

BRIEF 1 | BALTIC STATES

Russia's Sub-Threshold Warfare

Against the Baltic States
in 2022–2026

2026



Sahaidachnyi
Security Center



Serpens Center for
International Security

PROJECT INFORMATION

This brief on the Baltic States is the first in a series of publications prepared as part of a project supported by the Prague Civil Society Centre. The project aims to raise awareness of Russia's expanding sub-threshold warfare against Europe by strengthening the Everywhere War Tracker (<https://sahasec.org/tracker/>) and translating its findings into policy-relevant analysis. The next two briefs will examine developments in Northern Europe and Central and Eastern Europe. The analysis covers the period from the start of Russia's full-scale invasion of Ukraine in February 2022 through 2026, providing a retrospective assessment of the evolution of Russia's sub-threshold warfare against Europe.

The Everywhere War Tracker is an OSINT-based interactive monitoring tool documenting officially attributed and suspected Russian hostile activities against Europe since 2022. It tracks incidents across the air, maritime, land and cyber domains, including airspace incursions, suspicious maritime activity, sabotage against critical, military and economic infrastructure, significant cyberattacks, and military activities that may indicate preparation for escalation. By identifying geographic, temporal and operational patterns, the Tracker helps distinguish isolated incidents from the broader evolution of Russia's campaign and provides an evidence base for assessing how sub-threshold warfare is changing across Europe.

Special thanks go to the Serpens Center for International Security and the Baltic Initiative for European Reform for their partnership and support.

This publication was produced with the support of the Prague Civil Society Centre. Its contents are the sole responsibility of the authors and do not necessarily reflect the views of the Prague Civil Society Centre.

Executive Summary

- **The trajectory in the Baltic states mirrors the broader evolution of Russia's sub-threshold warfare across Europe**, with the timing, intensity and methods of escalation shaped by changes in the wider political and military environment since 2022. Moscow's tactics were shaped by its own evolving capabilities and geopolitical frame like growing uncertainty over US support for Europe and Ukraine, political fragmentation inside Europe, Russia's reconstruction of intelligence networks, and lessons from the new generation warfare. The transition from reactive signalling in 2022–23 to sabotage in 2024 and more overt military pressure in 2025–26 reflect this changing environment.
- **The number and frequency of incidents have risen markedly.** The Tracker records more than a hundred incidents between January 2022 and September 2026 across Estonia, Latvia and Lithuania. These include airspace and maritime incidents, sabotage, cyber operations, GNSS interference, and increasingly intensive air-policing activity that can no longer be treated as routine peacetime background. The Tracker also captures potential military threats, including large-scale war rehearsals and forward military construction, because these form part of the wider coercive environment in which sub-threshold operations occur. This must be read against intelligence warnings that Russia may seek an overt or covert test of NATO's Article 5 commitments in the near term.
- **Since March 2025, Russian hostile activity against the Baltic states has become a monthly phenomenon.** The apparent 2026 peak is driven largely by Russian military-aircraft activity, while the deeper trend is the diversification and persistence of pressure since 2024: cyber operations remain continuous, jamming and spoofing have expanded, drone incursions have become recurrent.
- **The political effect of sub-threshold operations can greatly exceed their physical damage.** The May 2026 Rēzekne drone incident caused limited material damage but generated school closures, a NATO response and a domestic political crisis culminating in government change. The case demonstrates that unclear procedures, fragmented responsibilities and weak crisis communication can multiply the effect of a relatively small hostile act, making governance itself part of the attack surface.
- **The pressure is structural rather than driven solely by spillover from the war in Ukraine or by efforts to deter Baltic support for Kyiv.** Russian rhetoric questioning Baltic sovereignty, the mobilization of historical claims and Russian-speaking populations, the strategic role of Kaliningrad and Belarus, and the Baltic states' position on NATO's eastern flank make the region a persistent arena for testing Alliance resolve.
- **The principal policy requirement is to shift from incident management to campaign-level deterrence.** Baltic and Allied governments should build a shared intelligence and incident picture across domains, establish graduated and predictable consequences for cumulative hostile activity, and respond to every Russian attack leaving the 'detering by ignoring' approach in the past. The objective is to deny Russia the advantage created by ambiguity, fragmented attribution and repeated low-cost testing.

Content

Executive Summary..... 3

Introduction..... 5

Why Does Russia Target the Baltic States?..... 6

1 Incident Overview by Year..... 8

 2022 Major Baltic State Incidents..... 11

 2023 Major Baltic State Incidents..... 12

 2024 Major Baltic State Incidents..... 13

 2025 Major Baltic State Incidents..... 14

 2026 Major Baltic State Incidents (January–September 2026)..... 15

2 Key Trends — 2022 to 2026..... 17

 2.1 Rising number and frequency of hybrid threat incidents..... 17

 2.2 Shift from Reconnaissance and Sabotage to Airspace Provocations..... 17

 2.3 Russia’s new tactic - the spoofing of Ukrainian drones into Baltic territory..... 18

 2.4 Persistent Pressure on the Land Border with Belarus..... 18

3 Russian Framing of its Aggression against the Baltics..... 19

Conclusion and Recommendations..... 21

About the Authors..... 23

Introduction

Russia's sub-threshold warfare — hybrid warfare, in EU terms — is a multidomain campaign spanning air, maritime, land, cyber, space and the cognitive domain. The *Everywhere War Tracker* indicates a clear escalation in 2024 and 2025 as incidents became more frequent, geographically dispersed and operationally audacious.

Reports by the International Institute for Strategic Studies identify the same trajectory. Russian sabotage operations in Europe nearly quadrupled from 2023 to 2024 and remained elevated into 2025, despite a temporary slowdown in the first half of the year.¹ A subsequent IISS investigation concluded that Russia also highly likely conducted a coordinated UAV campaign across Europe between August 2024 and February 2026, spanning a dozen NATO states and Ireland and exploiting persistent gaps in European air defence, attribution and response mechanisms.²

The Baltic States have been among the prime targets of Russia's sub-threshold warfare for the whole period since the beginning of the full-scale invasion of Ukraine in February 2022. This brief traces that period in full through all domains. Even when routine NATO Baltic Air Policing intercepts of Russian military aircraft flying without transponders are excluded, the overall pattern, frequency and diversity of incidents affecting Latvia, Lithuania and Estonia show that Russia's sub-threshold activity in the region cannot be dismissed as mere spillover from its aggression against Ukraine.

These attacks are unfolding against increasingly explicit warnings from European leaders that Russia's sub-threshold campaign is intensifying and risks further escalation, possibly within months.³ German intelligence assessed in late 2024 that Moscow may be preparing a limited operation against the Baltic States or Svalbard by the end of the decade, designed to test and fail NATO's Article 5 guarantee.⁴ Denmark's Defence Intelligence Service has set out scenarios ranging from a local war against a frontline European state within months of a ceasefire in Ukraine to a wider European war within five years.⁵ Lithuania's 2026 National Threat Assessment added that Russia keeps building military capability near NATO's eastern borders, despite its losses in Ukraine⁶.

None of this amounts to a prediction that an attack is imminent. But it is the context in which the incidents catalogued in this brief are best read: not as isolated provocations, but as part of a campaign.

