia is focused on executing special sabotage and intelligence operations. For sabotage activities, it is increasingly recruiting financially motivated individuals who are previously unknown to security services, tasking them with both reconnaissance and direct sabotage. Several operatives detained by NATO counter-intelligence services have claimed they were unaware they were acting on behalf of Russia, having been recruited via social media platforms such as Telegram and paid mainly via

[16] For more see: M. Wojnowski, "The concept of 'new-generation warfare' as understood by strategists at the General Staff of the Armed Forces of the Russian Federation", *Internal Security Review*, No. 13/2025, www.abw.gov.pl.

[17] "Выступление генерала армии Валерия Герасимова на конференции по развитию военной стратегии," LiveJournal, https://bmpd.livejournal.com/3557155.html

[18] К.Е. Кожухова, „Концепция политической войны: подходы Запада и Китая", *Вестник Московского государственного лингвистического университета. Общественные науки*, No. 3 (856), 2024, p. 17–22.

cryptocurrencies.[19] Russian intelligence services often seek to subvert and exploit local radical groups, while also weaponising refugee and migrant flows to further intensify internal political disputes in the targeted countries.

To achieve its strategic objectives, Russia also leverages state-backed proxies. Consequently, for CBSS members such as Poland, Lithuania and Latvia, hostile actions undertaken by Belarus are of great significance. Beyond supporting Russian activities, Belarusian security services also conduct independent operations designed to overload the counter-intelligence capabilities of neighbouring states, thereby increasing the effectiveness and success rate of diversionary and sabotage attacks.

In line with General Gerasimov's concept, military demonstrations are a core component of Russia's influence toolkit. Russia projects this power through large-scale exercises in the Baltic Sea[20] and near NATO borders[21]—often in cooperation with Belarus and the Collective Security Treaty Organisation.[22] Finnish intelligence services also consistently report an increasing Russian military presence near their borders and the reinforcement of the Leningrad Military District, which was re-established in 2024.[23]

Russia's hostile actions against CBSS members (and, more broadly, against NATO countries) indicate that it is seeking to provoke a crisis that will enable it to achieve political and military objectives, which include recognition of its expanded spheres of influence and the significant weakening of the countries on the Alliance's eastern flank. This also suggests that Russia is prepared to undertake a long-term effort, using a wide range of tools to weaken NATO countries, including CBSS members. Consequently, the Russian threat must be treated as persistent and serious, which requires the planning of long-term preventive measures. An analysis of Russia's foreign policy clearly indicates that its authorities view NATO countries as hostile; consequently, the hybrid actions taken against them are now permanent features of the political landscape and are not expected to cease.

[19] M. Miłosz, "Jarosław Stróżyk: Zachowań prorosyjskich jest w Polsce coraz więcej," *Rzeczpospolita*, 16 March 2026, www.rp.pl.

[20] A.M. Dyner, "Ocean 2024 Exercises Demonstrate Russian Naval Capabilities, Strategic Signalling," *PISM Bulletin*, No. 138 (2446), 26 September 2024, www.pism.pl.

[21] A.M. Dyner, "Zapad 2025: Russia, Belarus Signalling Military Capacity Despite the War in Ukraine," ***PISM Bulletin***, No. 101 (2602), 23 September 2025, www.pism.pl.

[22] A.M. Dyner, "CSTO Exercises in Belarus a Display of Unity and Strength," *PISM Spotlight*, No. 63/2025, 8 September 2025, www.pism.pl.

[23] "Finnish Military Intelligence Review 2026," The Finnish Defence Forces, https://puolustusvoimat.fi.

Russian Operations Targeting CBSS Members

Hostile Russian acts of diversion and sabotage have focused on the maritime, land and air domains. The activities carried out as part of these operations were often interlinked (such as the jamming of GNSS signals, which impacted both air and maritime navigation) and were undertaken simultaneously against several countries. This approach was intended to produce additional psychological effects, creating the impression of an omnipotent Russia, capable of effectively operating across multiple domains throughout the Baltic Sea region.

The maritime domain

Since 2022, the Baltic Sea has become a focal grey zone, with Russia conducting increasingly active operations which bear the hallmarks of hybrid warfare.[24] Although the operational intensity is lower than in the air and land domains, it can have far-reaching consequences for the environment, shipping and the economy. Given the nature of the Baltic Sea, a relatively small and semi-enclosed body of water, even a minor incident can affect many countries in the region, and this takes on particular significance.

Russia conducts operations bearing the hallmarks of hybrid warfare, employing methods that obscure any direct link to its state military or intelligence structures. To this end, it has developed a cross-domain toolkit of instruments for diversion and sabotage. These campaigns are massive in scale and executed over protracted timelines, and the multi-domain nature of these operations masks their true nature and frustrates detection efforts.

Hybrid operations in the maritime domain take two main forms, differentiated by the strategies applied.

[24] G. Giannopoulos, H. Smith, M. Theocharidou, "The Landscape of Hybrid Threats," European Commission & the European Centre of Excellence for Countering Hybrid Threats, *Publications of the European Union*, 2021, https://op.europa.eu.

Reconnaissance operations:

- Enable the gathering of information on the opponent's strengths and weaknesses.
- Serve to prepare for future kinetic (hybrid or military) operations.
- Are conducted by entities linked to the Russian state.

Subversive and sabotage operations:

- Target the damage or disruption of a specific facility or system.
- Serve to implement planned kinetic operations.
- Are conducted by intermediaries.

These activities are complemented by measures that, while not direct attacks, align with the hybrid warfare objectives by degrading the maritime operating environment for military and civilian vessels alike. These include disruptions to shipping, through the systematic disabling of AIS[25] transponders, dangerous manoeuvres around other vessels or objects, and the creation of "ghost ships"—decoy vessels that are only visible on radar.[26] These actions are designed to distract the Baltic Sea region states or to redirect their attention away from other operational tasks.

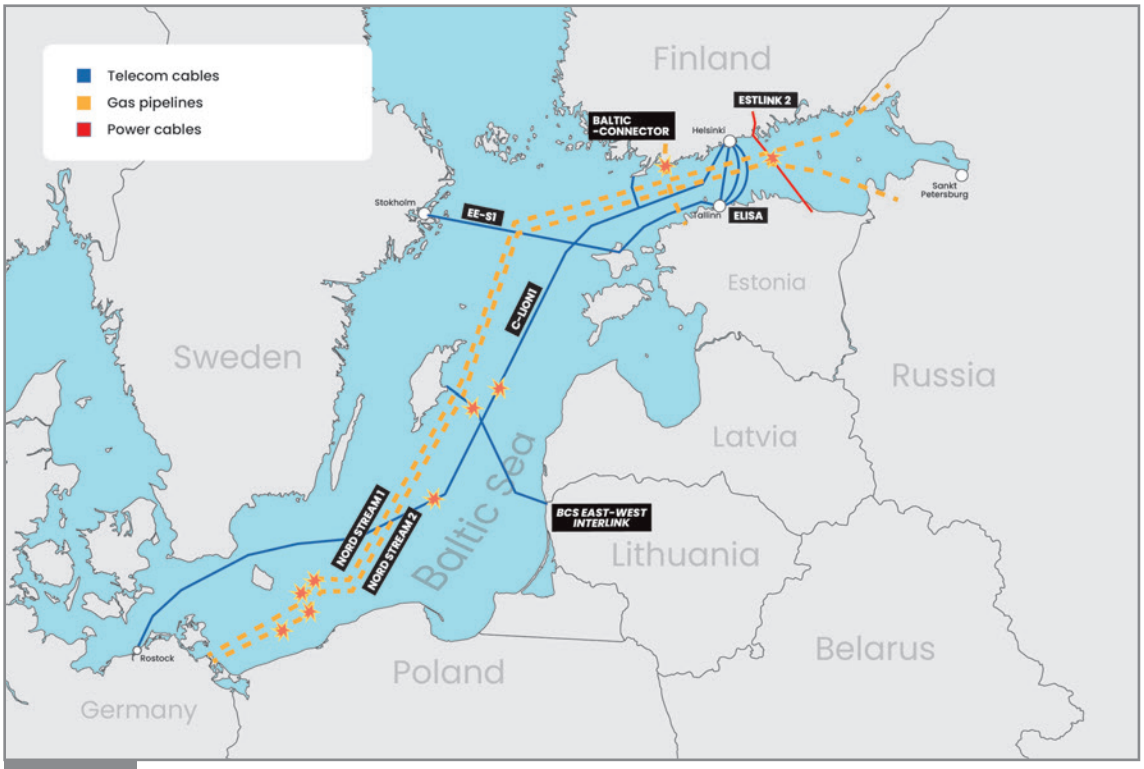
Russia's hybrid operations in the Baltic Sea region to date have been characterised by a high degree of repetition in their modus operandi. Sabotage operations are the least frequently used, but have the greatest impact. Documented sabotage since 2022 includes three attacks on subsea energy infrastructure and six on subsea communications infrastructure (see appendix). Only two incidents involved vessels identified as part of Russia's "shadow fleet";[27] in the remaining cases, the perpetrators either remained unidentified or utilised third-country flags to obscure their origin. Notably, four incidents involved Chinese vessels, raising concerns regarding potential PRC involvement in supporting Russia's hybrid war.

[25] The Automatic Identification System (AIS) is an internationally recognised system used for maritime traffic management. It enables the exchange of real-time data between vessels and coastal authorities regarding the position, course and speed of vessels. In accordance with International Maritime Organisation standards, its use is mandatory for larger passenger ships and commercial vessels.

[26] In Poland, this is the Automated Radar Surveillance System for Maritime Areas, used mainly by the Border Guard.

[27] "Russia's 'shadow fleet' consists of ageing tankers used by Russia to circumvent Western sanctions (primarily the price cap) when exporting crude oil and petroleum products. These vessels do not rely on services provided by entities in the maritime industry from countries participating in the sanctions coalition. They avo-id flag-state and port-state inspections, as well as commercial audits. They also do not have full P&I (protection and indemnity) insurance coverage, or only have minimal coverage. Often obsolete or in poor technical condition, they feature non-transparent ownership structures, frequently change flags, conceal their identity and position through manipulation of the Automatic Identification System (AIS) and name changes, and conduct risky and illegal ship-to-ship transfers." Quoted from: T. Pastucha, "Environmental Challenges," in: A. Dziubińska, A. Kozioł (eds.), *(Un)safe Waters: The Baltic Sea Region and the Redefinition of Security in Europe*, PISM Report, April 2026, www.pism.pl.

Acts of sabotage in the Baltic Sea (2022–2026)



Source: Author's own work.

The launch of Operation "Baltic Sentry" within NATO[28] was a direct response to the December 2024 attack on the power cable linking Estonia and Finland (see table). This incident marked the first time a vessel from Russia's "shadow fleet" had been identified as being directly responsible for the destruction of critical infrastructure. Russia's modus operandi was particularly evident in this case, as the destruction occurred shortly before the scheduled disconnection of the Baltic states from the Russian power grid. Regular patrols, reinforced by "Baltic Sentry," improved monitoring and response to hybrid operations. In 2025, there were indeed two acts of sabotage, but in both cases the vessels responsible were monitored, detained and inspected.

Reconnaissance operations are far more difficult to track, and this includes violations of the Exclusive Economic Zones (EEZ) of the Baltic Sea region states. Security services take different approaches to such incidents, but most are not publicly reported. In Poland's EEZ alone, more than a dozen incidents bearing the hallmarks of hybrid activities have been detected since 2022. Civilian vessels have conducted reconnaissance of the marine environment, targeting the locations of planned underwater and surface installations, naval exercises, and naval operations involving the transport of military equipment.

[28] "Baltic Sentry to enhance NATO's presence in the Baltic Sea," SHAPE Public Affairs Office, 14 January 2025, https://shape.nato.int/.

Table 1

Characteristics of Russian maritime reconnaissance operations

TYPE OF VESSEL	FAVOURABLE FACTORS
Military reconnaissance units	- military-grade reconnaissance equipment capable of operating across a wide range of frequencies (electromagnetic, hydroacoustic, infrared) - capable of sustained operation - specialised crew
Military combat units	- able to quickly relocate - reconnaissance data integration with combat systems
Fishing vessels and factory ships	- large area covered by fishing grounds - ease of moving between fishing grounds - length of stay at fishing grounds
Scientific research vessels	- choice of research areas give freedom of movement - length of stay at research sites - specialised research equipment
Sailing ships	- freedom of movement and observation of naval vessels, exercises and other selected activities
General cargo vessels	- ability to coordinate with other units - ease of deploying unmanned vessels

Source: Compiled by the author, partly based on data from the Intelligence Agency.

