

THE DETERRENCE GAP:

How can NATO protect its front line from Russia?

Agnia Grigas



Russia's full-scale invasion of Ukraine in February 2022 challenged much of the common Western understanding of Russia. How can the world better understand Russia? What are the steps forward for Western policy? The Eurasia Center's new "Russia Tomorrow" series seeks to reevaluate conceptions of Russia today and better prepare for its future tomorrow.

This report is written and published in accordance with the Atlantic Council Policy on Intellectual Independence. The authors are solely responsible for its analysis and recommendations. The Atlantic Council and its donors do not determine, nor do they necessarily endorse or advocate for, any of this report's conclusions.

Atlantic Council
1400 L Street NW, Suite 200
Washington, DC 20005

For more information, please visit
www.AtlanticCouncil.org.

ISBN: 978-1-61977-702-6

October 2026

Design: Donald Partyka and Amelie Chushko

Cover: Aleksander Cwalina, Donald Partyka, Amelie Chushko

Icons: Font Awesome

THE DETERRENCE GAP:

How can NATO protect its front line from Russia?

Agnia Grigas

TABLE OF CONTENTS

INTRODUCTION	2
RUSSIA'S THREATS AGAINST NATO'S EASTERN FLANK	4
RESPONSE MEASURES TAKEN BY THE BALTIC STATES, POLAND, AND ROMANIA	11
RECOMMENDATIONS	18
ABOUT THE AUTHOR	21

INTRODUCTION

➤ **T**hese are tense times for NATO's European frontline states. Russia's invasion of Ukraine is well into its fifth year. US President Donald Trump is **reducing** troop presence in Europe and questioning America's commitment to NATO, while the European powers are yet to take on full responsibility for their continent's security. And the war in the Middle East is consuming finite resources and diverting attention from other security topics.

In this challenging geopolitical environment, it is NATO's frontline states—especially Estonia, Latvia, Lithuania, Poland, and Romania that are the focus of this report and are feeling the Kremlin's threat most acutely. While Finland, Norway, and Turkey similarly share a maritime or land border with Russia, they do not share a Cold War history of being under Moscow's domination and are not targeted by Russia to the same extent. Russia regularly probes the Baltic states, Poland, and Romania—remaining below the threshold for invoking Article 5, but increasingly employing kinetic means, including drone incursions and sabotage to test their resolve and capacity to respond. This constant atmosphere of intimidation results in psychological pressure on populations, hampers investment, dampens economic outlook, and calls into question NATO's resolve to deter Russia and other hostile actors.

Geography is key when considering the range of Russian threats and, to a degree, the measures these five eastern flank countries can pursue. Estonia and Latvia share land borders with the Russian Federation proper; and both Lithuania and Poland border Russia's Kaliningrad exclave and Belarus. Moreover, as Ukraine's neighbors, Poland and Romania face the spillover effects—including drones and missiles—of Russia's war in Ukraine.

Land borders with Russia's de facto satellite state of Belarus constitute a direct military threat since Belarusian territory served as a launch pad for Russia's 2022 full-scale invasion and Belarusian and Russian intelligence services operate in close coordination. Romania borders its closest cultural and linguistic partner, the Republic of Moldova, where the unresolved, Russian-backed conflict in Transnistria poses **enduring security risks**.

This report examines Russia's military, cyber, economic, infrastructure, information, and espionage threats to NATO's eastern flank, and assesses the responses of Estonia, Latvia, Lithuania, Poland, and Romania. The threats discussed are illustrative rather than exhaustive: The report's scope does not permit a comprehensive account of Russia's continuing provocations and operations, and any such catalog would quickly be overtaken by new developments. Nonetheless, with NATO and EU support, as well as regional cooperation, these five frontline

states have developed defense strategies across four pillars: military deterrence and territorial defense; strategic communication and societal resilience; cyber defense and critical-infrastructure protection; and counterintelligence to safeguard democratic systems.

The study finds that while conventional military deterrence-building has advanced systematically, measures addressing Russia's hybrid tactics—particularly in cyber, infrastructure, and information domains—remain more fragmented, under-resourced, and unresolved. Overall, the current response measures do not inspire full societal confidence of frontline states in defense and deterrence capabilities. More significantly, NATO and national responses have largely been reactive and defensive: They have focused on detecting and countering individual provocations but have not built a record of effective deterrence by consistently dissuading Moscow from continuing or escalating them. The prevailing approach remains rooted in a peacetime framework, despite the reality that the frontline security environment increasingly occupies a “gray zone” between peace and war.

The final recommendations offer a critical assessment of the current deterrence record. They argue that frontline states bear a disproportionate and unsustainable burden for safeguarding NATO's eastern flank, strengthening societal resilience, and deterring Russian aggression and Belarusian involvement. These states therefore require enhanced and sustained support from NATO, the United States, and leading European powers to establish credible deterrence and deliver tangible responses—not merely observation and condemnations—to Russia's continuing kinetic and hybrid threats. This will require the political will to complement deterrence by denial, which strengthens Allied resilience and closes defensive gaps, with deterrence by punishment: imposing credible and proportionate costs for Russian provocations.

RUSSIA'S THREATS AGAINST NATO'S EASTERN FLANK



➤ **R**ussia's threats against NATO's eastern flank states are both implicit and explicit, with the former stemming from geography, geopolitics, and Russia's war in Ukraine and the latter involving Russia's specific operations targeting the five states. These operations can be summed up as the Kremlin's coordinated hybrid warfare campaign combining military, informational, cyber, and intelligence instruments and seeking to weaken frontline states and the alliance's resolve to deter Russia. NATO, the European Union, and most Western defense doctrines define hybrid warfare as the coordinated use of military and nonmilitary tools, applied below the threshold of open war, to coerce, destabilize, or weaken a state while maintaining plausible deniability. Over the years Russia had generally maintained its actions just below the Article 5 threshold, while ensuring they are constant enough to shape behavior, resource allocation, and political debate in frontline states. However, recent provocations—whether in drone incursions, infrastructure sabotage, or border violations—have kinetic components. These ambiguities both provide Moscow with deniability of aggression and likewise limit the responses the target states or their allies can or are willing to pursue. The second veil of ambiguity involves the ties between Putin's and Lukashenko's regimes and makes it difficult to disentangle the actions of Minsk from those of Moscow.