¹ Charlie Edwards and Nate Seidenstein, *The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure* (London: International Institute for Strategic Studies, August 2025), 4, 11, <https://www.iiss.org/globalassets/media-library---content---migration/files/research-papers/2025/08/pub25-095-the-scale-of-russian-sabotage-operations.pdf>

² Charlie Edwards, Rex Fox O'Loughlin, and Louis Bearn, *Russia's UAV Campaign Over Europe* (London: International Institute for Strategic Studies, July 2, 2026), <https://www.iiss.org/research-paper/2026/06/russias-uav-campaign-over-europe/>

³ Ursula von der Leyen, "2026 State of the Union Address," European Commission, September 16, 2026, https://cyprus.representation.ec.europa.eu/news/2026-state-union-address-president-von-der-leyen-2026-09-16_en; Shaun Walker, "European Spy Chiefs Warn Moscow Is Planning More Decisive Action against NATO," *The Guardian*, September 20, 2026, <https://www.theguardian.com/world/2026/sep/20/baltic-spy-chiefs-warn-moscow-is-preparing-for-more-decisive-action-in-europe>

⁴ Business Insider, 17 March 2024. "Geheimdienst-Szenario kursiert in Regierung: Greift Putin ab 2026 die Nato an?", <https://www.businessinsider.de/politik/welt/greift-putin-ab-2026-die-nato-an/>

⁵ Danish Defence Intelligence Service (FE) (2025), "Intelligence Outlook".

⁶ Defence Intelligence and Security Service (AOTD) and State Security Department (VSD) of the Republic of Lithuania, *National Threat Assessment 2026* (Vilnius, 2026), <https://kam.lt/wp-content/uploads/2026/03/National-Threat-Assesment-2026.pdf>.

Why Does Russia Target the Baltic States?

Russia is already waging a full-scale sub-threshold war against Europe.⁷ Moscow seeks to weaken and ultimately hollow out NATO and the EU, deepen political fragmentation, empower forces sympathetic to the Kremlin, and restore a Russian sphere of influence. The strategic end-state is a Europe divided into weaker, less cohesive and increasingly illiberal states that are easier for Moscow to pressure, penetrate and dominate.⁸ Within this broader confrontation, the Baltic States occupy a particularly exposed and symbolically important position.

Russia's historical aspiration for access to the Baltic predates the Soviet Union: Peter the Great's conquest of the eastern Baltic coastline gave the Russian Empire its "window to Europe" and enabled the construction of St Petersburg. Today, the Baltic Sea remains essential for Russia's military posture, commercial access and connection with Kaliningrad. Kaliningrad hosts the principal base of Russia's Baltic Fleet at Baltiysk and a concentration of missile, air-defence and other military capabilities capable of threatening NATO movement across much of the region.⁹ Lithuania lies directly between Kaliningrad and Belarus. Between Lithuania and Poland sits the roughly 100-kilometre Suwałki corridor, the Baltic States' only land connection with the rest of NATO territory. In a conflict, severing this corridor would both isolate Estonia, Latvia and Lithuania from NATO reinforcement by land and create a connection between Belarus and Kaliningrad.¹⁰

Finland's and Sweden's accession to NATO radically improved the alliance's geographical position and made Russian domination of the Baltic Sea considerably more difficult. Yet this has also increased the strategic value of disruption. Russia retains access through St Petersburg/Kronstadt and Kaliningrad and can use missiles, drones, electronic warfare, mines, covert action and ostensibly civilian vessels to complicate NATO operations without attempting to defeat NATO's combined naval forces directly.¹¹

The Baltic States are attractive targets for sub-threshold warfare because they combine strategic importance with exploitable vulnerabilities. Estonia and Latvia have sizable Russian-speaking populations that Moscow has for years portrayed as victims of discrimination. Russia's 2023 Foreign Policy Concept formally commits the state to defending "compatriots" abroad, particularly in what it calls unfriendly states, providing a ready-made narrative for political

⁷ Elena Davlikanova (2026) Russia's Everywhere War Against Europe, Sahaidachnyi Security Centre. <https://sahasec.org/news/russia-s-everywhere-war-against-europe/>; Illimar Lepik von Wiren (2026) The Russian Federation's Sub-Threshold Warfare: An Emerging Threat for European Security. Master's Thesis, University of Tartu, <https://dspace.ut.ee/server/api/core/bitstreams/50757970-6c52-4f8e-9160-9e3e9935abbc/content>

⁸ Mario Baumann, Katri Pynnöniemi (2025) European Security in the Era of Hybrid Warfare. Policy Brief. DGAP; Eitvydas Bajarūnas (2025) The Hybrid Threat Imperative: Deterring Russia Before it is Too Late. CEPA.

⁹ Everycrsreport.com, "Kaliningrad: Background and U.S.-Russia Policy Considerations," <https://www.everycrsreport.com/reports/R46139.html>.

¹⁰ NATO, press conference transcript, 31 March 2022, <https://www.nato.int/en/news-and-events/events/transcripts/2022/03/31/press-conference>.

¹¹ IISS, "NATO and maritime security in the Baltic," Strategic Comments, August 2026, <https://www.iiss.org/publications/strategic-comments/2026/08/nato-and-maritime-security-in-the-baltic>

pressure and information operations.¹² Geography facilitates intelligence collection, border provocations, GNSS interference and airspace penetration, while the Kaliningrad exclave, the Russian mainland and Belarus provide multiple directions from which pressure can be applied. At the same time, the Baltic States are among Europe's strongest supporters of Ukraine and among the most vocal advocates of sanctions and a harder policy towards Moscow. Attacking them therefore serves both a regional and a wider strategic purpose.

The Baltic Sea is one of the most infrastructure-dense maritime spaces in the world, with a shallow, semi-enclosed basin. It carries the undersea power cables, gas pipelines and telecommunications links that physically connect Estonia, Latvia and Lithuania to the rest of the EU and to each other. Because the region is shallow, congested with shipping and relatively easy to survey, individual connectors are both easy to locate and hard to protect continuously.¹³

Several connectors carry outsized strategic weight. Balticconnector, the gas pipeline linking Finland and Estonia, and the EstLink and EE-S1 power and telecoms cables between Estonia and Finland, underpin Baltic energy security after the region has moved off the Russian-controlled BRELL power grid. The BCS East-West Interlink telecoms cable between Lithuania and Sweden, and C-Lion1 between Finland and Germany, carry much of the region's digital link to the rest of Europe. All have suffered damage or suspected sabotage since 2023 (see Section 1 below), most involving vessels linked to Russia's so-called "shadow fleet". NATO responded to these cases of sabotage by launching Operation Baltic Sentry, reinforcing naval and air patrols across the Baltic Sea specifically to deter and respond to attacks on undersea infrastructure.¹⁴

Most importantly, the Baltics are one of the geographical areas where Russia can test NATO itself. Estonia, Latvia and Lithuania are small frontline states whose defence depends not only on their own will and capacity to resist, but also on the credibility and speed of allied reinforcement. At the same time, as in the case of hybrid attacks on other EU and NATO countries, every sabotage operation, unexplained drone incursion or border incident does more than damage an immediate target – it tests readiness to attribute and deter, not just by the country in question, but also by NATO as a whole. Russia does not need to reconquer the Baltic States to benefit from targeting them. Persistent pressure can raise the costs of their Western orientation, intimidate their populations, interfere with support to Ukraine and probe how far Moscow can go without triggering a collective response.

¹² The 2023 Foreign Policy Concept of the Russian Federation, approved by Presidential Decree No. 229, 31 March 2023, <https://legalacts.ru/doc/ukaz-prezidenta-rf-ot-31032023-n-229-ob-utverzhdenii/>.