Between March 2025 and March 2026, Poland detected and responded to at least four incidents involving Russian vessels that were conducting reconnaissance, probing the response of the authorities, or potentially engaging in sabotage (no damage was caused). The pattern of activity observed in Poland's Exclusive Economic Zone corresponded to incidents in other maritime areas, including outside the Baltic Sea region.

Table 2

Incidents in Poland's Exclusive Economic Zone

DATE	TYPE OF UNIT	PROBABLE TARGET	RESPONSE
May 2025	a vessel belonging to Russia's "shadow fleet"	power cable linking Poland and Sweden	intervention by the Polish Navy
October 2025	a Russian fishing vessel	gas pipeline	intervention by the Polish Border Guard
November 2025	the Russian research vessel Akademik B. Petrov	violation of Poland's Exclusive Economic Zone	surveillance
February 2026	the Russian research vessel Akademik Ioffe	reconnaissance along the Polish coast	surveillance (previously carried out by German and Danish vessels)

Source: Compiled by the author based on data from the Internal Security Agency.

At the political level, the Russian authorities are evidently in support of kinetic hybrid operations, as underlined by the Ministry of Defence of the Russian Federation's proposal on 21 May 2024.[29] It challenged the 1985 maritime border demarcations with Finland and Lithuania in the eastern part of the Gulf of Finland, as well as the areas of Baltiysk and Zelenogradsk in Kaliningrad Oblast. The challenged states' reactions to this proposal were uncoordinated—Finnish Foreign Minister Elina Valtonen described the proposal as "routine," whilst her Lithuanian counterpart Gabrielius Landsbergis called it an "escalation." Comments from Kremlin spokesperson Dmitry Peskov confirmed that the matter served as a means for Russia to test the reactions of the Baltic Sea region states. Highlighting regional tensions and confrontational stances towards Russia, he called the border redefinition an appropriate step by Russia to ensure its security.[30] This is a classic example of the Russian disinformation strategy, where accusations against the opponent describe the actual actions of the Russian side and are intended to prepare public opinion for future hybrid or military actions.

[29] The information appeared on the website of the Ministry of Defence of the Russian Federation, but was removed the following day.

[30] C. Szumski, "Russia's push to change Baltic Sea border sparks concern in the region," Euractiv, 22 May 2024, www.euractiv.com.

Land domain

Russian subversion and sabotage activities carried out in the land domain vary in their sophistication and harmfulness—ranging from reconnaissance and intelligence-gathering operations, through acts of vandalism and political violence, to subversion, sabotage and terrorist attacks. These kinetic actions are coordinated with disinformation operations aimed at exerting psychological influence on the public and decision-makers by instilling fear and a sense of danger. Physical attacks, combined with false narratives disseminated via Russian disinformation channels (including trolls, bots and agents of influence), impose a manipulated interpretation of events on the audience, shifting responsibility away from Russia and attributing it to other parties, such as Ukraine or the authorities of the attacked state.

Just as Russia's main tool in the maritime domain is its "shadow fleet," in the land domain, Russian intelligence services increasingly employ "disposable" or "single-use agents." These are typically untrained amateurs recruited via social media to minimise the costs and risks of diversionary and sabotage operations. This model provides Russia with a layer of plausible deniability, making it challenging for Western services to attribute ultimate responsibility to the state. Russia developed this model following its full-scale invasion of Ukraine, when NATO and EU countries decided to expel over 600 Russian diplomats—including around 400 intelligence officers operating in Europe under diplomatic cover.[31] Although this action significantly weakened Russia's traditional intelligence networks in Europe, the Russians responded by expanding their "illegal" intelligence resources and aggressively recruiting local proxies as "disposable agents."

However, research by the ICCT and Globsec indicates that, contrary to the "disposable" designation, 62% of these agents are involved in at least two attacks.[32] Their "single-use" nature refers to the absence of attention by Russian intelligence to protecting their operational security. If detected and neutralised by counter-intelligence, they are simply abandoned and replaced by fresh recruits to maintain the tempo of operations.

Recruitment is predominantly digital, through the Telegram messaging app (88% of cases analysed by ICCT and Globsec),[33] as well as via Viber, Zengi and Facebook. This is driven through the use of channels linked to the Wagner Group and "volunteer battalions" (e.g. Españ ola), and purpose-built chatbots such as Eye of Sauron, created by the Russian military intelligence service GU (formerly GRU). Further outreach takes place through channels run by military Z-bloggers (e.g. Alexandr Kots, Yevgeny Pod-

[31] S. Jones, J.P. Rathbone, R. Milne, "Russia plotting sabotage across Europe, intelligence agencies warn," *Financial Times*, 5 May 2024, www.ft.com.

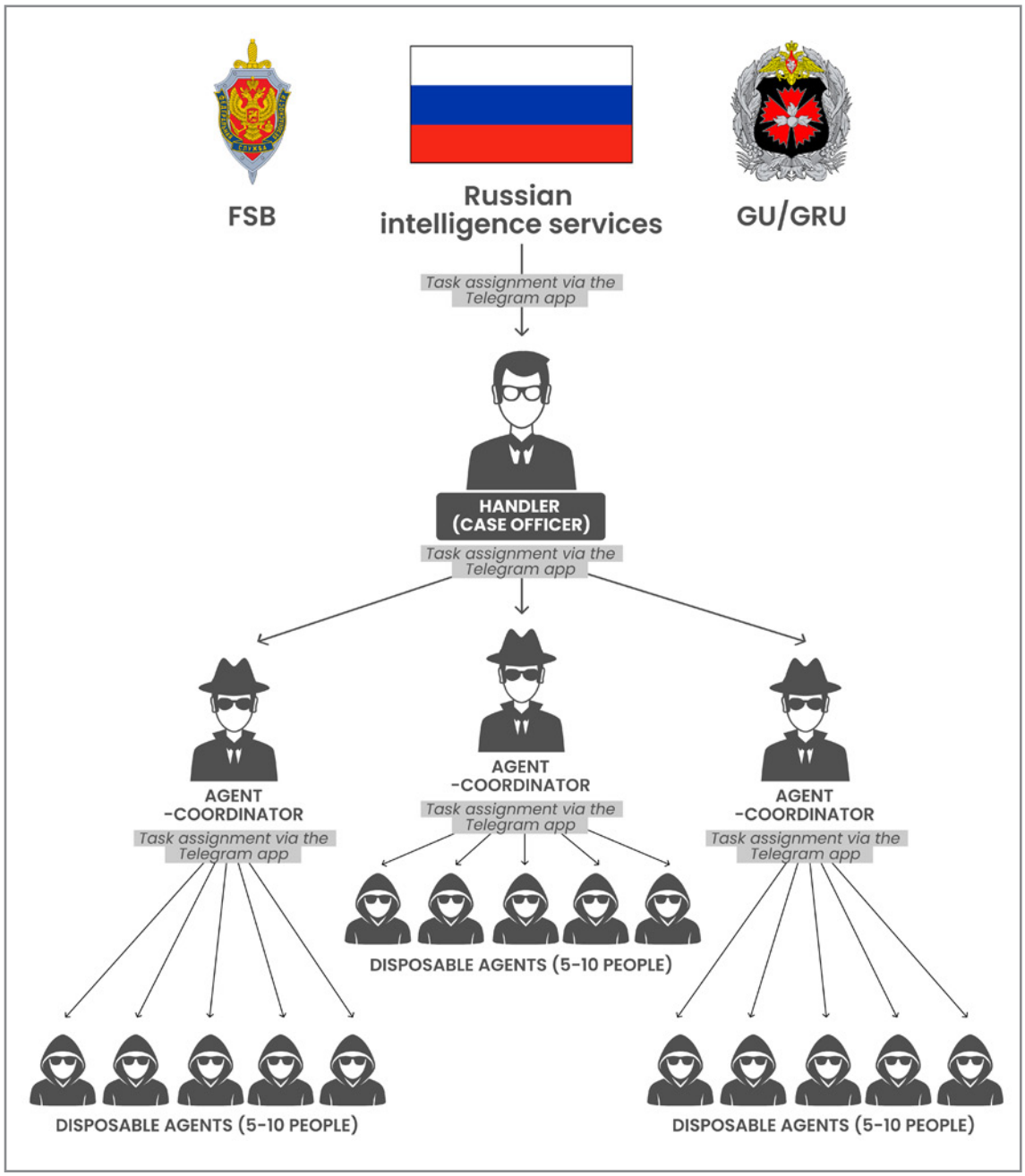
[32] D. Hajdu (ed.), *op. cit*., p. 22.

[33] *Ibidem*, p. 28.

dubny, Alexander Malkovich, Yevgeny "TopaZ" Rasskazov, Russkaya Vesna, Dva Majora) and groups with job offers (e.g. Rabota Polsha, Warsaw Revelations, Bomba Poland Media).[34] Once recruited, approximately 90% of individuals operate in hierarchical groups led by a coordinator who expands the network through direct contact (44%), and the connections of existing (13%).[35]

Diagram 1

Russian intelligence services



[34] Д. Беловодьев, "'Ваше сообщение отправлено в ГРУ'. Как военная разведка совместно с неонацистом "Топазом" создает телеграм-ботов для вербовки диверсантов," *Настоящее время*, 25 September 2025, www.currenttime.tv.

[35] D. Hajdu (ed.), *op. cit.*, pp. 28-29.

According to statements by captured and detained agents, their primary motivation for cooperating with Russian intelligence was financial gain (around 96% of cases), only occasionally accompanied by ideological motives (around 15% of cases).[36] Notably, recruits are often unaware that they are cooperating with a foreign intelligence service (58% of cases),[37] a result driven by the covert recruitment campaigns used by the Russian secret services during the first two years of sabotage operations. Initially, agents were used to carry out simple tasks, such as distributing propaganda leaflets or painting graffiti. By committing minor offences, they demonstrated their willingness to break the law in exchange for attractive financial rewards, paid primarily in cryptocurrencies. They were then entrusted with more serious tasks, such as purchasing surveillance equipment or installing it near railway lines, military units, seaports and other critical infrastructure facilities, and finally escalating to arson and other acts of sabotage, for which they received remuneration of around €10,000 per operation. This mechanism allows recruiters to gradually draw agents into cooperation with Russian intelligence, often without them fully understanding the gravity of their involvement until already compromised. This shared criminal history deters the agents from coming forward or cooperating with law enforcement, and the financial rewards received for previous tasks can serve as a basis for blackmail. However, journalistic investigations indicated that by 2025, the modus operandi of Russian recruiters had changed and is now far more direct. They primarily seek individuals with access to critical infrastructure, willing to undertake tasks such as starting fires or planting explosives.[38] However, after completing the task, the perpetrators often do not receive the promised payment and are abandoned by their handlers, who disappear and cut off all contact.[39]

Russia's recruitment base consists of criminal circles (26% of cases),[40] martial arts clubs, football fans, volunteers fighting on Russia's side against Ukraine, and right-wing radicals. The Lithuanian authorities have also noted an increased number of recruitment attempts targeting teenagers.[41] Citizens of the Baltic states travelling to Russia and Belarus for private purposes (such as family visits and tourism) have also been targets of (coercive) recruitment.[42] According to the Latvian State Security Service (VDD), the typical agent-saboteur is a young person with a criminal record who is facing finan-

[36] J. Lanchès, K. Rękawek, *op. cit.*

[37] D. Hajdu (ed.), *op. cit.*, pp. 23-24.

[38] Based on interviews with investigative journalists from the Baltic states.

[39] "Apdraudējuma novērtējums un 2025. gada darbības pārskats," Militārās izlūkošanas un drošības dienests, saīsināti (MIDD), pp. 19-21, www.midd.gov.lv.

[40] J. Lanchès, K. Rękawek, *op. cit.*, for more see: M. Galeotti, "Gangsters at War: Russia's use of organized crime as an instrument of statecraft," Global Initiative Against Transnational Organized Crime, November 2024, https://globalinitiative.net.

[41] „Граждане третьих стран должны будут сообщать о цели визита в Латвию, решила комиссия Сейма," *Delfi*, 23 March 2025, www.delfi.lt.

[42] Compare: "National Threat Assessment 2026," Defence Intelligence and Security Service / State Security Department of the Republic of Lithuania (VSD), Vilnius 2026, pp. 27–28, www.kam.lt; "Apdraudējuma...," *op. cit.*, pp. 24–25.

cial difficulties. Of low socio-economic status, these recruits lack both steady income and formal education, and possessing low moral standards, they are prone to abuse of alcohol, drugs or psychotropic substances.[43] In most cases, those recruited are men (93%) aged between 16 and 59 (average 30 years old) from former Soviet states (mainly Ukraine, Belarus, Russia and Moldova) living within the EU and able to move freely within the Schengen Area, which gives their activities a cross-border dimension. This enables the same individuals to carry out operations in multiple jurisdictions, as exemplified by the linked attacks on IKEA stores in Vilnius[44] and Riga (foiled), as well as an OBI store and a shopping centre at 44 Marywilska Street in Warsaw.[45] Thanks to international cooperation between law enforcement and investigative agencies, five individuals belonging to this Russian intelligence-directed group have been arrested. Two individuals are still being sought under European Arrest Warrants and national wanted notices.

