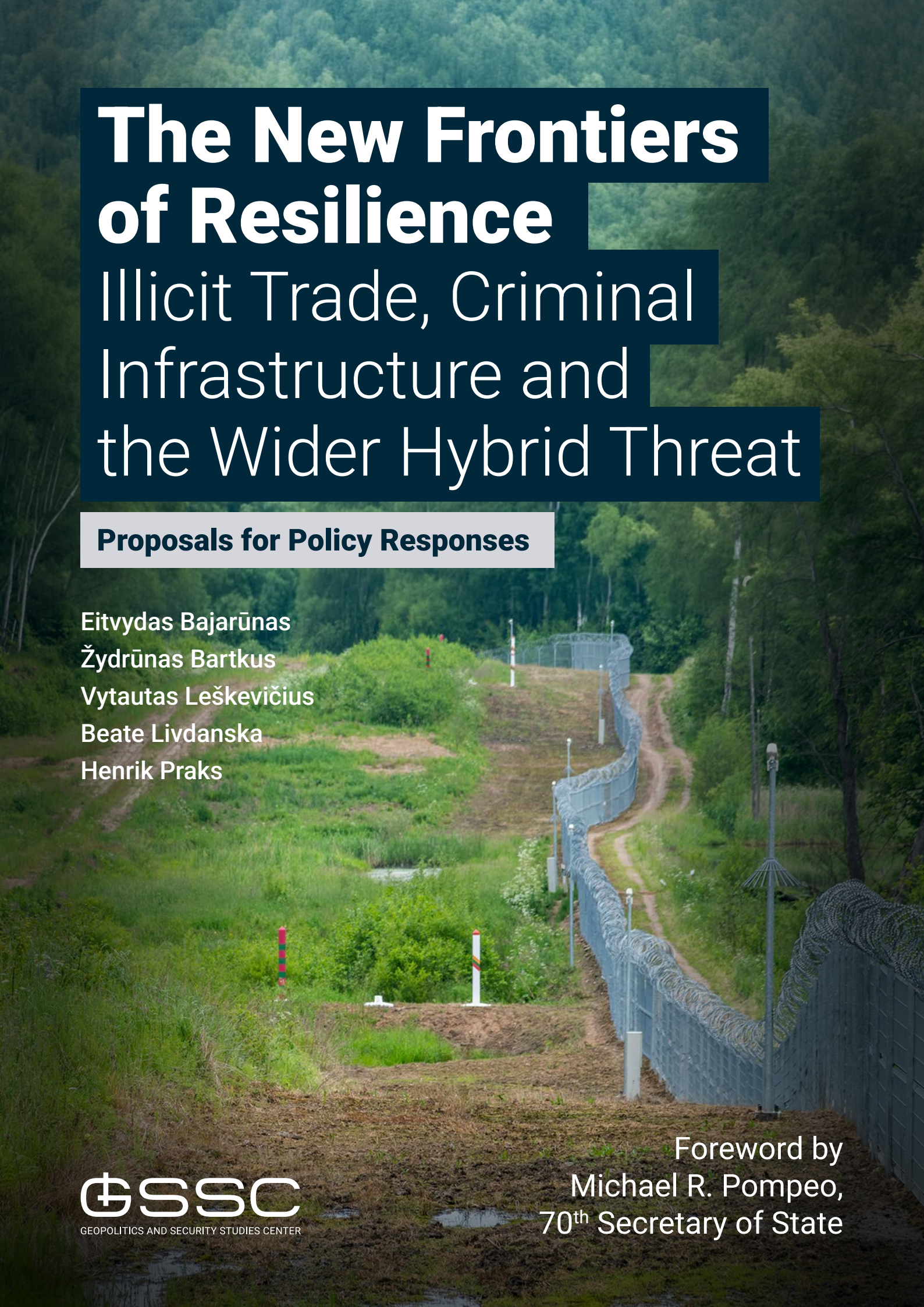




The New Frontiers of Resilience

Illicit Trade, Criminal Infrastructure and the Wider Hybrid Threat

Proposals for Policy Responses

Eitvydas Bajarūnas
Žydrūnas Bartkus
Vytautas Leškevičius
Beate Livdanska
Henrik Praks



In partnership with:



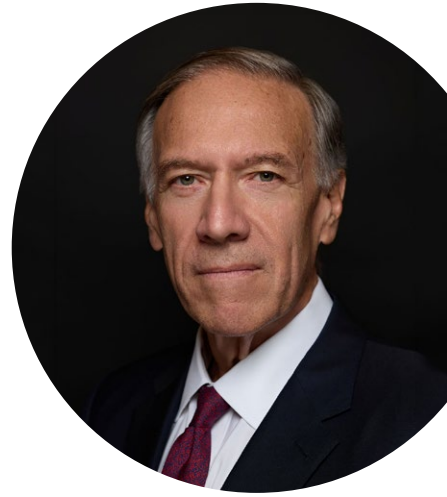
The study was commissioned by UAB Philip Morris Baltic.
The content of the study was not coordinated with UAB Philip Morris Baltic,
and UAB Philip Morris Baltic exercised no editorial control.



Table of Contents

Foreword to the New Frontiers of Resilience	4
Executive Summary	5
Introduction	7
A New Security Environment	7
Building on Existing Cooperation	7
Beyond Conventional Threats	8
From Illicit Trade to Criminal Infrastructure	9
The Transatlantic Dimension	10
1. Analytical Approach	11
2. The Security Environment	12
3. The Criminal-Hybrid Nexus	14
4. From Commodity to Capability	16
5. Resilience: Another Side of the Same Problem	19
6. Lithuania Case Study: How an Illicit Network Adapts	22
A Large Illicit Market	22
Public-private Partnership: from Exposure to Contribution	22
Weaponized Migration and the Hardening of the Land Border	23
From Land to Air	24
From Smuggling to a Wider Security Problem	26
7. Estonia: When Criminal Infrastructure Becomes an Intelligence Asset	27
Adaptation and Displacement	28
Sanctions Evasion: From Illicit Market to Strategic Effect	28
8. Latvia: Sanctions Evasion and the Displacement of Criminal Infrastructure	30
From a High-Risk Non-Resident Banking Model to a Different Risk Landscape	30
Sanctions Evasion as Service-Based Criminal Infrastructure	31
The TGR Group: a Latvia-Linked Transatlantic Financial-Network Case	32
Border Strengthening and the Engineering of Alternative Routes	32
The Latvian Lesson	33
9. From National Cases to a Baltic Network Picture	34
10. Why This Is a Transatlantic Issue	36
11. Policy Implications and Recommendations	39
Conclusion	41
Selected Sources	42

Foreword to the New Frontiers of Resilience



By Michael R. Pompeo, 70th Secretary of State

What does it look like when democracies inspire a more prosperous, safer, and freer world? America is one answer: from joining with our allies to defeat Nazism to directing initiatives like PEPFAR that have saved millions of lives. The formerly Soviet-occupied Baltics are another sterling example of democracy turning hard-won liberty into security, prosperity, and hope within—and beyond—their borders.

Estonia, Latvia, and Lithuania emerged from Soviet domination understanding that freedom is precious—neither inevitable nor free. Out of that conviction, they built vibrant democracies and market economies. They anchored their futures in the transatlantic community, becoming standard-bearers of post-Soviet democratic renewal and the only formerly Sovietized countries to join both NATO and the European Union.

While America is a comparatively young nation, Baltic peoples belong to some of Europe's oldest societies. Their restored republics are among its most compelling recent democratic achievements. America and the Baltic nations are different but share a common purpose with deep roots: to prove that free people—not tyrants—must determine the future.

Those ideas ground our alliance, and our alliance gives those ideas strength. Free nations acting in common cause possess both the moral clarity as

well as the material power to preserve peace. I saw those stakes in the Cold War as a young Army cavalry officer, leading patrols along the Iron Curtain. The line separating freedom from tyranny was never merely geographic. Nor was our alliance reducible to simply sharing resources or narrow calculations of national advantage. It was moral, sustained by free peoples who chose principled deterrence over retreat—and who understood that peace endures when aggression meets unity, united strength, and unbending resolve.

The lessons of World War II and the Cold War are urgent again. It is time to recommit to defending what grows from our common values. Russia's aggression offends the principle that free people and nations should choose their own path. If the free world permits force to redraw borders, every ally is less secure and every adversary emboldened. Our Baltic allies are keenly aware of this reality.

America must stand with the Baltic states—not as charity, but as strategy; not only because stability has value, but because the cause of free peoples is beyond calculation. Honoring our commitments strengthens NATO, protects American interests, safeguards Baltic sovereignty, and tells the world that free nations will not abandon one another. We stand together. Now we must act together.

A handwritten signature in black ink that reads "Michael Pompeo". The signature is stylized, with the first name "Michael" written in a cursive script and the last name "Pompeo" in a more formal, slightly cursive script.

Executive Summary

The distinction between criminality and hybrid threats is blurring. Not because everyday crime has become hybrid warfare overnight. But because the infrastructure that supports criminal activity can also offer capabilities to malign states and non-state actors.

This policy report analyses this intersection of threats, where criminal infrastructure – its pathways, logistics, finance, technology, enablers, access and operational know-how – meets the intent of malign states. Infrastructure is often built for profit. However, once it exists, it can be infiltrated, co-opted, redirected or exploited for strategic goals, particularly by hostile and non-democratic regimes.

This is the crucial distinction the report makes. Not all crime is a hybrid threat. Not all criminal networks are a state proxy. The question is when criminal infrastructure gains strategic-level importance, when hostile regimes use it for their political, military, strategic and economic purposes, and whether we have a system to identify that moment.

Therefore, the report proposes a simple analytical sequence to track the problem at hand: starting with an individual incident, tracing the network of actors and connections behind it, and then assessing whether it forms part of a wider pattern.

While an incident refers to what happened, the network shows how it became possible and repeatable. The wider pattern points to whether the capability matters beyond crime. Accordingly, the focus shifts from commodities to capabilities and from cases to supporting infrastructure, or, as we refer to it throughout the report, the criminal infrastructure.

The Baltic experience is a particularly strong test case demonstrating both the use of criminal networks by hostile neighbours and the adaptability of criminal infrastructure. Once the Baltic states had tightened control over their land borders, smuggling routes shifted, first to low-altitude airspace and then to tunnels and high-altitude meteorological balloons. Criminal mobility and knowledge of border environments have been leveraged for intelligence purposes,

while sanctions-evasion networks have brought together companies, professional intermediaries, digital finance and cross-border logistics. Although the methods vary, the underlying pattern is consistent: networks adapt, infrastructure persists and capabilities developed for one purpose can be repurposed for another.

Our allies and partners increasingly understand the reality faced by the Baltic states and are responding by strengthening our shared ability to confront the full spectrum of threats posed by hostile regimes and the networks they operate. Our geography and threat perception may differ, yet we share a common task and interest – to defend one billion people and preserve our countries and societies from all types of hostile interference, stemming from both hostile states and criminal networks.

The United States (US) and the Baltic countries of Estonia, Latvia and Lithuania face different border pressures, malign actors and geopolitical circumstances, yet they share the same ultimate goal: providing security for their people. However, this report does not assume the threats and challenges we face are the same. The relevant comparison is not between borders or commodities, but between networks. On both sides of the Atlantic, authorities confront transnational infrastructures that move goods and money across jurisdictions, use legitimate and illicit business structures, adapt technologies and routes, and exploit gaps between institutions.

Our different experiences are also complementary. The Baltic states are on NATO's border with Russia and Belarus, where criminal ecosystems overlap with sanctions circumvention, hostile intelligence activity and persistent hybrid pressure. The US, in turn, has considerable experience in tracing and disrupting complex transnational criminal ecosystems through financial intelligence, sanctions, export controls, asset recovery and robust enforcement capabilities.

The central conclusion of this report is not that 'a mere crime' should be relabeled as a hybrid threat. It is that criminal infrastructure should be seen in-

creasingly as a security issue. If the same routes, finance, companies, technologies, facilitators or access are repeatedly used for illicit trade, sanctions circumvention, intelligence activity or sabotage, the analytical threshold should be different. A law enforcement problem may also be a national security concern. This has immediate relevance for existing policy instruments. The solution is not another institutional framework. A large number of relevant tools already exist within border security, customs, law enforcement, financial intelligence, counterintelligence, sanctions enforcement, defense and resilience agencies and departments. It is the relationships between them, and what they seek, that must evolve.

Currently, approaches to this issue remain too incident-driven and institutionally stove-piped. A shipment is seized, a courier is arrested and a suspicious transaction is blocked or a company sanctioned. Each may be an operational success in and of itself. But none necessarily tells us whether the underlying network has been degraded. A seizure interrupts an incident, but network disruption removes capability. Therefore, the report calls for adapting existing mechanisms around various principles: build a shared picture of networks rather than separate national case files; systematically connect criminal and financial investigations with counterintelligence and national security analysis; track how networks adapt following enforcement pressure; establish clearer indicators for when criminal infrastructure requires national security scrutiny; and aim to measure success by capabilities dismantled, assets recovered and networks degraded, not just by the number of seizures and arrests.

It would also provide a workable agenda for Baltic–US cooperation in this regard. An important foundation already exists. Over three decades of National Guard partnerships, Proliferation Security Initiative cooperation, and the US-backed Nuclear Security Centre of Excellence in Lithuania have already shown how intelligence, border security, law enforcement, defense, specialized detection and international cooperation can be networked around a shared threat. The challenge is to extend that logic to a security landscape where the enabling infrastructure itself becomes increasingly important.

The wider point is resilience. NATO and its Allies have understandably focused on strengthening critical infrastructure that the defense of countries and their societies relies upon. The next logical step is to view resilience from the other side as well: what pre-existing infrastructure can an adversary exploit against us? Criminal networks can offer routes, finance, technology, access, local knowledge and expendable manpower that a hostile actor would otherwise have to develop from scratch. Protecting our infrastructure will remain important, but finding and degrading our enemies' infrastructure is also becoming a resilience issue.

Introduction

A New Security Environment

Following Russia's full-scale invasion of Ukraine in February 2022, NATO's assessment of the security environment has hardened considerably. The 2022 Strategic Concept, adopted at the Madrid Summit, marked a break with the post-Cold War paradigm, stating: 'The Euro-Atlantic area is not at peace'.¹ Russia was identified as 'the most significant and direct threat to Allies' security and to peace and stability in the Euro-Atlantic area'.² Two years later, the 2024 Washington Summit Declaration described a broader environment shaped by 'strategic competition, pervasive instability, and recurrent shocks' and explicitly pointed to hybrid, cyber, space and other malicious activities by state and non-state actors.³ In late 2024, NATO Secretary General Mark Rutte sharpened the message, stating 'we are not at war. But we are certainly not at peace either' and calling for a 'wartime mindset'.⁴ The 2026 Ankara Summit Declaration went further, identifying the long-term threat posed by Russia and describing the broader security environment as one of 'strategic competition, pervasive instability, hybrid threats and recurrent shocks'.⁵

This persistent condition between peace and open war is particularly relevant to the Baltic states: Estonia, Latvia and Lithuania. All three are frequently referred to as the most exposed Allies. All border Russia, Belarus or both, defending the third-longest NATO external border; and all face sustained Russian and Belarusian hybrid pressure alongside the conventional military threat. Their response has been

equally clear: higher defence spending, accelerated military modernization and strengthening total defense models. According to NATO's 2026 defense expenditure estimates, the three Baltic states are the top three spenders on defense relative to their GDP in the Alliance.⁶ At the same time, all three are among the most pro-Atlanticist and pro-American-oriented European countries. As the Alliance's policies evolve, with a greater emphasis being placed on burden sharing and shifting, the Baltic states continue to view the US as an essential pillar of NATO's deterrence and defense posture.

Building on Existing Cooperation

Since Russia's first invasion of Ukraine in 2014 and the launch of Operation Atlantic Resolve, the US has maintained a persistent rotational military presence on NATO's eastern flank. The Baltic states have consistently sought to preserve and deepen that presence while building broader bilateral security relationships with Washington. Some of those relationships predate NATO membership. The US National Guard's State Partnership Program (SPP) began in the Baltics in 1993: Estonia with Maryland, Latvia with Michigan and Lithuania with Pennsylvania. What began as support for defense transformation has evolved into more than three decades of practical military cooperation focused increasingly on readiness, interoperability and deterrence. During a 2026 visit to the Baltic states, US National Guard leaders described these partnerships as 'an investment in de-

¹ North Atlantic Treaty Organization (NATO), *NATO 2022 Strategic Concept* (Brussels: NATO, 2022), 3, <https://www.nato.int/en/about-us/official-texts-and-resources/strategic-concepts/nato-2022-strategic-concept>.

² NATO, *NATO 2022 Strategic Concept*, 4.

³ North Atlantic Treaty Organization (NATO), "Washington Summit Declaration," July 10, 2024, <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/washington-summit-declaration>.

⁴ Mark Rutte, "To Prevent War, NATO Must Spend More," speech at Carnegie Europe, December 12, 2024, <https://www.nato.int/en/news-and-events/events/transcripts/2024/12/12/to-prevent-war-nato-must-spend-more>.

⁵ North Atlantic Treaty Organization (NATO), "The Ankara Summit Declaration," July 8, 2026, <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/07/08/the-ankara-summit-declaration>.

⁶ North Atlantic Treaty Organization (NATO), *Defence Investment of NATO Countries (2014–2026)*, July 3, 2026, <https://www.nato.int/content/dam/nato/webready/documents/finance/def-exp-2026-en.pdf>.

terrence'.⁷ The relationship also extends beyond conventional defense. The Baltic states have supported wider US-led security and non-proliferation efforts, including the Proliferation Security Initiative (PSI) and the Container Security Initiative. Vilnius, Riga and Tallinn also endorsed the PSI Statement of Interdiction Principles, committing participants to improve information sharing, strengthen national authorities and develop practical capabilities to interdict transfers of weapons of mass destruction, their delivery systems and related materials. This cooperation has already acquired a practical regional dimension. A 2024 PSI Baltics Workshop and Tabletop Exercise held in Tallinn brought together more than 60 civilian and military representatives from 14 countries, including all three Baltic states and the US.⁸ Participants examined proliferation pathways, interdiction obligations, legal frameworks and real-world cases, with particular emphasis on intra-governmental information-sharing, trade controls and coordinated decision-making.⁹ The exercise offers a useful precedent for the argument developed here: effective interdiction already requires customs, law enforcement, security, defense and diplomatic actors to operate across traditional institutional boundaries.