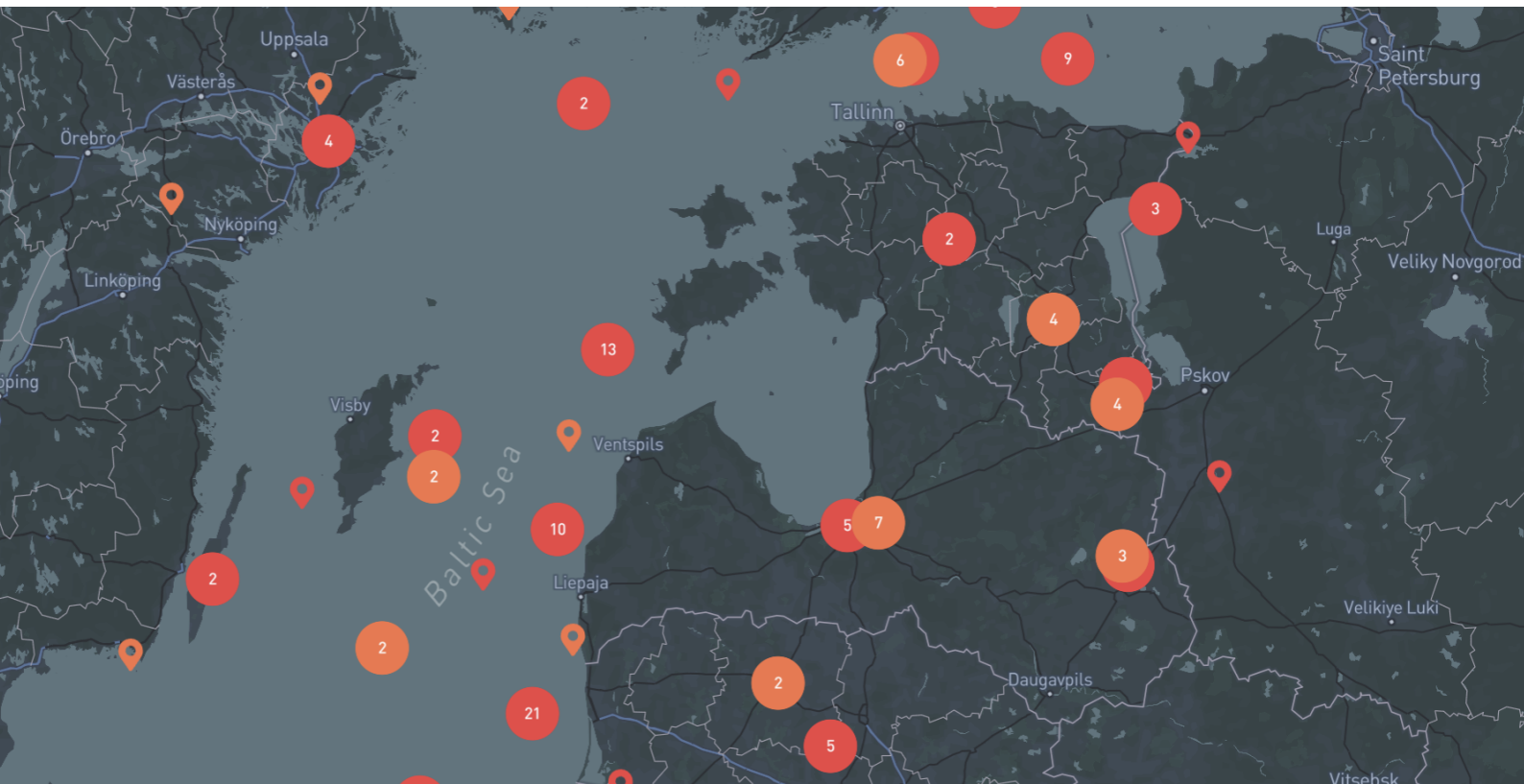
¹³ Filip Bryjka, Anna Maria Dyner and Aleksandra Kozioł, "White Paper on Russian Acts of Sabotage and Subversion against Members of the Council of the Baltic Sea States," Polish Institute of International Affairs (PISM), Warsaw, May 2026, <https://pism.pl/publications/white-paper-on-russian-acts-of-sabotage-and-subversion-against-members-of-the-council-of-the-baltic-sea-states>

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

1 Incident Overview by Year

This section presents the Baltic-specific incident record documented by the Everywhere War Tracker and corroborating open-source reporting for each year since the start of the full-scale invasion. Incidents are grouped by year to show how Russian activity against Lithuania, Latvia and Estonia has changed.

MAP OF RUSSIA'S SUB-THRESHOLD ATTACKS IN THE BALTIC REGION, 2022–2026

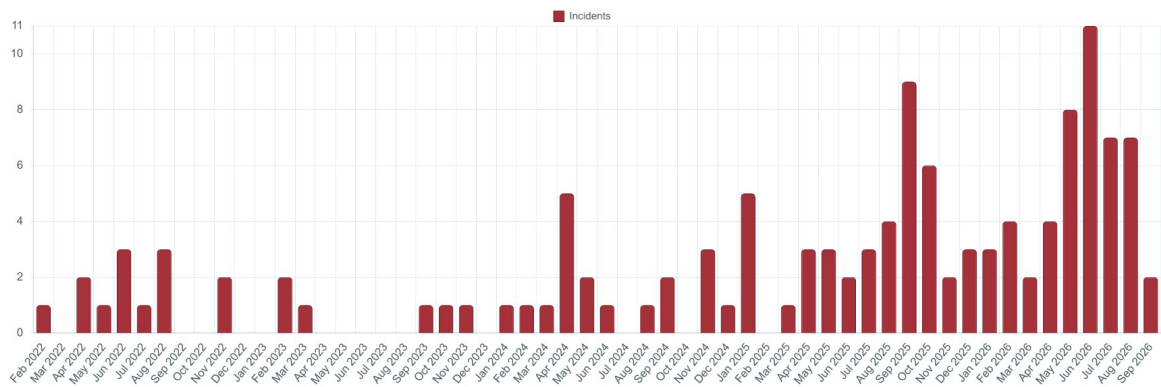


Source: *Everywhere War Tracker*

The Everywhere War Tracker records over a hundred incidents affecting Estonia, Latvia and Lithuania between January 2022 and September 2026, combining officially attributed cases with incidents that fit established patterns of Russian activity. It is important to note that because incidents affecting more than one state are counted under each, the country totals overlap.

The timeline shows a clear escalation since spring 2025, but the apparent 2026 peak requires qualification: military-aircraft incidents account for roughly four-fifths of the 2026 total, while all other incident types are on about the same level of intensity: 35 in 2025 and 20 in the first eight months of 2026.

TIMELINE OF RUSSIAN SUB-THRESHOLD ATTACKS ON BALTIC STATES (2022–2026)



Source: Everywhere War Tracker (sahasec.org/tracker). 126 incidents matched (officially attributed and fitting the pattern), 24 February 2022 – 24 September 2026, grouped by month.

The more significant underlying trend is the diversification of pressure in 2024–25. Cyber-attacks were recorded in every recorded year, while jamming and spoofing rose sharply in 2024–25. Drone incursions became a regular feature from 2025 on. Sabotage against critical infrastructure and economic targets appeared together in 2024, with a first recorded case against a military target in 2026. Maritime intrusions, concentrated in 2024–25.

The findings of the Polish Institute of International Affairs (PISM) in the *White Paper* shows that Russia increasingly relies on low-cost and expendable instruments – including digitally recruited “disposable agents,” shadow-fleet vessels, drones and inexpensive GNSS-jamming equipment – that minimise Moscow’s operational costs and exposure while forcing Baltic states to bear substantially higher costs of surveillance, interception, infrastructure protection and attribution.¹⁵

It should be noted, however, that attribution and reporting gaps leave the overall picture incomplete. Recording and attribution remain works in progress for governments, intelligence and security services, and researchers, meaning that the documented incident set should be treated as a conservative minimum rather than a comprehensive account of Russian activity.

The year-by-year analysis below focuses on the most consequential cases rather than reproducing the full incident record. It highlights episodes that best illustrate changes in Russian methods, targets, operational scale and escalation patterns across the Baltic states. Air policing and potential military threats like war rehearsal and forward military construction are not included into the following trend analysis but they still need to be mentioned separately.

