Deterring the Undeterrable? NATO's Warfighting Focus and the Challenge of Russia's Hybrid Threats

Megi Benia

Introduction

Russia's full-scale war against Ukraine has accelerated NATO's return to territorial defence, high readiness force generation, regional planning, military mobility, and higher defence expenditure, thereby confirming that major interstate conflict in Europe can no longer be treated as a remote contingency. In this strategic environment, renewed emphasis on warfighting preparedness is not optional but necessary: the Alliance must remain capable of deterring and, if required, defeating conventional aggression by a revisionist power prepared to use force to achieve its strategic objectives. Yet the transformation of the Allied's military posture does not by itself resolve the wider challenge posed by Russian statecraft.

Alongside conventional force, Russia has repeatedly relied upon cyber operations, sabotage, political interference, disinformation, infrastructure disruption, covert influence activities, and other indirect destabilization measures which are deliberately calibrated to remain below the threshold of open war. These methods seek to weaken cohesion, erode confidence, exploit institutional vulnerabilities, and shape political outcomes, while reducing the likelihood of unified military retaliation. Such activities also seek to exploit political polarization, social fragmentation, and declining trust in democratic institutions within Allied societies, thereby weakening societal resilience and complicating collective political responses. In these circumstances, while NATO may become stronger at deterring overt attacks, it will remain insufficiently prepared for coercive competition conducted through deniable and sub-threshold means.

This article examines whether NATO's growing focus on warfighting readiness constitutes an adequate deterrence strategy against the broader spectrum of Russian hybrid threats. It argues that although conventional military power remains indispensable, it cannot serve as a complete answer to persistent peacetime coercion. Effective deterrence in the contemporary security environment requires a wider framework that combines credible military strength with three additional pillars: stronger societal and infrastructural resilience, faster collective attribution, and coordinated responses below the threshold of Article 5. Unless these domains receive strategic priority comparable to force posture and defence planning, the Alliance risks preparing effectively for the war Russia might openly wage while remaining less prepared for the coercion Russia is already conducting today across Europe.

NATO's Return to Warfighting and the Limits of Conventional Deterrence

NATO's strategic adaptation did not begin in 2022: Russia's invasion of Ukraine dramatically accelerated trends that were already visible following the illegal annexation of Crimea in 2014. By 2022, the Alliance had already initiated important adjustments through Enhanced Forward Presence, readiness initiatives, renewed deterrence concepts, and a gradual recognition that conventional defence could no longer be treated as secondary (NATO Allied Land Command, 2026; Latvia Ministry of Foreign Affairs, 2025). After February 2022, however, these measures expanded considerably. The Alliance reinforced multinational deployments along its Eastern Flank, approved new regional defence plans, restructured command arrangements, increased the scale of high readiness forces, and witnessed sustained growth in defence spending across much of the Allied community (Latvia Ministry of Foreign Affairs, 2025).

The NATO Secretary General's recent report demonstrates that the return to warfighting readiness is no longer an abstract strategic ambition, but an ongoing institutional transformation visible across force posture, planning, readiness, and capability development (NATO, 2025). The report highlights the implementation of new regional defence plans designed for large scale collective defence operations, the expansion of high readiness forces to substantially larger levels, and the reinforcement of forward-deployed multinational formations across the Eastern Flank: from battlegroup structures toward more robust brigade level arrangements where required (NATO, 2025).

The report further notes sustained increases in defence spending among Allies, accelerated procurement and defence industrial production, expanded stockpiles of key munitions, and greater emphasis on sustainment for prolonged operations. Additional changes include intensified multinational exercises, modernised command structures, improved military mobility for rapid reinforcement across Europe, stronger air and missile defence efforts, and deeper integration of national force planning within Alliance deterrence requirements (NATO, 2025).

Taken together, the report portrays an Alliance that has shifted decisively from a posture shaped by crisis management assumptions, toward one organised for high intensity collective defence against a peer adversary. The return to warfighting should therefore be understood not as militarised overreaction, but as overdue strategic correction. For too long, important segments of the European security community treated major war as improbable and conventional defence as an increasingly marginal requirement. Russia's actions have decisively invalidated those assumptions.

However, the effectiveness of conventional deterrence should not be overstated beyond its proper sphere. Conventional military power is optimised primarily to deter or defeat overt armed aggression. It is far less effective when an adversary deliberately adopts methods designed to avoid conventional confrontation (Rynning, 2024).