This section will examine four categories of Russia's threats with case country examples:

- 1. Military threats, coercions, and risks.**
- 2. Cyber operations and infrastructure sabotage.**
- 3. Information warfare.**
- 4. Espionage and covert operations.**

1. MILITARY THREATS, COERCIONS, AND RISKS

Russia's approach to the Baltic states, Poland, and Romania combines visible military pressure with calibrated kinetic actions designed to remain below the threshold of open war while shaping NATO decision-making. Military pressures have also reflected the region's strategic setting. Prior to the 2023 and 2024 accessions of Finland and Sweden to NATO, respectively, the Baltic Sea littoral states faced a more constrained operating environment and a greater prospect of Russian dominance at sea and in the air. Romania anchors NATO's Black Sea frontage and land access to Ukraine and Moldova, but it is exposed to Russian power projection via the Black Sea and occupied Ukrainian territories.

Russia launched a major force expansion even before 2022, and its military presence and operations near the NATO frontier is an ever-present regional threat. In 2024 Russia recreated the Leningrad Military District and rebuilt the 6th Combined Arms Army and associated corps for operations along NATO's northeastern flank. Forward-deployed Russian and Belarusian units near the Suwałki corridor (the narrow border between Poland and Lithuania linking the Baltics to the rest of NATO), Kaliningrad, and the borders of Poland and Lithuania are central to this posture: Kaliningrad hosts the 11th Army Corps and, since late 2025, an expanded 336th Guards Naval Infantry Division. In addition, large Russian-Belarusian exercises such as the Zapad-series routinely mobilize forces in the high tens of thousands across the Suwałki–Kaliningrad–Belarus triangle. Estimates **suggest** that Russia maintains roughly 40,000 ground forces in the wider Baltic theater but could mass up to about 100,000 troops in the region under the guise of exercises, drawing on multiple commands in western Russia.

Russian airspace violations and missile spillover are becoming alarmingly routine. During repeated Russian strikes on Ukraine, Romania has recorded at least eleven drone incursions into its airspace since 2022, including a drone that struck an apartment building in the eastern Romanian city of Galati on May 30, 2026, and **a Russian "Shahed" exploded in Moldova** on June 13, 2026. Poland has had to **scramble jets and temporarily close airports** in response to Russian drone swarms and missile penetrations (including cruise missile in July 2026). A drone entered Latvian airspace because of **Russian electronic warfare** in August 2026, and **another one** entered Lithuanian airspace in September 2026, prompting NATO fighter jets from Lithuania's Šiauliai Air Base to shoot it down. These incidents feed public anxiety and force costly readiness measures without crossing the point of an acknowledged "attack" on NATO soil. Belarus has also launched waves of surveillance balloons that have forced nearly routine temporary suspensions of operations at Vilnius airport, showing how low-cost, deniable tools can generate disproportionate disruption to Lithuanian civilian air traffic and regional security. Across the region, the number of Russian incursions into NATO airspace jumped to **eighteen cases** in 2025 alone.

This coercive signaling is reinforced by nuclear rhetoric and explicit demands to roll back NATO presence. Since 2022, Russian leaders have repeatedly paired threats of "consequences" for further NATO enlargement and new deployments with explicit references to nuclear capabilities in Kaliningrad, Belarus, and the wider Baltic Sea region. The Iskander-M systems in Kaliningrad have been upgraded and exercised in the Zapad-2025 drills, while Russian officials

reported deployment of tactical nuclear weapons and nuclear-capable Iskander and Su-25 systems to Belarus from 2023 onward, with Belarusian forces training for nuclear missions in 2023–2024 and announcing combat readiness in May 2024. As a result, Russian nuclear exercises and bomber patrols in the Baltic and over Belarus are perceived by allied strategists as **pressure on front-line states to limit host-nation support** and **responses to Russia's actions**. This view is reinforced by the Russian Foreign Ministry **draft treaty published in 2021**, which was essentially an ultimatum demanding an end to NATO enlargement coupled with an explicit threat to invade Ukraine, and a provision stating: NATO members “shall not deploy military forces or weaponry” in countries that joined the alliance after May 1997, which would include the Baltic states, Poland, and Romania, among others.

Russian transit routes via Lithuania to Kaliningrad are persistent security and political vulnerabilities for Vilnius. Since the EU–Russia transit arrangements of 2003 introduced facilitated rail and passenger transit between mainland Russia and Kaliningrad via Lithuania, Russian trains and cargoes have been carrying passengers and both civilian and sanctioned goods on this corridor. Since 2022, Lithuania has halted specific oil shipments to Kaliningrad under US–UK sanctions and has tightened controls after a Russian citizen jumped from a transit train in 2025, prompting interagency drills that rehearse responses to security incidents on these trains. Moscow's control over road and rail access to Kaliningrad gives it the ability to engineer crises over sanctions enforcement and cargo inspections.

The instrumentalization of irregular migration has become a further element of pressure. Since 2021 Belarus, with Russian support, has channeled migrants toward the Polish and Baltic borders, combining humanitarian pressure with recurrent border-security incidents and placing sustained demands on border guards, police, and armed forces. While pressure on the Polish and Lithuanian sections has eased, it has **intensified sharply** on Latvia's border and generated increased secondary movement into Lithuania. In July 2026, roughly twenty migrants entered Lithuania from Belarus through a cross-border tunnel and **attacked Lithuanian border guards** and attempted to pull an officer into Belarus.

Taken together, forward-deployed forces, kinetic airspace incidents, nuclear signaling, and pressure via transit and migration form a coherent strategy of military coercion that keeps the Baltic region, Poland, and Romania under constant stress while staying just below the formal thresholds that would trigger collective defense.

2. CYBER OPERATIONS AND INFRASTRUCTURE SABOTAGE

Russia uses cyber operations and infrastructure sabotage to keep the Baltic states, Poland, and Romania under persistent pressure while seeking to avoid open military confrontation and preserve plausible deniability. Probing and attacks against government, military, and commercial networks have become routine. Poland recorded nearly 273,000 handled cyber incidents in 2025, a 144 percent increase compared to the previous year, with **Polish officials identifying Russia as the source of the most serious threats**. The Baltic states and Romania likewise **remain exposed** to persistent Russian cyber and information operations

directed at state institutions, GPS interference, and threats to critical infrastructure in the Baltic and Black Sea regions.