Amid growing concern about a potential Russian attack on NATO’s eastern flank, Russia’s military preparations cannot be ignored. NATO itself is planning against this possibility. According to the Chair of the NATO Military Committee, Admiral Giuseppe Cavo Dragone, the Alliance now has around 4,000 pages of defence plans for its eastern flank, covering scenarios from a limited incursion to full activation of Article 5.¹⁶ The following exercises represent the most important Russian and Russia–Belarusian military drills affecting the Baltic states’ security environment since 2022. They are particularly relevant because they combine large-scale force mobilisation, rehearsals of operations in and around the Baltic Sea, activity in Kaliningrad and Belarus, and increasingly direct application of lessons from the war against Ukraine.

¹⁵ Filip Bryjka, Anna Maria Dyner, and Aleksandra Koziol, “White Paper on Russian Acts of Sabotage and Subversion against Members of the Council of the Baltic Sea States,” Polish Institute of International Affairs (PISM), May 29, 2026, <https://pism.pl/publications/white-paper-on-russian-acts-of-sabotage-and-subversion-against-members-of-the-council-of-the-baltic-sea-states>

¹⁶ Joint Threats (Europe/NATO) covers activity directed at European or NATO security collectively, with implications for individual member states—for example, war rehearsals or nuclear deployments intended to exert pressure across Europe. Cross-hatched areas in the graphs mark incidents affecting several countries. Each incident appears in the totals of the affected countries, while the overall total counts it once. Country totals can therefore add up to more than the number of distinct incidents recorded.

In June 2022, the Russian Baltic Fleet conducted missile and artillery drills shortly after Lithuania restricted the transit of sanctioned goods to Kaliningrad, giving the exercise a clear coercive-signalling dimension. In January–February 2023, Russia and Belarus held a joint air exercise using all Belarusian military airfields and rehearsing reconnaissance, border patrols, tactical landings and strikes against mock airfields, demonstrating the increasingly integrated military environment directly adjacent to Lithuania and Latvia. Later that year, Ocean Shield 2023 brought together more than 30 combat vessels, 20 support ships, 30 aircraft and around 6,000 personnel in the Baltic Sea, with more than 200 combat-training events focused on weapons employment, protection of sea lines, troop and cargo movement and coastal defence.

In 2024, Belarus conducted drills in the Grodno region directly bordering Lithuania and Poland, rehearsing territorial defence and operations under martial law. The same year, Ocean-2024, Russia's largest naval exercise since the Soviet period, involved more than 90,000 personnel, around 400 vessels and 125 aircraft across several theatres, including the Baltic Sea, where Baltic Fleet units practised anti-submarine and other combat operations. In 2025, July Storm extended this pattern, involving more than 150 vessels, 15,000 personnel and 120 aircraft across multiple seas and rehearsing long-range weapons employment, unmanned systems, anti-submarine warfare and attacks against enemy naval groups.

The most consequential land-oriented exercise for the Baltic region was Zapad-2025, conducted across Belarus, Kaliningrad and the Baltic Sea. Lithuanian intelligence assessed that around 30,000 personnel participated overall and highlighted the incorporation of lessons from the war in Ukraine, including extensive use of UAVs, electronic warfare, assault tactics and dispersed logistics.¹⁷ The pattern continued in June 2026, when Baltic Fleet units in and around Kaliningrad conducted exercises involving roughly ten aircraft and two missile ships practicing bombing, unguided rocket launches and missile strikes. Their timing, during NATO's BALTOPS exercise, made them particularly significant as a direct demonstration of Russian military activity alongside NATO's largest annual exercise in the Baltic region.

Other indications of a deteriorating security environment reflected in the Tracker include transfer of troops, nuclear and conventional weapons as well as forward military construction. In March 2026 Lithuania's intelligence service warned that Russia is expanding military units along NATO's borders and preparing for a possible wide-scale conflict with the alliance within six years, with an army 30 to 50 per cent larger than before the war and strategic reserves fully restored.¹⁸ Swedish intelligence puts the timeline at as little as a year.¹⁹ Satellite imagery reviewed by SVT shows at least five nuclear weapons facilities built or modernised near Europe, including the Kaliningrad storage site 270 km from Sweden, where Poland estimates some 100 tactical warheads are held, and the Soviet-era facility at Asipovichy in Belarus.²⁰ Russia is also building a major signals-intelligence complex in Kaliningrad that would allow it to monitor communications across the Baltic region, Poland and Germany.²¹

¹⁷ Giuseppe Cavo Dragone, "We Have 4,000 Pages of Plans for the Eastern Flank, Covering the Full Spectrum of Situations," Defence.Tech, September 21, 2026, <https://defence.tech/we-have-4000-pages-of-plans-for-the-eastern-flank-covering-the-full-spectrum-of-situations/>

¹⁸ State Security Department of the Republic of Lithuania and Second Investigation Department under the Ministry of National Defence, National Threat Assessment 2026 (Vilnius, 2026), section "During the Strategic Exercise Zapad 2025 Russia Applied Lessons Learned in Ukraine," <https://www.vsd.lt/en/reports/russia/during-the-strategic-exercise-zapad-2025-russia-applied-lessons-learned-in-ukraine/>

¹⁹ "Russia Massing Troops on NATO Borders for Potential Conflict Within Six Years, Lithuania Warns," UNITED24 Media, 6 March 2026, <https://united24media.com/latest-news/russia-massing-troops-on-nato-borders-for-potential-conflict-within-six-years-lithuania-warns-16590>, citing Reuters, 6 March 2026.

²⁰ Swedish Armed Forces, Military Intelligence and Security Service (MUST), MUST Annual Report 2025 (Stockholm, February 2026), 13, <https://www.forsvarsmakten.se/contentassets/22e980ab3d88466e80d81966fcd139b7/must-annual-report-2025.pdf>.

²¹ "Russia Modernizes at Least Five Nuclear Bases near Europe," Espresso Global, 16 June 2025, <https://global.espresso.tv/military-news-russia-modernizes-at-least-five-nuclear-bases-near-europe>, citing SVT and Planet Labs imagery.

RUSSIAN ATTACKS ON BALTIC STATES BY COUNTRY, YEAR AND CATEGORY (2022–2026)



126 incidents matched (officially attributed and fitting the pattern), 24 February 2022 – 24 September 2026, grouped by year.

Source: Everywhere War Tracker²²

2022 Major Baltic State Incidents

Russia's full-scale invasion was accompanied by an expansion of hostile activity into Europe, but in 2022 its sub-threshold campaign remained comparatively dispersed and less systematised than it would later become. Moscow was also absorbing the shock of its failed blitzkrieg and the collapse of assumptions that had underpinned the invasion, while the mass expulsion of Russian intelligence officers from European capitals disrupted established covert networks and forced the services to begin rebuilding them through more deniable channels. Sub-threshold activity was therefore already expanding, but much of it still appeared fragmented, opportunistic or difficult to distinguish from wartime spillover and conventional military signalling.

²² "Russia Builds Major Signals Intelligence Hub near NATO Borders in Kaliningrad," bne IntelliNews, 24 August 2025, <https://www.intellinews.com/russia-builds-major-signals-intelligence-hub-near-nato-borders-in-kaliningrad-397640/>.

The first year of the full-scale invasion saw the Baltic States absorb mostly coercive signalling, reconnaissance and cyber pressure rather than direct sabotage on their own soil. Kaliningrad functioned as the main lever. When Lithuania briefly restricted the rail transit of EU-sanctioned goods to the exclave in June 2022, Russia responded with a show of force, while Estonia bore the brunt of hacktivist cyber activity tied to the removal of Soviet-era monuments.