A similar pattern was apparent in the case of a Colombian national who, after setting fire to a building materials yard in Radom (Poland), started a fire at a bus depot in Prague, having also planned an attack on a shopping centre. He was arrested in the Czech Republic and sentenced to eight years' imprisonment, having been identified as part of a wider Latin American sabotage and reconnaissance group utilised by Russian intelligence. The Lithuanian authorities dismantled this network, which had been linked to two arson attempts at the premises of a military equipment manufacturer that supplies Ukraine. Among the network were a Spanish national, a dual citizen of Spain and Colombia, a Russian and a Belarusian who had travelled to Lithuania from Spain, as well as a Cuban national and a Colombian intermediary living in Spain.[46]

Russian sabotage activities also include widespread vandalism, such as defacing monuments and cultural sites and the promotion of disinformation slogans. These acts aim to deepen social polarisation and fabricate evidence of "Russophobia," which is then systematically leveraged to justify the Kremlin's narrative concerning the "Nazification" of the Baltic states. At the end of 2023, the Estonian security services (KAPO) arrested 13 people for desecrating several national memorial sites (particularly those related to the Second World War), whilst in Latvia, two men attempted to set fire to the Museum of the Occupation.[47] In Poland, acts of vandalism have primarily been directed at sites relating to the difficult history of Polish-Ukrainian relations. In 2025, a monument in Domostawa commemorating the Volhynia massacre was vandalised, as was the UPA monument and grave in Monasterz. These acts were carried out by

[43] "Annual Report for 2024," Latvian State Security Service (VDD), 2025, www.vdd.gov.lv.

[44] L. Peter, "Lithuania accuses Russia over Ikea store fire in Vilnius," BBC, www.bbc.com.

[45] E. Matysiak, "Nie tylko Marywilska i OBI płonęły na rozkaz Kremla. Śledczy ujawniają plan ataku na kolejny sklep," Biznes Info, 4 April 2026, www.biznesinfo.pl.

[46] "Baudžiamoji byla dėl teroro išpuolių Šiauliuose perduota teismui," Lietuvos Respublikos Prokuratura, 16 January 2026, www.prokuraturos.lt.

[47] H. Praks, "Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage," *Hybrid CoE Working Paper*, No. 32, May 2024, www.hybridcoe.fi.

a 17-year-old Ukrainian citizen on the orders of Russian intelligence to fuel ethnic tensions in Poland.

Since 2024, the diversionary and sabotage operations instigated by the Russian secret services have taken on an increasingly offensive character, including political violence, in the form of targeted beatings and attempted murders. They aimed to force a change of stance on the war in Ukraine amongst politicians, investigative journalists, opposition figures and the defence industry. In Estonia, cars belonging to Interior Minister Lauri Läänemets and Andriy Shumakov, editor-in-chief of the Delfi news portal, were damaged. In Lithuania, Leonid Volkov, a former close associate of Alexei Navalny, was brutally beaten in an attack organised by Russian lawyer Anatoly Blinov and Belarusian businessman Viktor Pavelka, the representative of Russian-Israeli billionaire Leonid Nevzlin.[48] However, the ultimate initiators were most likely the Russian or Belarusian secret services. In Poland, Russia planned to carry out an assassination attempt on Ukrainian President Volodymyr Zelensky at Rzeszów-Jasionka Airport, which he uses for most of his foreign trips.[49] In Germany, Rheinmetall CEO Armin Papperger was targeted for assassination due to his role leading Europe's largest ammunition manufacturer. This plot, aimed at disrupting the supply of artillery shells and military vehicles to Ukraine, was uncovered and thwarted by American and German intelligence agencies.[50]

In October 2025, the Latvian State Security Service (VDD) apprehended four individuals responsible for sabotage targeting the state's defence and critical infrastructure. This cell's activities had escalated from a 2024 arson attempt on a Ukrainian-registered lorry at a sensitive site to a successful strike against a private defence contractor in late 2025. The Latvian authorities found evidence that the group had carried out detailed reconnaissance and surveillance, drawing up maps of entrances, exits and security protocols. The suspects had also photographed and filmed other sensitive sites, passing this information on to Russian intelligence services, presumably to facilitate future attacks.[51]

In addition to the material damage instigated on the orders of Russian intelligence (for example, around 1,400 shops and service outlets were destroyed by the fire at the shopping centre at 44 Marywilska Street in Warsaw; see appendix), some of the Russian-planned attacks could have had serious consequences on the lives and health of the population. In January 2024, the Internal Security Agency detained a Ukrainian national who, on behalf of Russian intelligence, was preparing an attack on a paint

[48] "Polish prosecutors say attack on Navalny ally Leonid Volkov was carried out at the behest of exiled billionaire Leonid Nevzlin," *The Insider*, 14 July 2025, www.theins.press.

[49] I. Vock, "Man arrested in Poland over alleged Russia plot to kill Zelensky," BBC News, 18 April 2024, www.bbc.com.

[50] K.B. Lillis, N. Bertrand, F. Pleitgen, "US and Germany foiled Russian plot to assassinate CEO of arms manufacturer sending weapons to Ukraine," CNN Politics, 11 July 2024, www.edition.cnn.com.

[51] "Annual Report for 2025," Latvian State Security Service (VDD), 2026, p. 8, www.vdd.gov.lv.

factory belonging to the American company PPG Industries. The target, located near strategic infrastructure (fuel depots) and the River Oder, could have led to serious environmental contamination. Serhiy S. (51) was promised $4,000 for carrying out the assignment. Investigations around this case not only thwarted the attack, but also uncovered another organised criminal group engaged in sabotage activities (setting fire to warehouses, factories and restaurants) on behalf of Russian intelligence.

In April 2024, two individuals of Russian origin were arrested in Germany and charged with acting on behalf of Russian intelligence with the intention of carrying out attacks on military installations, arms factories, industrial facilities and transport infrastructure used to supply Ukraine. These actions, taking the form of arson and the detonation of explosives, included targeting the US military base in Grafenwöhr, Bavaria, where Ukrainian soldiers were being trained to operate M1 Abrams tanks.[52] As a result, the alert level at US military bases in Europe was raised to FPCON CHARLIE.[53] This status is triggered when an incident occurs or intelligence is received indicating that attacks on facilities and personnel are likely.

In 2024, several acts of sabotage targeting warships also took place in Germany. A minesweeper was damaged at the shipyard in Wilhelmshaven, and, in Hamburg, approximately 30 kg of metal filings were poured into the engine of the newly built corvette "Emden." Only the timely detection of this interference prevented the potential immobilisation of the vessel and a significant delay in its handover to the German Navy. Romanian and Greek nationals were arrested in connection with this case, but to date, the German public prosecutor's office has been unable to conclusively prove their links to Russian intelligence. In 2025, in Erfurt, central Germany, six Rheinmetall MAN military vehicles, located on the premises of a vehicle repair workshop and identified by Bundeswehr and NATO markings, were set alight.[54]

Since 2024, the Russian security services have specifically stepped up their efforts to establish international smuggling routes for materials used in subversive and sabotage activities (including explosives, parts for drones used to reconnoitre critical infrastructure, and SIM cards). In July 2024, Polish authorities in Katowice arrested a couple identified as Russian opposition activists on charges of collaborating with the FSB to traffic explosives. In October, the Internal Security Agency arrested four individuals involved in an operation to identify air-smuggling routes for explosives to the US and Canada. As part of a test phase of the operation, a flammable substance was placed in packages containing sex toys that were due to be posted from Warsaw; however,

[52] N. Bertrand, "Intelligence on Russian sabotage threat prompted increase in security at US military bases in Europe," CNN Politics, 9 July 2024, https://edition.cnn.com.

[53] CHARLIE is the third level on a four-tier alert scale, indicating a high risk of terrorist attacks. This status entails stringent security measures, including: heightened security checks at base entrances; an increased security presence; restrictions on access and movement within military facilities; and increased surveillance and patrols on the periphery.

[54] "BKA zählt mehr als 320 Sabotage-Verdachtsfälle," *Tagesschau*, 5 February 2026, www.tagesschau.de.

the plot was exposed after parcels prematurely ignited at DHL hubs in Leipzig, Germany, and Birmingham, UK,[55] and a third device detonated in Warsaw before dispatch.

Lithuania was the primary dispatch point for a GU-directed sabotage group smuggling flammable and explosive materials, drone parts, and SIM cards. The operatives transported the materials in maize tins, which were then concealed in dead-drop locations such as cemeteries.[56] Investigation of the case resulted in the arrest of 15 people (including citizens of Russia, Lithuania, Latvia, Estonia and Ukraine) and the seizure of 6 kg of TNT, intended for use in further attacks. The operation was supervised by 44-year-old Russian national Alexander Bezrukavyj, who was apprehended by the Security and Investigation Agency of Bosnia and Herzegovina (SIPA) and then deported to Poland. His capture was linked to his role in organising paramilitary training for Moldovan sabotage groups aimed at destabilising the 2024 elections.

In October 2025, a shipment of explosives was successfully intercepted thanks to cooperation between the Internal Security Agency and the Romanian Security Service (SRI). The sabotage plot involved sending flammable materials through the Ukrainian courier company Nova Post's EU-Ukraine transport network. The devices were intended to ignite at and destroy the courier company's headquarters in the centre of Bucharest.[57]

In August 2024, Germany suffered several attacks on military and transport infrastructure, such as the sabotage of the water supply network near a German military base not far from Cologne Airport. In March 2025, the Swedish police launched an investigation into suspected sabotage after damage to power cables connected to a pumping system on the island of Gotland. In July 2025, a Ukrainian national, Ihor H. (aged 36), was arrested in Poland, disrupting a plot targeting the water supply system in Sopot. The planned attack was intended to paralyse water distribution in the city. These incidents pointed to the potential for further escalation of activities initiated by Russian intelligence, targeting essential services such as water and electricity supplies.

In 2025, the German Federal Criminal Police Office recorded 321 incidents of sabotage, mainly targeting the energy sector, railway lines and military facilities, as well as 1,289 reports of unauthorised drone flights over strategic infrastructure sites.[58]

Russia's readiness to escalate its offensive operations is evidenced by the 15 and 17 November 2025 terrorist attacks on railway lines in Poland. Two serious incidents occurred on the vitally important Warsaw–Lublin railway line. These sabotage operations were intended to derail trains on a primary route for passenger, freight and military trans-

[55] W. Wallis, J.P. Rathbone, O. Telling, "UK counterterror police probe whether Russia planted parcel bomb," *Financial Times*, 15 October 2024, www.ft.com.

[56] For more, see M. Weiss, K. Kopaleishvili, "Revealed: How Russia's GRU Plotted Europe's Parcel Explosions," *VSquare*, 17 September 2025, www.vsquare.org.

[57] J. Lanchès, K. Rękawek, *op. cit*.

[58] "BKA zählt mehr als 320 Sabotage-Verdachtsfälle," *Tagesschau*, 5 February 2026, www.tagesschau.de.

port. In the village of Mika, C4 explosives were attached to the tracks and triggered to target a freight train. A catastrophic derailment was only prevented by the failure of one of the explosive charges. Near the village of Gołąb, the overhead contact line was damaged and two specially constructed metal components were placed on the tracks to cause a derailment. These devices were ultimately detected and neutralised before the train arrived. Both incidents demonstrate the risk of a major land transport disaster caused by sabotage and terrorist activities carried out at Russia's orders. The perpetrators have been identified as Ukrainian citizens Yevhen Ivanov and Oleksandr Kononov, who used forged documents to enter Poland before fleeing to Belarus after the attacks. Ivanov had previously been sentenced in absentia in Ukraine to 15 years' imprisonment in May 2024 for organising sabotage against a drone production facility in Lviv.

The railway sabotage and terrorist attacks were accompanied by a disinformation campaign framing the incidents as false-flag operations orchestrated by Ukraine and Poland. In late September 2025, the Russian Foreign Intelligence Service (SVR) had already spread this narrative in a press release claiming that Ukrainian and Polish intelligence services planned to stage attacks using Russian and Belarusian volunteers from the Ukrainian side. The goal, according to SVR was to pin the blame on Russia and Belarus, and thus trigger NATO's entry into the war. Analysis of 14,000 comments by Res Futura Data House[59] revealed that 42% assigned guilt to Ukraine, while 19% targeted the Polish government. These figures do not represent genuine Polish public opinion; rather, they illustrate the reach of Russian disinformation and propaganda tools, such as troll farms and bots, in distorting the digital infosphere.