These operations increasingly move beyond espionage to disruptive and sometimes destructive attacks. In December 2025, Poland suffered an **unprecedented cyber assault** on its energy system, targeting a combined heat-and-power plant serving nearly half a million residents and several renewable installations. In June 2022, Lithuania experienced **large-scale DDoS attacks** against government and private-sector websites, including its secure national data transfer network, by pro-Kremlin groups retaliating for Kaliningrad transit restrictions. Russian-linked actors intensified disruptions affecting **Baltic aviation and maritime safety** in 2024, while in Romania, cyberattacks and coordinated information operations targeted electoral and judicial institutions during the 2024 election cycle.

Cyberattacks are complemented by physical sabotage and prepositioning against infrastructure. Polish investigators linked the November 2025 sabotage of the Warsaw–Lublin railway—an important route for supplies to Ukraine—to **networks working with Russian intelligence**. Subsequently, Warsaw announced the deployment of up to 10,000 troops to protect critical infrastructure and transport networks. NATO launched its **Baltic Sentry** maritime-surveillance activity in January 2025 in response to a series of incidents damaging or threatening critical undersea energy and communications infrastructure in the Baltic Sea, including pipelines and fiber-optic cables. The combined result of these Russian operations is a sustained campaign that tests defenses, imposes economic costs, and signals that Moscow can disrupt critical services in frontline states without openly crossing into armed conflict.

Certain Russian-built infrastructure in the region has itself become a source of coercion. The Ostrovets nuclear power plant in Belarus, located close to the Lithuanian border and twenty-five miles from Vilnius, was **financed and constructed** with support of Russia’s Rosatom. It is not only a safety hazard but a potential hybrid threat that Moscow and Minsk can instrumentalize in crises or as a pretext for disinformation campaigns about nuclear accidents and emergency responses.

3. INFORMATION WARFARE AND PSYCHOLOGICAL PRESSURE

Russia’s information warfare against NATO frontline states relies on a dense mix of propaganda, historical revisionism, and targeted psychological pressure that has intensified since the fullscale invasion of Ukraine in 2022. Information warfare often instrumentalizes “Russian compatriots”—a loose Kremlin catch-all category of Russian speakers and other minorities residing abroad. Russia’s policy of “protecting compatriots” in neighboring states to seek influence, sow ethnic discord, launch military operations, and fuel separatism has been demonstrated in Moldova, Georgia, Ukraine, and beyond. Russian-language media ecosystems in Estonia, Latvia, and Lithuania, as well as online networks in Poland and Romania, are used to amplify such framing and present Moscow as the defender of a besieged “Russian world.”

In 2026, Moscow **announced plans** to take Lithuania, Latvia, and Estonia to the International Court of Justice, alleging systemic discrimination against Russian-speaking residents and invoking the United Nations Convention on the Elimination of All Forms of Racial Discrimination. The Baltic governments rejected the allegations as groundless propaganda. However, Estonia and Latvia each have a **sizable population** of Russian-speaking minorities that are a legacy of the Soviet occupation era. In recent years, Lithuania, Poland and—more modestly—Romania have experienced an increase in Russian-speaking migrant and refugee populations **from Ukraine**, Belarus, Russia, and from Central Asia.

A key line of Russia's effort is the exploitation of societal cleavages, including ethnic and religious tensions. Russian and pro-Kremlin information channels have long targeted Russian-speaking communities in Latvia and Estonia with false claims of systemic discrimination, "Russophobia," and even ethnic cleansing. Since Russia's full-scale invasion of Ukraine, **related campaigns** in Poland and Romania have portrayed Ukrainian refugees as criminals, an unfairly privileged group, or a burden on public resources, seeking to deepen social divisions and weaken public support for Ukraine. Antisemitic themes, documented in recent analyses of Kremlin cognitive warfare in both the Baltics and Romania, are woven into this mix: Pro-Kremlin commentators **have pushed** Holocaust-denying narratives and conversely conspiracy theories that cast Western and especially Baltic and Polish elites as "Nazis" or Nazi collaborators. The purpose is less to convince than to polarize—turning existing grievances over language, history, migration, minority rights, or identity into instruments of Russian influence. Russian and Belarusian intelligence services also **target refugees** fleeing persecution and diaspora communities from Belarus and Russia who have settled in Lithuania, Poland, and elsewhere, using intimidation, infiltration, online harassment, and assassination attempts to sow mistrust and fracture exile networks that support democratic opposition movements.

The Kremlin-linked outlets and diplomatic channels routinely recycle narratives depicting the Baltic governments and Poland as "Russophobic," fascist, or illegitimate, while denying Soviet occupation and the Molotov–Ribbentrop treaty legacy, a trend the European Parliament **formally condemned** in 2025 as posing a particular threat to the sovereignty of Poland and the Baltic states. In 2025, Russia's foreign-ministry-run MGIMO institute **published** a 400-page history of Lithuania—complete with a foreword by Foreign Minister Sergey Lavrov and financed by a state diaspora fund—which openly questions the existence of the Lithuanian language and statehood and portrays Lithuania as a Baltic-Slavic (and ultimately Russian) creation, signaling that the Kremlin is prepared to use pseudoacademic history as a tool to deny Lithuanian statehood and justify future pressure.

The main outcomes are the amplification of fear among the population and the erosion of trust in state institutions to protect citizens and manage crises. This also has an impact on the economy, as uncertainty and fear of Russian threats dampen foreign and domestic investment. This combination of narrative warfare and military and cyber threats keeps frontline societies in a state of constant psychological pressure.

4. ESPIONAGE AND COVERT INFLUENCE OPERATIONS

Russia, frequently acting in concert with Belarus, is conducting sustained espionage, sabotage, and covert-influence operations against NATO's eastern flank. These activities combine conventional intelligence collection with reconnaissance of military and critical infrastructure, attempted sabotage, and efforts to disrupt the logistics networks supporting Ukraine. Poland has dismantled multiple Russia-linked espionage and sabotage networks. In October 2025, Polish authorities said that fifty-five people had been detained in recent months on suspicion of acting for Russian intelligence; the allegations included reconnaissance of military facilities and critical infrastructure, preparation for sabotage, and direct attacks. A linked Polish-Romanian investigation concerned an **alleged plan** to transfer self-igniting or explosive parcels through Poland and Romania to Ukraine.