DATE	COUNTRY	TYPE	DESCRIPTION
27.06.2022	Lithuania	Cyber – Major Cyberattack	Pro-Russian hacktivist group Killnet claimed a DDoS attack on Lithuania, saying it had knocked out 1,652 web resources, and tied it to Lithuania's transit restrictions.
15.04.2022	Estonia	Cyber – Major Cyberattack	Pro-Russian hacktivist group Killnet defaced or DDoS'd the NATO Cooperative Cyber Defence Centre of Excellence website and several Estonian state e-services.
18.06.2022	Estonia	Airspace Violation – Aircraft	A Russian helicopter violated Estonian airspace, prompting an Estonian protest to Moscow.
09.08.2022	Estonia	Airspace Violation – Aircraft	A Russian Mi-8 helicopter violated Estonian airspace in the Koidula border region.
18.08.2022	Estonia	Cyber – Major Cyberattack	Coordinated cyberattack wave, triggered by the removal of Soviet-era war monuments, described by officials as Estonia's most extensive cyberattack since 2007; banking and government online services briefly disrupted.
11.08.2022	Latvia	Cyber – Major Cyberattack	Killnet targeted the website of the Saeima, Latvia's parliament, after it declared Russia a state sponsor of terrorism.
19.11.2022	Estonia	Cyber – Major Cyberattack.	The Eesti Energia website went down after a pro-Kremlin cyberattack.

Source: Everywhere War Tracker

2023 Major Baltic State Incidents

Russia's sub-threshold campaign was already expanding, but it had not yet acquired the tempo, geographic reach or operational confidence visible from 2024 onward. This allowed Western decision-makers to leave the problem out of public discussions.

Moscow continued rebuilding covert networks disrupted by the 2022 expulsions of intelligence officers, increasingly turning to remotely recruited proxies and deniable actors, while testing methods that would later become routine in sabotage and other covert operations. At the same time, the broader strategic environment still looked relatively favorable to the West: transatlantic cohesion appeared solid and Ukraine's counteroffensive was the center-focus. Thus, 2023 was less a year of full-scale sub-threshold warfare than one in which Russia was reconstituting the networks, methods and deniable infrastructure that enabled the much sharper escalation beginning in 2024.

In the Baltic region, in 2023, Russian pressure shifted from open signalling toward quieter reconnaissance and preparation. This year was marked by a new signals-intelligence hub in Kaliningrad, an airspace violation in Latvia, a cyberattack on Estonian public transport, and the first confirmed damage to a Baltic Sea pipeline.

DATE	COUNTRY	TYPE	DESCRIPTION
04.02.2023	Latvia	Cyber – Major Cyberattack	Pro-Russian hacker groups targeted Latvia's banking sector and the National Defence Academy.
20.09.2023	Estonia	Cyber – Major Cyberattack	A pro-Russian DDoS campaign knocked out Elron's train-ticketing service.
07.11.2023	Latvia	Airspace Violation – Aircraft	A Russian military aircraft violated Latvian airspace near the Russian border.

Source: Everywhere War Tracker

2024 Major Baltic State Incidents

By 2024, Russia's sub-threshold campaign had moved from adaptation to sustained expansion. This escalation unfolded amid growing political uncertainty across the West. US military assistance to Ukraine was delayed for months by congressional deadlock, while the presidential election campaign raised questions about the future direction of US support and transatlantic security policy. Europe was also entering a more unsettled political period, with the European Parliament elections strengthening nationalist and far-right parties and triggering a snap election in France. Against this backdrop, Russia had both a more developed covert toolkit and a more fragmented political environment in which to test European response thresholds, exploit divisions and impose costs while remaining below the level expected to trigger conventional retaliation.

2024 brought the first confirmed cases of GRU-linked sabotage on Baltic soil, the largest cyberattack recorded against Estonia, and two attacks on undersea cables. The year ended with the Eagle S incident, weeks before the Baltic States' planned disconnection from the Russian-controlled BRELL power grid.

DATE	COUNTRY	TYPE	DESCRIPTION
09.03.2024	Estonia	Cyber – Major Cyberattack	Estonian state institutions were hit by the largest cyberattack recorded against the country to date.
29.04.2024	Estonia	Cyber/EW – Jamming and Spoofing	Sustained GPS interference near eastern Finland and Estonia forced Finnair to suspend flights to Tartu Airport.
23.05.2024	Estonia	Potential Military Threat – Border/Sovereignty Provocation	Russian border guards removed 25 of 50 navigation buoys marking the Estonia–Russia border on the Narva River, on the night of 22–23 May 2024.
20.08.2024	Latvia	Cyber – Major Cyberattack	Cyberattacks hit Latvian public-sector websites, targeting shared state platforms and ministries.
07.09.2024	Latvia	Airspace – Drone Incursion	A Russian Shahed-type drone carrying explosives crashed in Latvia's Gaigalava parish.
13.02.2024	Lithuania	Cyber – Major Cyberattack	A pro-Russian cyber group targeted a Lithuanian military computer system.
09.05.2024	Lithuania	Sabotage – against Economic/ Industrial targets	Arson destroyed part of the IKEA store in Vilnius. Lithuanian prosecutors said Russia's military intelligence organised the attack; two young Ukrainian citizens were arrested and brought to trial.

DATE	COUNTRY	TYPE	DESCRIPTION
17.09.2024	Lithuania	Sabotage – Against Economic / Industrial targets	Six people were charged over a planned attack on TVC Solutions in Šiauliai, which makes mobile radio-spectrum analysis equipment for Ukraine's armed forces. Investigators said the plot was ordered by Russia's GRU.
11–12.11.2024	Lithuania	Airspace Violation – Aircraft	Russian Il-20 aircraft made two transits between mainland Russia and Kaliningrad through international airspace, logged as part of a wider wave of interceptions that week.
19.11.2024	Lithuania / Sweden	Sabotage – Against Critical Infrastructure	The BCS East-West Interlink undersea telecoms cable linking Lithuania and Sweden was severed, in the same window as damage to the Finland-Germany C-Lion1 cable further north.
25.12.2024	Estonia / Finland	Sabotage – Critical Infrastructure	The Russia-linked tanker Eagle S dragged its anchor across the Gulf of Finland, severing the EstLink2 power cable and four telecoms cables, weeks before the Baltic States' scheduled disconnection from the Russian-controlled BRELL power grid. NATO launched Operation Baltic Sentry in direct response.

Source: Everywhere War Tracker

2025 Major Baltic State Incidents

By 2025, Russia’s sub-threshold campaign benefited from several enabling conditions converging at once. The post-election shift in Washington created strategic uncertainty across the transatlantic relationship. The new US administration opened direct negotiations with Moscow without Ukraine or European allies at the table and temporarily suspended military assistance and intelligence sharing with Kyiv, while European governments were simultaneously reassessing the reliability and future extent of US security guarantees.

Operationally, Russia had by then largely recovered from the disruption of its traditional intelligence networks after 2022. Its services had developed a scalable model based on online recruitment of third-country nationals and disposable proxies, exploiting differences between national legal systems and the difficulty of attributing remotely directed operations. European responses remained fragmented and imposed insufficient costs on Moscow.

Europe’s slow recognition of emerging threats enabled by new technologies and tactics refined through Russia’s continued aggression against Ukraine created an additional vulnerability. The result was an increasingly favorable environment for sustained sub-threshold pressure: growing Russian operational capacity coincided with political uncertainty, persistent attribution gaps, technological asymmetries and a European deterrence architecture still struggling to translate individual incidents into predictable collective consequences.