In response to the railway attacks in Poland, Operation "Horizon" was launched, deploying 10,000 soldiers to monitor the railway infrastructure. In previous incidents, radio signals had been used to disrupt train services in Poland, as well as the uncoupling of individual freight wagons and the forced stopping of trains carrying hazardous materials across Poland and Germany.

In September 2025, major disruptions hit Germany's rail network as the Hamburg–Berlin and Cologne–Düsseldorf lines were targeted by sabotage. An explosive device was detonated in a tunnel on the Hamburg route, while on the Cologne–Düsseldorf line, electrical cables were deliberately severed. In January 2026, a freight train loaded with chlorine, formaldehyde, and nitrobenzene derailed in Essen. Metal clamps had been attached to the tracks, similar to those used in the earlier Polish attack. The incident occurred on a day when a shipment of ammunition and equipment for US forces in Europe was scheduled to use the same route. The Swedish authorities are also investigating two derailment incidents on the Malmbanan line in December 2023 and February 2024, as well as repeated damage to railway and underground cables in the western part of the country since early 2025.

[59] Res Futura brings together experts specialising in the analysis of the information space and issues relating to national security Source: https://resfutura.pl/res-futura-o-nas.

Russian acts of sabotage and subversion in CBSS states

Source: Compiled by the author.

Air domain

In the air domain, the most significant hybrid activities conducted by Russia against members of the CBSS include GNSS signal jamming and incidents involving the violation of their airspace by Russian and Belarusian aircraft, fighter jets, and unmanned systems, forcing them to scramble fighter jets on duty. GNSS signal jamming has continued uninterrupted since Russia launched its full-scale aggression against Ukraine, and intensified significantly in the second half of 2024, which corresponds to the Russian services undertaking increasingly offensive operations in the land domain. Airspace violations by aircraft and helicopters, however, have been sporadic, although since the second half of 2025 there has been an increase in activities involving the use of unmanned systems and weather and smuggling balloons.

GNSS signal jamming

Since the start of Russia's full-scale aggression against Ukraine, GNSS signal disruptions have been observed daily. Between 2022 and 2024, these were mainly concentrated in the Eastern Baltic states, Finland, Estonia (particularly the Gulf of Finland), Latvia, Lithuania and Poland. Jamming was also frequently identified in northern Norway. From the second half of 2024, the jamming campaign broadened in scope, extending to Sweden, Denmark and, periodically, Germany. According to gpsjam.org, which has tracked GNSS signal interference since February 2022, the period between 1 March 2022 and 31 March 2026 saw significant interference across several nations. The total number of days with recorded issues—ranging from minor interference to large-scale disruptions—was 1,028 for Poland, 997 for Lithuania, 1,055 for Latvia, 1,041 for Estonia, 1,127 for Finland, 625 for Sweden, 889 for Norway, 478 for Denmark, and 211 for Germany.

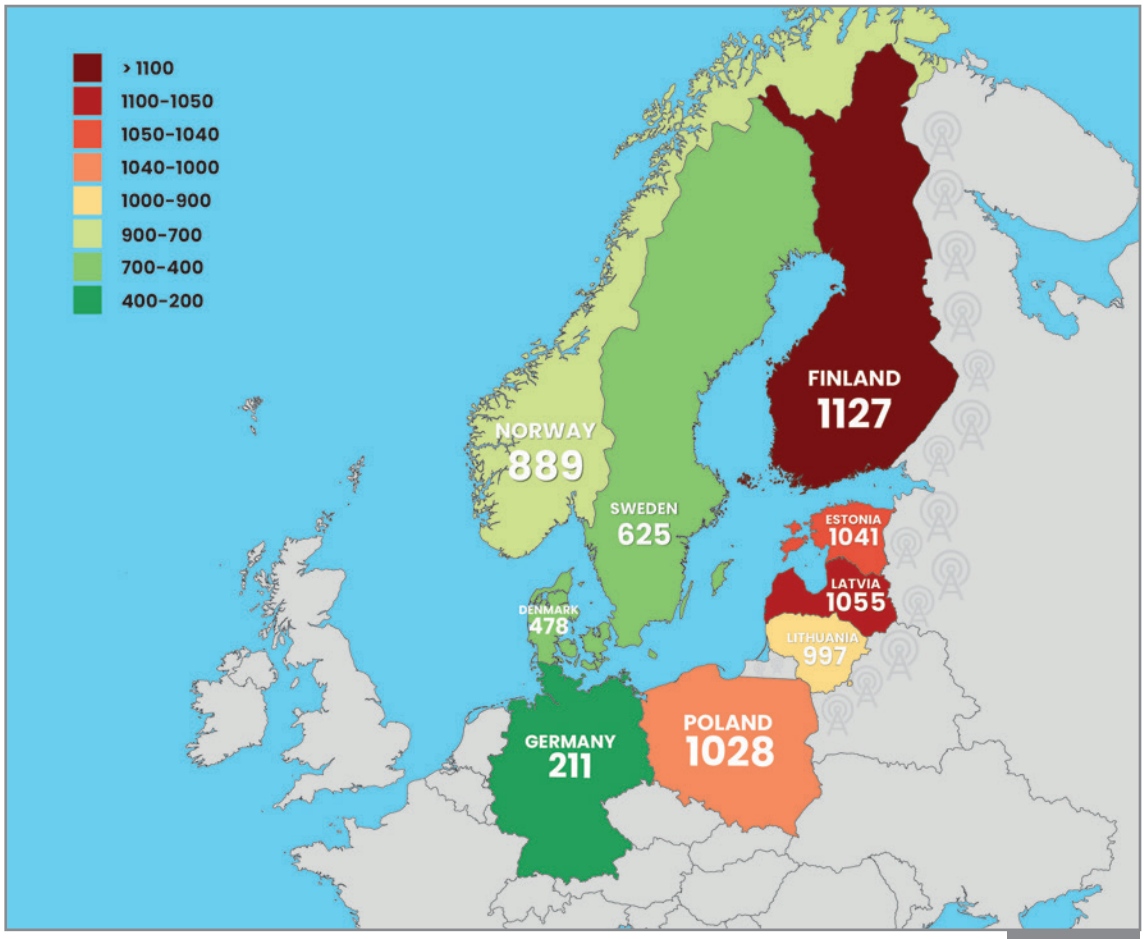
In 2022, GNSS signal disruptions occurred in waves, often affecting Poland, Lithuania, Latvia, Estonia, Finland and Norway, with incidents extending from individual target countries to 6–7 simultaneous locations. Constant GNSS signal disruptions occurred in the Gulf of Finland, and by 2023, disruptions in the Baltic states and Norway had become a daily occurrence. Increasingly, all Baltic states were affected simultaneously. By the end of 2023, there were almost daily disruptions across the entire region, a trend that continued into 2024. On many days, they occurred in unison in all CBSS countries and across vast areas of the Baltic Sea. These phenomena intensified in 2025, now affecting significant areas of the Baltic Sea region, and continued in the first quarter of 2026, when disruptions affected Poland, the Baltic states, Finland, Norway, Sweden, Denmark, Germany, and the Baltic Sea.

The sources of GNSS signal interference was mainly traced to the Kaliningrad and Leningrad regions. These activities compromised the safety of air traffic and civilian maritime navigation across the affected areas. There were constant reports by Polish vessels of GPS signal interference, as well as distorted readings in the AIS[60] system, posing a threat to the safety of maritime navigation. Since February 2022, nearly 100 such incidents have been recorded; however, the true number is difficult to determine, partly because, upon encountering GPS issues, many vessels switch immediately to navigating with analogue maps, rather than officially reporting an incident. After this threat was identified, the Finnish Transport and Communications Agency (Traficom) urged seafarers to reduce their reliance on satellite systems and revert to traditional navigation methods.[61]

[60] The AIS system includes data such as a vessel's position, course and speed, broadcast to other system users with the aim, amongst other things, of preventing collisions at sea.

[61] "Finland and Estonia warn vessels in the Gulf of Finland of an increase in GNSS disruptions," Transport and Communications Agency, https://www.traficom.fi.

Number of days with GNSS signal disruptions between 1 March 2022 and 31 March 2026



Source: Compiled by the author based on data from gpsjam.org.

Some of the most significant incidents involving GNSS signal interference have occurred in Norway. In June 2025, GPS signal tampering was detected in the eastern Finnmark region at altitudes of up to 150 metres above ground level, and analysis pointed to the source being on the Russian side of the border. In September 2025, a Widerøe aircraft was forced to abort landing in Vardø due to the loss of GPS[62] signal. The Norwegian Communications Authority (Nkom) acknowledged significant interference in the northern regions and established a local office in Tromsø to respond more quickly to jamming incidents. The Norwegian authorities have acknowledged that interference is a daily problem in several areas and recommend using a map and compass as a precaution.

In early 2025, GPS signal disruptions affected the Swedish islands of Gotland and Öland. Sweden's Minister of Defence, Pål Jonson, speaking about the issue, assured

[62] "GPS jamming prevented plane from landing," *Newsinenglish.no*, 16 September 2025, https://www.newsinenglish.no.

the public that the government was closely monitoring the situation and maintaining close dialogue with both Finland and the Baltic states, as well as within NATO and the EU. Jonson also stated that the Swedish Armed Forces (Försvarsmakten) were considering measures to strengthen resilience and robustness and reduce vulnerability to GNSS satellite navigation interference. Sweden also identified Kaliningrad Oblast as the primary source of interference.[63] In July 2025, the Swedish Maritime Administration (Sjöfartsverket) issued an urgent warning following a significant increase in interference affecting GPS and the AIS system in the Baltic Sea, including areas off the west coast of Sweden.[64] The Maritime Administration advised seafarers to remain vigilant and to use alternative navigation methods, including traditional charts and visual bearings, to mitigate the risks associated with unreliable GPS and AIS data.

In response to GNSS signal interference, Finland, together with thirteen other European countries, including the Baltic states and Germany,[65] officially informed the International Maritime Organisation (IMO) of disruptions to the GNSS system and tampering with the maritime AIS system, recognising these as safety threats. Finland, together with Estonia, has also issued navigational warnings concerning the Gulf of Finland and updated notices to mariners, advising vessels to use alternative positioning methods due to the GNSS system malfunctions.[66]

In light of the threat posed by interference, Lithuania's Oro Navigacija (an air navigation service provider) and the armed forces have introduced additional guidelines for pilots and drone operators, requiring them to fall back to traditional navigation methods (radar, paper maps, and ground-based radio navigation) in the event of a loss of GPS signal. Meanwhile, the Latvian Electronic Communications Authority has begun cooperating with foreign partners to enhance its capabilities for detecting and analysing interference in GNSS systems.

In 2024, Poland announced that the National Research Institute and the Main Office of Geodesy and Cartography had launched a project entitled "Real-Time GNSS Signal Monitoring System in Poland (RTGMS)," funded by the European Space Agency. The RTGMS system is designed to detect GNSS signal disruptions, such as access issues or errors in satellite navigation.[67] The system features integrated alerts and a user-accessible website to display measurement results.

[63] A. Walsh, "Sweden accuses Russia of GPS jamming over Baltic Sea," BBC, 4 September 2025, www.bbc.com/news/articles/clyx3ly54veo.

[64] "Warning of GPS interference in the Baltic Sea," Emergency information from Swedish authorities, 20 June 2025, www.krisinformation.se.

[65] "Coastal States of the Baltic Sea and the North Sea: Safety risks in navigation increased by GNSS interference," Ministry of Transport and Communications, Finnish Government, 26 January 2026, https://valtioneuvosto.fi.

[66] "A report recently published by the Finnish Geospatial Research Institute recommends new measures to protect against interference," *Space Finland*, 18 February 2026, https://spacefinland.fi.

[67] "W Polsce powstanie system monitorowania sygnałów GNSS," Ministerstwo Cyfryzacji, 13 November 2024, www.gov.pl/web/cyfryzacja.

Furthermore, in 2025, the European Union Aviation Safety Agency (EASA) and the International Air Transport Association (IATA) published a comprehensive plan aimed at mitigating the risks arising from disruptions to the global navigation satellite system.[68] This plan includes, amongst other things, agreeing standard radio messages for reporting GNSS disruptions and standardised message coding, ensuring the rapid and reliable restoration of GPS equipment following signal loss or disruption, maintaining a backup GNSS system, better utilisation of military air traffic management capabilities, improved civil-military coordination, and the refinement of contingency and backup planning procedures in airspace, so that aircraft can navigate safely even during interference.