Latvia and Lithuania have reported separate espionage and covert-action cases. Latvia **detained** a citizen suspected of collecting information for Russian military intelligence on NATO forces, defense infrastructure, and aviation-related facilities. In April 2026, Lithuanian authorities **charged thirteen suspects** from several countries over an alleged GRU-directed plot to murder a Lithuanian pro-Ukraine activist and a Russian political exile in Vilnius.

Intelligence services also exploit proxies and influence networks through minority communities and economic ties. Investigations into “**amateur spy rings**” in Poland and the Baltics have highlighted the role of **paid spotters**—often students, truck drivers, or local entrepreneurs—recruited to photograph trains, warehouses, or energy facilities and to spread tailored narratives in Russian-language social media spaces. Russian and Belarusian operatives systematically approach Baltic citizens when they travel to Russia or Belarus to visit relatives, seeking kompromat and leverage for future recruitment; Baltic counterintelligence **now warns** such travelers that they are **high-risk targets for blackmail and pressure**. In parallel, Moscow and Minsk **export repression** against their own diasporas and refugees in Lithuania, Latvia, Poland, and Romania, using surveillance, cyber harassment, and threats to family members at home.

A newer line of concern is the acquisition of real estate near strategic sites through front companies or local intermediaries. Western intelligence reporting in 2024–2026 **has highlighted** how Russian entities have bought houses, warehouses, and land close to air bases, ports, and energy infrastructure across Northern Europe, prompting Finland, Latvia, and Estonia to **restrict property purchases** by Russian and Belarusian citizens. Although many of these properties are outside the immediate frontline area, officials in Estonia, Latvia, Lithuania, and Poland increasingly treat such holdings—whether cabins overlooking training grounds or small marinas near key sea lanes—as potential Trojan horses for signals collection, drone launches, safe houses, or sabotage staging in a crisis. The cumulative effect is a gray-zone environment in which ordinary travel, business, and real-estate transactions can be quietly repurposed for hostile intelligence activity, eroding the sense of security in frontline societies. The ultimate aims of these activities are often long-term penetration of political, military, and economic spheres of the countries.

Russia's campaign against the Baltic states, Poland, and Romania is multidomain, combining kinetic incidents, cyberattacks, espionage, and information warfare against the same targets. These tools are increasingly synchronized in time and space—for example, cyber and disinformation operations amplifying the impact of airspace violations, sabotage plots, or migration pressure. Most activities are deniable or ambiguous, from drone and missile “spillover” and proxy sabotage cells to front companies buying real estate near military sites, keeping them below the threshold for open retaliation. Yet they are clearly politically coercive, aiming to deter NATO reinforcement, undermine support for Ukraine, and question the sovereignty and historical legitimacy of frontline states. Above all, these operations increasingly have a kinetic component and are persistent rather than episodic, forming a continuous pressure campaign that normalizes a higher level of risk for the Baltics, Poland, and Romania.

RESPONSE MEASURES TAKEN BY THE BALTIC STATES, POLAND, AND ROMANIA



➤ **S**ince 2022, NATO's frontline states have faced a dual imperative: sustaining substantial material support for Ukraine while rapidly strengthening their own defenses against Russia. The Baltic states and Poland rank among Ukraine's most committed donors and NATO's **highest defense spenders** as a share of gross domestic product (GDP). This has made them leading advocates within both NATO and the EU for a stronger military posture and more credible deterrence, but it has also imposed burdens disproportionate to those borne by allies farther from Russia's borders.

For many political leaders and citizens in these states, however, the measures adopted still appear insufficient given their geographic exposure and the breadth of Russian threats. Persistent Russian activities in a gray zone between peace and war—from cyberattacks and sabotage to airspace violations, disinformation, and coercive pressure—have reinforced this sense of vulnerability. At the same time, the Alliance's caution over escalation and fear of provoking a wider confrontation with Russia have often produced an ambiguous response. The result is a continuing gap between the frontline states' threat perceptions and the level of deterrence they consider necessary.

1. MILITARY DETERRENCE AND TERRITORIAL DEFENSE

Frontline governments have responded to Russia's coercive military posture by seeking to turn the Baltic–Polish–Romanian arc into a layered deterrence zone rather than a vulnerability. By 2025, all five frontline states were spending well above NATO's 2 percent benchmark on defense, with Poland at roughly 4.3 percent of GDP, Lithuania and Latvia above 3.5 percent, Estonia around 3.3 percent and planning to move toward 5 percent, and Romania at about 2.5 percent and signaling a rise toward **3 percent**. NATO's multinational Forward Land Forces—battlegroups in Estonia, Latvia, Lithuania, Poland, and Romania—provide a standing allied presence on the eastern flank. The United Kingdom leads the multinational force in Estonia, Canada in Latvia, Germany in Lithuania, the United States in Poland, and France in Romania. Since 2022, this land presence has **been reinforced** by heightened air policing, air defense, and counterdrone measures; NATO's **Eastern Sentry**, launched in September 2025 following Russian drone

incursions into Polish airspace, adds multidomain assets designed to strengthen surveillance, air defense, and protection against drone threats.

All frontline states have been reorienting force planning to territorial defense. Poland is embarking on one of Europe's largest land-force modernizations and has launched the “**Eastern Shield**” (Tarcza Wschód) border-defense project to build a 700 to 800 kilometer system of bunkers, anti-vehicle barriers, sensors, and designated mine-laying zones along its borders with Belarus and Kaliningrad, explicitly designed to deny Russia a quick fait accompli. Launched in 2024, the three Baltic states' joint **Baltic Defense Line combines** anti-tank ditches, concrete “dragon's teeth,” bunkers, obstacle-storage sites, and preplanned wartime mining areas along their borders with Russia and Belarus; their **2025 withdrawal from the Ottawa Convention** restored the right to acquire, stockpile, and use anti-personnel mines in wartime, alongside anti-tank mines and other countermobility measures already permitted under the treaty. Romania **has intensified** Black Sea **mine countermeasures** and coastal-security planning after drifting mines were detected and neutralized near its coast beginning in 2022, including through the trilateral Romanian–Bulgarian–Turkish Mine Countermeasures Black Sea Task Group, which strengthens allied maritime security and interoperability on NATO's eastern flank. Technology and regional cooperation have become central to this defense posture. Poland and Romania are early adopters of the **US-made Merops counterdrone system**, deploying it under NATO's **Eastern Sentry** activity to detect, track, and intercept Shahed-type and other long-range UAVs, while the EU's 2025 European Drone Defense Initiative seeks to integrate surveillance and counterdrone capabilities across the eastern flank, from Finland to Romania.