The Tracker records 7 serious incidents affecting the Baltic States during 2025, concentrated in the second half of the year. This aligns with the broader European trend identified by the IISS, with incidents overall escalating in 2025.

DATE	COUNTRY	TYPE	DESCRIPTION
02.10.2025	Lithuania	Sabotage – Terrorism Plot	GRU-planned terror attacks; explosives in canned goods from a GRU cache in a Lithuanian cemetery
10.10.2025	Estonia	Potential Military Threat – Border/Sovereignty Provocation	~10 masked Russian soldiers appeared on Estonian road in Saatse Boot enclave
17.10.2025	Estonia	Airspace – Drone	Two UAVs near Camp Reedo military base; one shot down by allied forces
19.09.2025	Estonia	Airspace Violation – Aircraft	Three Russian MiG-31s deliberately entered Estonian airspace for 12 minutes, penetrating ~100 km inside sovereign territory [most severe single incident of the year]
23.10.2025	Lithuania	Airspace Violation – Aircraft	Two Russian military aircraft briefly entered Lithuanian airspace; described by President Nausėda as "the most serious incident in recent years"
17.12.2025	Estonia	Potential Military Threat – Border/Sovereignty Provocation	Three Russian border guards on a hovercraft entered Estonian territory along the Narva River
31.12.2025	Estonia/ Finland	Sabotage – Critical Infrastructure	Cargo vessel <i>Fitburg</i> detained for suspected deliberate anchor-dragging to sever undersea telecoms cables in Gulf of Finland

Source: Everywhere War Tracker

2026 Major Baltic State Incidents (January–September 2026)

By 2026, the strategy of “*deterrence by ignoring*” had exhausted itself. The frequency and audacity of Russian sabotage, drone incursions and other sub-threshold operations made the problem impossible to downplay. By the fifth year of Russia’s largest war of aggression in Europe since the Second World War, the threat had become so acute that gaps in government preparedness were themselves emerging as a security problem. The May 2026 drone incident in Latvia, where one UAV struck an oil-storage facility in Rēzekne and triggered a political crisis, exposed how limited response procedures could amplify the impact of a relatively small attack.

However, mainstream European discourse shifted, accompanied by expanding relevant institutions and protocols. At the same time, repeated US-led efforts to end the war had brought Moscow back into high-level diplomacy without producing a settlement, and demonstrating the Kremlin’s willingness to escalate in Europe despite paying higher costs as Ukraine expanded long-range strikes against military and energy infrastructure. Moscow continues to rely on political fragmentation, this and next year elections and social polarisation in Europe as strategic opportunities. The sub-threshold campaign thus became more openly aggressive.

Twelve serious incidents (plus routine BAP interceptions of Russian military aircraft) have been noted in the first six months of 2026 alone – surpassing the 2025 total, within half the time frame. The character of incidents has also shifted significantly, with an increase in drone incidents. But most importantly, drones with explosives in Leipzig airport have become a fat red line Russia has crossed.

INCIDENT SUMMARY — 2026 (JANUARY–SEPTEMBER)

DATE	COUNTRY	TYPE	DESCRIPTION
02.01.2026	Lithuania/ Latvia	Sabotage – Critical Infrastructure	Undersea optical cable Šventoji (LT)–Liepāja (LV) found deliberately damaged; criminal investigation opened
18.03.2026	Estonia	Airspace Violation – Aircraft	Russian Su-30 entered Estonian airspace near Vaindloo Island; Estonia summoned Russian chargé d'affaires
01.04.2026	Lithuania	Airspace – Drone Incursion	Multiple unidentified objects crossed from Kaliningrad into Lithuanian airspace
27.04.2026	Lithuania	Sabotage – Murder plot	Lithuanian law enforcement prevented planned murders and terrorist attacks in international operation
07.05.2026	Latvia	Airspace – Drone Incursion	Two drones crash on Latvian territory; one strikes oil storage facility in Rēzekne , causing fire and triggering Latvian government crisis
21.05.2026	Estonia/UK	Cyber – GPS Jamming	RAF aircraft carrying UK Defence Secretary GPS-jammed near Russian border on return from Estonia
17.04.2026 – 22.05.2026	Lithuania/ Latvia	Drone incident surges (6 distinct drone-incursion incidents apart from the Rēzekne incident, treated separately.)	Multiple Ukrainian drone intrusions attributed to Russian GPS jamming; Baltic joint statement called for NATO BAP upgrade to full air defence
24.06.2026	Estonia	Airspace violation – Aircrafts	Portuguese F-16s escort Russian Il-76, Il-78 and Il-20M near Baltic NATO airspace.
09.07.2026	Estonia	Potential military threats – Military Drills	Russia conducts the first unannounced live-fire exercise on Lake Peipus at the Estonian border.
08.07.2026 – 07.08.2026	Lithuania	Airspace violation – Aircrafts (11 distinct incidents of Russian aircrafts operating without transponder, flight plan or radio contact over the Baltic Sea.)	NATO intercepted multiple Russian aircrafts operating without transponders, flight plans or radio contact over the Baltic Sea.

Source: Everywhere War Tracker

In a wider perspective, since Russia's full-scale invasion of Ukraine, the Baltic region has faced a steady rise in both the number and frequency of sub-threshold incidents. The sharp acceleration from 2024 reflected the convergence of several factors: Russia had moved beyond the initial shock of the failed blitzkrieg, stabilised politically after the ritual voting in the 2024 presidential election, and concluded that society had absorbed the costs of war while the economy had adapted to a prolonged war of attrition. At the same time, U.S. domestic turmoil and the temporary halt in military aid to Ukraine exposed fractures in Western cohesion and signaled Europe's growing uncertainty over the durability of American security guarantees. Together, these developments created a more permissive environment for Moscow to intensify pressure on the Baltic region and test European resilience, response mechanisms and political resolve.

2 Key Trends — 2022 to 2026

2.1 Rising number and frequency of hybrid threat incidents

The number, frequency and diversity of incidents have increased steadily since 2022. The Tracker records over a hundred incidents between January 2022 and September 2026 across Estonia, Latvia and Lithuania, with hostile activity becoming effective monthly from March 2025 onward. The dataset includes not only major sub-threshold attacks analysed in details above such as cyber operations, sabotage, GNSS interference, drone and maritime incidents, but also intensified Baltic Air Policing activity and potential military threats such as major war rehearsals, force movements and forward military construction. These are important to factor in because they shape threat perception and provide the coercive military context for sub-threshold pressure, particularly amid increasingly explicit intelligence warnings that Russia could prepare for a direct or limited attack against NATO.

The apparent 2026 peak is driven largely by Russian military-aircraft activity, while the deeper trend is the persistence and diversification of pressure since 2024. Stripping out those routine intercepts and military drills, the serious-incident count still climbs on the same curve: seven serious incidents in 2025, and twelve in the first six months of 2026 alone. This matches the wider European picture. NATO's Secretary General Annual Report 2025 confirmed that Russia kept "testing the Alliance" with growing recklessness, including airspace violations and sabotage.²³

2.2 Shift from Reconnaissance and Sabotage to Airspace Provocations

The predominant types of incidents also changed over time. In 2022 and 2023, most activity was preparatory, such as cyberattacks, signalling around Kaliningrad, and reconnaissance of Baltic Sea infrastructure. In 2024, the focus moved to physical sabotage, including arson on logistics and commercial targets, a border provocation on the Narva River, and two attacks on undersea cables. By 2025, sabotage of critical infrastructure was still the single most common serious incident type. From 2026, airspace interceptions and violations became the largest category by far.

