

Ready for the Grey Zone? Assessing EU and NATO Response to Russian Hybrid Threats in the Baltics

28 OCTOBER 2026

Maksym Loharzhevskiy and Arianna Beretta



Photo by Waldemar Brandt on Unsplash

Introduction

In early October, Latvia's interior minister reported that masked men crossed from Belarus, disabled an electrical cabinet, and stole surveillance cameras before escaping (Meduza, 2026). Hours earlier, armed men on the Belarusian side threatened Latvian soldiers while pushing over twenty migrants across the border (Meduza, 2026).

Though minor, the intruders left before anyone arrived, and this episode exposed Latvia's response times. Such incidents are cheap, hard to attribute, and well below the threshold of collective defence. Supported by

Belarusian services operating alongside or independently of Moscow, they belong to a broader Russian-aligned hybrid campaign (Bryjka et al., 2026).

The core question is whether NATO and the EU can address pressure preceding conventional conflict. This article argues they handle the technical stages of a crisis better than the political ones.

Russian Hybrid Threats in the Baltics

Russia's toolbox is cumulative. Estonia's 2007 cyberattack remains the benchmark case (CCDCOE, n.d.-b). Jamming is widespread: Lithuania recorded a 22-fold annual increase in interference, while Estonia reported over 85 per cent of flights affected (ERR News, 2025; Hess, 2025). Between March 2022 and March 2026, interference occurred on roughly a thousand days in each Baltic state, mainly originating from Kaliningrad and Leningrad (Bryjka et al., 2026).

Sabotage is shifting toward physical attacks by proxies (Bryjka et al., 2026). Undersea cables represent a primary target, though establishing jurisdiction remains complex (Capacity Global, 2025). Airspace violations, such as Russian drones entering Poland and MiG-31s penetrating Estonian airspace, test NATO's resources and force Article 4 consultations (Szymański et al., 2025). Meanwhile, Belarus continues weaponising migration, forcing Lithuania to reclassify smuggling balloons as terrorism and declare an emergency (Dapkus, 2025).

Why the Baltics Are Vulnerable

Geography creates inherent vulnerabilities: Estonia and Latvia border Russia, Latvia and Lithuania border Belarus, and Lithuania is pinched between Belarus and Kaliningrad. The Suwałki corridor remains the only land connection to NATO allies (Chatzitheodorou, 2022). Were it closed, reinforcements would have to come by air and sea, the very approaches that jamming already degrades.

Small-scale incidents heavily strain local services, as size compounds geography. The three states are among Ukraine's most active supporters, which is the profile of countries PISM finds Russia has targeted most (Bryjka et al., 2026). Against this stand real strengths, among them capable national services and, since 2016, multinational NATO battalions on the ground (NATO, 2016).

Furthermore, society presents openings: ethnic Russians comprise roughly a quarter of Latvia's population and a fifth of Estonia's (Minority Rights Group International, 2018; Statistics Estonia, 2026). Highly digitalised services and newly westward-oriented energy links create further attack surfaces, prompting operations like NATO's Baltic Sentry (Szymański et al., 2025). Their security depends on decisions taken elsewhere, and hybrid ambiguity makes it hard to know when those decisions will come.

How to Assess Europe's Response

Asking whether NATO would defend the Baltics is too blunt a question for hybrid threats, which rarely resemble an armed attack. This article uses six stages, in the spirit of EU resilience policy, which speaks of preventing, responding to and recovering from hybrid attacks.

First, prevention: can deterrence, hardened infrastructure and resilience stop an attack or blunt it? Second, detection: does anyone notice quickly? Third, identification: can the perpetrator be named with enough confidence, and soon enough, to act on? Fourth, decision: does someone have the authority and the political will to agree to a response? Fifth, response: do proportionate tools exist, from diplomatic protests to military measures? Last, recovery: how fast are services and public trust restored?

The chain is only as strong as its weakest link. Excellent detection is of little use if attribution takes months, and without definitive attribution, coordinated prevention and response become far harder.

Who Does What?

Baltic national agencies are the first responders and handle attribution locally, as they deal with most hybrid incidents long before an alliance is involved, and naming the culprit is, as a rule, a national decision. NATO provides deterrence, potential Article 5 military responses, and operational monitoring like Eastern Sentry (NATO, 2016; Maślanka & Szymański, 2025). The EU supplies critical-infrastructure and cybersecurity rules, a hybrid toolbox, a dedicated sanctions regime for Russia's destabilising activities since October 2024, and the mutual-assistance clause of Article 42(7) TEU (Council of the EU, 2024; Deen et al., 2022).