Regional defense is increasingly organized through overlapping Nordic–Baltic, allied, and bilateral frameworks that augment national preparedness and NATO's posture. The Baltic states cooperate through the Baltic Defense Cooperation (B3) format—Estonia, Latvia and Lithuania—on military mobility, air defense, joint capability development, logistics and host-nation support, while all three participate in the UK-led Joint Expeditionary Force (JEF), a flexible high-readiness mechanism for regional contingencies in the Baltic Sea area. Bilateral initiatives reinforce this regional architecture: Lithuanian and Polish forces have affiliated the Iron Wolf and Polish 15th Mechanized Brigades with NATO's Multinational Division North-East, supporting shared planning, exercises, intelligence exchange and contingency preparation for the Suwałki corridor; the two countries are also considering a cross-border training area around Kapčiamiestis. Regional military exercises **have expanded**, including Estonia's **Spring Storm 2026**, involving more than 12,000 Estonian and allied troops, and Romania's Eastern Phoenix 26, where NATO forces tested a **layered counter-UAS architecture** integrating radars, acoustic and radio-frequency detectors, electronic-warfare systems, and kinetic and nonkinetic interceptors.

Ukraine's combat experience has become a key benchmark for frontline adaptation, particularly in developing affordable, scalable drone and counterdrone capabilities integrated with air defense, electronic warfare, sensors, resilient communications, and rapid procurement. A proposed structured **NB8–Ukraine security partnership would help** institutionalize this learning by linking Ukraine with the Nordic and Baltic states through defense-industrial cooperation, intelligence sharing, military exchanges, and deeper integration into European air-defense and counterdrone efforts. Estonia and Latvia have advanced cooperation

with Ukraine through exercises, testing and defense-industrial links; Poland and Romania are developing similar approaches, while Lithuania has identified **counter-UAS** as an urgent requirement but must still translate this priority into a layered, deployable capability at scale.

Eastern-flank states are also major beneficiaries of EU defense financing. Under the EU's **SAFE loan instrument**, Poland and Romania have been allocated about €60.4 billion (\$70 billion) combined to strengthen their armed forces, buy military equipment, and upgrade defense capabilities. The EU is thus becoming an increasingly consequential security actor on the eastern flank—not a substitute for NATO's military guarantee but an enabler **of the capabilities that make that guarantee credible**: defense-industrial capacity and joint procurement, military mobility, air and drone defense, cybersecurity, critical-infrastructure protection, and tools to counter hybrid coercion.

Taken together, these measures aim to ensure that Russian operations below the threshold of open war encounter prepared forces, prepositioned obstacles, resilient infrastructure, and agreed reinforcement plans. They are transforming NATO's eastern flank from a potential seam into a more integrated defensive front, designed to deny Russia a rapid fait accompli, raise the costs of escalation, and strengthen collective defense. Yet the posture remains largely reactive and defensive, limiting its ability to deter every form of Russian threat.

2. STRATEGIC COMMUNICATION AND SOCIETAL RESILIENCE

Russia's threats and information warfare have pushed frontline governments to view strategic communication and societal resilience as core security tasks. Since 2022, Estonia, Latvia, Lithuania, Poland, and Romania have **strengthened dedicated strategic-communications** capacities across their foreign and defense institutions, supporting rapid crisis messaging, countering Russian narratives, and explaining military posture to domestic audiences. NATO's **Eastern Sentry** enhanced-vigilance activity has been accompanied by public allied messaging that signals unity and resolve to both local populations and Moscow.

Counter disinformation and fact-checking capacities have become more institutionalized across the region. Estonia combines cooperation with civil-society initiatives such as Propastop with **media literacy education** in schools. Latvia treats protection of the information space as a **national-defense priority**, has restricted numerous Russian state channels, and in 2024 criminalized certain uses of deepfake technology to influence elections. Lithuania's **Debunk.org** monitors and exposes foreign information manipulation and supports media-literacy initiatives. In Poland, the Ministry of Foreign Affairs established a **Council for Resilience to International Disinformation** in 2024, alongside wider investment in cybersecurity and resilience. In Romania, policy debate **increasingly emphasizes** cognitive security, media literacy, and critical thinking as elements of resilience against hybrid threats.

Media-literacy and minority-integration efforts seek to undercut Moscow's exploitation of social fault lines. Baltic programs supported by EU and Nordic partners have engaged Russian-speaking residents through **community-based**

media-literacy initiatives and **Russian-language civic-information campaigns**, seeking to strengthen information resilience. Latvia and Estonia have supported locally produced public-interest media in Russian and other minority languages as credible alternatives to Kremlin-sponsored outlets, while also **tightening restrictions** on Russian state-controlled broadcasters and foreign-owned media deemed to pose security risks.

Yet the results remain uneven. Although restrictions have reduced the reach of Russian state broadcasters, Kremlin-aligned narratives continue to reach parts of Russian-speaking audiences in all three Baltic states through Russian-language social media, Telegram channels, proxy websites, and locally amplified content. These channels **often recast Moscow's themes**—especially alleged discrimination against Russian speakers, hostility to NATO, and criticism of support for Ukraine—as domestic grievances, making them harder to counter through broadcast restrictions alone.

Across the five countries, governments now fund permanent units for strategic communication, fact-checking, and civic-education programs and explicitly describe them in strategies and doctrines as components of national security and deterrence against foreign information operations. Nonetheless, government bureaucratic initiatives do not consistently translate to results on the ground or alter societal perceptions. The persistent perception of insecurity also shapes private citizen contingency planning. While the scale and form of such responses are difficult to measure, personal preparations may range from considering relocation or maintaining options abroad to postponing longer-term household or business commitments.