Airspace violations by Russian military aircraft have also grown sharply, reaching 40 reported incidents in the first half of 2026, against 14 for the whole of 2025. These are concentrated around the Kaliningrad-Lithuania corridor, where Russia has flown repeated transponder-off flights since January 2026. This pattern looks designed to normalise the provocation, with a sharp jump in April-May 2026. The October 2025 incursion by two Russian aircraft into Lithuanian airspace marked a clear break from the routine BAP escort pattern of earlier years.

2.3 Russia's new tactic – the spoofing of Ukrainian drones into Baltic territory

Perhaps the most strategically novel trend of 2026 is the Russian exploitation of Ukraine's long-range drone campaign. Ukrainian drones targeting Russian energy and military infrastructure in areas near the Baltic Sea are being deflected by Russian electronic warfare and jamming into

²³ Mark Rutte, The Secretary General's Annual Report 2025 (Brussels: NATO, 2026), 5, <https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/annual-reports/sgar25-en.pdf>

Baltic airspace, producing a pattern where Russia generates destabilising incidents in NATO territory while bearing no direct fingerprint.

This vector produced the most significant domestic political consequence of any hybrid incident in the Baltic States to date: after two drones crashed near an oil storage facility, the Latvian government coalition collapsed over its handling of the situation. The Rēzekne drone incident on 7 May 2026 triggered school closures across Rēzekne municipality and a NATO jet scramble²⁴. Russia immediately weaponised the incident narratively, issuing implicit military threats against Latvia and claiming intelligence that Ukraine had deployed drones from Latvian territory. Nordic and Baltic foreign affairs ministers have collectively rejected Russia's misleading framing of these events, affirming that "Russia and Belarus bear direct responsibility for drones threatening the lives of people on our Eastern flank."²⁵

2.4 Persistent Pressure on the Land Border with Belarus

Alongside the maritime and airspace track, Belarus-facilitated migration pressure on the Latvian and Lithuanian borders has run constantly since 2021. Latvia prevented 5,286 illegal crossings in 2022 and 5,388 in 2024, with pressure shifting to whichever segment of the border was least fortified at any given time.²⁶ Lithuania's numbers fell more sharply, from 11,211 prevented entries in 2022 to roughly 1,000-1,700 a year in 2024.²⁷ This is a sign the border protection has held, not that the pressure has stopped. Tactics have shifted from fence-climbing to digging tunnels, and Estonia has had to send extra border guards to reinforce Latvia's border as pressure built up again in 2026.

²⁴ BBC (2026) Latvian PM resigns after row over stray Ukrainian drones. <https://www.bbc.com/news/articles/cwy21k5917jo>

²⁵ Statement of the Ministers of Foreign Affairs of the Nordic - Baltic countries on Russia's latest disinformation campaign (May 2026). <https://www.government.se/statements/2026/05/statement-of-the-ministers-of-foreign-affairs-of-the-nordic--baltic-countries-on-russias-latest-disinformation-campaign/>

²⁶ The Baltic Times, 1 August 2024, "No persons detected attempting to illegally cross Latvia-Belarus border for tenth day in a row" https://www.baltictimes.com/no_persons_detected_attempting_to_illegally_cross_latvia-belarus_border_for_tenth_day_in_a_row/; State Border Guard, 1 January 2025, "December 31, 2024 at the state border and within the country", <https://www.rs.gov.lv/en/article/december-31-2024-state-border-and-within-country>

²⁷ Emma Wallis, 10 April 2026, "Lithuania: Operation launched after 30 migrants attempt to enter country from Belarus," InfoMigrants, <https://www.infomigrants.net/en/post/70841/lithuania-operation-launched-after-30-migrants-attempt-to-enter-country-from-belarus>

3 Russian Framing of its Aggression against the Baltics

Physical incidents do not tell the whole story. Alongside them runs a steady, non-kinetic campaign to shape political outcomes and public opinion, what Russian strategists now call "mental warfare."²⁸ The goal is not just to change what people think, but what narratives they identify with, priming audiences long before any specific influence operation launches.

The Baltic States are a priority target here. Estonia and Latvia have sizeable Russian-speaking minorities, and Moscow has long cast them as discriminated against. Russia's 2023 Foreign Policy Concept formally commits the state to defending "compatriots" abroad, which gives the Kremlin a ready-made script for political interference and information operations.²⁹ Russian-language media, social platforms and diaspora networks give Moscow a direct line into Baltic information spaces, although influence operations had to become more sophisticated after Lithuania, Latvia, and Estonia have each banned Russian state broadcasters and tightened the rules on platform accountability, reflecting a shared reading of the threat.

Since 2022, Russian influence operations have combined the old playbook, amplifying nationalist, populist and Eurosceptic voices with newer AI-enabled and platform-based tools. Across Europe, this has had mixed electoral results: pro-European candidates have generally won where Russian interference was most visible, as in the case of Moldova. But the stronger effect may lie elsewhere, in slowly shifting political agendas, wearing down institutional trust, and eroding public support for continued help to Ukraine. As some of Europe's most vocal advocates of a harder line on Moscow, the Baltic States are a natural target.

Recent information operations in 2026 included campaigns aimed at damaging the Baltic states' image in Western security perceptions by the Storm 1516 bot-account network linked to Russia's GRU, and Russian narrative-laundering through large-language models.³⁰

Russia's pressure on Estonia, Latvia and Lithuania is not simply a reaction to their support for Ukraine. The Baltic States occupy a particular place in Moscow's imperial imagination: they are seen as former Soviet republics that successfully escaped Russia's political, economic and security orbit and embedded themselves in the EU and NATO. Moscow has never fully reconciled itself to this loss. It continues to reject the Baltic interpretation of 1940 as Soviet occupation and annexation, while senior Russian figures increasingly speak about the region in openly revisionist terms. In 2023, former president and current Security Council deputy chairman Dmitry Medvedev referred to Estonia, Latvia and Lithuania as "our Baltic provinces."³¹

In June 2022, a United Russia deputy introduced a bill to revoke the Soviet recognition of Lithuania's independence, on the grounds that it had been granted illegally.³²

Putin's own historical narrative makes such statements more consequential. In June 2022, discussing Peter I's wars on the Baltic coast, Putin argued that the tsar had not conquered territory but had "returned" it, explicitly mentioning Narva, today an Estonian border city. He

²⁸ University of Jyväskylä, "From Information to Cognition: Mental Warfare from the Russian Perspective," JYU Reports 55 (2025), <https://jyx.jyu.fi/handle/123456789/102978>.

²⁹ The 2023 Foreign Policy Concept of the Russian Federation, approved by Presidential Decree No. 229, 31 March 2023, <https://legalacts.ru/doc/ukaz-prezidenta-rf-ot-31032023-n-229-ob-utverzhdenii/>.

³⁰ Jānis Sarts, head of NATO StratCom COE, on X: https://x.com/janis_sarts, 22 September.

³¹ Euronews, "Russia's Dmitry Medvedev claims Baltic countries belong to Russia," 17 May 2023, <https://www.euronews.com/2023/05/17/russias-dmitry-medvedev-claims-baltic-countries-belong-to-russia>.

³² Lietuvos Radijas ir Televizija (LRT), "Russia's Duma mulls revoking recognition of Lithuanian independence," June 2022, <https://www.lrt.lt/en/news-in-english/19/1714852/russia-s-duma-mulls-revoking-recognition-of-lithuanian-independence>.

then added that it had apparently fallen to contemporary Russia to “return and strengthen” territories as well.³³ This cannot be taken as evidence of an operational plan to annex the Baltic States, but demonstrates the ideological framework within which Moscow increasingly interprets borders. The Baltic States are therefore not ordinary European neighbours. Their very existence as prosperous EU and NATO member states contradicts the Kremlin's claim to a privileged sphere of influence over the former Soviet space.