Airspace violations

Since the start of its full-scale aggression against Ukraine, Russia has triggered a series of incidents through airspace violations in CBSS member states. Other incidents in the region include flights near borders, which forced CBSS member states to respond by scrambling fighter jets from standby. Numerous instances have also been recorded of unmanned aerial vehicles being used by Russia and Belarus to violate the borders of the CBSS states, compelling the targeted countries to implement countermeasures.

In the case of Poland, among all the identified violations, particular attention should be paid to incidents involving aircraft and helicopters, unmanned aerial systems, aerostats and weapons. However, only the 25 April 2025 incident, involving a Russian Ka-27 helicopter which breached the border three times without authorisation, has been classified as intentional; the most prominent incidents in Poland were those involving the fall of munitions onto the country's territory on 15 November 2022 and 16 December 2022. In the South and South-East Baltic regions, there were also provocations in the form of risky manoeuvres carried out by Russian pilots in the vicinity of Polish vessels and critical maritime infrastructure, aimed primarily at emphasising their presence and demonstrating force.

The vast majority of violations of Polish airspace involve unmanned aerial systems, the overwhelming majority of which are civilian smuggling drones. However, Russia's use of unmanned aerial systems against Poland on the night of 9–10 September 2025 is considered to be the most dangerous incident in Polish airspace. This event was again accompanied by a massive disinformation campaign,[69] which claimed that these were Ukrainian drones. In response to the incident, Poland convened meetings of the North Atlantic Council in accordance with Article 4 of the North Atlantic Treaty, and this

[68] "EASA and IATA outline comprehensive plan to mitigate GNSS interference risks," European Union Aviation Safety Agency, 18 June 2025, www.easa.europa.eu.

[69] F. Bryjka, A. Wójtowicz, "Russia Launches Drone and Disinformation Attack on Poland," *PISM Bulletin*, No. 99 (2600), 19 September 2025, www.pism.pl.

incident prompted NATO's decision to launch Operation Eastern Sentry on 12 September 2025.

Since 2025, there have also been sporadic mass incursions from Belarus by smuggling balloons carrying cigarettes; whilst not posing a direct threat to national security, the Joint Forces Operational Command has emphasised that they are also being used to test Poland's air defence system. On the night of 24–25 December 2025 and on the night of 16–17 January 2026, several dozen weather balloons were flown from Belarus into Polish territory, used to smuggle tobacco products.[70] The major scale of the smuggling and the commitment of financial resources clearly indicate that these were primarily diversionary actions, designed to disguise the perpetrators' real objective of paralysing air traffic and Polish airports. In response to these threats, the Polish Armed Forces have undertaken a series of measures aimed at better calibrating air defence systems for the Polish border, and have deployed electronic warfare systems to counter the threat.

Table 3

Identified violations of Polish airspace between 2022 and March 2026

YEAR	VIOLATIONS OF POLISH AIRSPACE	MANNED AIRCRAFT	DRONES	BALLOONS	WEAPONS	UNIDENTIFIED AERIAL OBJECTS
2022	477	0	471	0	2	4
2023	252	1	223	2	1	24
2024	290	2	279	2	1	6
2025	392	5	292	64	0	31
2026 (since March)	308	0	32	274	0	2

Source: Armed Forces Joint Operational Command.

Lithuania has also been frequently targeted, but much of the increase in violations of Lithuanian airspace and acts of sabotage was seen in 2025. Previously, there had been sporadic smuggling by balloons carrying cigarettes, but the massive and systematic increase from October 2025 onwards was deemed by the Lithuanian authorities to be a serious threat to civil aviation and security. At the same time, in December 2025, the Lithuanian authorities reclassified the balloons from hybrid attacks to terrorist acts, seeing them not only as a violation of borders but also a threat to civil aviation and the lives of aircraft passengers. In response to a series of such incidents, the Lithuanian government declared a state of emergency at the border with Belarus and at

[70] A.M. Dyner, "Białoruś coraz częściej wykorzystuje balony przeciw Polsce," *Depesza PISM*, 6 February 2026, www.pism.pl.

Vilnius Airport.[71] In 2025, there were further incidents involving violations of Lithuanian airspace. On 23 October, two Russian military aircraft from Kaliningrad Oblast briefly violated Lithuanian airspace near Kibart. The incident saw a Su-30 fighter jet and an Il-78 tanker aircraft, likely conducting in-flight refuelling exercises, fly approximately 700 metres into Lithuanian airspace, spending around 18 seconds there, causing two Spanish fighter jets from NATO's Baltic Air Policing mission to be scrambled in response. The Russian Ministry of Defence claimed that the Su-30 fighter jets were conducting a "training flight" over Kaliningrad Oblast, and had not violated any country's borders.[72]

Between 2022 and 2026, Latvia recorded the lowest number of airspace violations in the region. The country's most serious incident occurred in September 2024, when a Russian Shahed-type drone crashed on Latvian territory.[73]

A serious violation of Estonian airspace on 19 September 2025 led the country to convene a meeting of the North Atlantic Council in accordance with Article 4 of the North Atlantic Treaty.[74] The Supreme Allied Commander Europe (SACEUR) reported that the incident, in which three armed Russian MiG-31 aircraft violated Estonian airspace, lasted for over ten minutes.

In Finland, there have been occasional sightings of unidentified drones. On 27 September 2025, a drone was spotted flying over the Valajaskoski power station in Rovaniemi, despite the fact that the area had been designated a no-fly zone for drones since August. A bystander reported the incident to the police, but the drone operator was not captured on the power station's CCTV and left the area before officers arrived. Kemijoki Oy, the company that manages the power station, confirmed the incident and stated that it receives occasional, infrequent reports of drones. At the turn of March and April 2026, Ukrainian drone crashes were recorded in Finland, Lithuania, Latvia, and Estonia. These drones were heading for Russian ports on the Baltic Sea, and their flight path was interrupted by GNSS signal interference originating from the Russian Federation.[75]

Between 2022 and 2026, there were also violations of Swedish airspace. In March 2022, shortly after the invasion of Ukraine began, four Russian combat aircraft—two Su-27s and two Su-24s—violated Swedish airspace near Gotland. In March 2022, a total of four Russian Su-24 and Su-27 aircraft violated Swedish airspace over the Baltic Sea east

[71] AM. Dyner, "Lithuania Declares State of Emergency Due to Belarus' Actions," *PISM Spotlight*, No. 83/2025, 10 December 2025, www.pism.pl.

[72] A. Sytas, NATO member Lithuania says two Russian jets briefly entered its airspace, Reuters, 23 October 2025, www.reuters.com.

[73] T. Nedwick, "Russian Shahed Kamikaze Drone Crashes In Latvia," TWZ, 9 September 2024, www.twz.com.

[74] A. Sytas, G. Slattery, "Russian jets enter Estonia's airspace in latest test for NATO," Reuters, 20 September 2025, https://www.reuters.com.

[75] F. Bryjka, "Ukraińskie uderzenia na rosyjskie cele nad Bałtykiem," *Depesza PISM*, 27 February 2026, www.pism.pl.

of Gotland.[76] In April 2022, a Russian An-30 aircraft violated Swedish airspace south of Blekinge. In June 2024, a Russian Su-24 bomber violated Swedish airspace east of Gotland. In October 2024, Swedish fighter jets were scrambled at NATO's request to identify an aircraft that had been detected above the Baltic Sea, which turned out to be a Russian Il-20 military electronic reconnaissance aircraft. In January 2025, a Russian aircraft was detected over the Swedish region of Skåne. The Swedish Armed Forces confirmed the illegal overflight of international territorial waters, though they did not specify the time of the sighting or the exact flight path. The aircraft was flying without a transponder, which meant it was not visible to civilian air traffic. In April 2025, Swedish fighter jets intercepted a Russian aircraft over the Baltic Sea, and in June 2025, Sweden scrambled two fighter jets over the Skåne region after detecting two Russian Su-30 fighter jets near its airspace.[77]

Beyond these clearly attributable incidents, there was the sighting of four unknown drones of various sizes on the night of 8–9 September 2024, which led to the immediate suspension of air traffic at Stockholm Arlanda Airport for several hours. The incursions recurred on subsequent nights. To date, the type of drones involved and who was behind the incident remain unknown, although the police believe it to be a deliberate act intended to threaten the airport. An investigation has been launched into suspected sabotage and a breach of security at a protected facility. Arlanda Airport, like all other Swedish airports managed by Swedavia, cannot currently detect or repel drone attacks.

Norwegian authorities have confirmed three incidents of Russian aircraft violating their airspace in the third quarter of 2025: on 25 April, a Su-24 fighter aircraft violated airspace near Vardø for 4 minutes; on 24 July a Russian L-410 Turbolet aircraft entered Norwegian airspace in the Finnmark region, remaining over an uninhabited area for approximately 3 minutes; and on 18 August a Su-33 fighter briefly (for around 1 minute) entered Norwegian airspace over the Barents Sea (north-east of Vardø). The Norwegian authorities demanded an explanation from Russia and emphasised that, regardless of whether these were navigational errors or deliberate actions, each incident posed a threat to security in the northern region.[78]

In 2025, Norway also experienced drone incidents. On 22–23 September, drones were reported near the runway at Oslo Airport (Gardermoen), leading to a temporary airspace closure and some flights being diverted. On 30 September at Brønnøysund Airport, the police detected an unidentified drone, but could not locate the operator. Similar sightings were also reported over the Sleipner offshore platform in the North Sea.

[76] "Swedish defence minister calls Russian violation of airspace 'unacceptable'," Reuters, 2 March 2022, www.reuters.com.

[77] F. Lemieux, "Russia tested NATO's airspace 18 times in 2025 alone—a 200% surge that signals a dangerous shift," *The Conversation*, 19 February 2026, https://theconversation.com.

[78] "Norway says Russia violated its airspace three times in 2025," Reuters, 23 September 2025, www.reuters.com.

Security services have emphasised the lack of clear evidence linking the observed drones to specific state entities; however, this phenomenon is still being treated as a real hybrid risk falling below the threshold of armed conflict.

The occurrence of similar incidents in Denmark during the same period has reinforced suspicions that Russia may be coordinating such activities to target multiple countries. In response to the operation of unidentified drones, including over airports (Copenhagen Kastrup, Aalborg and South Jutland airports) and military bases (Karup) in September 2025,[79] the Danish authorities closed their airspace to private drones from 28 September to 3 October 2025.

Furthermore, Danish F-16 fighter jets were scrambled 81 times in 2024 alone to investigate and monitor aircraft entering the vicinity of Danish airspace.[80] One of Russia's objectives in taking actions is to continuously test Danish air defence capabilities.

In 2025, flights by unidentified drones also became an increasingly serious problem for Germany. According to the President of the Federal Criminal Police Office (BKA), over 1,000 suspicious drone flights were recorded in Germany over the past year – mostly over military facilities, defence sector companies and critical infrastructure.[81]

2025 saw the highest total number to date of airspace violations of the CBSS states (see appendix), which, alongside the increasing number of acts of sabotage and subversion, indicated a hardening of Russia's policy towards the region.

[79] I. Aikman, "Drones seen over Danish military bases in latest air disruption," BBC, 27 September 2025, www.bbc.com.

[80] "F-16 deployed many times in 2024," Danish Defence, 4 February 2025, www.forsvaret.dk.

[81] K. Neubert, "Germany records more than 1,000 suspicious drone sightings this year," Euractiv, 22 December 2025, www.euractiv.com.

Russia's Potential for Escalation

The steady intensification of hostile Russian hybrid activities observed since 2022 indicates that Russia possesses further potential for escalation, which it may deploy depending on the political situation in the region. The Russians are most likely to utilise hybrid operations to temporarily increase the pressure, especially during pre- and post-election periods in the CBSS states, as a means of influencing political processes. The primary goal of such actions will be a continuous, multidimensional undermining of the security of the CBSS states. Russia's future policy, however, will depend to a significant extent on the ability of the targeted states to respond and take retaliatory measures.

The maritime domain

Russian hybrid operations in the Baltic Sea region rely on the readiness of the civilian sector—ships and crews, as well as maritime facilities—to augment the capabilities of the Armed Forces of the Russian Federation, and this premise is laid out in the Maritime Doctrine of the Russian Federation of July 2022.[82] It must therefore be assumed that civilian vessels are, and will continue to be, involved in operational activities, and carrying out designated reconnaissance or sabotage tasks not on an incidental basis, but as part of a systematic approach.