Despite Poland's major military buildup, **public confidence remains limited**: Only 31 percent of Poles believed Poland could defend itself effectively against a Russian attack, according to a September 2024 survey, while more than one-third said they would flee or seek refuge elsewhere if the country were attacked. In Lithuania, public polling in March 2024 found that about 70 percent of respondents regarded Russia as a **real threat to national security**. The three Baltic states have begun joint planning for potential **cross-border mass evacuations**. The central challenge, therefore, is not simply to inform societies about the threat, but to convert awareness and anxiety into confidence, practical preparedness, and the collective resolve required to sustain deterrence in a prolonged crisis.

3. CYBER DEFENSE AND CRITICAL INFRASTRUCTURE PROTECTION

Across the Baltic states, Poland, and Romania, cyber defense and critical-infrastructure protection have moved from niche technical issues to core national-security priorities. Poland's experience is emblematic: After recording around 270,000 cyberattacks in 2025 and suffering a **major assault** on its energy system (that hit a combined heat-and-power plant and more than thirty wind and solar facilities on December 29, 2025), Warsaw strengthened CERT Polska, launched detailed incident-response reporting for the energy sector, and accelerated work on a new Act on the National Cybersecurity System to tighten obligations on operators of essential services.

Estonia, Latvia, and Lithuania leverage their long-standing cyber expertise to anchor regional defense. Since 2008, Estonia hosts NATO's Cooperative Cyber Defense Centre of Excellence in Tallinn, which runs the annual Locked Shields exercise—now the world's largest live-fire cyber-defense drill—training NATO and partner teams to keep military bases and critical infrastructure running under thousands of simulated attacks. The Baltic states have strengthened national cybersecurity and critical-infrastructure frameworks, including cooperation among public authorities, grid operators, telecommunications providers, and financial institutions. A particular priority has been safeguarding the 2025 desynchronization from the Russia- and Belarus-linked BRELL system (an energy ring that had involved Belarus, Russia, Estonia, Latvia, and Lithuania) and the **integration of the three states' electricity grids** into the **Continental European network**.

Cooperation with NATO and the EU has deepened in parallel. Baltic and Polish authorities have been central to NATO and EU-led efforts to protect critical under-sea infrastructure in the Baltic Sea. In May 2025, the Baltic Sea states and the EU adopted a **cooperation framework** on the protection and resilience of undersea energy and communications infrastructure, following a series of incidents damaging: the Baltic connector gas pipeline in 2023; the C-Lion1 and Lithuania–Sweden telecommunications cables in November 2024; the Estlink 2 power interconnector in December 2024; and the Latvia–Sweden fiber-optic cable in January 2025. Romania has responded to heightened Black Sea security risks by making the protection of energy and telecommunications infrastructure a priority in its **2025–30 National Defense Strategy** and by deepening cooperation with Bulgaria, Turkey, and other regional partners. Its **2022–27 National Cybersecurity Strategy** strengthens protection of government, defense, and critical-sector networks through improved institutional coordination, public–private cooperation, and incident-response capacity, while EU-funded CYRESRANGE training develops cyber-defense skills for energy, transport, finance, and telecommunications operators.

Frontline states are also adapting for hybrid sabotage scenarios that blend physical and cyber threats. In February 2026, Lithuania held **national-level interagency exercises** to test responses to emergencies involving Russian transit trains traveling to Kaliningrad. EU-backed investment is **strengthening electricity interconnectors** in the Baltic states and Poland, while NATO's Baltic Sentry and the proposed **EU Black Sea Maritime Security Hub** are improving surveillance and protection of undersea infrastructure. These concrete steps—stronger agencies, joint exercises, hardened networks, and legal tools—aim to ensure that government services and core economic functions can continue operating even under sustained Russian cyber pressure and sabotage attempts. Yet these measures remain primarily reactive and defensive: they strengthen resilience and continuity, but do not consistently deter Russian probes or impose meaningful costs on further operations.

4. COUNTERINTELLIGENCE AND PROTECTION OF DEMOCRATIC SYSTEMS

Frontline governments have intensified counterintelligence and countersabotage efforts in response to Russia's hybrid operations. Poland is the clearest case: By late 2025, its Internal Security Agency had detained fifty-five people in overlapping investigations into suspected Russian intelligence activity, including reconnaissance of military facilities and critical infrastructure. **One Ukrainian national** was accused of collecting information in both Poland and Romania, while other suspects were linked to **surveillance and sabotage plots** targeting rail routes and military logistics. Polish prosecutors have since filed charges against at least one Russian national **alleged to have orchestrated a broader sabotage network**, illustrating a shift from merely disrupting plots to building court-ready cases.

The Baltic states have likewise moved aggressively against Russian intelligence. Latvia's State Security Service (or VDD) demonstrated its zero-tolerance approach through multiple 2025–2026 operations; in January 2026, it detained **four individuals** suspected of collecting intelligence for Russia through a pro-Kremlin Baltic anti-fascists network described by the VDD as a criminal organization; in a separate March case, the VDD referred four individuals for prosecution over allegedly **procuring and supplying satellite-internet equipment to the Russian armed forces**. In 2026, Latvia strengthened sanctions enforcement by implementing EU rules that **expanded criminal liability** for sanctions violations. Lithuania has sought to reduce the Russian intelligence footprint under diplomatic cover: Between 2018 and 2023 it expelled eleven Russian diplomats for activities “incompatible with diplomatic status,” including five after February 2022; in April 2022 the state closed the Russian consulate in Klaipėda and **ordered** Ambassador Alexei Isakov to leave. These steps, combined with similar expulsions by other EU states, have degraded Russia's legal-cover networks in the region.

Romania has taken parallel measures. Romania **arrested six citizens** in March 2025 for organizing a Russia-backed paramilitary group plotting to overthrow the constitutional order (prompting expulsion of the Russian defense attaché and deputy), thwarted a Russian sabotage operation targeting the Bucharest headquarters of Nova Post, a Ukrainian delivery company, in October 2025, and charged **two individuals** with Russian-directed sabotage in April 2026. These actions sit alongside tighter monitoring of foreign funding and influence channels, including scrutiny of opaque foundations, media portals, and “cultural centers” suspected of serving as Russian or Belarusian fronts.