A forward-deployed brigade may deter territorial incursion, but it does not directly prevent malicious cyber activity against financial systems. Advanced artillery and air defence capabilities may strengthen battlefield deterrence, but they do not automatically expose covert sabotage networks operating through criminal intermediaries. Naval patrols can contribute meaningfully to maritime security, yet they remain only one component of protecting vulnerable subsea infrastructure and undersea communications networks (May, 2020).

As such, the dimension of signalling needs to be considered. Specifically, as NATO visibly strengthens its capacity for high intensity conflict, adversaries may adapt by relying more heavily on ambiguous, deniable, and indirect forms of coercion in areas where Allied military superiority is more difficult to convert into a timely political response: greater conventional strength can accidentally increase the utilization of alternative methods of pressure if non-military vulnerabilities remain insufficiently protected. Thus, the central issue is not whether NATO should prioritise warfighting, which it unquestionably should, but whether warfighting can serve as a complete deterrence strategy. And against Russia's broader coercive toolkit, the answer is clearly negative.

Understanding Russia's Hybrid Threats as a Persistent Form of Competition

Russia's challenge to Euro-Atlantic security should not be understood only through the lens of potential future conventional aggression. It is already visible in a sustained pattern of hostile conduct pursued during peacetime through instruments deliberately calibrated to remain below the threshold of open interstate war. These activities are more accurately described as hybrid threats, influence operations, indirect actions, and broader destabilization efforts rather than warfare in the strict sense, as their purpose is not necessarily the immediate defeat of an opponent through armed force, but the gradual weakening of political cohesion, institutional confidence, societal resilience, and strategic resolve. In practical terms, Russia has developed a persistent model of competition in which pressure is applied continuously across multiple domains to shape the security environment in its favour, while reducing the likelihood of unified military retaliation by NATO and other Western actors.

From 2018 to 2025, Russian activity against European members of the Alliance evolved from episodic covert incidents into a broader and more systematic campaign of destabilization activities directed at the physical, logistical, and psychological foundations of Allied security. According to the IISS assessment, this trajectory included sabotage against transport systems, energy assets, military facilities, undersea infrastructure, warehouses, and other strategically relevant objects whose importance derived less from symbolic value than from their role in sustaining mobility, supply chains, and societal continuity (Edwards & Seidenstein, 2025).

The pattern revealed a preference for numerous low to medium intensity incidents complicating attribution, diffusing investigative resources, and preserving escalation control while still

generating multidimensional strategic effect. Particularly notable was the increasing use of decentralized operational methods, including proxies, criminal intermediaries, temporary recruits, and covert networks able to execute burning, vandalism, reconnaissance, cable damage, and infrastructure interference without overt institutional fingerprints (Edwards & Seidenstein, 2025).

This tendency became increasingly visible in a series of incidents across Europe. In 2024, European intelligence services linked Russian operatives to parcel bomb plots targeting cargo and logistics networks across several European states, where incendiary devices hidden in parcels were reportedly intended to ignite during transportation in order to disrupt civilian supply chains and commercial infrastructure (Gonzalez, 2024).

Similar dynamics emerged in the Baltic Sea region, where the severing of two undersea telecommunications cables between Finland and Germany, and between Lithuania and Sweden, raised immediate concerns about sabotage and hybrid threat tactics. German Defence Minister Boris Pistorius stated that “nobody believes that these cables were cut accidentally,” while Finnish, Swedish, and Lithuanian officials connected the incidents to the broader security environment created by Russia’s war against Ukraine and the increasing threat of hostile hybrid activities targeting European critical infrastructure (Astier&Kirby, 2024).

The escalation of these activities became even more evident in Germany, where U.S. and German intelligence reportedly foiled a Russian plot to assassinate Armin Papperger, the CEO of Rheinmetall, one of Europe’s largest defence manufacturers supplying military assistance to Ukraine (Lillies et al., 2024). The alleged operation reflected an expansion from sabotage against infrastructure toward direct targeting of individuals associated with the European defence-industrial sector. Such methods allowed Russian actors to exploit legal and procedural vulnerabilities within open European societies while reducing the political costs associated with direct state involvement.

Over time, the geographical spread and sectoral diversity of incidents indicated that the objective was the formation of enduring insecurity, the demonstration of vulnerability within Allied territory, and the steady erosion of public confidence in the capacity of democratic states to protect critical systems (Edwards & Seidenstein, 2025).