This support also allows the Baltic Fleet to be tasked with activities beyond conducting hybrid operations, an operational freedom made all the more significant given that, as demonstrated by the large-scale "Ocean 2024" exercises,[83] it still has major resources which have not been expended in the war with Ukraine. Russia therefore has the capability both to continue its current pattern of hybrid operations in the Baltic Sea and to undertake more far-reaching actions while remaining below the threshold

[82] "Морская Доктрина Российской Федерации, утверждена Указом Президента Российской Федерации от 31 июля 2022 г. № 512," Министерство иностранных дел Российской Федерации, 31 July 2022, www.kremlin.ru.

[83] The exercises have shown that, although Russia's A2/AD system in the Baltic Sea region has been weakened by the war with Ukraine, it remains fully operational.

of war. If the activities of the "shadow fleet," which supports the financing of Vladimir Putin's war machine, were effectively curtailed, Russia might decide to escalate in the maritime domain in response. One example of this type of escalation occurred in May 2025, when a Russian fighter jet (in violation of NATO airspace) hindered the Estonian services' attempt to detain a "shadow fleet" vessel. Further escalation could therefore entail the systematic escorting of "shadow fleet" vessels by its navy, though this would disrupt the modus operandi of such vessels, which are intended to hide any direct links with the Russian state. Confirmation of Russia's increased maritime activity was shown in April 2026, when Russian warships were tasked with protecting 40 "shadow fleet" vessels in the Gulf of Finland, following the suspension of exports from the ports of Primorsk and Ust-Luga due to Ukrainian shelling. The Commander of the Estonian Navy, Ivo Vark, expressed concerns about escalation should these vessels be detained by Estonia, although the threat of inspections and detentions has so far been one of the few tools available for the CBSS states to curb the activities of the "shadow fleet."[84]

Land domain

Analysis of the evolution of methods employed by Russian intelligence services as part of their diversionary and sabotage campaign since 2022 indicates Russia's readiness to escalate by carrying out kinetic operations, which could ultimately result in fatalities. In the land domain, the most serious incidents involved attempts to derail trains and attacks on infrastructure containing chemical substances. The next stage of escalation could involve attacks using explosives or flammable materials on energy infrastructure (which to date has mainly been targeted by cyberattacks) and telecommunications infrastructure (e.g. since June 2025, the Swedish authorities have been investigating around 30 acts of sabotage targeting telecommunications masts) or water supply systems.

To date, Russia has also not utilised its full potential to conduct large-scale sabotage and subversion operations. Existing sabotage and subversion campaigns have been carried out by untrained amateurs, but in future Russia may deploy career intelligence officers and special forces soldiers (Spetsnaz) to perform these tasks. Within the structure of the General Directorate of Military Intelligence (GU), one unit that could deliver this function is the Special Operations Service (Military Unit 29155, alias Centre 161), led by Major General Andrei Averianov. In 2014, officers from this unit were implicated in the explosion of ammunition depots in Vrbětice, Czech Republic, where two people were killed and 150 tonnes of ammunition, intended for Ukraine, were destroyed. Sabotage and disruption activities in Europe could also be carried out by officers and soldiers from the GU unit "Senezh" (Military unit 92154, also known as Training Centre 322), which was established in 1999 for the Second Chechen War. It was this unit that organised

[84] A. Sytas, "Estonia says detaining Russia's tankers in Baltic Sea is too risky," Reuters, 10 April 2026, www.reuters.com.

Yevhen Ivanov's attack on the drone factory in Lviv and subsequently participated in the attack on railway lines in Poland, with Yuri Sizov identified as the officer in charge. All these units, despite Russia's ongoing operations in Ukraine, have significant potential for escalation.

Air domain

In the airspace domain, Russia has the potential to further escalate tensions not only by increasing the frequency of military aircraft flights near the airspace of regional states or even violating their borders, but above all through larger-scale drone deployment, which offers a low-cost, high-impact strategy for provocation. GNSS signal jamming should be expected to continue, and at times intensify, jeopardising the safety of civilian air and maritime navigation in particular. In the worst-case scenario, as in the land domain, these actions could trigger an air disaster with a significant number of casualties.

The recurrence of incidents involving the mass incursion of combat drones into the airspace of the Baltic Sea region states cannot be ruled out, with them being used to increase the impact of cognitive warfare operations conducted mainly in the land domain. Acts of diversion and sabotage may also be carried out using FPV drones, deployed not only in border regions but also by "one-off agents."

Russia can conduct these operations at virtually no additional cost, for example, by including them as part of routine military exercises or by utilising inexpensive hardware to increase the number of GNSS signal-jamming sources. The Russian strategy exploits the fact that the response from attacked CBSS members will be far more costly, requiring not only the constant scrambling of fighter jets, but also investment in jamming-resistant geolocation systems. Operations in the air domain also allow Russia to constantly test the air defence systems of NATO countries.

Best Practices

The patterns of behaviour employed by Russia are becoming increasingly well-known and repetitive. This makes it possible for a catalogue of best practices to be drawn up on this basis, setting out common rules for monitoring, reporting and responding to hybrid operations. The Baltic Sea region states should commit to the consistent application of these rules, as only a united and coherent response can effectively influence Russia.

Thus, in order to effectively prevent and respond to threats generated by Russia, the member states of the Baltic Sea Region should develop a joint catalogue of best practices covering the maritime, air and land domains, enabling them to respond more effectively to Russia's hybrid operations.

The maritime domain

To date, the services of most CBSS members have acted independently when responding to cases of hostile activities in the maritime domain—monitoring, preventing, intercepting and escorting suspicious vessels in accordance with national regulations and operational procedures. Additionally, due to existing legislation, it is rarely possible to impose and subsequently enforce penalties for violations, primarily due to limited jurisdictional powers available within the exclusive economic zone and international waters.

The most striking example of these limits is the case against the Russian "shadow fleet" vessel Eagle S, which damaged the undersea power cable between Finland and Estonia in December 2024. The Finnish court had to dismiss the proceedings after ruling that it lacked jurisdiction. This case was one of the most decisive and far-reaching responses taken in response to Russian hybrid operations, and its failure will discourage other states from undertaking similar efforts.

Preventive measures have proved more effective, as on 10 January 2026 when the vessel Tavian, part of the Russian "shadow fleet," was blocked from entry into German territorial waters. The German authorities dispatched a helicopter, demanded the presentation of documents and threatened to seize the vessel, which forced the crew to turn back and head for the Barents Sea.

The Baltic Sea states have not yet undertaken coordinated action, so best practices are based on individual state interventions. However, although operational models for the services and national legislative systems are slowly being adapted to the new conditions, the lack of prior examples limits their development.

The only large-scale action undertaken so far is the Baltic Sentry mission, made possible by closer cooperation among NATO countries in the Baltic Sea under the command of Combined Task Force BALTIC (CTF B) in Rostock, which reports to Allied Maritime Command (MARCOM) and Joint Force Command Brunssum (JFC BS). Its activities reinforce deterrence by presence, and are intended to reduce the potential for escalation on the Russian side.

Land domain

In response to Russian acts of sabotage, subversion and terrorism, Poland has gradually escalated its diplomatic retaliatory measures. Firstly, the freedom of movement of Russian diplomatic personnel was restricted to the provinces in which their diplomatic missions are located. Following evidence from the public prosecutor's office linking Russian intelligence to preparations for an attack on a factory in Wrocław, the Consulate of the Russian Federation in Poznań was closed. Similar retaliatory actions were taken after investigations into the arson attack on the shopping centre at 44 Marywilska Street and the railway line terrorist attack, resulting in the closures of the consulates in Kraków and Gdańsk, respectively.

To make it more difficult for Russia to conduct intelligence operations, Latvia has introduced additional requirements for foreigners wishing to enter the country without a visa or residence permit. Forty-eight hours before crossing the border, they have to provide their destination, planned duration and place of stay, travel itinerary and contact details. From September 2025, the Latvian authorities have also required information on the foreign national's profession and whether they are a member of parliament, a diplomat, a civil servant, or a member of the uniformed services. Refusal to provide this information or providing false details will be punishable by a fine of up to €2,000. To counter the recruitment of Latvian citizens by Russian intelligence services, a ban on travel to Russia and Belarus has been introduced for public sector employees who have access to state secrets, are responsible for the security of critical infrastructure, are employees of the Ministries of Defence, the Interior and Justice, officers of services subordinate to the aforementioned ministries, diplomats and staff of diplomatic and consular missions, and staff of courts and public prosecutors' offices.

The Latvian VDD also conducts regular in-depth vetting of personnel employed at critical infrastructure sites and various service providers in order to identify individuals who pose an intelligence threat. In June 2025, amendments to the National Security Act came into force in Latvia, imposing restrictions on access to Latvia's critical infrastructure facilities for citizens of Russia and Belarus, as well as citizens of other states

supporting Russia's aggression. The VDD participated in drafting these amendments, which aimed to strengthen the protection of critical infrastructure vital to the security of the state and society by pre-emptively mitigating potential security threats. In 2025, on the basis of these amendments, several dozen citizens of Russia and Belarus were prohibited from working or providing services at critical infrastructure facilities due to their access to information and technical equipment necessary for the operation of the facility.[85]

One factor intended to discourage "one-off agents" from cooperating with Russian intelligence is the tightening of penalties for acts of subversion and sabotage, which are now treated as equivalent to terrorism. To address the rise in sabotage, the Polish authorities have broadened the scope of Article 130 of the Criminal Code (espionage), to explicitly include participation in acts of sabotage and terrorist activities on behalf of foreign intelligence services. These offences are punishable by sentences ranging from a 10-year minimum to life imprisonment. From the beginning of 2023 to January 2026, Polish law enforcement agencies brought charges under the aforementioned Article against 82 individuals. By comparison, over the previous seven years (2016–2023), only 46 arrests related to foreign intelligence activities were recorded. The rising number of arrests highlights both the intensification of Russian intelligence activities and the effectiveness of Polish counter-intelligence.

The February 2025 sentencing in Kraków of Russian nationals Alexei Titov and Andrei Gontarev set a new precedent for how European courts handle Russian hybrid threats. The two men received five and a half years for espionage and terrorism-related crimes tied to the Wagner Group. The Polish authorities arrested them in August 2023 for distributing recruitment and propaganda materials, as well as conducting reconnaissance operations across the country. Their superiors invested at least $24,000 in numerous intelligence and influence operations in Poland, France and Germany.[86]

Adoption of the measures outlined above by a wider group of countries would be beneficial to efforts to combat the activities of the Russian Federation's special services. CBSS members may therefore consider introducing similar actions aimed, among other things, at enhancing the security of critical infrastructure. Simultaneously, raising the severity of penalties across other EU and NATO countries will send a powerful message to any individuals considering collaboration with Russian intelligence services.

Air domain

The launch of Operation Eastern Sentry was one of the most significant measures taken by NATO member states. Developed following the mass incursion of Russian com-

[85] "Annual Report for 2025," Latvian State Security Service (VDD), 2026, p. 14, www.vdd.gov.lv.

[86] C. Rondeaux, "The legal counteroffensive to Russia's hybrid war," *Lawfare*, 6 April 2025, www.lawfaremedia.org.

bat drones into Polish territory in September 2025, it has so far succeeded in preventing any further incidents on that scale. It is important that the Alliance continues such activities, and that its member states jointly conduct missions to protect those regions most vulnerable to Russian actions, such as the Baltic Sea area.

Cooperation between countries in conducting NATO Air Policing missions, coordinated by the Allied Air Command (AIRCOM) at Ramstein Air Base, also plays a significant role in preventing air domain threats. AIRCOM was actively involved in securing Polish airspace during the incursion of Russian drones on the night of 8–9 September 2025.

It is also worth noting the cooperation by CBSS members to combat GNSS signal jamming. Activities within international agencies and joint projects to develop jamming-resistant systems are important initiatives to enhance the safety of air and maritime navigation.

These examples of action taken by CBSS states provide a blueprint for a shared catalogue of best practices. Formalising these successes would allow Council members to exchange vital information and work together more closely on the implementation of regional security protocols.

Conclusions and Recommendations

The growing number of sabotage and subversion incidents in Baltic Sea Region states since 2022 suggests that Russia is waging a concerted campaign, intended to raise the cost of Western aid to Ukraine, erode public and political backing for this policy, and exploit these issues to create divisions within European and transatlantic structures. Despite these efforts, Russia has so far failed to achieve its objectives.

To date, Russia has acted to escalate tensions during periods when the EU and NATO have been discussing additional tranches of military aid for Ukraine and imposing further rounds of sanctions on Russia. It can be assumed that, in future, Russia will continue seeking to escalate tensions in similar political circumstances, using this to exert pressure on European decision-makers. Furthermore, the methods developed by the Russians will be further refined in order to systematically weaken the targeted states. The growing number of acts of subversion and sabotage also indicates that Russia is conducting a comprehensive campaign against NATO and EU countries, aimed at increasing the costs of Western aid to Ukraine, undermining public and political support for the continuation of this policy, and, against this backdrop, creating divisions within European and transatlantic structures.