³³ The Guardian, “Putin compares himself to Peter the Great in quest to ‘take back’ Russian lands,” 10 June 2022, <https://www.theguardian.com/world/2022/jun/10/putin-compares-himself-to-peter-the-great-in-quest-to-take-back-russian-lands>.

Conclusion and Recommendations

The trends identified in this brief confirm that Russia's sub-threshold attacks on the Baltic States have been growing since 2022, paralleled by information warfare, and by constant migration pressure from Belarus. Airspace incidents have escalated in 2026. The joint appeal by the Baltic States to NATO in May 2026 to transform Operation 'Baltic Air Policing' into a fully-fledged air defence mission reflects a growing realisation that the current system may prove insufficient for what lies ahead.

As Russia's aggression against Ukraine and Europe continues, the threat will grow with Baltic states being in Moscow's top target list. Russians are accumulating experience in sub-threshold operations while technological advances expand the range, precision and deniability of available methods. A future test of Article 5 need not resemble a full-scale invasion. NATO itself recognises that significant cyber or other hybrid attacks may amount to an armed attack on a case-by-case basis.³⁴ A coordinated operation combining cyber disruption, UAV and missile activity, maritime sabotage and cognitive operations could therefore probe Alliance cohesion across several domains simultaneously. The *Denied War* scenario explicitly explores this trajectory: a campaign designed to generate strategic effects while keeping attribution, intent and escalation sufficiently ambiguous to complicate a collective response.³⁵

01 Further strengthen cooperation among Baltic national-security agencies.

Estonia, Latvia and Lithuania should deepen intelligence sharing and data fusion, and boost cross-border investigative capacity in order to identify emerging patterns of drone activity, sabotage, proxy recruitment, and cyber-attacks. A standing Baltic anti-sabotage cell should link intelligence services, police, border guards, coast guards, customs authorities, transport regulators and critical-infrastructure operators.

02 Complete the shift from treating airspace violations as a monitoring issue to a deterrence approach.

NATO and EU states should establish clear common procedures for rapid attribution and public communication on hostile drone, missile, aircraft and GPS-interference incidents. Decisive deterrence posture in response to repeated violations should be framed as *protection* of allied territory and critical infrastructure—not as *escalation*.

03 Establish a graduated response framework for confirmed hostile activity at EU and NATO level.

Both EU and NATO have structures and/or officers coordinating response to hybrid threats (INTCEN Hybrid Fusion Cell in the EU, Special Coordinator for Hybrid Threats in NATO), but neither has a common graduated response framework endorsed by member states. It is crucial to reach an EU and/ or NATO agreement on a policy of proportionate

³⁴ Eitvydas Bajarūnas, "Using NATO's Article 5 Against Hybrid Attacks," Res Publica – The Center for Civil Resistance, February 12, 2025, <https://en.respublica.lt/using-nato-s-article-5-against-hybrid-attacks>

³⁵ Stanislav Boiko, Elena Davlikanova, and Lesia Ogryzko, *The Denied War: The Russian Grey-Zone Aggression against Europe and Its Unfolding Trajectory* (Kyiv: Sahaidachnyi Security Center, December 2025), https://sahasec.org/wp-content/uploads/2026/03/The-Denied-War_Stanislaw-Boiko.pdf

measures for sabotage, cyberattacks, drone incursions and attacks on critical infrastructure: coordinated attribution and deterrence measures, including, where lawful, active cyber posture. The purpose is to ensure that Moscow and its proxies face considerable operational costs. Where EU-wide or NATO-wide agreement is not possible, a defence-oriented coalition of the willing could be established among EU and NATO countries committed to deter sub-threshold attacks and impose costs on the state actors behind such attacks.

04 Make hybrid threats a permanent agenda item in defence cooperation among the EU states and Ukraine.

While Russia's sub-threshold warfare is Europe-wide, specifically airspace incursions, GNSS spoofing and jamming, weaponization of migration, and hostile maritime activity have a pronounced regional character across Europe's northern and eastern flanks. Deepening of cooperation should establish common warning indicators, common infrastructure-vulnerability assessments and rapid channels for exchanging operational information.

05 Build dedicated resilience against cognitive and electoral interference.

Given the Baltic States' exposure to Russian-language information operations, national and EU efforts should go beyond tracking physical incidents. They should systematically monitor election-period influence operations, coordinated and AI-amplified hostile information campaigns, and narrative-laundering through Russian-language media and large-language models.

06 Enhance analytical understanding of Russia's sub-threshold activities.

NATO, EU Hybrid Fusion Cell, Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats (HWP ERCHT) or the EU Hybrid Rapid Response Teams, should join forces to maintain a shared incident database combining verified government reporting with open-source monitoring, such as the Everywhere War Tracker. The system should identify geographic clusters, repeat target types, recruitment patterns, transport and logistics vulnerabilities, and links between physical attacks, drone incidents, cyber incidents and information operations. Ukrainian expertise should be integrated systematically into analysis, training and resilience planning.

About the Authors

Elena Davlikanova

Dr. Olena Davlikanova is a security and political analyst specialising in Russia's sub-threshold warfare against Europe, strategic foresight, and security policy. She is a Senior Fellow at the Sahaidachnyi Security Center and the Center for European Policy Analysis (CEPA), and a Research Fellow with the Department of War Studies at King's College London. She co-authored CEPA's *Containing Russia*, *Securing Europe* and contributed to the strategic foresight projects *Scenarios: Ukraine 2032* and *Scenarios: Russia 2032*. Her research focuses on Russian operational practices, European security, and the political and societal dimensions of Russia's aggression. She has published with the Atlantic Council, Jamestown Foundation, *The Moscow Times*, and other international outlets.

Marija Golubeva

Dr. Marija Golubeva is a security and governance expert specialising in European resilience, hybrid threats and crisis simulations. She is the founder of the Baltic Initiative on European Reform, a Distinguished Non-Resident Fellow at CEPA, and founder of the crisis-simulation platform Meleys. She served as Latvia's Minister of the Interior from 2021 to 2022 and previously as a Member of Parliament, including on the European Affairs and National Security committees. She holds a PhD in History from the University of Cambridge.

Polina Istomina

Polina Istomina is a UK-Ukraine Programs Specialist at the Sahaidachnyi Security Center, focusing on defence and security cooperation between the two countries. With experience in Silicon Valley and London across the technology and life sciences sectors, she has since 2022 concentrated on strengthening Ukraine's defence ecosystem, particularly miltech and emerging technologies. She supports and mentors defence-tech companies through platforms including Brave1. Polina holds an MBA from INSEAD and an undergraduate degree from Kyiv-Mohyla Academy.

Vlad Panov

Vladyslav Panov is a junior analyst specialising in security and defence policy, with a focus on defence-industrial cooperation, military modernisation, U.S. policy, and Russia's sub-threshold activities against Europe and NATO. He has worked with the Research Service of the Verkhovna Rada of Ukraine and the Reform Support Office of the Ministry of Defence. Vladyslav holds BA and MA degrees in Political Science from Taras Shevchenko National University of Kyiv.

Ilia Torkanievskyi

Ilia Torkanievskyi is an early-career professional specialising in European security, with a focus on disinformation policy, hybrid and sub-threshold threats, and energy security. He is the European Student Think Tank's Ambassador to Lithuania, where he has built the organisation's national network of students and researchers and produced policy-oriented analysis on regional security and disinformation issues. He previously worked with the Centre for the Study of Democracy, where he researched Foreign Information Manipulation and Interference (FIMI) and global disinformation trends.



Everywhere War Tracker

sahasec.org/tracker/

An OSINT-based monitoring tool documenting officially attributed and suspected Russian hostile activities against Europe since 2022.



Sahaidachnyi
Security Center



Serpens Center for
International Security

Produced with the support of the Prague Civil Society Centre.