Between September and December 2025, Russian pressure against European members of the Alliance displayed a calibrated pattern of coercive activity designed to generate insecurity below the threshold of open armed confrontation, while imposing persistent political, economic, and psychological costs on Allied societies. The most visible manifestations concerned repeated violations of European airspace and hostile interference with critical systems; developments that prompted the European Parliament to condemn Russian incursions, infrastructure targeting, and

broader hybrid threats as serious dangers to public safety and stability in Europe (European Parliament, 2025; European Parliament, 2025).

In late September 2025, heightened alarm followed reports linked to military activity near Poland during large-scale Russian aerial operations against Ukraine, reinforcing concerns that spill-over risks were no longer hypothetical, but were structurally rooted in the security environment of the Eastern Flank (Tanno et al., 2025).

These incidents were strategically significant not only because of their immediate military dimension, but because they tested surveillance systems, decision-making speed, escalation management, and political cohesion among exposed Allied states.

During the subsequent months, Russian activity increasingly relied on deniable and disruptive methods intended to erode normal societal functioning, while preserving ambiguity regarding attribution and proportional response. Across Europe, repeated drone sightings forced temporary closures of airports and disrupted civilian transport networks, illustrating how low-cost aerial tools could create disproportionate economic and psychological effects when directed at highly interconnected civilian infrastructure (Paternoster&Schumann, 2025).

Contemporary reporting also pointed to organized efforts involving operatives moving from the east into European states, reinforcing wider fears of clandestine networks capable of sabotage, reconnaissance, and covert tasking (Loginov, 2025; Jones, 2026).

By December, official European assessments had explicitly linked ongoing Russian hybrid conduct to cyber operations, information manipulation, espionage, and attempted sabotage, demonstrating that the threat spectrum extended far beyond isolated incidents, and reflected a multidomain campaign of attrition against Allied resilience (European Parliament, 2025; European Parliament, 2025).

Taken together, the period revealed a Russian preference for cumulative destabilization through synchronized pressure points rather than a singular large escalation, complicating deterrence and stretching the defensive attention span of the Alliance.

In strategic terms, the campaign illustrated how persistent hybrid threats, influence operations, and indirect actions conducted below the threshold of conventional war can impose substantial security burdens on the Alliance by forcing continuous vigilance, raising protection costs, and normalising a state of competitive pressure across the European theatre.

Importantly, this conclusion is no longer derived only from academic interpretation or policy commentary, but is increasingly reflected in the official threat perceptions of multiple Allied governments and intelligence institutions.

Germany’s 2026 Military Strategy document states that Russia is already conducting hostile hybrid activities against NATO member states, while simultaneously preparing conditions for a

possible future confrontation with the Alliance (German Federal Ministry of Defence, 2026). The same document further notes that espionage, sabotage, cyberattacks, and disinformation campaigns can no longer be treated as exceptional or peripheral developments, but have become enduring security challenges whose mitigation now constitutes a permanent task of defence and state preparedness (German Federal Ministry of Defence, 2026).

Comparable conclusions emerge from the public assessments of Baltic security institutions, whose proximity to Russia and long experience with coercive pressure give their analyses particular relevance. Estonia's 2026 security report warns that Russian sabotage and influence efforts remain active, while emphasizing that credible deterrence depends upon sustained preparedness, societal resilience, and the political will to resist pressure over time (Estonian Foreign Intelligence Service, 2026).

Lithuania's 2026 National Threat Assessment describes a security environment shaped not only by Russian military modernisation near NATO's eastern borders, but also by airspace violations, cyberattacks, hostile intelligence activity, and continuous information operations designed to spread insecurity and distrust (State Security Department of the Republic of Lithuania, 2026). It notes that even where the immediate conventional threat may remain limited in the short term, unconventional pressure continues and therefore requires constant vigilance, adaptive institutions, and close cooperation with Allies (State Security Department of the Republic of Lithuania, 2026).

Latvia's 2025 Annual Report of the State Security Service reaches similar conclusions, describing Russia as the highest threat to Latvian security, and documenting malign activities directed against military and civilian critical infrastructure, psychological operations, aggressive intelligence collection, and continuous attempts to identify vulnerabilities that could be exploited for destabilization (Latvian State Security Service, 2026). These assessments are important not because they use identical terminology, but because separate Allied states, operating from different national contexts, independently identify the same multidimensional pattern of Russian behaviour.