A particularly relevant example of Baltic-US cooperation for this report – and beyond – is Lithuania's Nuclear Security Centre of Excellence (NSCoE), established at the Border Guard School in Medininkai, Lithuania, in 2012 in close cooperation with the US Departments of State and Energy and the International Atomic Energy Agency (IAEA). In 2013, Lithuania and the US reinforced this cooperation through a Joint Action Plan on Combating Illicit Trafficking of Nuclear and Radioactive Materials and Related Technology.¹⁰ The Centre has since developed into a regional training and capacity-building hub, strengthening the ability of border guards, customs, police and other authorities in Lithuania and partner countries to detect illicit nuclear and radioactive materials, investigate suspicious incidents and coordinate

inter-agency responses. Its reach extends beyond Lithuania to include partners across the Nordic-Baltic region, the European Union (EU) and NATO Eastern Partnership countries. It is argued that this model is practical and has relevance beyond nuclear security: it brings together specialized detection, border control, law enforcement, information sharing and international cooperation to detect and disrupt illicit flows. This experience matters because the problem is no longer confined to 'classical' proliferation, and the cooperative model might be extended to broader collaborative formats.

Beyond Conventional Threats

Russia's full-scale invasion of Ukraine, and the accompanying escalation of hostile activity across the Baltic region, have further blurred the boundaries between state action, hybrid operations and criminal activity. Instrumentalized migration, sanctions circumvention, smuggling and other illicit flows can exploit the same routes, networks and vulnerabilities used by conventional organized crime. The actor, purpose and strategic effect may differ; much of the enabling infrastructure does not. This also creates a potentially useful transatlantic parallel. The Baltic states face hostile regimes on their borders and increasingly treat cross-border illicit activity as part of a wider security problem. The US, under very different geopolitical circumstances, is likewise recasting parts of its southern border challenge in national security terms. The 2025 US National Security Strategy explicitly states controlling migration and drug flows, countering criminal cartels and strengthening security in the Western Hemisphere is a national security issue.¹¹ Furthermore, the 2026 US Annual Threat Assessment puts it bluntly: transnational organized crime and illicit drug trafficking are among the top

⁷ Zach Sheely, "Where the State Partnership Program Began: National Guard Leaders Visit Baltics," National Guard Bureau, June 11, 2026, <https://www.nationalguard.mil/News/Article-View/Article/4513946/where-the-state-partnership-program-began-national-guard-leaders-visit-baltics/>.

⁸ U.S. Department of State, Office of the Spokesperson, "Joint Statement on the PSI Baltics Workshop and Tabletop Exercise," June 6, 2024, <https://2021-2025.state.gov/joint-statement-on-the-psi-baltics-workshop-and-tabletop-exercise/>.

⁹ U.S. Department of State, "Joint Statement on the PSI Baltics Workshop."

¹⁰ U.S. Department of State, "U.S. and Lithuania Sign Agreement on Countering Nuclear Smuggling," *Atlantic Council*, April 23, 2013, <https://www.atlanticcouncil.org/blogs/natosource/us-and-lithuania-sign-agreement-on-countering-nuclear-smuggling/>.

¹¹ The White House, *National Security Strategy of the United States of America*. Washington, DC: The White House, November 2025, <https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf>.

concerns for the US Homeland.¹² The 2026 National Defense Strategy goes a step further, placing the fight against 'narco-terrorist organizations' within homeland defense and explicitly preserving the option for the US military to take decisive action against them.¹³ At the same time, the comparison should not be overstated: the Baltic states face hostile state actors on their borders, whereas Mexico is a US partner, and the threats, political contexts and legal frameworks are fundamentally different. The relevant parallel lies instead in the networks themselves. In both cases, authorities face transnational networks that withstand individual seizures, adapt routes and technologies, move goods and money across jurisdictions, and exploit gaps between institutions and national authorities. This creates a common operational challenge: effective responses increasingly require intelligence, border security, law enforcement, financial tools and international cooperation to operate as parts of the same security architecture. This provides both a rationale and a practical opening for deeper Baltic-US cooperation and mutual learning on the security implications of illicit activities, particularly illicit trade as part of a wider factor undermining national, regional and transatlantic security.

From Illicit Trade to Criminal Infrastructure

This report examines the point at which illicit trade, economic security, criminal infrastructure and hostile-state activity overlap. Traditionally, these areas have largely been treated as separate domains, with limited interaction between their respective policy and expert communities. However, their growing convergence represents an important, yet underexplored part of the transatlantic security agenda. Arguably, illicit trade is first and foremost an economic security problem. It drains public revenue, distorts competition, rewards illegal operators and weakens legitimate markets.

But the distinction here is important. Our focus is not solely on what illicit trade costs, even though its

economic impact is substantial: illicit cigarette consumption resulted in an estimated €224 million (approximately \$260 million) in lost tax revenue across the Baltic states in 2025, while the corresponding figure across the European markets covered by KPMG was €22.4 billion (approximately \$26 billion).^{14,15} More importantly, persistent illicit activity creates and sustains infrastructure that can be exploited beyond the original criminal purpose. Our analysis therefore focuses primarily on what it enables, as the security implications of illicit trade extend well beyond lost tax revenue. Persistent illicit activity can sustain cross-border routes, logistical networks, financial channels, technological capabilities, local facilitators and operational knowledge that may subsequently be adapted or exploited for purposes beyond the original criminal activity, including by hostile-state actors.

An important distinction is necessary at the outset. Illicit trade is a broad phenomenon driven by different actors, motivations and economic incentives, and in most cases, it should be understood primarily through the lenses of crime, law enforcement and economic security. The growing involvement of hostile states and state-linked actors does not change this basic reality. We do not argue that every instance of an illicit trade constitutes hybrid warfare or a national security issue. Smuggling, illicit finance and organized crime remain primarily profit-driven activities and, as such, should be addressed through law-enforcement instruments. Nor should a criminal network be considered a state proxy simply because a hostile government may find its capabilities useful. Yet, once established, such networks may become available for exploitation by hostile-state or non-state actors. Recent studies and practitioner insights suggest that criminal networks – or criminal infrastructure, as we refer to them hereafter – may provide capabilities, access or services to hostile actors, willingly or unwillingly, for profit or for other reasons.

So why discuss hybrid threats in the context of illicit trade? Because the dividing line begins to blur when criminal infrastructure developed primarily for profit is exploited by hostile-state or state-linked actors in pursuit of strategic objectives. One major current fea-

¹² Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Washington, DC: Office of the Director of National Intelligence, March 2026), 5, <https://archive.dni.gov/files/ODNI/documents/assessments/ATA-2026-Unclassified-Report.pdf>.

¹³ U.S. Department of War, 2026 National Defense Strategy (Washington, DC: U.S. Department of War, January 23, 2026), 16, <https://media.defense.gov/2026/Jan/23/2003864773/-1/-1/0/2026-NATIONAL-DEFENSE-STRATEGY.PDF>

¹⁴ KPMG, *Illicit Cigarette and Heated Tobacco Consumption, and Oral Nicotine Share in Europe: 2025 Results*, commissioned by Philip Morris Products S.A., June 2, 2026, 86-89, 130-139, <https://www.pmi.com/content/dam/pmicom/global/docs/itp/kpmg-illicit-cigarette-consumption-europe-2025-results.pdf>.

¹⁵ KPMG, *Illicit Cigarette and Heated Tobacco Consumption*, 10.

ture is that the hybrid threat landscape is expanding. NATO describes hybrid threats not as a fixed category of individual activities, but as combinations of military and non-military, covert and overt means employed by state and non-state actors. It also notes that the speed, scale and intensity of such activities have increased with technological change and global interconnectivity.¹⁶ The implication is important: the relevant question is increasingly not whether one particular incident fits neatly into a predefined hybrid category, but how different activities, actors and capabilities connect across domains. A recent Baltic analysis of the Baltic states similarly describes contemporary Russian hybrid activity as a continuously evolving strategy dispersed across domains and exploiting the openness, technological connectivity and institutional seams of democratic societies.¹⁷

Throughout this report, the term ‘criminal infrastructure’ serves as a central framework for examining the intersection between illicit trade and wider security threats. With this term, we mean the routes, logistics, finance, technology, intermediaries and actors, local facilitators, corrupt or insider access, and operational knowledge that sustained criminal activity creates and maintains. While individual shipments are expendable, infrastructure is not. It can withstand seizures, switch commodities, move between jurisdictions and, in some circumstances, be repurposed for hostile-state activity.

Furthermore, criminal infrastructure should be understood as physical, financial and digital. It includes routes, vehicles and facilitators, but also shell companies, payment channels, cryptocurrency, encrypted communications, digital identities and commercially available technologies. This creates a particularly strong basis for Baltic–US cooperation by combining Baltic regional and operational intelligence with US financial intelligence and sanctions capabilities.

The Transatlantic Dimension

The US–Baltic relationship is arguably no longer defined by the traditional questions of military presence and defense cooperation. Economic and energy security, technological cooperation, resilience, and addressing various forms of vulnerabilities increasingly

enter our strategic dialogue. This report asks a further question: whether addressing the problem of illicit markets and the infrastructure behind them also belongs in that wider security agenda.

The US and the Baltic states operate in very different geographic, political and security environments. Their borders, illicit markets and actors are different. Therefore, we do not directly equate the US southern border with the borders that Lithuania, Latvia and Estonia share with Russia and Belarus. As already mentioned, the relevant comparison lies in the illicit transnational networks themselves. In both cases, authorities face transnational networks that survive individual seizures, adapt routes and technologies, move goods and money across jurisdictions, and exploit gaps between institutions and national authorities.

This makes the relationship reciprocal rather than unidirectional. The US is not only a source of expertise for the Baltic states; it also faces its own resilient criminal infrastructure, and the financial and logistical reach of these networks carries economic and public safety costs. The value of a Baltic–US security agenda lies in comparing how authorities in different threat environments detect and dismantle networks that can withstand individual seizures and adapt to enforcement pressure.

For the Baltic states, this challenge exists in a particularly difficult security environment. Illicit networks operate along NATO and EU external borders with Russia and Belarus, where their activities intersect with sanctions circumvention and sustained hostile-state activity. Networks created for profit can also provide logistics, financing, local knowledge and intermediaries that hostile states may exploit. This is why the illicit commodity only represents the visible part of the problem. Behind it are routes, facilitators, financial channels and logistical infrastructure that can be reused for different purposes.

Therefore, this report examines how tackling illicit markets and the criminal infrastructure behind them could form part of a wider Baltic–US security agenda. It is argued that the strategic significance of illicit trade lies not only in the commodities or revenues involved, but in the networks, capabilities and access that persistent illicit activity creates, and that these can, under certain circumstances, be exploited by hostile actors.

¹⁶ North Atlantic Treaty Organization (NATO), “Countering Hybrid Threats,” updated January 29, 2026, <https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats>.

¹⁷ Eitvydas Bajarūnas, “Russia’s Hybrid Warfare Tactics Target the Baltics,” The Jamestown Foundation, May 27, 2025, <https://jamestown.org/russias-hybrid-warfare-tactics-target-the-baltics/>.

1.

Analytical Approach

To provide actionable recommendations, we approach this as a policy report rather than a comprehensive analysis of hybrid threats or illicit trade. We combine available quantitative evidence, official threat assessments, law-enforcement and institutional reporting, recent analytical work by relevant think tanks, and qualitative insights from experts and practitioners working directly on the issues covered here.

For this policy report, we follow a sequence that can be broadly summarised as (1) incident, (2) network and (3) wider pattern. This qualification is rooted in Lithuania's new legal definition of a hybrid threat. In 2026, Lithuania amended its Law on Crisis Management and Civil Protection to define a hybrid threat not by the nature of a single act, but by a variety of factors, including who stands behind it; how other actors are organized, controlled or coordinated; the extent of the harm an activity causes or could cause; and whether the activity requires a coordinated response by the state.¹⁸ The definition covers natural and legal persons, as well as groups of persons, who are organized, controlled or coordinated by foreign states or other foreign actors. The incident is what happened. The network is how it became possible and repeatable. The wider pattern helps determine whether the activity should be considered ordinary crime or part of a broader hostile effort. Thus, the focus of analysis cannot be the incident alone; it must also include the infrastructure, actors and relationships behind it.

This can be illustrated by the example of cigarette smuggling. A balloon crossing the Belarusian–Lithuanian border while carrying illicit cigarettes constitutes a smuggling incident. The commodity is illicitly bought and traded cigarettes, and the crime is smuggling. However, if we zoom out to the network and infrastructure required to repeatedly launch such balloons, including sourcing balloons and launch equipment, GPS monitoring, specificity of directions, retrieval teams, logistical and financial flows, and connections to facilitators on the other side of the border, the analytical picture changes. If this infrastructure is owned, managed, directed or leveraged by a hostile state or other foreign actor to create broader security consequences, the same criminal infrastructure acquires a national security dimension. The criminal act does not have to become something else; its strategic context does.

Hence, the key policy question is not whether criminal activity is inherently hybrid, but when criminal infrastructure acquires strategic relevance. Crime is primarily driven by profit, whereas hybrid exploitation is driven by strategic purpose. However, infrastructure originally developed for criminal purposes may also provide capabilities that can be exploited for strategic objectives. Links to hostile state actors, critical infrastructure, military logistics, intelligence collection, sabotage or sanctions circumvention should therefore trigger closer national security scrutiny.

¹⁸ Republic of Lithuania, Law No. XV-1002 Amending the Law on Crisis Management and Civil Protection No. VIII-971, June 11, 2026, art. 1(8), Register of Legal Acts (TAR), June 26, 2026, no. 11088, <https://e-tar.lt/portal/lt/legalAct/86c35e02715711f1b53dfa020e517810>.

2.

The Security Environment

The security environment in the Baltic region is characterized by the blurring of traditional lines between war and peace and between military and non-military threats. The latest assessments of the security situation in the region by NATO, the US Intelligence Community and the three Baltic states are broadly in agreement: Russia continues to be the main military threat to the region, and the tools that it employs are increasingly moving beyond the use of conventional military forces and are characterized by sabotage, cyber operations, intelligence activities, pressure on critical infrastructure and other means of action short of armed conflict.

Belarus remains closely aligned with Russia and, from the Baltic perspective, an important source and enabler of security pressures.

NATO continues to see Russia as ‘the most significant and direct threat’ to Allied security. The Alliance has responded not only by reinforcing conventional deterrence and defense by forward deployment of troops to the region but also through Baltic Sentry and Eastern Sentry military activities, aimed at helping to observe and, to an extent, deter the threats that increasingly cross land, maritime, air, cyber and other domains.

A similar picture emerges from the 2026 US Annual Threat Assessment. The US Intelligence Community assesses that Russia maintains the ability to compete with and confront US interests using military and non-military tools and explicitly points to Moscow’s use of ‘grey zone tactics’ to apply pressure and compete below the threshold of armed conflict.¹⁹ The

report also identifies state-linked disruption of European critical infrastructure as a threat to European and US commercial interests and to the transport of military goods to Ukraine.²⁰ More broadly, the report highlights overlapping risks from state and non-state actors: Russia and other state actors seek to compromise critical infrastructure to gain intelligence and facilitate future disruption, while non-state ransomware groups increasingly target networks for financial gain.

Baltic intelligence services provide the regional detail. Lithuania’s 2026 National Threat Assessment, jointly produced by the State Security Department (VSD) and the Defence Intelligence and Security Service (AOTD), states that ‘Reduced Western pressure on Moscow would accelerate Russia’s preparations for conflict with NATO’²¹ and notes that ‘Russia is expanding its military capabilities near NATO’s eastern borders despite losses in the war’.²² Meanwhile, the threat is already being felt below that threshold. The assessment states that ‘The GRU is changing the methods of conducting kinetic operations and expanding the range of targets’,²³ while entities acting against Lithuania’s national security interests continue to target strategically important infrastructure and projects. It also finds that the scale of international sanctions circumvention remains high and describes Russian and Belarusian efforts to gain access to Western technologies through companies operating in Lithuania and other Western countries. Latvia arrived at a broadly similar conclusion. A 2025 report from Latvia’s Constitution Protection Bureau states that the Russian threat will be high in the long term no matter what the outcome of the war

¹⁹ Office of the Director of National Intelligence, *Annual Threat Assessment*, 26-27.