Across the region, counterintelligence services now work more closely with electoral commissions, parliaments, universities, and critical industries to protect democratic systems and decision-making. Measures range from party-financing transparency to stronger oversight of foreign funding for nongovernmental organizations and media. Romania's 2024–25 presidential election crisis exposed the vulnerability of democratic processes to coordinated online manipulation, opaque campaign financing, and suspected foreign interference, widely linked to Russia. The Constitutional Court's annulment of the 2024 vote was an extraordinary step that protected electoral integrity, but its late timing and limited public explanation also fueled distrust and political polarization. The successful

2025 rerun nevertheless **demonstrated institutional resilience**, prompted stronger cooperation between security services and institutions, **while underscoring** the need for earlier and more transparent safeguards against digital interference. Together, expanded authorities, dismantled spy networks, stricter oversight of foreign influence, and high-profile expulsions aim to safeguard sovereignty and institutional integrity against Russian and Belarusian covert operations.

Baltic, Polish, and Romanian responses form a layered defense below the threshold of war. They have sharply increased defense spending, built the Baltic Defense Line and Poland's Eastern Shield, reinforced NATO's forward presence, and upgraded air, missile, and drone defenses. In parallel, governments have institutionalized strategic communication, fact-checking, and media-literacy programs, while protecting minority integration and electoral integrity. Cyber and infrastructure security have been strengthened through expanded CERTs, joint NATO–EU initiatives, and drills for hybrid sabotage. Finally, counterintelligence authorities, prosecutions, expulsions, and tighter control of foreign funding aim to disrupt Russian and Belarusian networks and safeguard democratic systems.

These are highly significant measures, yet they remain works in progress. Russian and Belarusian intelligence, cyber, information, and sabotage operations continue to expose gaps in readiness, coordination, resilience, and deterrence. Counterintelligence operations, prosecutions, diplomatic expulsions, and tighter controls on foreign funding can disrupt individual networks—but they have not ended the persistent pressure on these frontline states and their democratic institutions.

RECOMMENDATIONS



The coming years are unlikely to bring greater reassurance to NATO's frontline states about Russia's intentions or the military threat it poses. Recent US intelligence assessments indicate that Russia **could attack** NATO territory in the coming years, potentially through a limited incursion or other sub-threshold operations designed to test the Alliance's resolve. To date, neither NATO nor the EU and its frontline members have established a sufficiently credible record of deterring persistent Russian hybrid operations, which are increasingly accompanied by kinetic elements.

The Alliance should strengthen deterrence by punishment alongside deterrence by denial: It must persuade the Kremlin that hostile action will carry predictable, material costs and leave no doubt that NATO will respond to military provocations. Too often, political caution and escalation anxiety encourage allies to treat kinetic provocations as falling below the Article 5 threshold rather than as deliberate tests of allied resolve. Future drone incursions, attempted assassinations, sabotage, or comparable attacks on allied territory should prompt more than condemnation. Responses should be proportionate, coordinated, and preagreed, drawing on measures such as targeted sanctions; restrictions on travel, trade and transit (including on Belarusian train and road traffic); major expulsions (not limited to Russian officials); defensive and, where appropriate, legally authorized cyber measures; and strategic communications that expose and impose costs on the responsible actors.

If the current trajectory persists over the coming decade, Russia is likely to continue rebuilding conventional forces oriented toward the Baltic region and the Suwałki corridor while using drones, cyber operations, sabotage, and information warfare to probe NATO. Estonia, Latvia, Lithuania, Poland and Romania are increasingly planning for this "chronic crisis" rather than for a single, discrete invasion: their emerging defense concepts emphasize prepositioned obstacles, rapid reinforcement, integrated air and missile defense, cyber resilience, critical-infrastructure protection, and strategic communication.

These states nevertheless carry a disproportionate and increasingly unsustainable burden: They must secure NATO's eastern flank, build societal resilience, deter Russian and Belarusian coercion, and sustain support for Ukraine simultaneously. They therefore require predictable, long-term support from NATO and the EU. Europe must assume greater responsibility for its own defense, but sustained US engagement remains indispensable: As NATO's leading military power, the United States provides a central source of assurance for frontline governments and publics. Such support, however, cannot be limited to conventional capabilities and force presence; it must also address the persistent gray-zone pressures that shape daily security on the eastern flank.

The balance between high-end deterrence and everyday resilience remains uneven. Deterring conventional military formations is increasingly well resourced; however, countering persistent gray-zone pressure on critical infrastructure, minority communities, and the information environment remains fragmented and often dependent on small expert teams and short-term funding. The priority should be to institutionalize hybrid-threat defense through multiyear financing, clear lead agencies, and permanent capabilities—especially in cybersecurity, critical-infrastructure protection, and strategic communication. Hybrid defense must be treated not as a collection of ad hoc responses but as a standing mission, supported by dedicated budgets, professional career paths, intelligence integration and NATO-standard exercises. Deterring Russia's hybrid operations needs to emerge as a priority.

Social cohesion and information resilience are equally important components of durable deterrence. Frontline states must counter Russian information warfare and “compatriot” policies without alienating the very communities whose resilience is essential. They need long-term integration strategies that combine language learning and civic education with targeted information-resilience initiatives in Russian and Ukrainian. At the same time, intelligence and law-enforcement services should identify and disrupt Russian influence networks and intelligence activity in a targeted, evidence-based manner. The objective is to reduce vulnerability to manipulation while avoiding indiscriminate suspicion of Russian-speaking residents who are loyal citizens and contributors to national resilience.

Belarus remains a critical variable. Russian nuclear deployments in Belarus, together with Minsk's role in weaponized migration, airspace incidents, and information operations, make the Belarusian frontier both an acute security challenge and an area of inconsistent regional policy. Frontline states and NATO partners should develop a more coordinated posture toward the Lukashenko regime, which increasingly functions as a Russian proxy. This should include clearer red lines on airspace violations, sabotage, and transit incidents; closer alignment of sanctions and visa policies; and fewer opportunities for competition over Belarusian transit to undercut collective leverage. Operationally, borders with Belarus require stronger screening of cross-border movements, systematic vetting in sensitive sectors, and contingency plans for sudden, large-scale population movements that could conceal hostile actors.