At the same time, the collective NATO level still appears to reflect a degree of conceptual underdevelopment in how this challenge is framed. NATO has for years relied on the terminology of "hybrid threats" as a central organising concept (NATO, 2026). Yet the 2025 Secretary General Annual Report introduces additional wording such as "destabilisation campaigns," alongside references to sabotage, cyberattacks, interference, and other hostile acts, rather than presenting a clearly consolidated conceptual framework (NATO, 2026).

The report recognises that Allies faced an increasing number of hybrid actions in 2025, but its evolving language may also suggest that the Alliance continues to describe the phenomenon through multiple overlapping labels rather than through a fully mature strategic concept. This

does not mean NATO ignores the challenge. On the contrary, it demonstrates growing awareness. However, compared with the sharper and more detailed threat assessments visible in several national strategies and intelligence reports, Allied national approaches often appear more precise in identifying methods, targets, and strategic intent than the collective language currently employed at the NATO level.

This conceptual ambiguity has also been accompanied by the absence of clearly articulated collective responsive measures capable of imposing visible strategic costs on Russia for malign activities conducted below the threshold of armed attack. Despite repeated incidents involving sabotage, cyber operations, disinformation campaigns, undersea infrastructure interference, and covert disruption activities across Allied territory, NATO responses have largely remained declaratory, defensive, and resilience-oriented rather than coercive or punitive (Associated Press, 2024). For example, following repeated incidents affecting Baltic undersea infrastructure and telecommunications cables, Allied reactions primarily focused on investigations, monitoring, and statements of concern rather than on publicly coordinated retaliatory measures or deterrence mechanisms directed at the perpetrators (Hoorman&Vincent, 2024).

Similarly, despite multiple Russia-linked cyber and sabotage incidents targeting logistics networks, defence industries, and transportation systems supporting Ukraine, NATO has not developed a visible collective framework outlining proportional countermeasures, attribution thresholds, or escalation consequences for persistent hybrid aggression below the Article 5 threshold (Greene et al., 2026).

The same pattern was observable after large-scale cyber operations, such as the SolarWinds compromise and other campaigns attributed to Russian actors (Greenberg, 2021), where responses remained fragmented across national jurisdictions and sanctions regimes rather than consolidated through a distinctly NATO-led deterrence posture. As a result, the Alliance has demonstrated increasing awareness of the hybrid threat environment, yet the gap between threat recognition and the establishment of predictable collective response mechanisms continues to raise questions regarding the credibility of deterrence between peace and armed conflict.

Strengthening Allied Deterrence beyond the Battlefield

For NATO, the central strategic implication is increasingly clear: Russian hybrid threats and indirect destabilization activities cannot be treated as peripheral disturbances existing alongside the challenge of conventional deterrence. Instead, they constitute a major arena of competition, precisely because they are designed to exploit the space between peace and open war, where traditional military superiority is least decisive.

Although the Alliance continues to strengthen force posture, readiness, reinforcement plans, and high intensity warfighting capabilities, these measures alone cannot close vulnerabilities that remain exposed to persistent coercion below the threshold of armed attack. The problem derives from the operational logic of the threat itself. Deniability delays attribution and complicates political consensus. Sub-threshold calibration creates uncertainty regarding proportional response.

Civilian systems are frequently more attractive targets than military formations because the disruption of energy networks, transport corridors, digital infrastructure, democratic institutions, and public confidence can generate strategic effects without immediate escalation. The continuous, rather than episodic, nature of such activity also risks fatigue, normalisation, and diversion of defensive attention over time. Effective deterrence must therefore extend beyond conventional force and address the mechanisms through which pressure is applied.

The first requirement is resilience as deterrence by denial. If hostile actors seek to expose fragility, then continuity planning, cybersecurity standards, and physical protection reduce the expected benefits of an attack. This applies equally to critical infrastructure, defence industrial supply chains, public administration, and societal preparedness.

The second requirement is faster attribution and shared awareness. NATO and Allied governments require standing mechanisms that connect intelligence services, cyber authorities, law enforcement institutions, and political leadership in real time. Public attribution, when supported by credible evidence, can impose reputational costs, strengthen societal awareness, and signal that anonymity will not guarantee impunity.