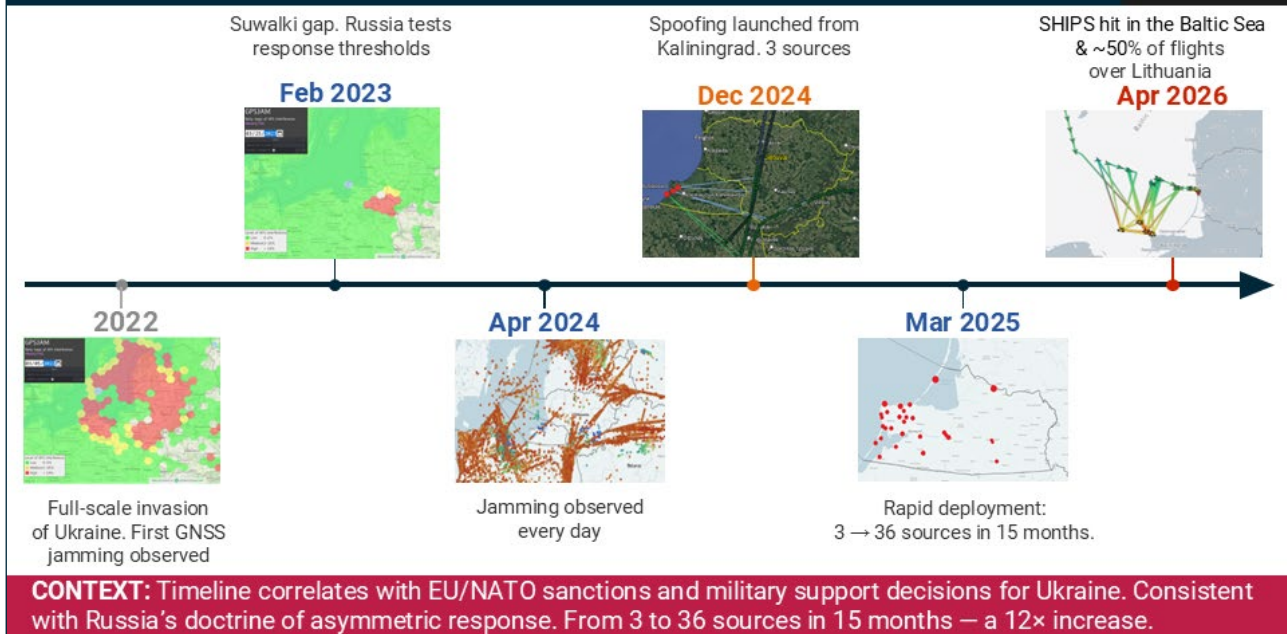
²⁰ Office of the Director of National Intelligence, *Annual Threat Assessment*, 26.

²¹ Defence Intelligence and Security Service under the Ministry of National Defence of the Republic of Lithuania (AOTD) and State Security Department of the Republic of Lithuania (VSD), *2026 National Threat Assessment* (Vilnius, 2026), 15, <https://kam.lt/wp-content/uploads/2026/03/2026-National-Threat-Assessment.pdf>.

²² AOTD and VSD, *2026 National Threat Assessment*, 17.

²³ AOTD and VSD, *2026 National Threat Assessment*, 25.

GNSS INTERFERENCE – TIMELINE 2022–2026



Source: Ryšių reguliavimo tarnyba / Communications Regulatory Authority of Lithuania (RRT) <https://rrt.lt/>

in Ukraine and that Moscow will continue to adapt existing and develop new hybrid instruments.²⁴ Estonia's Foreign Intelligence Service goes as far as referring to Belarus as 'a Russian vassal state'.²⁵

Importantly, Lithuania's 2026 National Threat Assessment places the criminal-hybrid nexus within this wider security context, identifying intelligence operations, sabotage, cyber activity, electronic interference, disinformation and sanctions circumvention among the forms of hostile activity occurring below the threshold of armed conflict.

Taken together, these assessments indicate that malign activity below the threshold is chronic, adaptive and increasingly multi-domain. This provides the broader security context in which the intersection between criminal activity and hostile-state activity must be examined.

²⁴ Constitution Protection Bureau of the Republic of Latvia (SAB), "The Constitution Protection Bureau Publishes the Annual Report 2025," January 26, 2026.

²⁵ Estonian Foreign Intelligence Service, *International Security and Estonia 2026* (Tallinn: Estonian Foreign Intelligence Service, 2026), 24, https://raport.valisluureamet.ee/2026/assets/VLA_ENG-raport_2026_WEB.pdf.

3.

The Criminal-Hybrid Nexus

Recent analysis by the Center for European Policy Analysis (CEPA) highlights an important additional consideration when addressing the hybrid-criminal nexus: resilience alone is insufficient when hostile actors systematically exploit the grey zone. Efforts to deny such activities must therefore be accompanied by credible costs for the perpetrators.²⁶ For the criminal-hybrid nexus, this means that the use of criminal intermediaries, proxies or pre-existing illicit infrastructure should not insulate the state exploiting them from consequences. Wider research into Russia's shadow activities has reached a similar conclusion: connected hostile activity is often processed through separate institutional categories, leaving the strategic picture fragmented even when individual institutional responses are appropriate.²⁷

This pattern is increasingly described as 'proxyisation': criminal networks, loosely affiliated intermediaries and other deniable actors reduce operational risk, complicate attribution and stretch investigative and legal systems.²⁸ The pattern is no longer simply an analytical suggestion or inference. Lithuania's 2026 National Threat Assessment states that Russia's military intelligence service, the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU), uses a long chain of intermediaries and is actively seeking experienced individuals with criminal records who are willing to carry out operations for relatively small financial rewards. The assessment links this recruitment model

to planned sabotage and other kinetic operations in Western countries, including Lithuania. This provides direct official evidence that a hostile intelligence service is deliberately tapping into existing criminal networks and infrastructure for operational purposes.²⁹

This also explains why disrupting individual actors may have limited effect. Convergent networks gain durability through substitution: a recruiter, courier, saboteur, payment channel or platform can be replaced, while the wider system reconstitutes through different suppliers, labour and communications. Criminal infrastructure is therefore relevant not simply because criminals may occasionally work for a hostile state, but because it provides a reusable market of access, logistics, finance and people from which hybrid operations can be assembled and reassembled.³⁰

For this report, the important point is that many of the same enabling systems can support both criminal and hybrid activity: cryptocurrency and other payment channels, encrypted communications, online recruitment, legitimate and illicit logistics, commercial cover, access brokers and disposable labour. A hostile state can therefore access, penetrate, co-opt or redirect capabilities already available within criminal and commercial networks, rather than developing them from scratch.³¹

Documented cases show that this secondary-use problem is already practical, not hypothetical. The hybrid-criminal nexus is expanding. This is far from

²⁶ Eitvydas Bajarūnas, "The Hybrid Threat Imperative: Deterring Russia Before It Is Too Late," Center for European Policy Analysis (CEPA), December 2, 2025, <https://cepa.org/comprehensive-reports/the-hybrid-threat-imperative-deterring-russia-before-it-is-too-late/>.

²⁷ Bajarūnas, "The Hybrid Threat Imperative."

²⁸ Donald Bowser, "Russian Organised Crime and Links to Hybrid War in Europe," GLOBSEC, December 9, 2025, <https://www.globsec.org/what-we-do/publications/russian-organised-crime-and-links-hybrid-war-europe>.

²⁹ AOTD and VSD, 2026 *National Threat Assessment*, section "The GRU is changing the methods of conducting kinetic operations and expanding the range of targets."

³⁰ Chris Kremidas-Courtney, "Everything, Everywhere, All at Once: Russia's Hybrid Campaign Against Europe, 2026–2030," Euro-Atlantic Resilience Centre (E-ARC), September 1, 2026, <https://e-arc.ro/en/category/authors/chris-kremidas-en/>.

³¹ Kremidas-Courtney, "Everything, Everywhere, All at Once."

being a Baltic-specific phenomenon. Cases from various countries are provided below to illustrate the breadth and depth of this phenomenon.

In June 2026, the Council of the EU imposed restrictive measures on individuals involved in Russian-funded operations targeting Moldova's September 2025 parliamentary elections. According to the Council of the EU, the operations involved vote-buying and disinformation and broadly relied on networks linked to Ilan Shor and the Russia-based organization Evrazia, which supported recruitment, training, propaganda and local operations. The case illustrates how illicit finance and local criminal and political networks can be leveraged for foreign interference. Financial investigations further linked suspicious funds used for electoral corruption and illegal political financing to Russia-based financial infrastructure, including the sanctioned Promsvyazbank and cash transfers facilitated through Telegram.^{32,33,34} The case also illustrates how financial intelligence can expose a hostile-influence network by connecting dispersed local actors to the organizers and infrastructure behind their activities.

Operation Destabilise^{35,36} provides a particularly clear-cut example of the value of a financial-network approach. Since 2022, the National Crime Agency (NCA) of the United Kingdom (UK) has targeted Russian-speaking professional money-laundering networks that service organized crime groups and other threat actors across jurisdictions. By 2026, the operation had resulted in 129 arrests and the seizure of more than GBP 25 million in cash and cryptocurrency in the UK, in addition to overseas seizures. Crucially, the investigation exposed a direct connection between ordinary criminal money laundering and Russian state-linked activity. The NCA reports that

individuals associated with Russian intelligence services attempted to use one UK-linked network to fund various individuals, including the leader of a Bulgarian network later convicted of running a spying operation for Russia across Europe.

Lithuanian prosecutors have documented a cross-border network that used recruited intermediaries and ordinary international logistics to organise attacks involving incendiary devices and explosives. In 2024, four parcels containing improvised incendiary-explosive devices were sent from Vilnius via DHL and DPD networks; the devices detonated or ignited in Germany, Poland and the UK. Lithuanian investigators established that the crimes were attributable to Russian citizens.³⁷ This case matters because it shows how hostile-state tasking can be distributed through deniable intermediaries while exploiting existing transport, communications and cross-border logistics rather than requiring purpose-built infrastructure.

These cases differ in commodity, geography and legal qualification, but they share a common operational feature. A hostile state does not need to own every element of a network. They can finance, recruit from, tolerate, direct or exploit pre-existing criminal, commercial and informal infrastructure already available in a criminal market.

³² Police of the Republic of Moldova, "Percheziții în dosarul privind coruperea alegătorilor, finanțarea ilegală a partidelor și spălarea banilor" [Searches in the Case Concerning Electoral Corruption, Illegal Party Financing, and Money Laundering], September 11, 2025, <https://igp.gov.md/en/node/1265>.

³³ Police of the Republic of Moldova, "46 de percheziții în dosarul privind coruperea electorală, finanțarea ilegală a partidelor politice și spălarea banilor" [46 Searches in the Case Concerning Electoral Corruption, Illegal Financing of Political Parties, and Money Laundering], September 18, 2025, <https://igp.gov.md/en/node/1373>.

³⁴ Council of the European Union, "Republic of Moldova: Council Lists Six Individuals for Actions Destabilising the Country," June 15, 2026, <https://www.consilium.europa.eu/en/press/press-releases/2026/06/15/republic-of-moldova-council-lists-six-individuals-for-actions-destabilising-the-country/>.

³⁵ National Crime Agency, "Investigating Russian-Speaking Money Launderers," in National Strategic Assessment 2026 of Serious and Organised Crime (2026), <https://www.nationalcrimeagency.gov.uk/nsa-domains-2026/nsa-soc-finance-2026>.

³⁶ National Crime Agency, "Operation Destabilise: NCA Disrupts \$Multi-Billion Russian Money Laundering Networks with Links to Drugs, Ransomware and Espionage, Resulting in 84 Arrests," December 4, 2024, <https://www.nationalcrimeagency.gov.uk/news/operation-destabilise-nca-disrupts-multi-billion-russian-money-laundering-networks-with-links-to-drugs-ransomware-and-espionage-resulting-in-84-arrests>.

³⁷ Prosecutor General's Office of Lithuania and Lithuanian Criminal Police Bureau, "Case on Terror Acts Organised and Planned in Different Countries Referred to Court," March 6, 2026, <https://www.prokuraturos.lt/lt/teis-mui-perduota-byla-del-skirtingose-valstybese-organizuotu-ir-planuotu-ivykdyti-teroro-aktu-with-text-in-english/12174>.

4.

From Commodity to Capability

This distinction changes the analytical lens. A shipment of illicit cigarettes, for example, is primarily a customs and criminal matter. A functioning system capable of repeatedly moving such shipments across a protected NATO and EU border, however, represents something more complex. It requires organizers and facilitators, communications, knowledge of terrain and enforcement patterns, and transport, storage, distribution and financial channels. Repeated activity also builds experience: networks learn where controls are strong or weak, adapt routes, test concealment methods and change intermediaries or logistics in response to enforcement. Therefore, the relevant question is not only what is being smuggled but also what the network has learned and is capable of.

The Belarusian cigarette trade provides a concrete illustration. An examination by the Belarusian Investigative Center (an independent investigative initiative) documented a ‘false transit’ scheme in which Belarusian cigarettes were declared for export to third countries but were allegedly diverted for illegal sale within the region. The scheme involved cross-border transport, intermediaries and customs documentation, while sources cited by the investigation alleged payments linked to facilitating fictitious transit.³⁸ The case illustrates how sustained illicit trade can depend on reusable infrastructure spanning logistics, documentation, financial arrangements and access to state-controlled systems.

The security risks associated with cigarette smuggling extend beyond lost tax revenue. In 2019, the chief of Lithuania’s State Border Guard Service (SBGS) stated that some individuals detained for cigarette and migrant smuggling were also suspected of working for Russian or Belarusian special services. Analysts cited by the Lithuanian public broadcaster, LRT, noted that smugglers’ knowledge of border areas, military facilities and border infrastructure could make them valuable intelligence sources. The same report described cases in Estonia in which cigarette smugglers were recruited by the Federal Security Service of the Russian Federation (FSB) to collect information on border security and military facilities.³⁹ These cases illustrate how established smuggling networks can provide hostile intelligence services with access to individuals possessing local knowledge, cross-border access and familiarity with border security systems.

The methods used to move cigarettes also demonstrate the operational sophistication and persistence of illicit networks in critical state infrastructure. In 2021, Lithuanian customs found almost 80,000 packs of cigarettes concealed in a fertilizer shipment carried on a Belaruskali train from Belarus; officials noted that large quantities of cigarettes were being found on trains arriving from Belarus almost every week.⁴⁰ In January 2023, border guards discovered a further 12,000 packs of Belarusian cigarettes hidden under crushed stone in a railway wagon carrying construction materials in transit from Belarus to

³⁸ Belarusian Investigative Center, “With ‘Korona’ at the Head: How Pavel Topouzidis Joined ‘Fake Transit’ and Built an Empire,” March 1, 2022, <https://investigatebel.org/en/investigations/z-karonaj-na-chale-yak-pavel-tapuzidzis-da-luchy-sya-da-falshyvaga-tranzitu-i-pabudava-biznes-imperyyu>.

³⁹ LRT TV News Service, “Cigarette Smugglers May Double as Russian Spies, Lithuanian Border Guards Warn,” LRT, June 11, 2019, <https://www.lrt.lt/en/news-in-english/19/1068201/cigarette-smugglers-may-double-as-russian-spies-lithuanian-border-guards-warn>.

⁴⁰ BNS, “Lithuania Steps Up Rail Freight Checks amid Rise in Cigarette Smuggling from Belarus,” LRT, August 6, 2021, <https://www.lrt.lt/en/news-in-english/19/1464016/lithuania-steps-up-rail-freight-checks-amid-rise-in-cigarette-smuggling-from-belarus>.

the Kaliningrad region.⁴¹ These cases show both the repeated use of legitimate freight systems and the development of sophisticated concealment methods to move illicit goods across borders.

There are also indications of a state-linked footprint in the Belarusian illicit tobacco supply chain. The EU has identified Hrodna Tobacco Factory Neman as a Belarusian state-owned enterprise and a major source of revenue for the Lukashenka regime, noting that Neman brands are among the cigarettes most frequently smuggled into the EU. The EU has also documented the use of railway wagons belonging to Belarusian state-owned enterprises, including Belaruskali and Grodno Azot, in cigarette smuggling into the EU.⁴² This does not by itself establish state direction of individual smuggling operations, but it shows that illicit tobacco flows can intersect with Belarusian state-owned production and transport infrastructure.

The 2021 Belarus-orchestrated migration crisis provides a broader illustration of how commercial and facilitation networks can become embedded in a state-driven coercive operation. An investigation by the Belarusian Investigative Center discovered that de facto Belarusian authorities granted 12 private companies the right to issue visa invitations for citizens of Middle Eastern countries, with most of the companies linked to Belarusian security structures or their affiliated entities. The investigation also documented the role of private transport and other intermediaries in facilitating migrants' movement towards the EU border.⁴³ The case illustrates how commercial and facilitation infrastructure can become part of a wider state-driven operation.

Together, these cases show why the security significance of illicit trade cannot be assessed solely by the commodity or the immediate criminal act. Repeated illicit activity can generate networks, knowledge, access and infrastructure that may later be exploited, penetrated, co-opted or redirected for purposes beyond the original criminal activity.

Money provides another way to reveal a network. The 'follow the money' approach should work in both di-

rections. First, every major proceeds-generating case should trigger a parallel financial investigation from the outset: where does the money come from, where does it go, who ultimately controls it, and what assets can be identified and frozen? This allows an investigation to move beyond a detected shipment or immediate perpetrator and towards financiers, beneficiaries, facilitators and the wider infrastructure. Second, the same system should work in reverse. Suspicious transactions, unexplained assets, shell companies, cryptocurrency flows, unusual trade payments or other financial intelligence signals may themselves become the starting point for an investigation, even before the underlying predicate offence is fully known. The investigation then moves backwards from the financial footprint towards the criminal activity and, where relevant, towards tasking or sponsorship by a hostile state.

Sanctions circumvention illustrates this shift particularly clearly. Sanctions and export controls are instruments of strategic pressure, whose effectiveness depends on restricting access to technologies, components, finance and services. Yet the infrastructure used to circumvent them often resembles that found in other illicit markets: transport companies, intermediaries, warehouses, corporate structures, false documentation, third-country routing and payment mechanisms designed to obscure origin, ownership or destination. Lithuania's 2026 threat assessment, already mentioned above, explicitly states that international sanctions circumvention remains extensive and that Russian and Belarusian entities continue to seek access to strategically important technologies through companies operating in Lithuania.

This criminal-hybrid interlinkage is increasingly reflected in the policy instruments European governments are prepared to utilize. In July 2026, acting through their common institutions, European states moved towards introducing a dedicated sanctions framework targeting migrant smuggling, human trafficking and other forms of serious, organized crime, including illicit firearms and drug trafficking and money laundering. The proposed measures include asset

⁴¹ Lithuanian State Border Guard Service, "Tranzitiniame traukinyje – 12 tūkst. pakelių paslėptų baltarusiškų cigarečių" [12,000 Packs of Hidden Belarusian Cigarettes Found on a Transit Train], January 16, 2023, <https://vsat.lrv.lt/lt/naujienos/tranzitiniame-traukinyje-12-tukst-pakeliu-pasleptu-baltarusisku-cigareciu-foto>.