Both organisations claim a stake in cables, energy networks and borders (Maślanka & Szymański, 2025), and the trouble lies in the overlaps. NATO has a process for judging an armed attack, but no agreed threshold, and how Article 42(7) fits alongside Article 5 remains unresolved (Deen et al., 2022). Intelligence sharing is a further gap: member states prefer bilateral exchange to sharing among all twenty-seven.

Possible Scenarios and Their Assessment

Scenario 1: Cyberattack and Disinformation

Suppose a major cyberattack takes down part of Latvia's or Estonia's power grid, while false claims blame the government and insist that NATO will not help. Estonia has lived with this threat since 2007, and recovery would rest on capable national agencies. NATO's Tallinn centre trains and researches but does not respond, since it sits outside the command structure (CCDCOE, n.d.-b). The weakness lies in the middle – attribution is a national task. NATO would probably stop at consultation, because the Article 5 threshold for cyberattacks is deliberately vague (CCDCOE, n.d.-

b). The Baltics could probably absorb the outage, but the political damage is the harder problem.

Scenario 2: Critical Infrastructure Sabotage

In November 2025, two incidents damaged the Warsaw-Lublin line, and Polish authorities identified suspects allegedly acting for Russian intelligence (Chancellery of the Prime Minister, 2025). A similar attack on Lithuania's railway network could disrupt civilian transport and delay military reinforcements. Prevention requires intelligence and infrastructure security, while national authorities and railway operators would handle detection and recovery. The harder question is attribution and response. Poland identified suspects through domestic investigations and allied cooperation, but tracing the operation to its organisers required further work. NATO could assess military mobility implications, while the EU could coordinate civilian support and consider sanctions. However, repairing the line leaves the network behind the attack intact. If organisers recruit new proxies across borders, another incident may occur before a coordinated response takes effect.

Scenario 3: Simultaneous Hybrid Attacks

NATO identifies sabotage, cyber activity and electronic interference among hybrid activities attributed to Russia (NATO, 2024). GPS interference could disrupt regional transport while a cyberattack targets energy operators and false claims blame Baltic governments. National agencies might detect incidents quickly, but determining whether they form one coordinated campaign would be harder. Intelligence sharing is crucial, as separate national assessments may miss connections. NATO could coordinate military awareness, while the EU could support civilian crisis management through its Hybrid Toolbox. However, simultaneous incidents may have different sources, and incorrect attribution could damage credibility. Recovery requires restoring essential services and countering disinformation. The main weakness is coordination: simultaneous disruptions could exploit delays in establishing a shared assessment and agreeing on a response.

Scenario 4: Limited Military Incursion

In October 2026, Vladimir Putin warned Russia would use all available weapons if it considered Kaliningrad under direct attack, accusing NATO of threatening the exclave (Kirby & Davies, 2026). This does not prove plans to invade a Baltic state, but shows how Moscow could frame confrontation as defensive. A limited incursion into Estonia, justified by claims of protecting Russian-speaking residents, would test this ambiguity. Border guards could detect armed personnel, but Estonia and its allies would need to establish events and operational direction. Estonia could respond nationally and request Article 4 consultations, as after Russian aircraft violated its airspace

in September 2025. NATO would assess whether the incident constituted an armed attack. Article 5 is not automatic; prolonged consultations could allow Russia to consolidate its temporary presence.

Where Are the Biggest Problems?

The scenarios show that Europe's main problem is agreeing on responses and leadership. In the railway sabotage scenario, Lithuania could identify the damage and restore services without being able to prove that Russia was behind it, complicating sanctions and allied coordination. NATO recognises that Russian hybrid operations use proxies, obscuring responsibility (NATO, 2024).

Simultaneous attacks could prevent national authorities, NATO and the EU from establishing a shared picture while essential services remain disrupted. A military incursion would create further pressure, as delayed decisions could allow Russian forces to consolidate their presence. Divided NATO-EU responsibilities and dependence on US military capabilities compound these weaknesses. Europe can manage individual incidents, but a coordinated campaign exploiting these vulnerabilities would be harder to contain.

Recommendations and Conclusion

The Baltic states, NATO and the EU should agree on responses to hybrid threats before a crisis. A response ladder could link suspicious sabotage to joint investigations and technical support, while stronger evidence could trigger coordinated diplomatic measures or sanctions.

Allies should assess incidents collectively, as seemingly unrelated attacks may form a wider campaign. A joint Baltic mechanism could compare evidence across countries and sectors, while a task force investigates networks financing and recruiting saboteurs. Governments could also take proportionate protective measures before Russian involvement is conclusively established, without making premature public accusations.