The third requirement is a scalable response architecture below Article 5. Coordinated sanctions, expulsions, cyber defensive assistance, maritime surveillance, counter sabotage cooperation, strategic communications, and targeted support for exposed sectors should form a predictable menu of consequences. In this context, closer NATO-EU coordination is indispensable, since many instruments of effective deterrence remain civilian, regulatory, and economic rather than purely military.

The Cost of Failing to Modernise Allied Deterrence

If NATO continues to strengthen conventional defence while underinvesting in deterrence against Russian hybrid threats and indirect destabilization activities, several long-term strategic risks are likely to deepen across the Euro-Atlantic area. The first is gradual strategic erosion, where repeated low intensity hostile acts weaken resilience, readiness, and institutional confidence, without generating the kind of dramatic crisis that would trigger a decisive collective response. In such circumstances, damage emerges gradually rather than catastrophically, but may prove no less consequential over time.

The second risk concerns deterrence credibility. If Allied societies observe persistent hostile behaviour that imposes visible costs, while producing only limited consequences for the perpetrator, confidence in the protective capacity of the Alliance may decline even as defence spending and military preparedness increase. A widening gap between declared resolve and observable outcomes would carry serious political implications.

Third, disparities among Allies may become more pronounced. States with stronger intelligence systems, civil preparedness structures, and resilient institutions will be better positioned to absorb pressure than those with weaker capacities, thereby increasing asymmetries of exposure and potentially generating internal friction regarding burden-sharing and priorities.

Fourth, democratic vulnerability may expand as hostile actors continue exploiting polarisation, manipulated information environments, and declining trust in public institutions to weaken cohesion from within.

Finally, the absence of established response frameworks may increase escalation dangers through either paralysis due to uncertainty, or disproportionate reaction under pressure, while an excessively narrow concentration on high-end warfighting risks leaving more frequently exploited civilian vulnerabilities insufficiently protected.

Conclusion

NATO's renewed emphasis on warfighting readiness is strategically justified and remains indispensable. The Alliance must retain the capacity to deter and, if necessary, defeat conventional aggression in Europe through credible force posture, readiness, defence planning, and sustained military modernisation. These are foundational requirements of contemporary security. Yet they are not sufficient on their own.

Russia has demonstrated a persistent willingness to compete through cyber operations, sabotage, disinformation, infrastructure disruption, and political coercion conducted below the threshold of open war. Such methods exploit ambiguity, target civilian systems, and seek cumulative strategic effects that conventional military power cannot reliably prevent or reverse on its own.

The central challenge for NATO is therefore not to choose between conventional defence and the deterrence of hybrid threats, but to integrate both within a coherent strategic framework. Effective deterrence now requires credible military strength combined with resilient societies, rapid attribution, and coordinated responses to persistent sub-threshold coercion. If NATO succeeds, it will be stronger across the full spectrum of competition and conflict.

Bibliography

Associated Press. *NATO Members 'Deeply Concerned' by Activities Such as Sabotage on Alliance Soil. They Blame Russia*. AP News, May 2, 2024. https://apnews.com/article/nato-russia-ukraine-war-73a3a226a6d036f8eafade7afca0ca5c

Astier, Henri, and Paul Kirby. *Germany Suspects Sabotage Behind Severed Undersea Cables*. BBC News, November 19, 2024. https://www.bbc.com/news/articles/c9dl4vxw501o

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

Estonian Foreign Intelligence Service. *International Security and Estonia 2026*. Tallinn: Estonian Foreign Intelligence Service, 2026. https://www.valisluureamet.ee/doc/raport/2026-en.pdf

European Parliament. *Call for a Unified EU Response to Russian Violations and Hybrid Warfare Threats*. News. October 3, 2025. https://www.europarl.europa.eu/news/en/press-room/20251003IPR30664/call-for-a-unified-eu-response-to-russian-violations-and-hybrid-warfare-threats

European Parliament. *Joint Motion for a Resolution on Russian Violations and Hybrid Warfare Threats against Europe*. RC-10-2025-0419. 2025. https://www.europarl.europa.eu/doceo/document/RC-10-2025-0419_EN.html

European Parliament. *Question for Oral Answer O-10-2025-000030 to the Commission on Russian Hybrid Threats.* 2025. https://www.europarl.europa.eu/doceo/document/O-10-2025-000030_EN.html

German Federal Ministry of Defence. *Verantwortung für Deutschland und Europa: Militärstrategie und Plan für die Bundeswehr*. Berlin: Bundesministerium der Verteidigung, 2026. https://www.bmvg.de/resource/blob/6093766/01b1718498c25db9010ea13724d7a37a/dl-gesamtkonzeption-der-militaerischen-download-deu-data.pdf