⁴² Council of the European Union, Council Regulation (EC) No. 765/2006 of 18 May 2006 concerning restrictive measures in view of the situation in Belarus and the involvement of Belarus in the Russian aggression against Ukraine, consolidated version of July 20, 2025, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02006R0765-20250720>.

⁴³ Stanislau Ivashkevich, Olga Ratmirova, and Kseniya Viaznikoutsava, "Undercover of Security Forces: Who Could Make Millions of Dollars on the Migration Crisis at the EU Border, Which Claimed Dozens of Lives," Belarusian Investigative Center, June 7, 2023, <https://investigatebel.org/en/investigations/who-could-make-millions-of-dollars-on-the-migration-crisis>.

freezes, restrictions on access to funds and economic resources, and travel bans. Their significance goes beyond the individual measures themselves. Sanctions, as instruments traditionally associated with foreign policy, national security and economic statecraft, are increasingly being deployed against criminal networks because of the wider threats those networks can pose to states and societies.⁴⁴

The emerging approach also shifts attention from individual offenders towards the capabilities that sustain criminal activity: financial facilitators, logistics networks, transport routes, access to the legitimate economy and other enabling infrastructure.

As a study by the UK-based Royal United Services Institute (RUSI) argues, the Western objective should be measurable degradation of criminal infrastructure rather than simply additional designations.⁴⁵ This does not make illicit trade inherently a national security threat. Rather, it is a sober acknowledgement of the new reality that where illicit markets sustain infrastructure that hostile states can exploit, support or redirect for strategic purposes, the issue can acquire direct national security significance.

⁴⁴ European Commission and High Representative of the Union for Foreign Affairs and Security Policy, "Commission and High Representative Propose New Sanctions Regime to Counter Threats from Migrant Smuggling, Human Trafficking, and Other Forms of Organised Crime," July 9, 2026, https://cyprus.representation.ec.europa.eu/news/commission-and-high-representative-propose-new-sanctions-regime-counter-threats-migrant-smuggling-2026-07-09_en.

⁴⁵ Tom Keatinge and Kinga Redłowska, "How Can the EU's Criminal Network Sanctions Succeed?," Royal United Services Institute (RUSI), June 18, 2026, <https://www.rusi.org/explore-our-research/publications/commentary/how-can-eus-criminal-network-sanctions-succeed>.

5.

Resilience: Another Side of the Same Problem

The same infrastructure-capability logic also has a resilience dimension. A recent publication on NATO resilience argues that resilience is no longer primarily about protecting civilian infrastructure as a separate civilian task. Modern defense depends on civilian transport, energy, communications, logistics and public administration. The real test is whether NATO can continue to move, reinforce, sustain, communicate, mobilize and fight under disruption.⁴⁶

We extend that argument here. Infrastructure is not only something an adversary attacks; it can also be something an adversary uses. The same logistics systems, transport companies, telecommunications networks and institutional access that support legitimate economic and defense activity can also facilitate illicit trade, sanctions circumvention and criminal coordination. Criminal networks can likewise provide routes, local knowledge and operational access that a hostile actor would otherwise have to develop from scratch. Therefore, resilience has two aspects: protecting the infrastructure we depend on and reducing the ability of hostile actors to exploit that infrastructure and the networks already operating around us.

Criminal finance creates a similar two-sided resilience equation. Europol estimates that law-enforcement authorities take less than 2% of the estimated annual proceeds of organized crime out of criminals'

hands; the remaining 98% funds the continuation and expansion of organized crime activity. Therefore, money that remains inside criminal networks is not passive wealth. It can finance replacement personnel, new shipments, technology, logistics, corrupt access, professional facilitators and the creation of new routes when existing ones are disrupted.⁴⁷

Effective asset tracing, freezing, confiscation and recovery do more than punish past conduct: they deny future capability. This is particularly important where criminal infrastructure may also be exploited by hostile states. If the financial base remains intact, individual arrests or seizures can be absorbed as a cost of doing business, and the network can reconstitute itself.

The balance can be shifted further where legal frameworks allow recovered assets to be used for public purposes. The US provides an established example: the Department of Justice Asset Forfeiture Program⁴⁸ explicitly uses forfeiture to deter, disrupt and dismantle criminal enterprises, while the Assets Forfeiture Fund can support victim compensation, forfeiture operations and certain investigative costs. Directive (EU) 2024/1260⁴⁹ likewise encourages using confiscated property for public-interest or social purposes and notes that social reuse can strengthen communities' resilience against criminal infiltration.

⁴⁶ Loneta Progni and Vytautas Leškevičius, "Civilian Infrastructure Is Now a Strategic Target. NATO Must Adapt to Protect It," Atlantic Council, July 2, 2026, <https://www.atlanticcouncil.org/dispatches/civilian-infrastructure-is-now-a-strategic-target-nato-must-adapt-to-protect-it/>.

⁴⁷ Europol, "Europol Holds Largest-Ever Operation to Increase Seizures of Criminal Assets Worldwide," January 17, 2025, <https://www.europol.europa.eu/media-press/newsroom/news/europol-holds-largest-ever-operation-to-increase-seizures-of-criminal-assets-worldwide>.

⁴⁸ U.S. Department of Justice, "Asset Forfeiture Program," <https://www.justice.gov/afp>.

⁴⁹ European Parliament and Council of the European Union, *Directive (EU) 2024/1260 of 24 April 2024 on Asset Recovery and Confiscation*, Official Journal of the European Union L 2024/1260 (May 2, 2024), <https://eur-lex.europa.eu/eli/dir/2024/1260/oj/eng>.

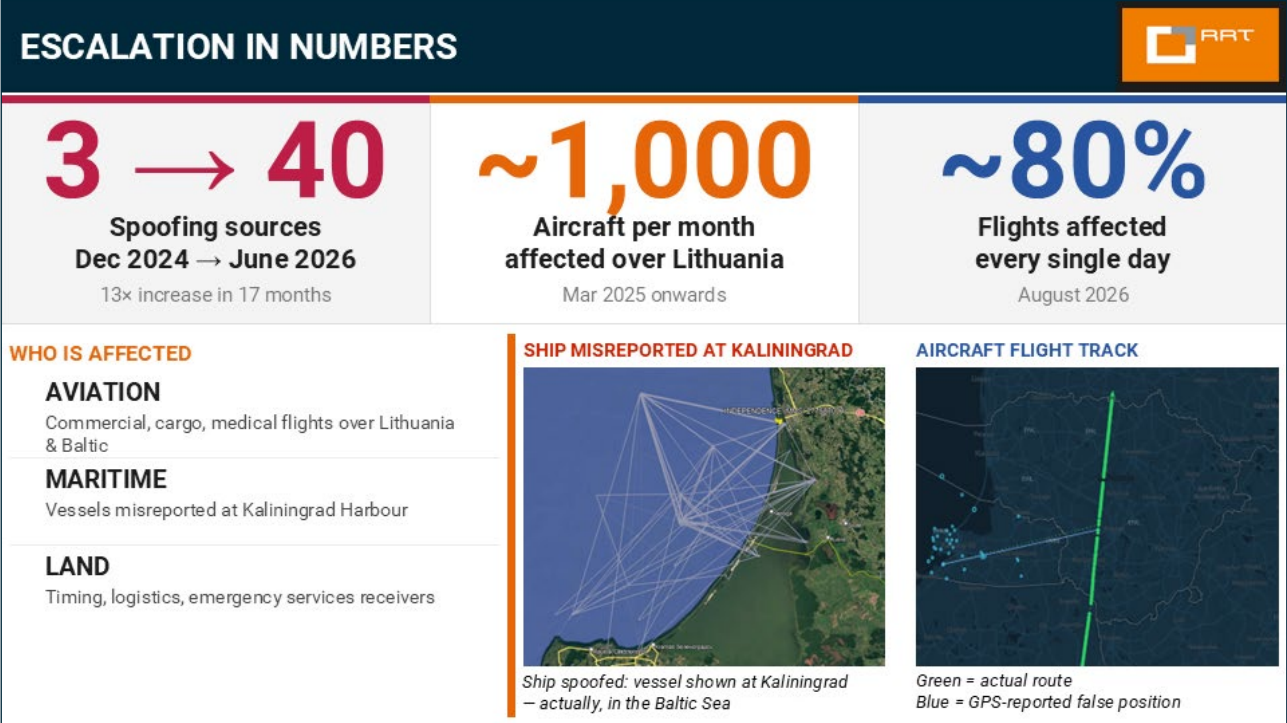
The strategic principle is simple: criminal capital left untouched strengthens a criminal network; criminal capital effectively recovered weakens the network. Where the law permits transparent reuse after protecting victims' and bona fide third-party interests, part of that value can also strengthen the state and society that the criminal infrastructure was undermining.

Resilience and deterrence by denial should therefore be complemented by consequences incurred by the culprit. Where hostile-state exploitation has been established, the response should move beyond prosecution of the immediate perpetrator and target the wider enabling system: recruiters, handlers, intelligence officers, financial networks, front companies and logistics providers. Resilience reduces the utility of criminal infrastructure; consequences increase the cost of exploiting it.⁵⁰

However, an institutional problem follows immediately from this. Different institutions see different parts of the same system: customs see a commodity, the police deal with the criminal organization, financial investigators follow the money flows, border guards see the routes, aviation authorities oversee airspace safety and violations thereof, and intelligence services investigate possible hostile-state interests. Business, meanwhile, sees disruptions in supply chains, unusual transactions and market anomalies. Each institution may therefore hold an important fragment of the picture, while no single actor necessarily sees how these fragments connect to form a broader network. The challenge is not simply a lack of information, but the fragmentation of information across institutions operating under different mandates, legal frameworks and analytical priorities.

The problem is not that every institution needs the same mandate. It is that somebody needs to see when several institutions are looking at different parts of the same system. Recent analysis reached the same operational conclusion: governments tend to encounter hybrid campaigns in fragments, with each incident entering a different institutional system and being analyzed in isolation. Therefore, the focus must shift from the incident to the campaign and, for the purposes of this report, from the shipment to the network and the enabling infrastructure behind it.⁵¹

At the state level, rather than creating new mechanisms for every emerging threat, existing structures should be used to bring together intelligence, law enforcement, border security, customs, infrastructure operators, business and other relevant actors when illicit activity begins to intersect with national security.



Source: Ryšių reguliavimo tarnyba / Communications Regulatory Authority of Lithuania (RRT) <https://rrt.lt/>

⁵⁰ Bajarūnas, "The Hybrid Threat Imperative."

⁵¹ Kremidas-Courtney, "Everything, Everywhere, All at Once." <https://e-arc.ro/2026/09/01/everything-everywhere-all-at-once-russias-hybrid-campaign-against-europe-2026-2030/>

rity. Resilience should therefore also make full use of existing crisis-management and response structures. In Lithuania, this includes, in particular, the National Crisis Management Centre. Lithuania's National Comprehensive Defence Coordination Council, which brings ministries, municipalities, critical infrastructure operators, business and civil society into one resilience framework, should also be expanded and strengthened. Its value lies in providing various stakeholders with a forum to share information, coordinate capabilities and strengthen preparedness across institutional, industrial and societal boundaries.⁵²

The objective is not to transfer responsibilities between institutions, but to ensure that an empowered structure can connect fragmented information, see the wider network and coordinate action across institutional boundaries.

⁵² Progni and Leškevičius, "Civilian Infrastructure Is Now a Strategic Target."

6.

Lithuania Case Study: How an Illicit Network Adapts

Lithuania provides a useful case study because the evolution of an illicit network is visible almost step by step. What began as conventional cross-border smuggling gradually developed routes, technologies, logistics, local facilitators and operational knowledge whose relevance extends beyond the illicit commodity itself, creating broader security risks and opportunities for hostile-state exploitation.

A Large Illicit Market

KPMG's 2025 study of the illicit cigarette trade estimated that counterfeit and smuggled cigarettes account for 21.1% of total cigarette consumption in Lithuania, up 1.6% from 2024 and the highest level in the 5-year reporting period. Lithuania has the highest share of smuggled cigarettes among the Baltic states, followed by Latvia at 18.7% and Estonia at 13.9%. This has important implications for tax revenue, fair competition and the investment environment. It is estimated that €109 million (approximately \$126 million) of total tax revenue was lost last year alone in Lithuania.⁵³

Furthermore, for legitimate producers, especially those working in an environment where similar products are highly exposed to smuggling, a large illicit market directly changes the conditions under which they invest and operate. So, for instance, Philip Morris International (PMI) has maintained a manufacturing presence in Lithuania since 1997, when it opened its Klaipėda factory. PMI reports cumulative investment of approximately €400 million in Klaipėda and

around 550 employees in its Lithuanian operations.⁵⁴ Therefore, a large illicit cigarette market not only affects public finances and law enforcement but also companies legitimately operating and investing in the country.

However, for our purposes, the scale of the illicit market matters for another reason, as it can sustain persistent criminal infrastructure that, in turn, could become a national-level security vulnerability. Products must be supplied, transported towards the border, moved across it, recovered and then distributed through inland transport and storage networks, while payments flow back through the system. Individual shipments may be intercepted or disappear, but the routes, relationships, knowledge and logistical capabilities behind them can remain and be reenacted. In other words, the commodity may change or disappear, but the network persists.

Public-private Partnership: from Exposure to Contribution

The private sector is not only a source of market data or a party affected by illicit trade. In many cases, it also possesses capabilities, expertise and information that can strengthen a state's ability to detect and disrupt illicit networks. In March 2026, PMI donated seven Autel Alpha drone systems to the Lithuanian government to support surveillance of balloon-borne

⁵³ KPMG, *Illicit Cigarette and Heated Tobacco Consumption*, 86–89, 130–139.

⁵⁴ Philip Morris International, "The First Investor's Recipe for Change: 30 Years of Growth, €400 Million Investment, and Exceptional Focus on Employees," September 21, 2023, <https://www.pmi.com/markets/lithuania/en/overview/the-first-investor-s-recipe-for-change-30-years-of-growth-400-million-investment-and-exceptional-focus-on-employees>.

cigarette smuggling from Belarus. The systems are equipped for day and night operations and are intended for use by the Lithuanian Riflemen's Union.⁵⁵ A different model is illustrated by the Lithuanian defense technology startup Luna Robotics, which has developed a night-vision camera system using its own resources to enable drones to detect smuggling balloons at night and has tested the technology with the Lithuanian military.⁵⁶ Together, these cases illustrate two complementary forms of public-private cooperation: companies can contribute existing resources and equipment, but they can also develop new capabilities in response to operational gaps.

This model is now being used more broadly. In July 2026, Lithuania launched a €3 million pre-commercial procurement program, inviting companies to develop technologies to detect, track and neutralize illegal airborne objects associated with weather balloons. The program is intended to develop and test innovative solutions for the protection of Lithuania's airspace.⁵⁷ The shift matters because it moves beyond ad hoc private support towards a structured mechanism through which the state can draw on private-sector innovation to address emerging security challenges.

The same principle should extend beyond technology donations and procurement. Businesses operating in sectors exposed to illicit trade often possess information and expertise that public authorities do not routinely see, such as unusual changes in supply chains, distribution patterns, payment behavior, logistics and market demand. Structured channels for sharing such information, combined with technology testing and joint problem definition, could help identify emerging risks before they become visible through seizures or other enforcement statistics. The objective is not to transfer enforcement responsibility to

the private sector, but to combine state authority and intelligence capabilities with private-sector technology, resources and sector knowledge.

Weaponized Migration and the Hardening of the Land Border

The 2021 migration crisis changed Lithuania's understanding of its border with Belarus. The border was no longer simply a line across which legal and illegal movement had to be controlled. It became a space where the Belarusian state could deliberately create pressure on Lithuanian institutions. During the initial phase of the crisis in 2021, more than 4,000 irregular migrants entered Lithuania through the border with Belarus.⁵⁸ As of September 2026, Lithuanian border guards have prevented more than 26,000 people from illegally entering Lithuania from Belarus since the crisis began.⁵⁹ The same dynamic was at play in Latvia, although the form and intensity of pressure have been changing over time and differ across countries. Latvia, like Lithuania, has treated the instrumentalization of migration from Belarus as a hybrid threat. In February 2026, Latvia, Lithuania and Poland committed to closer cooperation on these issues, including information sharing and coordinated responses.⁶⁰

Lithuania responded across several domains, combining border security, law enforcement, crisis management, diplomacy and international action. By the end of 2022, it had completed 530.8 km of physical barrier and installed 356.6 km of concertina wire along its border with Belarus.^{61,62}

⁵⁵ LRT, "Tobacco Giant Philip Morris Donates Drones to Lithuania to Fight Smuggling Balloons," 2026, <https://www.lrt.lt/en/news-in-english/19/2870160/tobacco-giant-philip-morris-do>.

⁵⁶ LRT, "Lithuanian Startup Develops Night-Vision Camera to Track Smuggling Balloons," 2026, <https://www.lrt.lt/en/news-in-english/19/2830544/lithuanian-startup-develops-night-vision-camera-to-track-smuggling-balloons>.

⁵⁷ Lithuanian State Border Guard Service, "3 mln. eurų inovatyviems sprendimams: verslas kviečiamas kurti technologijas Lietuvos oro erdvės apsaugai" [€3 Million for Innovative Solutions: Businesses Invited to Develop Technologies for Protecting Lithuania's Airspace], 2026, <https://vsat.lrv.lt/lt/naujienos/3-mln-euru-inovatyviems-sprendimams-verslas-kvieciamas-kurti-technologijas-lietuvos-oro-erdves-apsaugai-03x>.

⁵⁸ Ministry of the Interior of the Republic of Lithuania, "Frequently Asked Questions about Irregular Migrants Detained at the Border with Belarus," last updated September 20, 2023, <https://vrm.lrv.lt/en/information-on-irregular-migration/>.

⁵⁹ Lithuanian State Border Guard Service, "Neįleistų neteisėtų migrantų statistika" [Statistics on Irregular Migrants Prevented from Entering], updated August 10, 2026, <https://vsat.lrv.lt/lt/naujienos/neileistu-neteisetu-migrantu-statistika/>.