These steps would not stop every attack, but they would make it harder for Russia to exploit uncertainty and disagreements between allies. NATO and the EU have the tools to address many hybrid threats; the challenge is to use them quickly and together, while keeping responses proportionate enough to avoid unnecessary escalation.

References

Bryjka, F., Dyner, A. M., & Koziół, A. (2026, May). *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). <https://pism.pl/webroot/upload/files/Raport/White%20Paper%20on%20Russian%20Acts%20of%20Sabotage%20and%20Subversion%20against%20Members%20of%20the%20Council%20of%20the%20Baltic%20Sea%20States.pdf>

- Capacity Global (2025). Finnish court rejects charges over Baltic subsea cable damage. <https://capacityglobal.com/news/finnish-court-rejects-charges-over-baltic-subsea-cable-damage/>
- CCDCOE (n.d.-b). Cyber attacks and Article 5 – a note on a blurry but consistent position of NATO. <https://ccdcoe.org/incyber-articles/cyber-attacks-and-article-5-a-note-on-a-blurry-but-consistent-position-of-nato/>
- Chancellery of the Prime Minister (2025, November 18). PM Tusk in Parliament: Russia behind sabotage attacks in Poland. Gov.pl. <https://www.gov.pl/web/primeminister/pm-tusk-in-parliament-russia-behind-sabotage-attacks-in-poland>
- Chatzitheodorou, C. (2022). *Security at the Polish-Lithuanian border*. Finabel. <https://finabel.org/wp-content/uploads/2022/02/42.-security-at-the-polish-lithuanian-border.pdf>
- Council of the EU (2024). Council Decision (CFSP) 2024/2643 concerning restrictive measures in view of Russia's destabilising activities. <https://eur-lex.europa.eu/eli/dec/2024/2643/oj>
- Dapkus, L. (2025, December 2). Lithuania accuses Belarus of cynical hybrid attack as balloons disrupt airport. *Anchorage Daily News*. <https://www.adn.com/nation-world/2025/12/02/lithuania-accuses-belarus-of-cynical-hybrid-attack-as-balloons-disrupt-airport/>
- Deen, B., Zandee, D., & Stoetman, A. (2022). *Uncharted and uncomfortable in European defence: The EU's mutual assistance clause of Article 42(7) — Executive summary*. Clingendael Institute. <https://www.clingendael.org/pub/2022/uncharted-and-uncomfortable/executive-summary>
- ERR News (2025). Damage from Russia's GPS jamming amounts to over €500,000, Estonia says. <https://news.err.ee/1609759581/damage-from-russia-s-gps-jamming-amounts-to-over-500-000-estonia-says>
- Hess, A. (2025, September 2). *What can Europe do to better defend against GPS interference from Russia?* Euronews <https://euronews.com/my-europe/2025/09/02/what-can-europe-do-to-better-defend-against-gps-interference-from-russia>
- Kirby, P., & Davies, A. (2026, October 1). *Putin warns West that Russia is ready to use every weapon to protect Kaliningrad*. BBC News. <https://www.bbc.com/news/articles/cqg7k7v499jjo>
- Maślanka, L., & Szymański, P. (2025, February 28). *The resilience of the European Union and NATO in an era of multiple crises*. Centre for Eastern Studies. <https://osw.waw.pl/en/publikacje/osw-commentary/2025-02-28/resilience-european-union-and-nato-era-multiple-crises>
- Meduza (2026, October 7). *Latvian officials say armed masked men threatened troops while trying to push 20 migrants across from Belarus, then crossed into Latvia themselves and stole surveillance cameras*. <https://meduza.io/en/news/2026/10/07/latvian-officials-say-armed-masked-men-threatened-troops-while-trying-to-push-20-migrants-across-from-belarus-then-crossed-into-latvia-themselves-and-stole-surveillance-cameras>
- Minority Rights Group International. (2018, March). *Russians in Latvia*. <https://minorityrights.org/communities/russians-4/>
- NATO (2016, 9 July). *Warsaw Summit Communiqué*. <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/09/warsaw-summit-communication>

NATO (2024, 2 May). *Statement by the North Atlantic Council on recent Russian hybrid activities*. <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/05/02/statement-by-the-north-atlantic-council-on-recent-russian-hybrid-activities>

Statistics Estonia (2026). *There are people of 224 different ethnic nationalities living in Estonia*. <https://stat.ee/en/news/there-are-people-of-224-different-ethnic-nationalities-living-in-estonia>

Szymański, P., Chmielewski, B., & Menkiszak, M. (2025, September 22). *Russian fighter jets in Estonian airspace: A test of NATO's unity*. Centre for Eastern Studies <https://www.osw.waw.pl/en/publikacja/33454/pdf>