Russia's hybrid operations at sea were effective due to carefully devised strategies that were implemented consistently and continuously. These strategies enabled Russia to destabilise the situation in the Baltic Sea region, resulting in immediate impacts, such as disruptions to energy and communications supplies, as well as systemic losses, such as the diversion of military forces and resources to counter hybrid threats, drawing them away from core defence and deterrence tasks. Since it is difficult to attribute sabotage activities to Russia, and reconnaissance operations generally do not cause damage to facilities or systems, they also facilitate the management of escalation risk, meaning responses will always be limited.

A series of incidents targeting critical infrastructure security have been carried out by Russia within the land domain, and the intensification of activities since 2024 indicates a growing determination to cause tangible damage, paired with psychological impacts.

Russia also remained active in the air domain, extending from incidents involving military aircraft and helicopters, to also repeatedly deploying unmanned aerial vehicles. GNSS signal jamming was a significant element of these activities and has caused ongoing problems for air and maritime navigation. Consequently, the Baltic Sea region now experiences the highest frequency and scope of GNSS interference of any area in Europe.

At the operational level in the maritime domain, it will be crucial for the EU to support the development of the CISE and MARSUR information-sharing networks, which will improve situational awareness in the Baltic Sea region. It will also be essential to implement the Mainsail system being developed within NATO,[87] which uses artificial intelligence to combine and analyse data from various sources, and will facilitate the detection of suspicious vessels or operations in the maritime domain and enable preventive action to be taken.

However, at the regulatory level, the most important development will be the implementation by Member States of the EU Directive of 14 December 2022 on the resilience of critical entities. The introduction of legal regulations concerning the collection and exchange of information between the private and public sectors regarding the protection of critical maritime infrastructure will also be crucial, alongside adoption of legal regulations concerning the use of surface and underwater unmanned platforms, and their potential neutralisation.

However, NATO and EU member states should regard the recently implemented policy of deterrence by presence as a temporary solution. This approach leaves the Alliance with the fundamental problem of being unable to hold Russia to account, forcing members to bear the disproportionate financial burden of defending against hybrid operations.

In order to effectively counter Russian subversive and sabotage activities at a political level, it is crucial to maintain a high level of situational awareness. This can be achieved through close cooperation between military and civilian intelligence and counter-intelligence services, border guards, and the police, at both national and international levels. This is particularly important given the freedom of movement within the Schengen area and the fact that saboteurs operate across several countries. For example, cooperation between the public prosecutors' offices of the Czech Republic, Lithuania, Poland and Romania within the framework of the EU Agency for Criminal Justice Cooperation (Eurojust) has enabled the arrest and conviction of a sabotage and terrorist network responsible for arson attacks on facilities in these countries.[88]

[87] "NATO advances maritime innovation and readiness through Exercise Dynamic Messenger 2025," Public Affairs Office at MARCOM, 29 September 2025, https://mc.nato.int/.

[88] "Terrorist group responsible for arson attacks across Europe taken to court," European Union Agency for Criminal Justice Cooperation, 27 January 2026, www.eurojust.europa.eu.

The NATO Counterintelligence Centre of Excellence (NATO CI CoE) in Kraków and the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) in Helsinki are international platforms that facilitate the exchange of experience and training in countering Russian sabotage. However, these institutions are not intended for intelligence sharing between states. Therefore, it is advisable for the CBSS states to consider establishing national Hybrid Threat Centres to coordinate the institutional exchange of information. Germany has announced plans to establish such a structure within the Federal Office for the Protection of the Constitution (BfV), while in Poland, the competences of the existing Anti-Terrorism Centre within the Internal Security Agency (ABW) could be further expanded, as it already acts as the national coordinator in Commission initiatives related to building the resilience of critical infrastructure. At the strategic and systemic level, the capabilities of the Government Centre for Security (RCB) will need to be expanded so that it can serve as the central institution bringing together the entire system of Polish critical infrastructure protection. At the EU level, the Hybrid Fusion Cell, established within the EU Intelligence and Situation Centre (EU INTCEN) in 2016, performs the role of coordinator for information exchange. However, the readiness and willingness of individual counter-intelligence and intelligence services to share sensitive information among the 27 Member States remains a challenge. Given these limitations, Member States prefer bilateral cooperation. CBSS members could overcome these limitations by establishing an intelligence-sharing system amongst themselves regarding hybrid threats.

As critical infrastructure facilities are usually operated by private entities, strengthening the exchange of information between the public and private sectors is also essential at operational and regulatory levels. The Critical Entities Resilience (CER) Directive governs issues relating to the division of competences and responsibilities in this area, and its effective implementation into national crisis management systems is essential for building the capacity to monitor and respond to diversion and sabotage threats, particularly in the context of countering aerial and maritime drones. Investments by private critical infrastructure operators in sensors that enable early threat detection can improve situational awareness and reduce the response time of law enforcement agencies (e.g. the police, border guards and the military). It is also crucial to raise awareness of the threat of sabotage and subversion among management and staff at critical infrastructure sites, and to ensure the highest safety standards, including by providing targeted training.

In order to reduce the vulnerability of railway lines to sabotage and subversion, given their dual-use nature, it is necessary to increase funding for their modernisation and adaptation to military standards. Monitoring and early-warning systems for damage to railway infrastructure will also need to be strengthened. The EU's Defence Readiness Action Plan for 2030 allocates €1.7 billion for this purpose. This includes investments in the Baltic and Scandinavian regions to adapt them to European track gauge standards. However, private companies have argued that the planned budget is insufficient,

believing that at least €100 billion is required, and have therefore requested that the EU allocate additional funds under the Connecting Europe Facility (CEF).[89]

To deter potential "one-off agents" from collaborating with Russian intelligence, the CBSS should act at the regulatory level to impose harsher penalties for subversive, sabotage and terrorist activities. At the same time, extensive public awareness campaigns should be conducted to inform the public about the nature of the threat and its possible consequences. Such campaigns should target the groups most susceptible to recruitment, including immigrants from Eastern European countries. Raising public awareness of situations that warrant attention and of how such incidents should be reported to the relevant authorities will provide an additional source of vital information. For example, the Internal Security Agency has set up a special chatbot on Telegram for reporting recruitment attempts via the app, and Russians operating in Poland were caught attempting to recruit for the Wagner Group after a member of the public informed the police about the distribution of recruitment materials.

To respond effectively to Russian subversion and sabotage and influence Russia's calculations, thereby deterring it from continuing or escalating its campaign, NATO and EU member states must impose greater costs on the aggressor. Measures taken may include diplomatic actions such as the further expulsion of Russian spies operating under diplomatic cover, sanctions, the downgrading of bilateral relations and the closure of Russian diplomatic missions or other institutions used to cover intelligence activities (e.g. Russian Houses).

At the operational level in the airspace domain, it may be necessary to introduce systems that allow the use of alternative positioning technologies, such as the 5G network. These systems will support the execution of flight procedures, particularly during critical stages (take-off and landing), when precise positioning is essential. Improving air traffic safety will require the development of capabilities to locate jamming sources and filter out jammed signals, and these systems could also be used to protect maritime navigation. Expanding civil-military cooperation regarding the use of jamming neutralisation devices used by military aircraft is also worth considering. Additionally, it may be necessary to develop a network of ground-based radars to assist aircraft and ships.

With an increasing number of threats being caused by unmanned aerial vehicles, strengthening the electronic defence of critical state infrastructure is essential, particularly transport, energy, telecommunications, and border facilities. In this regard, Ukraine's experience offers a rich source for CBSS members to draw on, as it is constantly developing its capabilities in this area. It may also be necessary for Finland, the Baltic States, and Poland to develop joint systems for countering weather balloons and establish joint response procedures (including diplomatic ones) to such incidents.

[89] E. Ferris, "Russian Sabotage of NATO Infrastructure: Identifying Alliance Vulnerabilities," RUSI, 26 March 2026, www.rusi.org.

If the number of incidents involving Russian military aircraft increases, amending the rules of engagement (ROE) at the regulatory level may be necessary. Granting greater authority to NATO pilots conducting air policing missions and to operators of ground-based air defence systems would enable them to defend NATO airspace more effectively.

Another issue is the need to build societal resilience, such as through wide-ranging educational campaigns and appropriate changes to school curricula, following the example of the Nordic countries. It would be beneficial for the CBSS states to share best practices and pool their experience in this area. Cooperation between the institutions responsible for strategic communication in the CBSS countries will also be essential in the fight against disinformation accompanying acts of sabotage and subversion. Jointly organising public awareness campaigns can enable a much wider audience to be reached.

In the coming years, the threat posed by Russia will remain the most significant security challenge for members of the CBSS. This stems from Russia's systemic approach towards the Baltic Sea region, which it regards as hostile. Therefore, we should expect an intensification of subversion and sabotage activities carried out by Russia in the coming months and years. Only extensive international cooperation within the framework of the CBSS, and more broadly within the EU and NATO, will enable us to increase our resilience to Russian hybrid activities.

Appendix

The Maritime domain

Table 1

Kinetic hybrid events in the maritime domain (2022–2026)

DATE	LOCATION	ATTACK	STATUS	TARGET SPECIFICATION	PERPETRATORS	ATTRIBUTION	RESPONSE	ADDITIONAL INFORMATION
26.09.2022	International waters, the exclusive economic zones of Denmark and Sweden	Damage to three of the four lines of the Nord Stream 1 and Nord Stream 2 gas pipelines	The case is ongoing in Germany, but was closed in Denmark and Sweden in 2024	Underwater energy infrastructure	Suspepcted to be a group of seven Ukrainians (the yacht Andromeda)	None	Investigation	Explosions
7.10.2023	Estonian territorial waters	Damage to the underwater communications cable between Sweden and Estonia (EE-S1)	Case closed	Underwater communication infrastructure	Suspected vessels: Newnew Polar Bear (China), Sevmorput' (Russia)	None	Investigation	The announcement was made on 17 October. The case is linked to Balticconnector and Elisa

DATE	LOCATION	ATTACK	STATUS	TARGET SPECIFICATION	PERPETRATORS	ATTRIBUTION	RESPONSE	ADDITIONAL INFORMATION
8.10.2023	The Gulf of Finland, Finland's exclusive economic zone	Damage to the Balticconnector gas pipeline between Finland and Estonia	Case pending	Underwater energy infrastructure	Newnew Polar Bear (Hong Kong flag)	China	Cooperation with China is ongoing as part of the investigation. China states that the accident was caused by adverse weather conditions	The ship was dragging an anchor. It was found at the scene. A nearby Russian nuclear-powered barge, the Sevmorput', was also under suspicion. The case is linked to EE-S1 and Elisa
10.2023	Estonia's economic zone, excluding territorial waters	Damage to the undersea communications cable between Estonia and Finland (operated by Elisa)	Case closed	Underwater communication infrastructure	Suspected vessels: Newnew Polar Bear (China), Sevmorput' (Russia)	None	Investigation	The case is linked to Balticconector and EE-S1
17.11.2024	Sweden's exclusive economic zone	Damage to the undersea telecommunications cable connecting Lithuania and Sweden (BCS East-West Interlink)	Case pending	Underwater communication infrastructure	Yi Peng 3 (China flag)	China	A request by the Danish Border Guard for a vessel to be anchored in the Danish Straits	The case is being investigated jointly with C-Lion1. The Russian vessel Yevgeny Churov was in the vicinity of the Yi Peng 3's anchorage

DATE	LOCATION	ATTACK	STATUS	TARGET SPECIFICATION	PERPETRATORS	ATTRIBUTION	RESPONSE	ADDITIONAL INFORMATION
18.11.2024	Sweden's exclusive economic zone	Damage to the undersea telecommunications cable linking Finland and Germany (C-Lion1)	Case pending	Underwater communication infrastructure	Yi Peng 3 (China flag)	China	A request by the Danish Border Guard for a vessel to be anchored in the Danish Straits	The case is being investigated jointly with BCS East-West Interlink. The Russian vessel Yevgeny Churov was in the vicinity of the Yi Peng 3's anchorage
25.12.2024	The Gulf of Finland	Damage to the undersea power cable between Finland and Estonia (Estlink2)	Case dismissed (lack of judicial jurisdiction over international waters)	Underwater energy infrastructure	Eagle S (Cook Islands flag)	Russian "shadow fleet" vessel	Detention of the vessel and crew by the Finnish Border Guard	The ship was dragging an anchor. Incident happened two months before the Baltic states disconnected from the Russian power grid
01/02.2025	Sweden's exclusive economic zone	Repeated damage to the undersea telecommunications cable linking Finland and Germany (C-Lion1)	Case pending	Underwater communication infrastructure	Arne (Antigua i Barbadua flag)	None	Monitoring of the vessel by German and Danish authorities, followed by an inspection	

DATE	LOCATION	ATTACK	STATUS	TARGET SPECIFICATION	PERPETRATORS	ATTRIBUTION	RESPONSE	ADDITIONAL INFORMATION
31.12.2025	The Gulf of Finland, Estonia's exclusive economic zone	Damage to the undersea telecommunications cable between Estonia and Finland (operated by Elisa)	Case pending	Underwater communication infrastructure	Fitburg (Saint Vincent and the Grenadines flag)	A ship belonging to Russia's "shadow fleet" was transporting steel subject to sanctions (it was not seized)	Detention of the vessel and crew by the Finnish Border Guard	The ship was dragging an anchor

Source: Own research..