⁶⁰ Cabinet of Ministers of the Republic of Latvia, "Joint LT, LV, and PL Declaration on Strengthened Cooperation on Security of External Borders and Responding to Hybrid Threats," February 25, 2026, <https://www.mk.gov.lv/en/article/joint-lt-lv-and-pl-declaration-strengthened-cooperation-security-external-borders-and-responding-hybrid-threats>.

⁶¹ Lithuanian State Border Guard Service, 2022 metų veiklos ataskaita [2022 Annual Activity Report] (Vilnius, March 17, 2023), 9, https://vsat.lrv.lt/uploads/vsat/documents/files/2022%20m_%20VSAT%20ATASKAITA.docx.pdf.

⁶² Lithuanian State Border Guard Service, "Antradienį pasieniečiai 4 kartus išbaidė fizinį barjerą gadinusius baltarusius," October 11, 2023, <https://vsat.lrv.lt/lt/naujienos/antradieni-pasienieciai-4-kartus-isbaide-fizini-barjera-gadinusius-baltarusius/>.

Crucially, the nature of the operation was recognized beyond Lithuania. In November 2021, the North Atlantic Council condemned the ‘instrumentalization of irregular migration artificially created by Belarus’ as part of hybrid actions targeting Poland, Lithuania and Latvia for political purposes.⁶³ In 2021, then-NATO Secretary General Jens Stoltenberg described the use of vulnerable migrants by the Lukashenka regime as a hybrid tactic.⁶⁴ During her November 2021 visit to Vilnius, the European Commission President Ursula von der Leyen described the situation as a state-sponsored hybrid attack and said that migrants were being used as instruments for political purposes.⁶⁵

This distinction matters for this report. Migration did not itself become a hybrid threat; its deliberate instrumentalization and orchestrated nature by the Belarusian regime did. The instrument remained familiar, but the actor behind it, the way it was organized and its strategic purpose changed. The episode also had a criminal dimension. An investigation by the Belarusian Investigative Center found that Belarusian authorities granted 12 private companies privileged rights to issue visa invitations for citizens of Middle Eastern countries, with most of the companies linked to Belarusian security structures or their associated entities.⁶⁶ Lithuanian authorities also recorded instances in which Belarusian border guards actively directed and pushed migrants towards Lithuania. In one incident, Belarusian officers used metal shields to push a group of 13 migrants towards the Lithuanian border, while Lithuanian border guards said they had regularly provided the group with food and water.⁶⁷

Lithuania’s response to Belarusian pressure since 2021 has involved substantially hardening the physical border, with direct consequences for illicit trade. The Lithuanian SBGS has noted that strengthened border protection has made traditional land-based cigarette smuggling considerably more difficult. In

2025, SBGS seized 4,440,576 packs of cigarettes, more than three times the 2024 total of 1,386,714 packs and the highest annual quantity recorded in the history of SBGS since the restoration of independence.⁶⁸ However, the illicit market has not disappeared. Instead, criminal networks have adapted, with alternative methods emerging as certain routes become more difficult to use.

From Land to Air

The scale and speed of this adaptation are striking. Lithuania recorded no balloon-smuggling cases in 2022 and only three in 2023. The number increased to 226 in 2024 and, by 2025, Lithuanian border guards had intercepted 635 balloon-borne cigarette consignments from Belarus, along with 59 drones used to transport contraband. More than 1.6 million packs of cigarettes transported by balloons and drones were seized, while 171 people suspected of involvement in airborne smuggling were detained. SBGS estimates that more than four-fifths of cigarettes entering Lithuania illegally from Belarus in 2025 were transported by air, using balloons or unmanned aerial vehicles.⁶⁹

This reflects more than the rapid adoption of a new smuggling technique. It marks a shift in the operational domain. As the land border became more difficult to penetrate, illicit activity moved into low-altitude airspace. Therefore, the border is no longer simply a physical line on the ground; it increasingly extends into the airspace above it.

The platform’s simplicity can obscure the complexity of the system behind it. A standard balloon shipment carries around 1,500 packs of cigarettes and is typically equipped with a GPS device to help locate the payload after landing. Lithuanian investigations have documented smugglers using GPS equipment and

⁶³ NATO, “Statement by the North Atlantic Council on the Situation at the Poland-Belarus Border,” November 12, 2021, <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2021/11/12/statement-by-the-north-atlantic-council-on-the-situation-at-the-poland-belarus-border>.

⁶⁴ Jens Stoltenberg, “Doorstep Statement,” NATO, November 16, 2021, <https://www.nato.int/en/news-and-events/events/transcripts/2021/11/16/doorstep-statement>.

⁶⁵ European Commission, “Statement by President Ursula von der Leyen at the Joint Press Conference with Lithuanian President Gitanas Nausėda, Prime Minister Ingrida Šimonytė, and NATO Secretary General Jens Stoltenberg,” November 28, 2021, https://lithuania.representation.ec.europa.eu/news/ek-pirmininkes-u-von-der-leyen-pareiskimas-bendroje-spaudos-konferencijoje-su-lr-prezidentu-g-2021-11-28_lt.

⁶⁶ Ivashkevich, Ratmirova, and Viaznikoutsava, “Undercover of Security Forces.”

⁶⁷ BNS, “Two Migrant Groups Stranded on Lithuanian Border,” LRT, September 2, 2021, LRT, 2021, <https://www.lrt.lt/en/news-in-english/19/1484503/two-migrant-groups-stranded-on-lithuania-s-border>.

⁶⁸ Lithuanian State Border Guard Service, “Pernai sulaikytas rekordinis VSAT veiklos istorijoje cigarečių kontrabandos kiekis” [Record Amount of Cigarette Contraband Seized in VSAT History Last Year], January 9, 2026, <https://vsat.lrv.lt/lt/naujienos/pernai-sulaikytas-rekordinis-vsatai-veiklos-istorijoje-cigareciu-kontrabandos-kiekis-foto-2P2>.

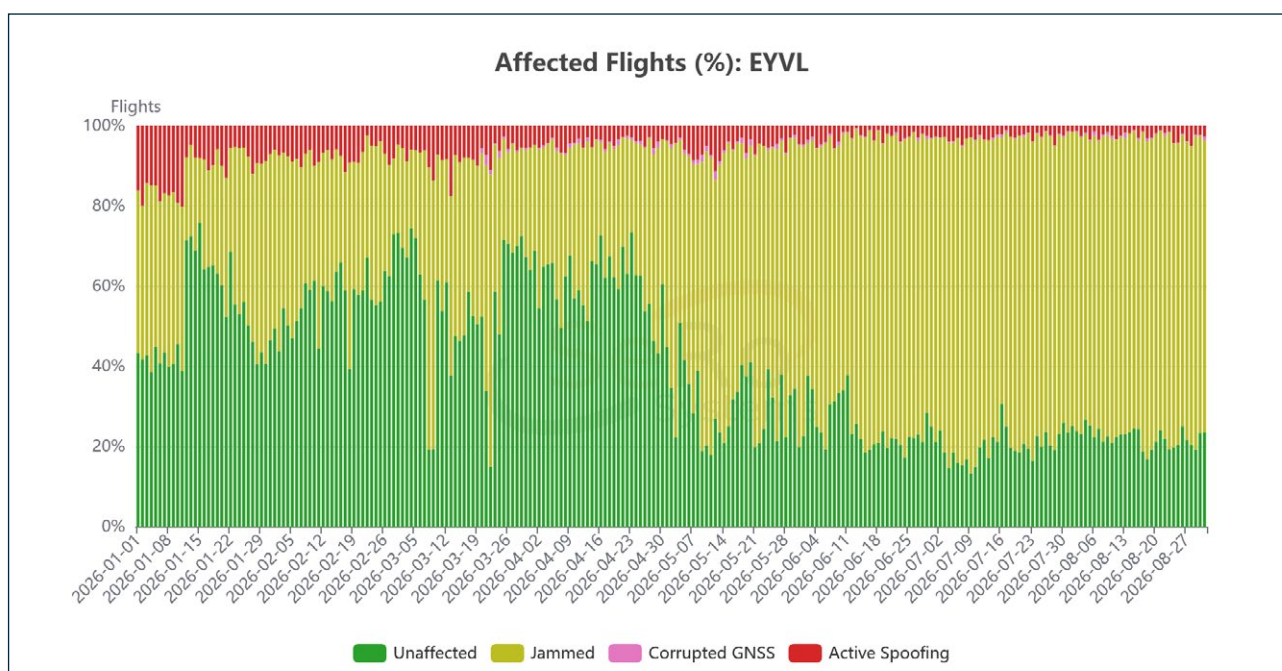
⁶⁹ Lithuanian State Border Guard Service, “Pernai sulaikytas rekordinis VSAT veiklos istorijoje cigarečių kontrabandos kiekis.”

specialized applications to track balloon movements and receive precise landing coordinates in Lithuania.^{70,71} For instance, in May 2026, police in Šalčininkai district dismantled an organized smuggling scheme. Searches uncovered GPS devices, communications-blocking equipment, night-vision equipment, binoculars, computers, mobile phones and cash used to coordinate the operation and monitor or hinder law-enforcement activity.⁷² The balloons themselves are cheap and disposable; the operational network behind them is not. It requires a launch point, tracking technology, a retrieval team operating inside Lithuania, and onward transport, storage and distribution, as well as communications and payment channels connecting the different stages of the operation.

Repeated operations also generate knowledge about a state's vulnerabilities: which areas are difficult to monitor, how quickly authorities respond, where payloads are likely to land successfully, which technologies are effective and where people can operate

with the least risk. Every successful or failed attempt thus contributes to organizational learning. The accumulated knowledge, experience and operational routines become a capability in their own right – precisely the capability this report seeks to understand.

The wider use of balloon technology in other parts of the world, such as the Korean Peninsula, reinforces this point. Beginning in late May 2024, North Korea sent thousands of balloons carrying waste and other materials into South Korea; some of these landed near or disrupted operations at Incheon International Airport. One balloon that landed on a runway contributed to a three-hour suspension of take-offs and landings. At the same time, GPS interference attributed to North Korea affected about 500 aircraft and hundreds of ships in the region over a five-day period.⁷³ The comparison should not be overstated, but it demonstrates how a relatively cheap and technically simple platform can be adapted from moving a payload into a more complex operational system.



Source: Ryšių reguliavimo tarnyba / Communications Regulatory Authority of Lithuania (RRT) <https://rrt.lt/>

⁷⁰ Lithuanian State Border Guard Service, "Pasieniečiai perėmė pirmą šiemet balionais iš Baltarusijos atskraidintą kontrabandos krovinį" [Border Guards Intercept the First Contraband Shipment of the Year Flown from Belarus by Balloons], January 6, 2026, <https://vsat.lrv.lt/lt/naujienos/pasienieciai-pereme-pirma-siemet-balionais-is-baltarusijos-atskraidinta-kontrabandos-krovini-foto-Tm7/>.

⁷¹ BNS, "Lithuanian Authorities Arrest 21 in Balloon-Based Cigarette Smuggling Probe," LRT, December 16, 2025, <https://www.lrt.lt/en/news-in-english/19/2777215/lithuanian-authorities-arrest-21-in-balloon-based-cigarette-smuggling-probe>.

⁷² Vilnius County Police, "Šalčininkų rajone užkardytas stambus kontrabandos kanalas – sulaikyti trys asmenys" [Major Smuggling Channel Disrupted in Šalčininkai District – Three People Detained], May 29, 2026, <https://vilnius.policija.lrv.lt/lt/naujienos/salcininku-rajone-uzkardytas-stambus-kontrabandos-kanalas-sulaikyti-trys-asmenys-cigaretes-gabentos-meteorologiniais-balionais-video-Pw6Q>.

⁷³ Lisa Barrington, "North Korea Balloons, GPS Interference Raise Safety Risks for Airlines," Reuters, July 10, 2024, <https://www.reuters.com/world/asia-pacific/north-korea-balloons-gps-interference-raise-safety-risks-airlines-2024-07-10/>.

The relevant capability lies less in the balloon itself than in the combination of payload, navigation, communications, launch and recovery systems, and the network able to operate them.

From Smuggling to a Wider Security Problem

The consequences extend well beyond customs and border enforcement. Balloon activity has repeatedly disrupted civilian aviation, affecting hundreds of flights and tens of thousands of passengers. In the second half of 2025, disruptions resulted in more than 60 hours of closures at Vilnius Airport, affecting more than 350 flights and approximately 51,000 passengers.⁷⁴ What begins as illicit cross-border trade can thus affect airspace security, aviation, policing, border protection, critical infrastructure and crisis management.

This distinction is important. Disruption alone does not prove that every balloon launch is intended to interfere with aviation, nor do we make that claim. But intent is not the only issue relevant to national security. At the same time, Lithuanian aviation authorities have identified indications that some launches were deliberately directed towards sensitive aviation areas. In December 2025, Oro Navigacija, the head of Lithuania's air-navigation service, said that balloons were being sent 'very precisely' into areas most sensitive for aviation and approaches to Vilnius International Airport.⁷⁵

A low-cost illicit network has also shown it can repeatedly cross a protected NATO and EU border and generate disproportionate disruption in a critical sector. It tests detection and response systems, forces multiple institutions to react, consumes resources, and exposes dependencies and coordination gaps. This also creates a potential learning opportunity for hostile actors. They can observe which methods

help to evade detection, what level of activity causes significant disruption, which institutions respond, how quickly decisions are made and where vulnerabilities remain.

The security concern is therefore broader than the balloons themselves. Repeated incidents expose vulnerabilities in border control, airspace safety and security, and crisis response that more capable hostile actors could study, adapt or exploit.

In response, Lithuania has stepped up enforcement in border districts through joint preventive operations involving the police, SBGS, the Customs Criminal Service and the Military Police, detaining more than 80 people.⁷⁶ This enforcement has increasingly focused on the networks behind balloon smuggling. On 22 May 2026, Lithuania's Prosecutor General's Office announced coordinated operations against two suspected criminal organizations involved in balloon-borne cigarette smuggling, with 27 people detained. Of note, this investigation covered not only smuggling but also suspected assistance to another state acting against Lithuania and other alleged offences.⁷⁷ The case demonstrates why national security scrutiny may become necessary when criminal infrastructure intersects with suspected hostile-state activity. Its significance lies less in the number of suspects detained than in what such investigations reveal about the underlying infrastructure.

Again, this does not establish that Belarus directs or controls all illicit cigarette trade targeting Lithuania and other European countries. Rather, it establishes something narrower and more useful. A criminal market that begins with cigarettes can sustain cross-border logistics, technology, recovery networks and knowledge of Lithuanian vulnerabilities. When those capabilities intersect with insider access or possible assistance to a hostile state, the security significance of the network becomes clear.

⁷⁴ European Parliament, "Ongoing Belarusian Hybrid Attacks against Lithuania," December 11, 2025, <https://www.europarl.europa.eu/news/en/agenda/plenary-news/2025-12-15/12/ongoing-belarusian-hybrid-attacks-against-lithuania>.

⁷⁵ BNS and LRT.lt, "Smugglers' Balloons Deliberately Launched into Aviation Danger Zones – Lithuanian Official," LRT, December 1, 2025, <https://archyvai.lrt.lt/en/news-in-english/19/2762185/smugglers-balloons-deliberately-launched-in-to-aviation-danger-zones-lithuanian-official>.

⁷⁶ Lithuanian Police, "Prevenčinių reidų pasienio rajonuose rezultatai" [Results of Preventive Raids in Border Districts], updated August 10, 2026, <https://policija.lrv.lt/lt/naujienos/reidu-pasienyje-rezultatai-kJ96/>.

⁷⁷ Prosecutor General's Office of the Republic of Lithuania and Lithuanian Criminal Police Bureau, "Plataus masto policijos ir prokuratūros operacija: ardomi „balionų“ kontrabandos nusikalstami tinklai" [Large-Scale Police and Prosecutor's Office Operation: Criminal Balloon-Smuggling Networks Dismantled], May 22, 2026, <https://www.prokuraturos.lt/lt/plataus-masto-policijos-ir-prokuraturos-operacija-ardomi-balionu-kontrabandos-nusikalstami-tinklai/12449>.

7.

Estonia: When Criminal Infrastructure Becomes an Intelligence Asset

Estonia provides a different and, in some respects, more direct window into the same problem. Its eastern border remains one of the few functioning land interfaces between Russia and the Euro-Atlantic community. The same channels that allow controlled legitimate movement can also be exploited by smugglers, sanctions evaders, organized criminal groups and intelligence operatives.

Estonia provides a particularly clear illustration of how criminal and cross-border networks can become intelligence assets. A report by the Estonian Internal Security Service (KAPO) outlined why the unit of analysis should be the network rather than the offence. Russian intelligence services have repeatedly exploited individuals involved in smuggling and other cross-border criminal activity. These activities aim to accomplish several objectives: fund clandestine influence operations, acquire restricted technology, evade international sanctions and recruit human intelligence assets.⁷⁸

The Estonian–Russian border also demonstrates how ordinary criminal activity can intersect with Russia’s broader hybrid toolkit. Russian intelligence services, principally the FSB and the GRU, have long exploited individuals engaged in cross-border criminal activity as sources of information and operational support. Since 2022, illicit trade has also become an increasingly relevant channel for sanctions circumvention.

The Eston Kohver case provided an early and stark example. When the KAPO officer was seized by Russian operatives in 2014, he was investigating a cigarette-smuggling network cultivated by Russian security services, offering the smugglers freer passage across the border in exchange for cooperation.⁷⁹ Other documented cases reinforce the pattern. Pavel Romanov was an experienced cigarette smuggler recruited by the FSB in 1994 and convicted in Estonia in 2015. According to investigative reporting, Romanov and members of his network were tasked with collecting information on Estonian police and border-guard posts, KAPO facilities and military installations used by NATO Allies. Other convicted FSB collaborators collected information on border-guard operations and the movement of Estonian and Allied military equipment.⁸⁰ The point is not simply that criminals can become spies. It is that infrastructure developed for criminal purposes, such as access, mobility, border knowledge, personal networks and clandestine operating experience, reduces the cost of building an intelligence capability. This is criminal infrastructure functioning as an intelligence asset.