All five states should treat support for Ukraine not as a separate theater but as part of forward defense. Training missions, defense-industrial cooperation, joint situational awareness, and structured lessons-learned mechanisms with Kyiv would enable them to absorb Russia's evolving tactics before they are deployed against NATO territory. Developing cost-effective, scalable, and layered counter-drone capabilities—integrated with air defense, electronic warfare, sensors, and resilient communications—should be a central priority.

Conscription or civic training could further strengthen deterrence while fostering civic responsibility, practical preparedness, and confidence in the state—areas that the Kremlin seeks to weaken. The Baltic states offer important examples: Estonia has retained conscription; Lithuania restored it in 2015 and is expanding annual intake; and Latvia reintroduced mandatory service in 2023. Poland and Romania, by contrast, rely primarily on professional forces, although Romania is expanding voluntary military training and its reserve force. Finland's broad pre-

paredness model, together with Israel's reserve-based approach, offers relevant lessons for frontline states.

Ultimately, the central task for frontline governments is to secure their citizens' confidence that their country can endure and be defended. Finland offers a useful model: Its comprehensive-security approach makes defense a whole-of-society responsibility, coordinating government, business, municipalities, civil society, and citizens to sustain essential functions through military, hybrid, and civil crises. With allied support, Estonia, Latvia, Lithuania, Poland, and Romania should build comparable total-defense systems that combine military readiness, civil preparedness, societal resilience, and credible public communication. Their ability to sustain this confidence will be decisive in a long contest in a persistently hostile neighborhood.

ABOUT THE AUTHOR



Agnia Grigas is a nonresident senior fellow at the Atlantic Council's Eurasia Center since 2015. She has advised US government institutions, multinational corporations, and academia. She is the author of three award-winning research books: *The New Geopolitics of Natural Gas*, *Beyond Crimea: The New Russian Empire*, and *The Politics of Energy and Memory Between the Baltic States and Russia*. She regularly provides commentary in US and international media.

Grigas holds a master's and a doctorate in international relations from the University of Oxford and a BA in economics and political science from Columbia University.



CHAIRMAN

*John F.W. Rogers

EXECUTIVE

CHAIRMAN EMERITUS

*James L. Jones

PRESIDENT AND CEO

*Frederick Kempe

EXECUTIVE VICE CHAIRS

*Adrienne Arsht

*Stephen J. Hadley

VICE CHAIRS

*Robert J. Abernethy

*Alexander V. Mirtchev

TREASURER

*George Lund

DIRECTORS

Stephen Achilles

Elliot Ackerman

*Gina F. Adams

Timothy D. Adams

*Michael Andersson

Ilker Baburoglu

Alain Bejjani

Colleen Bell

Peter J. Beshar

*Karan Bhatia

Stephen Biegun

Linden P. Blue

Brad Bondi

John Bonsell

Philip M. Breedlove

R. Nicholas Burns

Kurt M. Campbell

David L. Caplan

Samantha A. Carl-Yoder

*Teresa Carlson

*James E. Cartwright

Christopher Cavoli

John E. Chapoton

Ahmed Charai

Melanie Chen

Michael Chertoff

George Chopivsky

Wesley K. Clark

Kellyanne Conway

*Helima Croft

Ankit N. Desai

*Lawrence Di Rita

Dante A. Disparte

Denelle Dixon

*Paula J. Dobriansky

Joseph F. Dunford, Jr.

Joseph Durso

Richard Edelman

Stuart E. Eizenstat

Mark T. Esper

Christopher W.K. Fetzner

*Michael Fisch

Alan H. Fleischmann

Jendayi E. Frazer

*Meg Gentle

Thomas H. Glocer

John B. Goodman

Sherri W. Goodman

William E. Grayson

Marcel Grisnigt

Jarosław Grzesiak

Murathan Günel

Michael V. Hayden

*Robin Hayes

Tim Holt

*Karl V. Hopkins

Kay Bailey Hutchison

Ian Ihnatowycz

Keoki Jackson

Deborah Lee James

*Joa M. Johnson

*Safi Kalo

Karen Karniol-Tambour

*Andre Kelleners

John E. Klein

Ratko Knežević

C. Jeffrey Knittel

Joseph Konzelmann

Keith J. Krach

Franklin D. Kramer

Laura Lane

Almar Latour

Yann Le Pallec

Diane Leopold

Andrew J.P. Levy

Jan M. Lodai

Douglas Lute

Jane Holl Lute

Mark Machin

Marco Margheri

Michael Margolis

Chris Marlin

William Marron

Roger R. Martella Jr.

Judith A. Miller

Dariusz Mioduski

Richard Morningstar

Georgette Mosbacher

Majida Mourad

Mary Claire Murphy

Scott Nathan

*Julia Nesheiwat

Edward J. Newberry

Franco Nuschese

Robert O'Brien

*Ahmet M. Ören

Ana I. Palacio

*Kostas Pantazopoulos

David H. Petraeus

Elizabeth Frost Pierson

Radu Pițurlea

*Lisa Pollina

Daniel B. Poneman

Robert Portman

Dina H. Powell

McCormick

Michael Punke

Ashraf Qazi

Laura J. Richardson

*Gary Rieschel

Christiana Riley

Charles O. Rossotti

Harry Sachinis

C. Michael Scaparrotti

*Ivan A. Schlager

Rajiv Shah

Wendy R. Sherman

Gregg Sherrill

Kris Singh

Varun Sivaram

Walter Slocombe

Christopher Smith

Clifford M. Sobel

Michael S. Steele

Richard J.A. Steele

Mary Streett

Nader Tavakoli

*Frances F. Townsend

Melanne Verveer

Kemba Walden

Michael F. Walsh

*Peter Weinberg

Ronald Weiser

*Al Williams

Ben Wilson

Maciej Witucki

Neal S. Wolin

Tod D. Wolters

Jenny Wood

Alan Yang

Guang Yang

Mary C. Yates

Dov S. Zakheim

HONORARY DIRECTORS

James A. Baker, III

Robert M. Gates

James N. Mattis

Michael G. Mullen

Leon E. Panetta

William J. Perry

Condoleezza Rice

Horst Teltschik

**Executive Committee Members*

List as of July 13, 2026



The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

1400 L Street NW, Suite 200

Washington, DC 20005

(202) 778-4952

www.AtlanticCouncil.org