Land domain

Table 2

Kinetic diversionary and sabotage attacks in the land domain (2022–2026)

DATE	LOCATION	ATTACK	STATUS	TARGET SPECIFICATION	PERPETRATORS	ATTRIBUTION	RESPONSE	ADDITIONAL INFORMATION
2023	Gdynia, Bydgoszcz, Warsaw, Rzeszów (Poland)	Preparations for sabotage	Thwarted	Monitoring of arms transport routes to Ukraine, reconnaissance of critical infrastructure and military bases	A spy network comprising 30 people, 16 of whom were arrested (13 Ukrainians, 2 Belarusians and 1 Russian)	Russian intelligence	Sentences ranging from 13 months to 6 years' imprisonment	
05-12.2023 r.	Sinimäed Hills, Tallinn x2, Mustla and Viljandi (Estonia)	Vandalism	Completed	Historical memorial sites, a Ministry of the Interior vehicle and the editor-in-chief of Delfi	13 people—Allan Hantsom's network	Russian intelligence	Group leader Allen Hantsom was sentenced to 6.5 years in prison	

DATE	LOCATION	ATTACK	STATUS	TARGET SPECIFICATION	PERPETRATORS	ATTRIBUTION	RESPONSE	ADDITIONAL INFORMATION
03.2023-07.2024	Gdańsk x2, Marki, Radom, Warsaw x2, Łódź (Poland)	Arson	Failed attempts in Gdańsk and Łódź, carried out in Marki, Radom and Warsaw	Construction centres	9 people arrested (Poles, Ukrainians and Belarusians); the arson attack in Radom was carried out by a Colombian		Investigation	
01.2024	Wrocław (Poland)	Arson	Thwarted	A chemical factory located near strategic infrastructure (fuel depot) and the Odra river	Ukrainian national	Russian intelligence	Closure of the Russian consulate in Poznań	The aim of the operation may have been to cause serious environmental contamination
02.2024	Riga (Latvia)	Arson	Thwarted	Museum of the Occupation	3 Latvian citizens			
03.2024	Vilnius (Lithuania)	Political assault	Completed	Leonid Volkov—Russian dissident	Two Polish citizens	Anatoly Blinov—Russian lawyer	Investigation	The Russian intelligence services were likely the actual instigators of these events, but the public prosecutor's office in Poland has not obtained conclusive evidence of this

DATE	LOCATION	ATTACK	STATUS	TARGET SPECIFICATION	PERPETRATORS	ATTRIBUTION	RESPONSE	ADDITIONAL INFORMATION
04.2024	Rzeszów-Jasionka (Poland)	Political assassination	Foiled	President of Ukraine	Paweł K.—a Polish citizen, former soldier of the 2nd Hrubieszów Reconnaissance Regiment	Russian intelligence	Investigation	The perpetrator expressed his willingness to cooperate with Russian intelligence and his desire to join the Wagner Group
04.2024	Germany	Sabotage	Thwarted	US bases in Bavaria, railway infrastructure	Three German citizens of Russian origin	Russian intelligence	Investigation, alert level raised to "CHARLIE"	
05.2024	Vilnius (Lithuania), Riga (Latvia), Warsaw (Poland)	Arson	Carried out in Vilnius, foiled in Riga and Warsaw	Construction centres	5 people (including Ukrainian nationals)	Russian intelligence	Investigation	The arson attack on the Ikea store in Vilnius has been classified as a terrorist attack
05.2024	Frankfurt (Germany)	Political assassination	Foiled	Ukrainian soldier	3 people arrested (an Armenian, a Ukrainian, a Russian)	Russian intelligence	Investigation	
05.2024	Warsaw (Poland)	Arson	Completed	Shopping centre at 44 Marywilska Street	5 people (including Ukrainian nationals)	Russian intelligence	Closure of the Russian consulate in Kraków	

DATE	LOCATION	ATTACK	STATUS	TARGET SPECIFICATION	PERPETRATORS	ATTRIBUTION	RESPONSE	ADDITIONAL INFORMATION
07.2024	Düsseldorf (Germany)	Political assassination	Foiled	Armin Papperger, Executive Director of Rheinmetall		Russian intelligence		Foiled thanks to cooperation between American and German intelligence services
07.2024	Wola Bykowska (Poland)	Sabotage	Thwarted	Transport of hazardous materials	3 people detained	Russian intelligence	Investigation	
09.2024	Šiauliai (Lithuania)	Arson	First attempt thwarted, second successfully completed	TVC Solutions, a supplier of military equipment manufacturing mobile radio spectrum analysis stations	Two Spanish nationals (including one with dual nationality) are alleged to have carried out the first (failed) attempt. The second attempt (which resulted in a fire) is alleged to have been carried out by two nationals of Russia and Belarus	Russian intelligence	Investigation	

DATE	LOCATION	ATTACK	STATUS	TARGET SPECIFICATION	PERPETRATORS	ATTRIBUTION	RESPONSE	ADDITIONAL INFORMATION
10.2024	Vilnius (Lithuania), Warsaw (Poland), Leipzig (Germany), Birmingham (United Kingdom)	Terrorist attack	Incomplete—the premature detonation of explosives in the logistics centres of shipping companies exposed the operation	Cargo aircraft operating transatlantic flights from Europe to the US and Canada	15 people detained (citizens of Russia, Lithuania, Latvia, Estonia and Ukraine)	Russian intelligence	Investigation	The aim of the operation was, among other things, to identify routes for the smuggling of explosives. The possibility of an attack on aircraft using flammable materials cannot be ruled out
10.2024	Riga (Latvia)	Arson	Completed	Arms manufacturer, vehicles with Ukrainian number plates, IK facilities	Four people, at least two of whom are Latvian citizens	Russian intelligence		
01.2025	Osula and Tallinn (Estonia)	Arson	Completed	Supermarket and restaurant	2 Moldovan nationals	FR intelligence		

DATE	LOCATION	ATTACK	STATUS	TARGET SPECIFICATION	PERPETRATORS	ATTRIBUTION	RESPONSE	ADDITIONAL INFORMATION
02.2025	Hamburg (Germany)	Sabotage	Completed	Corvette Emden (F266), under construction at the NVL Blohm + Voss shipyard	Citizen of Romania and Greece		Investigation	Nearly 30 kg of metal filings were found in the propulsion system, which could have led to a serious engine failure. The detection of this tampering prevented the potential immobilisation of the vessel and a significant delay in its handover to the German Navy
02.2025	Wilhelmshaven (Germany)	Sabotage	Completed	The frigate "Hessen" belonging to the German Navy			Investigation	
03.2025	Gotland (Sweden)	Sabotage	Completed	Waterworks			Investigation	Damage to the power cables supplying the pump system
08.2025	Sopot (Poland)	Sabotage	Thwarted	Waterworks	Ukrainian citizen		Investigation	
04-08.2025	Monastery and Homestead (Poland)	Vandalism	Completed	Memorial sites relating to Polish-Ukrainian relations	Ukrainian citizen	Russian intelligence	Arrest of the perpetrator	Fomenting tensions in Polish-Ukrainian relations

DATE	LOCATION	ATTACK	STATUS	TARGET SPECIFICATION	PERPETRATORS	ATTRIBUTION	RESPONSE	ADDITIONAL INFORMATION
06.2025	Erfurt (Germany)	Arson	Completed	6 vehicles belonging to the Bundeswehr			Investigation	
08.2025	Latvia	Sabotage	Completed	Railway infrastructure				The perpetrators set fire to a train and train control stations. Footage of the incident was used for disinformation purposes
09.2025	Railway line between Hamburg and Berlin and between Cologne and Düsseldorf (Germany)	Sabotage	Completed	Railway infrastructure			Investigation	
10.2025	Poland and Romania	Sabotage	Thwarted	Nova Post headquarters in Bucharest				Seizure of explosives supply
11.2025	Mika and Gołąb (Poland)	Sabotage	Completed	Railway line No. 7 between Warsaw and Dorohusk – railway lines of strategic importance for the transport of humanitarian and military aid to Ukraine	Two Ukrainian citizens	Russian Federation Consulate	Closure of the Russian consulate in Gdańsk	

DATE	LOCATION	ATTACK	STATUS	TARGET SPECIFICATION	PERPETRATORS	ATTRIBUTION	RESPONSE	ADDITIONAL INFORMATION
01.2026	Essen (Germany)	Sabotage	Completed	Freight train carrying hazardous substances			Investigation	A derailment forced a change of route for a train transporting ammunition for US forces in Europe

Source: Own research.

Air domain

Table 3

Identified airspace violations

DATE	COUNTRY	LOCATION	TYPE OF OBJECT
02.03.2022	Sweden	Gotlandia	2x Su-24, 2x Su-27
29.04.2022	Sweden	Blekinge	An-30
17.06.2022	Denmark	Bornholm	KA-31/KA-27
18.08.2022	Finland	Porvoo	2x MiG-31
16.12.2022	Poland	Bydgoszcz	Kh-55 millsile
12.05.2023	Estonia	Vaindloo	Russian fighter
01.08.2023	Poland	Białowieża	2x helicopter (Mi-24/8)
24.03.2024	Poland	Osera	Cruise missile
14.06.2024	Sweden	Gotland	Su-24
07.09.2024	Latvia	Rēzekne	Shahed-type drone
11.02.2025	Poland	Ustka Region	Su-24
25.04.2025	Poland	Vistula Spit	Helicopter Ka-27
22.06.2025	Estonia	Vaindloo	Il-76
20.08.2025	Poland	Mazury (Mamry lake region)	Orlan-10 Drone
09.09.2025	Poland	Eastern border	19x UAV
19.09.2025	Estonia	Tallinn	3x MiG-31
23.10.2025	Lithuania	Suwałki Gap / Border	Il-76MD (Eskorta Su-30SM)
24.11.2025	Estonia	Vaindloo / The Gulf of Finland	Tu-134 & 2x Su-30SM
01.01.2026	Estonia	Vaindloo / Tallinn	3x MiG-31BM
18.03.2026	Estonia	Vaindloo Island	Su-30
25.03.2026	Estonia	Auvere (Narva)	Drone (UAV)

Source: Own research.

Table 4

Interceptions in international airspace

COUNTRY (BASE)	DATE	REGION	TYPE OF OBJECT	INTERCEPTION
Lithuania (Šiauliai)	19.12.2022	Balctic Sea	An-26 & 2x Su-24M	1
Denmark	01.04.2023	Bornholm	Il-20	1
Norway	23.08.2023	Far North	Tu-95 & Su-33	1
Poland (Malbork)	25.04.2025	Baltic Sea	Il-20M & 2x Su-30SM	1
Norway (Evenes)	12.02.2026	Norwegian Sea	2x Tu-160	1
Norway	10.03.2026	The Finnmark Coast	Il-20M	1
Norway	11.03.2026	Lofoten / Vesteralen	Il-20M	1
Lithuania (Šiauliai)	18.03.2026	Baltic Sea	2x Su-30SM	1
Finland	22.03.2026	Åland	Il-20M	1

Source: Own research.

The Polish Institute of International Affairs (PISM) is a leading Central European think tank that positions itself between the world of politics and independent analysis. PISM provides analytical support to decision-makers and diplomats, initiates public debate and disseminates expert knowledge about contemporary international relations. The work of PISM is guided by the conviction that the decision-making process in international relations should be based on knowledge that comes from reliable and valid research.

Polski Instytut Spraw Międzynarodowych
The Polish Institute of International Affairs
ul. Warecka 1A
00-950 Warszawa
tel. (+48) 22 556 80 00
pism@pism.pl
www.pism.pl

ISBN 978-83-68555-33-2
e-ISBN 978-83-68555-34-9