Several recent criminal cases illustrate the continuing convergence of cross-border business, sanctions evasion and espionage. In July 2025, Pavel Kapustin, a Russian citizen living in Narva, was sentenced to 6.5 years in prison for cooperating with the FSB and

⁷⁸ Estonian Internal Security Service (KAPO), “Annual Reviews,” <https://kapo.ee/en/content/annual-reviews/>.

⁷⁹ Holger Roonemaa, “How Smuggler Helped Russia to Catch Estonian Officer,” Re:Baltica/Postimees, September 13, 2017, <https://en.rebaltica.lv/2017/09/how-smuggler-helped-russia-to-catch-estonian-officer/>.

⁸⁰ Holger Roonemaa, “These Cigarette Smugglers Are on the Frontlines of Russia’s Spy Wars,” BuzzFeed News, September 13, 2017, <https://www.buzzfeednews.com/article/holgerroonemaa/these-cigarette-smugglers-are-on-the-frontlines-of-russias>.

violations of sanctions. He provided the FSB with information concerning developments in Narva and local public attitudes. At the same time, he operated a sanctions-evasion scheme in which luxury goods ordered by customers in Russia were procured in Estonia and elsewhere in Europe, brought to Narva, and then transported to Russia.⁸¹

An even more direct illustration of the border as an intelligence operating environment is provided by the case of Anatoly Privalov, who was sentenced in 2026. He lived between Narva and St Petersburg and frequently crossed the border because of his transport business. During approximately a decade of cooperation with the FSB, his tasks reportedly expanded from reporting observations made during his travels to photographing specified locations, identifying potential recruits and transporting Estonian SIM cards to Russia. His movements allowed him to collect information on military exercises, military columns, border fortifications, concrete obstacles and other security-related infrastructure. His role subsequently expanded to preparations for potentially high-impact acts of sabotage.⁸²

These cases show how frequent border crossers can become valuable intelligence assets precisely because their activities provide them with mobility and plausible reasons for travelling. Their importance may increase, as effective Estonian counterintelligence has severely constrained Russia's ability to maintain traditional intelligence networks on Estonian territory.

Adaptation and Displacement

Estonia also shows the adaptive nature of the networks themselves. Stronger physical border infrastructure has reduced traditional green-border smuggling but has not eliminated illicit activity. Instead, activity has shifted towards official crossing points, with more sophisticated concealment, courier networks and procurement structures.

Border hardening creates deterrence, but it can also create displacement. In April 2026, KAPO Director General Margo Palloson stated that Russian intelli-

gence services could no longer operate in Estonia in the same way as previously and were therefore seeking alternative methods and easier agents.⁸³ Russian intelligence services have consequently adapted by recruiting agents remotely, tasking individuals from Russian territory, and relying increasingly on criminal or otherwise expendable proxies to conduct operations inside Estonia.

This is an important point of convergence with the situation in Lithuania. In Lithuania, stronger land-border protection contributed to smuggling moving into low-altitude airspace. In Estonia, stronger controls pushed activity towards official crossings, better concealment and more complex procurement mechanisms. The methods differ, but the underlying logic of adaptation is the same.

Sanctions Evasion: From Illicit Market to Strategic Effect

Estonia adds another dimension particularly relevant to the transatlantic argument: sanctions circumvention. Since 2022, the most strategically important aspect of illicit trade on the Estonian–Russian border has been sanctions evasion. Following Russia's full-scale invasion of Ukraine, the US, the EU and their partners imposed extensive restrictions on exports of advanced technologies, dual-use items, electronics and industrial components to Russia. These measures are intended to degrade Russia's ability to sustain its war against Ukraine, including by restricting access to technologies and components relevant to its military–industrial sector. Attempts at sanction evasion range from individual couriers carrying restricted goods to sophisticated corporate networks using shell companies, false declarations and intermediary jurisdictions. Here the commodity itself can become strategically relevant: electronics, drone components, precision optics and satellite equipment can contribute directly to Russian military and technological capability.

Estonian authorities have identified cases in which companies operating in Estonia, sometimes with no

⁸¹ ERR News, "Narva Resident Handed 6.5 Year Prison Sentence for Espionage, Violating Sanctions," July 22, 2025, <https://news.err.ee/1609751090/narva-resident-handed-6-5-year-prison-sentence-for-espionage-violating-sanctions>.

⁸² Prosecutor's Office of Estonia, "The Court Convicted a Resident of Narva of an Offence against the State," February 20, 2026, <https://www.prokuratuur.ee/en/news/court-convicted-resident-narva-offence-against-state>.

⁸³ ERR News, "Estonia Caught a Record Number of Russian Collaborators in 2025," April 13, 2026, <https://news.err.ee/1609994248/estonia-caught-a-record-number-of-russian-collaborators-in-2025>.

genuine business activity in the country, became involved in procurement networks that transferred strategic goods from Western manufacturers through intermediary countries before the goods ultimately reached Russia. Such networks can exploit the same logistical pathways and commercial relationships used in traditional smuggling operations. Goods may be falsely declared in customs documentation, routed through intermediary jurisdictions, exported to shell companies, re-exported through third countries or concealed within legitimate commercial shipments.

Strategic technologies, electronics and dual-use goods are particularly sensitive categories because they can support Russian weapons production, communications systems, drones and military logistics.

The Serniya Network illustrates this point clearly. Vadim Konoshchenok, detained by Estonian authorities and subsequently extradited to the US in late 2022, operated as part of an FSB-linked procurement network that used an Estonian front company to move US-origin ammunition, advanced semiconductors and high-precision electronic components into Russia. Operating through this Estonian front company, he systematically smuggled thousands of US-origin military-grade rifle cartridges, advanced semiconductors and high-precision electronic components across the Estonian border into Russia to support the Russian military industry.⁸⁴

Estonia therefore sharpens this report's central argument. Criminal infrastructure matters not because a hostile state might one day find it useful, but because documented cases show it already has.

⁸⁴ Mihkel Kärmas and Irina Kablukova, "How Did a Man from Estonia Become a Valuable Prisoner for the Kremlin?," ERR News, September 4, 2024, <https://news.err.ee/1609443845/how-did-a-man-from-estonia-become-a-valuable-prisoner-for-the-kremlin>.

8.

Latvia: Sanctions Evasion and the Displacement of Criminal Infrastructure

Latvia adds a third and distinct perspective on the same problem. Its relevance lies less in one illicit commodity than in the interaction between financial-sector reform, sanctions-evasion prevention, logistics and border adaptation. Latvia borders both Russia and Belarus, while its roads, railways, ports and transport hubs connect the eastern border with the European Single Market. This geography creates exposure. But Latvia's experience is particularly useful because it also shows how a state can substantially strengthen one vulnerable system while still needing to identify the risks that remain – or emerge – in adjacent channels.

From a High-Risk Non-Resident Banking Model to a Different Risk Landscape

For years, Latvia's banking sector relied heavily on non-resident business and large cross-border financial flows, which made the country particularly exposed to money-laundering risks associated with foreign customers, shell companies and opaque ownership structures. This became a major vulnerability for the Latvian financial system and eventually

prompted a deliberate policy shift aimed at reducing high-risk non-resident business and reshaping the banking sector.⁸⁵

Latvia enters this discussion with a particular financial history. MONEYVAL's sixth-round mutual evaluation describes how, since 2017, Latvia has moved away from its former position as a regional financial center heavily oriented towards non-resident customers. Between 2017 and 2023, deposits from non-EU non-resident customers decreased by 87%, credit turnover involving beneficial owners from high-risk countries by 95%, and credit turnover linked to shell companies by 99%. MONEYVAL concludes that the cross-border illicit-flow risks associated with Latvia's former financial-centre model no longer pose the same significant threat. In other words, Latvia substantially reduced one of its most important structural money-laundering vulnerabilities; the policy question then becomes where the remaining illicit-finance risks moved and how the broader criminal infrastructure adapted.⁸⁶

That transformation is important for resilience. It demonstrates that a vulnerable financial gateway can be deliberately strengthened through political commitment, supervision, financial intelligence and inter-institutional cooperation. At the same time, the underlying money-laundering risk has not disappeared. MONEYVAL identifies today's principal threats pri-

⁸⁵ Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), Anti-Money Laundering and Counter-Terrorist Financing Measures: Latvia, Sixth Round Mutual Evaluation Report, MONEYVAL(2026)2 (Strasbourg: Council of Europe, February 2026), 14, <https://rm.coe.int/moneyval-2026-2-mer-latvia-en/48802ab1ea>.

⁸⁶ MONEYVAL, *Latvia: Sixth Round Mutual Evaluation Report*, 14.

marily in the shadow economy, fraud and corruption, while also noting exposure to proceeds generated by foreign crime. It highlights cash, tax-related crime, smuggling of excise goods and narcotics, and weaknesses in aligning some non-financial-sector supervision with national risk.⁸⁷

This establishes a wider policy lesson. Success in one channel cannot be treated as eliminating the underlying threat. Authorities must ask where the activity, facilitators and financial flows go next. In that sense, Latvia provides a financial analogue to the physical border problem described elsewhere in this report: when a route becomes more difficult to use, a network may adapt through another route, intermediary, payment mechanism or business structure.

Sanctions Evasion as Service-Based Criminal Infrastructure

Sanctions enforcement makes that adaptation problem clearly visible. Latvia's proximity to Russia and Belarus, historic commercial links and role in regional transport create recurring exposure to attempts to conceal the true nature, origin, destination or beneficiary of transactions. Several recurring methods can be identified from specific cases in Latvia and from customs reports, including incorrect commodity codes, third-country routing, intermediary companies and accounts, altered documentation, and payment arrangements that make the final beneficiary or destination more difficult to establish.⁸⁸

Not every unusual trade flow constitutes sanctions evasion, but repeated evasion creates a market for professional facilitation. Public reporting based on information from the Latvian State Revenue Service

has described cases in which declarants or customs brokers advise clients on how to structure documentation to reduce scrutiny. Once such expertise becomes commercially available, sanctions evasion begins to resemble a service-based criminal market. In other words, the same facilitator, corporate structure, customs knowledge or payment channel can potentially serve multiple clients and commodities.⁸⁹

Latvian customs data illustrate the enforcement burden. In 2023, the State Revenue Service recorded 7,789 sanctions-related violations, including 2,175 cases in which customs prevented procedures involving goods subject to sanctions. In 2024, the corresponding figures increased to 9,175 sanctions-related violations and 3,147 cases in which customs prevented goods from leaving the EU or entering it from Russia or Belarus (increases of approximately 18% and 45%, respectively). These numbers do not prove there is organized crime or state involvement in every case, but they do illustrate the scale of the burden associated with sanctions enforcement.⁹⁰

This is a telling example of criminal infrastructure. The reusable capability is not necessarily a hidden border path or a vehicle. It may be a customs broker who knows where scrutiny is weak, a company that can generate plausible commercial cover, an intermediary jurisdiction, a payment mechanism, a cryptocurrency service, or a network of entities that obscures beneficial ownership and destination. In sanctions cases, those capabilities can have direct strategic effects by helping Russian or Belarusian actors retain access to finance, technology, components or markets that restrictive measures are intended to deny.

⁸⁷ MONEYVAL, *Latvia: Sixth Round Mutual Evaluation Report*, 14–16, 48–49, 62.

⁸⁸ Matīss Arnicāns, "Sankcijas pret Krieviju apiet, mainot preču kodus un iesaistot starpniekus" [Sanctions against Russia Are Circumvented by Changing Commodity Codes and Using Intermediaries], LSM, August 28, 2022, <https://www.lsm.lv/raksts/zinas/ekonomika/sankcijas-pret-krieviju-apiet-mainot-precu-kodus-un-iesaistot-starpniekus.a471231/>; Ella Semjonova, "«De facto»: Latvijas uzņēmumi sankcijas pret Krieviju šogad apiet vairāk; tiesas pagaidām netiek galā" [Latvian Companies Are Circumventing Sanctions against Russia More Often This Year; Courts Are Not Yet Keeping Up], LSM, November 24, 2024, <https://www.lsm.lv/raksts/zinas/latvija/24.11.2024-de-facto-latvijas-uznemumi-sankcijas-pret-krieviju-sogad-apiet-vairak-tiesas-pagaidam-netiek-gala.a577607/>.

⁸⁹ Semjonova, "«De facto»: Latvijas uzņēmumi sankcijas pret Krieviju šogad apiet vairāk."

⁹⁰ State Revenue Service of the Republic of Latvia, "Pagājušajā gadā muitas kontroles pasākumu rezultātā novērsti vairāk nekā 14 500 pārkāpumi" [More than 14,500 Violations Prevented as a Result of Customs Control Measures Last Year], January 26, 2024, <https://www.vid.gov.lv/lv/jaunums/pagajusaja-gada-muitas-kontroles-pasakumu-rezultata-noversti-vairak-neka-14-500-parkapumi>; State Revenue Service of the Republic of Latvia, Valsts ieņēmumu dienesta Publiskais pārskats 2024 [State Revenue Service Public Report 2024], 19, <https://www.vid.gov.lv/lv/media/30752/download?attachment=>.

The TGR Group: a Latvia-Linked Transatlantic Financial- Network Case

The TGR Group provides Latvia with a particularly compelling financial and transatlantic example. In December 2024, the US Department of the Treasury described the TGR Group as an extensive sanctions-evasion and money-laundering network used by Russian elites to circumvent US and international sanctions, including through digital assets. A Latvian national, Andrejs Bradens, was identified as associated with several TGR Group companies and as owner or director of various entities in the network.⁹¹

The wider picture is even more instructive. The UK NCA identified the TGR Group and the closely cooperating Smart network as professional money-laundering infrastructures servicing transnational organized crime groups, Russian elites and sanctioned actors. Their activities combined street cash, cryptocurrency, cross-border settlement, sanctions evasion and access to legitimate Western markets. The Smart network was used to fund Russian espionage operations, while TGR-linked activity included concealing transfers most likely intended to support a Russian state-funded media organization and an associated company facilitating exports of electronic components to Russia.⁹²

This is precisely the type of case that moves the analysis beyond a single offence. The strategic value lies in the infrastructure: professional financial intermediaries, companies across several jurisdictions, crypto-to-cash conversion, property transactions, trade-based laundering and access to Western financial and commercial systems. It also provides a second

concrete Baltic–US cooperation precedent alongside the Serniya Network. In both cases, Baltic-linked actors or infrastructure became visible within a wider Russian state-related network, while US sanctions and financial and criminal-enforcement tools helped disrupt it.

Border Strengthening and the Engineering of Alternative Routes

Latvia also illustrates the physical aspect of the same displacement problem. Its eastern-border policy increasingly combines fencing, patrol roads, sensors, video surveillance, data-transmission networks and real-time operational response – a model often described as a ‘smart border’. This approach matters not only for increased physical protection but also because it creates a data-generating system in which attempted violations can be detected, compared and linked to an operational response.⁹³

However, stronger barriers also generate adaptation. In November 2025, Latvian authorities intercepted eight meteorological balloons carrying illicit cigarettes from Belarus after the objects crossed into Latvian airspace. The operation began after Latvian services received early signals from Lithuanian partners, making the case notable not only for the use of balloons but also for the regional diffusion of a method already seen at scale in Lithuania. The platform differed from conventional land smuggling, but the infrastructure logic remained familiar: launch, navigation, tracking, recovery, inland logistics and coordination.⁹⁴

Underground routes represent another way to bypass barriers. In August 2026, Latvian border guards identified two separate tunnels used by individuals

⁹¹ U.S. Department of the Treasury, “Treasury Exposes Money Laundering Network Using Digital Assets to Evade Sanctions,” December 4, 2024, <https://home.treasury.gov/news/press-releases/jy2735>.

⁹² National Crime Agency, “Operation Destabilise: NCA Disrupts \$Multi-Billion Russian Money Laundering Networks with Links to Drugs, Ransomware and Espionage, Resulting in 84 Arrests,” December 4, 2024, <https://www.nationalcrimeagency.gov.uk/news/operation-destabilise-nca-disrupts-multi-billion-russian-money-laundering-networks-with-links-to-drugs-ransomware-and-espionage-resulting-in-84-arrests>.

⁹³ Cabinet of Ministers of the Republic of Latvia, “Patrulēšanas joslas izbūve stiprinās mūsu robežu un atvieglos kontrabandas apkarošanu” [Construction of the Patrol Strip Will Strengthen Our Border and Facilitate the Fight against Smuggling], August 30, 2024, <https://www.mk.gov.lv/lv/jaunums/patrulesanas-joslas-izbuve-stiprinas-musu-robezu-un-atvieglos-kontrabandas-apkarosanu>; Ministry of the Interior of the Republic of Latvia, “Austrumu robežas infrastruktūras izbūve tuvojas noslēgumam” [Construction of the Eastern Border Infrastructure Nears Completion], July 28, 2026, <https://www.iem.gov.lv/lv/jaunums/austrumu-robezas-infrastrukturas-izbuve-tuvojas-noslegumam>.

⁹⁴ State Border Guard of Latvia, “Latvijā fiksēti vairāki kontrabandistu baloni no Baltkrievijas” [Several Smugglers’ Balloons from Belarus Detected in Latvia], November 24, 2025, <https://www.rs.gov.lv/lv/jaunums/latvija-fikseti-vairaki-kontra-bandistu-baloni-no-baltkrievijas>.

to cross the border from Belarus, first by 15 individuals and later by 28. Similar tunnels were detected on the Lithuanian side of its border with Belarus in July and August 2026; the Lithuanian SBGS reported 12 attempts that year to enter Lithuania by digging underground tunnels. Poland had already repeatedly encountered the same method in 2025, including an incident in December that year in which a tunnel beneath the physical barrier was used by more than 180 migrants.^{95,96}

The importance of these cases lies in the method employed, not in assuming functions not established by evidence. The tunnels were identified in connection with irregular migration; they should not be considered as proven routes for smuggling cigarettes, cash or other goods. They demonstrate a regional capacity to engineer routes around strengthened physical barriers. The same analytical rule applies as with balloons: the immediate payload explains the incident, but the method and the people capable of financing, constructing, concealing and operating the route explain the infrastructure.