Gonzalez, Jenipher Camino. *Russia-Linked Group Planned Parcel Bomb Attacks in Europe*. Deutsche Welle (DW), September 17, 2025. https://www.dw.com/en/russia-linked-group-planned-parcel-bomb-attacks-in-europe/a-74033597

Greenberg, Andy. *US Sanctions on Russia Rewrite Cyberespionage's Rules*. *Wired*, April 15, 2021. www.wired.com/story/us-russia-sanctions-solarwinds-svr/

Greene, Sam; David Kagan, Mathieu Boulègue, Minna Ålander, and Douglas White. *War Without End: Deterring Russia's Shadow War*. Washington, DC: Center for European Policy Analysis

(CEPA), March 31, 2026. https://cepa.org/wp-content/uploads/2026/03/CEPA-Russia-Shadow-War-3.26.26.pdf

Hoorman, Chloé, and Elise Vincent. *How NATO Is Organizing to Protect Submarine Cables After Series of Incidents*. Le Monde, December 28, 2024. https://www.lemonde.fr/en/international/article/2024/12/28/how-nato-is-organizing-to-protect-submarine-cables-after-series-of-incidents_6736513_4.html

Jones, Sam. *Russia's Wagner Group Pivots to European Sabotage, Say Western Officials*. Financial Times. February 15, 2026. https://www.ft.com/content/dbd1d803-ab37-43f1-920f-fce74952313a?syn-25a6b1a6=1

Latvia Ministry of Foreign Affairs. *NATO Enhanced Forward Presence*. Last modified April 24, 2025. Accessed April 23, 2026. https://www.mfa.gov.lv/en/nato-enhanced-forward-presence

Latvian State Security Service (VDD). *Annual Report 2025*. Riga: VDD, February 2026. https://vdd.gov.lv/uploads/materials/42/en/annual-report-2025.pdf

Lillis, Katie Bo, Natasha Bertrand, and Frederik Pleitgen. *US and Germany Foiled Russian Plot to Assassinate CEO of Arms Manufacturer Sending Weapons to Ukraine*. *CNN*, July 12, 2024. https://edition.cnn.com/2024/07/11/politics/us-germany-foiled-russian-assassination-plot

Loginov, Vladimir. *They Came from the East*. Novaya Gazeta Europe, November 4, 2025. https://novayagazeta.eu/articles/2025/11/04/they-came-from-the-east-en

May, Andrew D. *The Future of Net Assessment*. In *Net Assessment and Military Strategy: Retrospective and Prospective Essays*, edited by Thomas G. Mahnken. Amherst, NY: Cambria Press, 2020.

NATO. *Secretary General Annual Report 2025*. Brussels: North Atlantic Treaty Organisation, 2026. Accessed April 23, 2026. https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/annual-reports/sgar25-en.pdf

NATO Allied Land Command. *Enhanced Forward Presence (eFP).* Accessed April 23, 2026. lc.nato.int/operations/enhanced-forward-presence-efp

North Atlantic Treaty Organization. *Countering Hybrid Threats*. Last modified January 29, 2026. https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats

Paternoster, Tamsin, and Noa Schumann. *Fact-Checking Europe's Drone Problem: Why Are Airports Shuttering over Drone Sightings?* Euronews, November 20, 2025. https://www.euronews.com/my-europe/2025/11/20/fact-checking-europes-drone-problem-why-are-airports-shuttering-over-drone-sightings

Rynning, Sten. *Comeback?: Classical NATO for a New Era*. In *NATO: From Cold War to Ukraine: A History of the World's Most Powerful Alliance*. New Haven: Yale University Press, 2024. https://doi.org/10.2307/jj.13110766.18

Tanno, Sophie, Antonia Mortensen, and Daria Tarasova-Markina. *Poland on Alert during Russian Aerial Assault on Ukraine.* CNN, September 20, 2025. https://edition.cnn.com/2025/09/20/europe/poland-russia-aerial-assault-ukraine-intl

State Security Department of the Republic of Lithuania and Second Investigation Department under the Ministry of National Defence. *National Threat Assessment 2026*. Vilnius: SSD and AOTD, 2026. https://kam.lt/wp-content/uploads/2026/03/2026-National-Threat-Assessment.pdf