The Latvian case also strengthens the evidence for a hostile-state nexus. In July 2026, Latvia's Prosecutor General's Office opened criminal proceedings over alleged criminal activity by Belarusian border-service officials. The proceedings followed a State Border Guard submission describing the migration pressure since 2021 not as a collection of isolated attempts at illegal crossing, but as deliberate and systematic unlawful activity by an organized group allegedly including Belarusian border officials and aimed at undermining Latvia. The case is under investigation and should be treated accordingly, but it is important because it moves the state-criminal interface from political assessment into a formal criminal-law process.⁹⁷

The Latvian Lesson

Latvia therefore adds a distinctive lesson to the Baltic picture. Lithuania shows how smuggling can shift from land to air and can acquire wider security significance. Estonia shows how criminal mobility, border knowledge and procurement infrastructure can become intelligence and sanctions-evasion assets. Latvia shows how both financial and physical controls can change the shape of the risk: the former non-resident banking model can be dismantled, while money-laundering threats persist in a different risk environment; physical borders can be strengthened, while networks test balloons, tunnels and other alternatives; sanctions can become stricter, while professional facilitators develop methods for disguising destination, ownership and payment.

The policy implication is not that enforcement merely displaces crime and therefore fails. The opposite is true: strengthening vulnerable systems is essential. The lesson is that success must be measured at a network level. A route closed, a banking vulnerability removed or a shipment stopped is a genuine result, but the next question should always be whether the underlying organizers, facilitators, financial channels and assets have also been disrupted – or whether they have simply moved.

⁹⁵ State Border Guard of Latvia, "Border Guards Detect 15 Persons Who Illegally Crossed the State Border through an Underground Tunnel," August 11, 2026, <https://www.rs.gov.lv/en/article/border-guards-detect-15-persons-who-illegally-crossed-state-border-through-underground-tunnel>; State Border Guard of Latvia, "Border Guards Detected 28 Persons Who Illegally Crossed the State Border through a Dug Underground Tunnel," August 21, 2026, <https://www.rs.gov.lv/en/article/border-guards-detected-28-persons-who-illegally-crossed-state-border-through-dug-underground-tunnel>.

⁹⁶ State Border Guard Service of Lithuania, "Varėnos pasieniečiai aptiko jau trečią iš Baltarusijos vedantį tunelį" [Varėna Border Guards Discover Third Tunnel Leading from Belarus], August 5, 2026, <https://vsat.lrv.lt/lt/naujienos/varenos-pasienieciai-aptiko-jau-trecia-is-baltarusijos-vedanti-tuneli-foto-B2v/>; Polish Border Guard, "Podziemne przejście pod polsko-białoruską granicą" [Underground Passage under the Polish-Belarusian Border], December 12, 2025, <https://strazgraniczna.pl/pl/aktualnosci/15117,Podziemne-przejscie-pod-polsko-bialoruska-granica.html>.

⁹⁷ Prosecutor General's Office of the Republic of Latvia, "Ģenerālprokuratūrā uzsākts kriminālprocess par Baltkrievijas Republikas robežsardzes struktūru amatpersonu noziedzīgajām darbībām" [Criminal Proceedings Initiated concerning Criminal Activities of Officials of the Border Guard Structures of the Republic of Belarus], July 15, 2026, <https://www.prokuratūra.lv/lv/aktualitates/2026/aktualitates/generalprokuratura-uzsakts-kriminalprocess-par-baltkrievijas-republikas-robezsardzes-strukturam-amatpersonu-noziedzigajam-darbibam-3809>.

9.

From National Cases to a Baltic Network Picture

The Lithuanian, Latvian and Estonian cases are most useful when considered together rather than as three separate national stories. Looking across all three, patterns and differences may emerge that would otherwise be harder to discern.

First, criminal infrastructure adapts, and displacement may be physical, financial or organizational. Lithuania strengthened its land border, and smuggling moved into low-altitude airspace. Latvia encountered the same balloon method and, together with Lithuania and previously Poland, observed underground routes engineered to bypass physical barriers. Estonia strengthened border controls, and illicit activity shifted towards official crossings, concealment, couriers and procurement structures. Latvia's financial-sector experience adds a parallel lesson: a major vulnerability in the former non-resident banking model was reduced, but the need to monitor money-laundering risk in cash, the shadow economy, non-financial sectors and cross-border trade remained. Therefore, enforcement success can change the channel through which a network operates without necessarily removing the organizers, facilitators or financial base behind it.

Second, the same infrastructure can support different activities. Routes, businesses, couriers, finance and cross-border access can move cigarettes, sanctioned goods or strategically relevant technology. The people operating them can also collect information, provide logistical services or become recruitment targets.

Third, capability matters more than commodities. A cigarette, semiconductor, or package of sanctioned or prohibited dual-use goods may trigger a different

legal regime. The underlying capability – moving goods, people, information or money covertly across jurisdictions – can be substantially the same.

Fourth, a border is more than a line on the ground. In Lithuania's case, the border was extended into low-altitude airspace. In Estonia's case, the border extended into mobility, business structures, procurement networks and intelligence activity.

Fifth, the nexus is institutional as well as operational. The same system may appear to customs as smuggling, to financial investigators as suspicious transactions, to police as organized crime, to counterintelligence as recruitment infrastructure, and to national security authorities as part of a hostile-state campaign. This is precisely the institutional seam that the novel hybrid-threat literature identifies.⁹⁸

The Baltic states should therefore be seen as countries targeted by foreign governments using domestic and cross-border criminal ecosystems to enable illicit trade, sanctions evasion, and illicit financial flows and logistics between Russia, Belarus and European countries further afield.

Criminal and sanctions-evasion networks rarely operate within neat national boundaries. The same company or intermediary may appear in several jurisdictions; routes disrupted in Lithuania may shift towards Latvia, Poland, ports or alternative transport corridors; technologies and operational methods can spread; and financial flows may pass through countries far removed from the location of a physical seizure. Pressure in one part of the region may therefore displace activity rather than eliminate it.

⁹⁸ Bajarūnas, "The Hybrid Threat Imperative."

The balloon and tunnel cases show why this regional frame matters. Latvian authorities intercepted balloon-borne cigarette consignments from Belarus after receiving early signals from Lithuanian partners, while underground routes designed to bypass strengthened border barriers have been detected in Latvia and Lithuania in 2026 and repeatedly in Poland in 2025. These cases do not establish that one

regional organization controls every method. They demonstrate something narrower but operationally important: techniques for bypassing enforcement can diffuse across borders, and neighboring states may detect the same adaptation at different times. Therefore, a Baltic network picture should track not only recurring actors and companies but also recurring methods, technologies and enabling know-how.

10.

Why This Is a Transatlantic Issue

The same logic provides the basis for a Baltic–US comparison. The US southern border is not the Baltic border with Russia and Belarus, and fentanyl trafficking is fundamentally different from illicit tobacco. The scale, social impact, actors and geopolitical context differ substantially. The useful comparison lies not in the commodities themselves, but in the structure and adaptability of the networks behind them.

The fentanyl crisis makes this infrastructure logic relevant for a US audience. Provisional data from the US Centers for Disease Control and Prevention estimate 69,973 drug-overdose deaths in the US in 2025, including 44,564 deaths involving opioids.⁹⁹ The human cost is immediate, but a transnational system sustains the ongoing operational problem. The Drug Enforcement Administration's 2025 National Drug Threat Assessment¹⁰⁰ identified the Sinaloa Cartel and the Jalisco New Generation Cartel as the dominant organisations trafficking the synthetic drugs driving US drug-poisoning deaths. Their procurement, distribution and financial-support networks extend across Latin America, China and other global nodes; they maintain precursor-chemical supply chains, clandestine production in Mexico, smuggling routes into the US and distribution hubs in US cities.

The financial layer is itself a specialized criminal market. In August 2025, the US Financial Crimes Enforce-

ment Network (FinCEN) reported analysing 137,153 Bank Secrecy Act reports associated with suspected Chinese money-laundering-network activity between 2020 and 2024,¹⁰¹ involving approximately \$312 billion in suspicious transactions. FinCEN assessed that such professional networks are heavily used by Mexico-based cartels to launder drug proceeds. The 2026 US National Money Laundering Risk Assessment¹⁰² makes a wider point: professional money-laundering networks operate as service providers, giving criminal organizations expertise, scale and access to financial channels that make crime more profitable and networks more difficult to unravel. This does not imply Chinese state direction; it illustrates how a transnational financial ecosystem can sustain criminal capability across jurisdictions.

The same infrastructure logic appears in organized migrant smuggling. The policy debate over migration is distinct from the criminal question. From a criminal-infrastructure perspective, the relevant actors are the transnational organizations that profit from moving people using routes, guides, vehicles, safe houses, document fraud, payments and coercive control. In 2025, the US Department of Justice expanded Joint Task Force Alpha's operations to additional northern and maritime border districts specifically to dismantle transnational human-smuggling and traf-

⁹⁹ U.S. Centers for Disease Control and Prevention, National Center for Health Statistics, "U.S. Overdose Deaths Decrease for Third Consecutive Year in 2025," May 13, 2026, <https://www.cdc.gov/nchs/pressroom/releases/20260513.html>.

¹⁰⁰ U.S. Drug Enforcement Administration, 2025 National Drug Threat Assessment (Washington, DC: U.S. Department of Justice, May 2025), <https://www.dea.gov/sites/default/files/2025-07/2025NationalDrugThreatAssessment.pdf>.

¹⁰¹ U.S. Department of the Treasury, Financial Crimes Enforcement Network (FinCEN), "FinCEN Issues Advisory and Financial Trend Analysis on Chinese Money Laundering Networks," August 28, 2025, <https://www.fincen.gov/news/news-releases/fincen-issues-advisory-and-financial-trend-analysis-chinese-money-laundering>.

¹⁰² U.S. Department of the Treasury, 2026 National Money Laundering Risk Assessment (Washington, DC: U.S. Department of the Treasury, 2026), <https://home.treasury.gov/system/files/246/2026-NMLRA.pdf>.

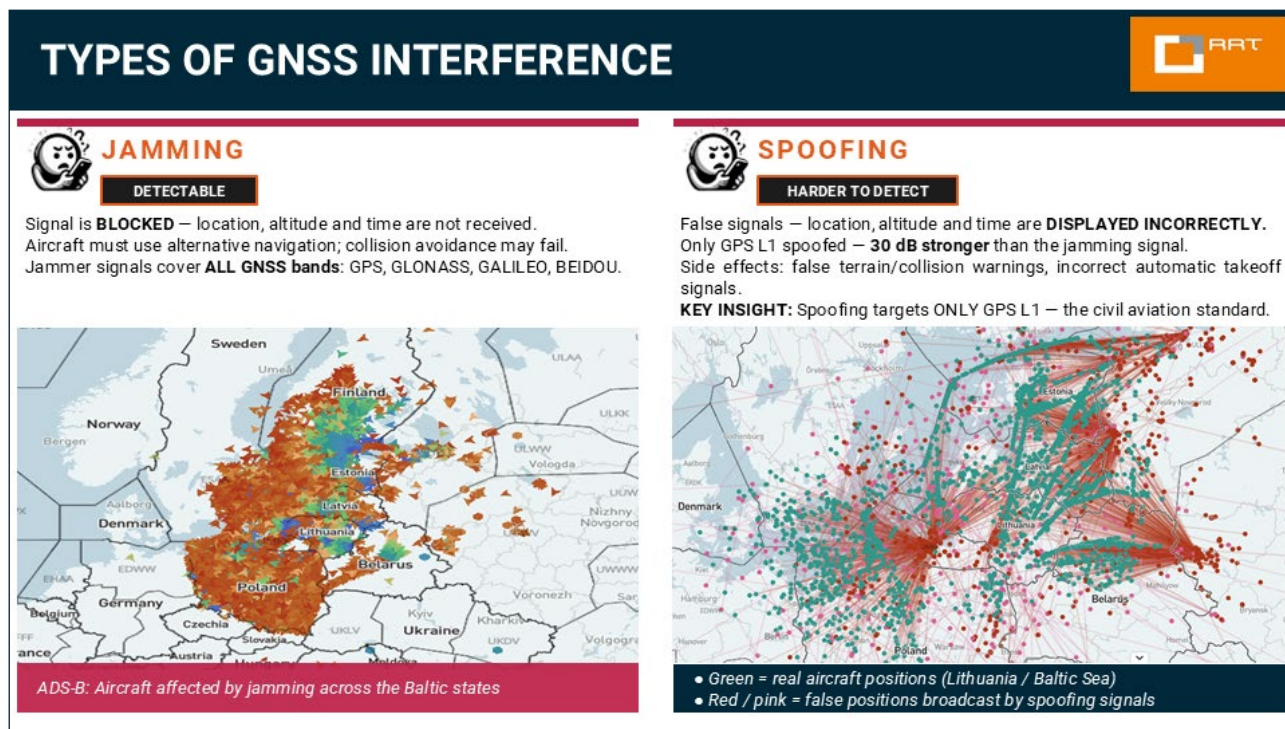
ficking networks.¹⁰³ The relevant security question is therefore not only how many people cross a border but also which networks organize and finance the movement, what infrastructure they control and what other illicit activity those capabilities can support.

Cartel-organized fuel theft and oil smuggling show how the same criminal capability can migrate into a different commodity and a strategically relevant legal sector. In May 2025, FinCEN warned financial institutions about Mexico-based cartels smuggling stolen crude oil across the US southwest border.¹⁰⁴ US authorities described fuel theft and crude-oil smuggling as the cartels' most significant non-drug illicit revenue source, involving complicit brokers and small US-based oil and natural-gas companies. The case closely mirrors this report's central proposition: once a network has finance, logistics, commercial cover, corrupt access and cross-border capability, it can apply those assets to a different market while preserving the infrastructure behind them.

These US-linked examples should not be equated with Baltic tobacco smuggling or Russia- and Belarus-linked hybrid activity. Their value is comparative. They demonstrate, at a much larger scale, the same

analytical problem: a seized commodity is only the visible endpoint of a system combining suppliers, finance, logistics, intermediaries, technology and access to legitimate business. Effective disruption therefore requires moving beyond the final shipment towards the infrastructure that allows the network to survive, reinvest and adapt.

The Baltic states bring a complementary experience. Here, illicit networks operate along the NATO and EU border with Russia and Belarus in an environment shaped by sanctions enforcement, hostile intelligence activity, instrumentalized migration and persistent hybrid pressure. This is accompanied by aggressive military posturing and messaging, including repeated drone and fighter jet incursions into NATO airspace over the Baltic countries, tinkering with undersea infrastructure in the Baltic Sea, and drastically increased instances of jamming and spoofing of Global Navigation Satellite System (GNSS) signals. Despite different operational contexts, many of the security concerns are similar: how networks adapt, how capabilities accumulate, how criminal infrastructure crosses jurisdictions and how it may be exploited for purposes beyond illicit profit.



Source: Ryšių reguliavimo tarnyba / Communications Regulatory Authority of Lithuania (RRT) <https://rrt.lt/>

¹⁰³ U.S. Department of Justice, "The Department of Justice Announces Significant Enforcement and Expansion Efforts to Dismantle Transnational Human Smuggling and Trafficking Networks," September 4, 2025, <https://www.justice.gov/opa/pr/department-justice-announces-significant-enforcement-and-expansion-efforts-dismantle>.

¹⁰⁴ U.S. Department of the Treasury, Financial Crimes Enforcement Network (FinCEN), "FinCEN Issues Alert on Oil Smuggling Schemes on the U.S. Southwest Border Associated with Mexico-Based Cartels," May 1, 2025, <https://www.fincen.gov/news/news-releases/fincen-issues-alert-oil-smuggling-schemes-us-southwest-border-associated-mexico>.

The Serniya Network discussed above shows that this exchange is already practical rather than theoretical. That case combined evidence-gathering and arrests in Estonia with US prosecution, sanctions and export-control capabilities against a Russian government-linked procurement and money-laundering network. It is a useful precedent precisely because neither side supplied the full capability: proximity and counterintelligence on the Baltic side were matched by the US's wider financial, technological and jurisdictional reach.¹⁰⁵

The Latvia-linked TGR Group provides a second, more financially focused precedent. In December 2024, the US Treasury sanctioned individuals and entities associated with the TGR Group, describing it as an extensive sanctions-evasion and money-laundering network used by Russian elites to circumvent US and international restrictions through cash, cryptocurrency, corporate structures and cross-border financial services. A Latvian national, Andrejs Bradens, was identified as being associated with and controlling several entities in the network.¹⁰⁶

The UK NCA placed the TGR Group within a wider professional money-laundering ecosystem operating together with the Smart network. The two networks serviced transnational organized crime and Russian clients seeking to bypass financial restrictions; the wider ecosystem also intersected with Russian espionage financing, sanctioned Russian media activity and the export of electronic components.¹⁰⁷ The case therefore adds a different Baltic–US lesson to that of the Serniya Network: the common target may be financial and corporate infrastructure rather than a physical shipment, and disruption may require sanctions, financial intelligence, criminal investigation and international coordination to operate together.

This difference in experience is precisely what makes the exchange valuable. Baltic–US cooperation already spans defense, cyber, energy, sanctions and economic security. Cooperation on preventing nuclear smuggling offers a particularly relevant precedent: a cross-border trafficking problem with national security implications is addressed through cooperation among border guards, customs, law enforcement and security institutions, supported by US expertise, rather than remaining confined to a single institutional silo.

A particularly useful area for structured Baltic–US cooperation would be financial-network disruption. The US authorities bring extensive experience in tracing cartel proceeds, professional money-laundering services, cryptocurrency and trade-related financial channels connected to fentanyl trafficking and other transnational crime. Baltic authorities operate close to Russian and Belarusian networks where financial channels intersect with sanctions evasion, illicit procurement, smuggling and hostile-state activity. Joint case-based analysis could therefore focus on beneficial ownership, front companies, payment and cryptocurrency channels, trade flows, asset tracking and the point at which financial intelligence should trigger broader criminal or national security scrutiny.

The purpose would be to use different threat environments to answer the same operational question: can financial intelligence expose a network early enough to prevent its assets from moving, its infrastructure from regenerating or its capabilities from being repurposed?

¹⁰⁵ U.S. Department of Justice, "Suspected Russian Intelligence Operative Extradited from Estonia to Face Charges Related to Providing American-Made Electronics and Ammunition to Russian Military," July 14, 2023, <https://www.justice.gov/usao-edny/pr/suspected-russian-intelligence-operative-extradited-estonia-face-charges-related>.

¹⁰⁶ U.S. Department of the Treasury, "Treasury Exposes Money Laundering Network Using Digital Assets to Evade Sanctions."

¹⁰⁷ National Crime Agency, "Operation Destabilise."

11.

Policy Implications and Recommendations

These recommendations are structured around the report's three analytical shifts: from incidents to networks; from commodities to capabilities; and from fragmented responses to a common security picture.

1. Make criminal infrastructure the standard unit of analysis.

Major cases involving smuggling, sanctions evasion or illicit finance should map recurring routes, companies, facilitators, technologies, financial channels, insider access and cross-border links.

2. Build a shared Baltic network picture.

Lithuania, Latvia and Estonia should supplement national statistics and cases with collaborative analysis of actors, companies, routes, technologies, financial channels and hostile-state connections. The network – not the national case file – should be the regional unit of analysis.

3. Integrate counterintelligence.

Establish reporting mechanisms to identify when hostile intelligence services co-opt, fund, or divert access, mobility, financial resources or technical expertise.

4. Track adaptation and displacement.

Track not only seizures and arrests but also where crime shifts following enforcement efforts – through-out supply routes, technologies, sectors and financial channels. Displacement can signal adaptation, not failure.

5. Use existing comprehensive total defense and crisis management structures as fusion mechanisms.

In Lithuania, the National Comprehensive Defence Coordination Council and the National Crisis Management Centre should be used more systematically to bring together expertise from intelligence, law en-

forcement, customs, border security, transport, infrastructure operators, industry, civil society and analytical communities. The goal is not to create another organisation but to obtain a comprehensive picture.

6. Institutionalize public-private cooperation.

Establish channels for industry to provide information, report unusual activity, test detection equipment and share resources. Shift from ad hoc assistance to collaborative engagement.

7. Target enabling structures, not just perpetrators.

Address the link between enablers, recruiters, financiers, access brokers, front companies, equipment suppliers, logistics providers and perpetrators. Make it harder and more costly to exploit criminal infrastructure.

8. Adopt a follow-the-money approach – in both directions.

Carry out parallel financial investigations in all major criminal cases. Success should be based on assets recovered and capability removed, not just assets frozen.

9. Combine resilience and denial with consequences.

Where evidence of hostile-state exploitation is found, responses must extend beyond a criminal case. Financial, diplomatic, cyber and other measures should make clear that such criminal proxies will inevitably face consequences.

10. Establish a Baltic-US practitioner workstream.

Enhance existing cooperation, including possibly expanding the Nuclear Security Centre of Excellence

model into broader areas, and institutionalize cooperation among Baltic and US border security, financial intelligence and other relevant authorities, including through exchanges of best practices, joint training and, where appropriate, learning through joint deployments.

11. Carry out exercises aimed at identifying criminal infrastructure.

Integrate criminal-infrastructure scenarios into national, quadrilateral (Baltic–US) and Allied comprehensive defense planning and exercise agendas.

12. Bring discussion of criminal infrastructure into NATO frameworks, where appropriate.

NATO's hybrid-threat analysis, resilience planning and exercises should incorporate scenarios in which hostile criminal networks are used by adversaries for logistics, financing, recruitment, surveillance or sabotage against individual Allies.

13. Explore the scope for developing relevant capabilities under NATO's Hague spending framework.

Where capabilities to counter hybrid-criminal infrastructure demonstrably serve national security and defense objectives, Allies should explore whether and to what extent their development could qualify as defense- and security-related spending under the Hague framework, particularly for shared regional capabilities.

14. Develop an EU-wide criminal infrastructure picture.

Interconnect existing capabilities among Europol, Frontex, customs, financial intelligence, sanctions enforcement and hybrid-threat infrastructure. The objective should not be to create another database but rather to strengthen cross-domain analysis. The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) could help develop a common analytical framework.

15. Use Baltic and Nordic–Baltic formats as an operational bridge.

Deepen the network-based approach through Baltic cooperation and increasingly the Nordic-Baltic Eight. Regional cooperation should provide a practical layer between national investigations and wider NATO and EU responses.

16. Establish escalation criteria from crime to national security.

Establish criteria (ties to hostile-state actors, penetration of critical infrastructure, military resupply, sanctions evasion, intelligence gathering, development of destructive or intrusive capabilities, or persistent testing) for when additional national security vetting is required.

Conclusion

Illicit trade is, first and foremost, an economic security and law enforcement problem. It undermines legitimate markets, siphons revenues from states and imposes costs on businesses and investors. Labeling each smuggling route, shipment or criminal network as a hybrid threat would have little analytical or operational value.

However, the converse assumption is also wrong: a divide between criminal infrastructure and hostile-state activity. These two worlds are increasingly interconnected. Sustained illicit markets provide a structure: networks, financial systems, logistics, technology, enablers, insider access and operational expertise. This structure creates an ability to act. Designed for financial gain, it can also be leveraged, infiltrated or otherwise used for strategic ends.

The Baltic cases are variations on a theme. In Lithuania, after stringent controls were introduced on the Belarusian border, cigarette smuggling expanded into low-altitude airspace, using balloons and drones linked to GPS-enabled recovery networks and local logistics. The activity remained criminal, but its implications broadened to include border security, the integrity of both airspace and civilian aviation, and, Lithuanian intelligence assesses, deliberately exploited by the Belarusian regime to apply political pressure. Estonia indicates another vector: Russian intelligence services harnessing individuals, access and capabilities already embedded within criminal and cross-border networks. The Serniya case reveals illicit procurement infrastructure being used directly to support Russian state and military interests. Latvia contributes the financial dimension: sanctions evasion, third-country routing, corporate structures, professional intermediaries, and digital finance operating as reusable infrastructure. The Latvia-linked TGR Group case, targeted by US and UK authorities, demonstrates that the transatlantic dimension is already operational, not hypothetical.

The unifying theme is criminal infrastructure. Routes, funds, technology, access, local expertise and individuals established for one purpose can offer capabilities for another. A hostile actor does not always have to build a network from the ground up. It may already exist. This means moving from focusing on seizures to targeting networks, and from commodities to capabilities. Confiscating a shipment is impor-

tant. Detaining an operative is important. But neither necessarily dismantles the infrastructure that enabled the activity. The same is true for cash: criminal capital left in place can help networks rebuild themselves; criminal capital that is traced, frozen and recovered weakens them.

The transatlantic dimension is therefore central to this approach. This is not a question nor a call to artificially invent new channels for Baltic-US cooperation. Rather, it is about recognizing and acting in concert in an area of strategic and policy convergence that already exists on both sides of the Atlantic. The US brings a different scale and scope of threat exposure, a mature body of methodologies for mapping and disrupting transnational networks. It also has financial, intelligence, law enforcement and, where appropriate, defense capabilities that are not available in the Baltic states. In turn, the Baltic states have direct experience of how criminal infrastructure can support and intersect with hostile-state activity at NATO's border. The value lies in combining the two: Baltic exposure with US scale, methodology and capabilities.

The answer must also be cross-institutional. The Baltic states need a common picture of the network, linked to their Nordic-Baltic and transatlantic partners. The EU also has many tools to disrupt networks through customs, border management, law enforcement, financial intelligence and sanctions enforcement. NATO has a different role: where criminal infrastructure weakens Allied resilience, military mobility or critical infrastructure, or where it enables hostile-state operations, it must be part of threat assessments, resilience and even defense planning and exercises.

This does not mean securitizing all illicit trade. It means recognizing when a law enforcement and economic security problem acquires national security relevance – and having the mechanisms to act when it does. Where exploitation by a hostile state is confirmed, denial must impose a cost on the culprits. Criminal actors and infrastructure cannot be a sanctuary for convenience beneath a response threshold. Sanctions, along with financial, diplomatic, cyber and other measures, should increase the cost of strategic exploitation. The strategic question is no longer only what crosses our borders. It is what the networks behind this can do, and who may be able to use them.

Selected Sources

Arnicāns, Matīss. "Sankcijas pret Krieviju apiet, mainot preču kodus un iesaistot starpniekus" [Sanctions against Russia Are Circumvented by Changing Commodity Codes and Using Intermediaries]. LSM, August 28, 2022. <https://www.lsm.lv/raksts/zinas/ekonomika/sankcijas-pret-krieviju-apiet-mainot-precu-kodus-un-iesaistot-starpniekus.a471231/>.

Bajarūnas, Eitvydas. "Russia's Hybrid Warfare Tactics Target the Baltics." The Jamestown Foundation, May 27, 2025. <https://jamestown.org/russias-hybrid-warfare-tactics-target-the-baltics/>.

Bajarūnas, Eitvydas. "The Hybrid Threat Imperative: Deterring Russia Before It Is Too Late." Center for European Policy Analysis (CEPA), December 2, 2025. <https://cepa.org/article/the-hybrid-threat-imperative-deterring-russia-before-it-is-too-late/>.

Barrington, Lisa. "North Korea Balloons, GPS Interference Raise Safety Risks for Airlines." Reuters, July 10, 2024. <https://www.reuters.com/world/asia-pacific/north-korea-balloons-gps-interference-raise-safety-risks-airlines-2024-07-10/>.

Belarusian Investigative Center. "With 'Korona' at the Head: How Pavel Topouzidis Joined 'Fake Transit' and Built an Empire." March 1, 2022. <https://investigatebel.org/en/investigations/z-koronaj-na-chale-yak-pavel-topuzidzis-daluchy-sya-da-falshyvaga-tranzitu-i-pabudava-biznes-imperyyu>.

BNS. "Lithuania Steps Up Rail Freight Checks amid Rise in Cigarette Smuggling from Belarus." LRT, August 6, 2021. <https://www.lrt.lt/en/news-in-english/19/1464016/lithuania-steps-up-rail-freight-checks-amid-rise-in-cigarette-smuggling-from-belarus>.

BNS. "Lithuanian Authorities Arrest 21 in Balloon-Based Cigarette Smuggling Probe." LRT, December 16, 2025. <https://www.lrt.lt/en/news-in-english/19/2777215/lithuanian-authorities-arrest-21-in-balloon-based-cigarette-smuggling-probe>.

BNS. "Two Migrant Groups Stranded on Lithuanian Border." LRT, September 2, 2021. <https://www.lrt.lt/en/news-in-english/19/1484503/two-migrant-groups-stranded-on-lithuanian-border>.

Bowser, Donald. "Russian Organised Crime and Links to Hybrid War in Europe." GLOBSEC, December 9, 2025. <https://www.globsec.org/what-we-do/publications/russian-organised-crime-and-links-hybrid-war-europe>.

Cabinet of Ministers of the Republic of Latvia. "Joint LT, LV, and PL Declaration on Strengthened Cooperation on Security of External Borders and Responding to Hybrid Threats." February 25, 2026. <https://www.mk.gov.lv/en/article/joint-lt-lv-and-pl-declaration-strengthened-cooperation-security-external-borders-and-responding-hybrid-threats>.

Cabinet of Ministers of the Republic of Latvia. "Patrulēšanas joslas izbūve stiprinās mūsu robežu un atvieglēs kontrabandas apkarošanu" [Construction of the Patrol Strip Will Strengthen Our Border and Facilitate the Fight against Smuggling]. August 30, 2024. <https://www.mk.gov.lv/lv/jaunums/patrulesanas-joslas-izbuve-stiprinas-musu-robezu-un-atvieglos-kontrabandas-apkarosanu>.

Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL). *Anti-Money Laundering and Counter-Terrorist Financing Measures: Latvia, Sixth Round Mutual Evaluation Report*. MONEYVAL(2026)2. Strasbourg: Council of Europe, February 2026. <https://rm.coe.int/moneyval-2026-2-mer-latvia-en/48802ab1ea>.

Constitution Protection Bureau of the Republic of Latvia (SAB). "The Constitution Protection Bureau Publishes the Annual Report 2025." January 26, 2026. <https://www.sab.gov.lv/en/news/russia-continues-to-use-and-develop-new-hybrid-instruments-to-influence-latvia-constitution-protection-bureau-states-publishing-its-annual-report/>.

Council of the European Union. *Council Regulation (EC) No. 765/2006 of 18 May 2006 concerning restrictive measures in view of the situation in Belarus and the involvement of Belarus in the Russian aggression against Ukraine*. Consolidated version, July 20, 2025. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02006R0765-20250720>.

Council of the European Union. "Republic of Moldova: Council Lists Six Individuals for Actions Destabilising the Country." June 15, 2026. <https://www.consilium.europa.eu/en/press/press-releases/2026/06/15/republic-of-moldova-council-lists-six-individuals-for-actions-destabilising-the-country/>.

ERR News. "Estonia Caught a Record Number of Russian Collaborators in 2025." April 13, 2026. <https://news.err.ee/1609994248/estonia-caught-a-record-number-of-russian-collaborators-in-2025>.

ERR News. "Narva Resident Handed 6.5 Year Prison Sentence for Espionage, Violating Sanctions." July 22, 2025. <https://news.err.ee/1609751090/narva-resident-handed-6-5-year-prison-sentence-for-espionage-violating-sanctions>.

Estonian Foreign Intelligence Service. *International Security and Estonia 2026*. Tallinn: Estonian Foreign Intelligence Service, 2026. https://raport.valisluureamet.ee/2026/assets/VLA_ENG-raport_2026_WEB.pdf.

Estonian Internal Security Service (KAPO). "Annual Reviews." <https://kapo.ee/en/content/annual-reviews/>.

European Commission. "Statement by President Ursula von der Leyen at the Joint Press Conference with Lithuanian President Gitanas Nausėda, Prime Minister Ingrida Šimonytė, and NATO Secretary General Jens Stoltenberg." November 28, 2021. https://lithuania.representation.ec.europa.eu/news/ek-pirmininkes-u-von-der-leyen-pareiskimas-bendroje-spauodos-konferencijoje-su-lr-prezidentu-g-2021-11-28_lt.

European Commission and High Representative of the Union for Foreign Affairs and Security Policy. "Commission and High Representative Propose New Sanctions Regime to Counter Threats from Migrant Smuggling, Human Trafficking, and Other Forms of Organised Crime." July 9, 2026. https://cyprus.representation.ec.europa.eu/news/commission-and-high-representative-propose-new-sanctions-regime-counter-threats-migrant-smuggling-2026-07-09_en.

European Parliament. "Ongoing Belarusian Hybrid Attacks against Lithuania." December 11, 2025. <https://www.europarl.europa.eu/news/en/agenda/plenary-news/2025-12-15/12/ongoing-belarusian-hybrid-attacks-against-lithuania>.

European Parliament and Council of the European Union. *Directive (EU) 2024/1260 of 24 April 2024 on Asset Recovery and Confiscation. Official Journal of the European Union L 2024/1260*, May 2, 2024. <https://eur-lex.europa.eu/eli/dir/2024/1260/oj/eng>.

Europol. "Europol Holds Largest-Ever Operation to Increase Seizures of Criminal Assets Worldwide." January 17, 2025. <https://www.europol.europa.eu/media-press/newsroom/news/europol-holds-largest-ever-operation-to-increase-seizures-of-criminal-assets-worldwide>.

Financial Crimes Enforcement Network (FinCEN). "FinCEN Issues Advisory and Financial Trend Analysis on Chinese Money Laundering Networks." August 28, 2025. <https://www.fincen.gov/news/news-releases/fincen-issues-advisory-and-financial-trend-analysis-chinese-money-laundering>.

Financial Crimes Enforcement Network (FinCEN). *FinCEN Alert on Oil Smuggling Schemes on the U.S. Southwest Border Associated with Mexico-Based Cartels*. FIN-2025-Alert002. May 1, 2025. <https://www.fincen.gov/system/files/shared/FinCEN-Alert-Oil-Smuggling-FINAL-508C.pdf>.

Ivashkevich, Stanislau, Olga Ratmirova, and Kseniya Viaznikoutsava. "Undercover of Security Forces: Who Could Make Millions of Dollars on the Migration Crisis at the EU Border, Which Claimed Dozens of Lives." Belarusian Investigative Center, June 7, 2023. <https://investigatebel.org/en/investigations/who-could-make-millions-of-dollars-on-the-migration-crisis>.

Kärmas, Mihkel, and Irina Kablukova. "How Did a Man from Estonia Become a Valuable Prisoner for the Kremlin?" ERR News, September 4, 2024. <https://news.err.ee/1609443845/how-did-a-man-from-estonia-become-a-valuable-prisoner-for-the-kremlin>.

Keatinge, Tom, and Kinga Redlowska. "How Can the EU's Criminal Network Sanctions Succeed?" Royal United Services Institute (RUSI), June 18, 2026. <https://www.rusi.org/explore-our-research/publications/commentary/how-can-eus-criminal-network-sanctions-succeed>.

KPMG. *Illicit Cigarette and Heated Tobacco Consumption, and Oral Nicotine Share in Europe: 2025 Results*. Commissioned by Philip Morris Products S.A., June 2, 2026. <https://www.pmi.com/content/dam/pmicom/global/docs/itp/kpmg-illicit-cigarette-consumption-europe-2025-results.pdf>.

Kremidas-Courtney, Chris. "Everything, Everywhere, All at Once: Russia's Hybrid Campaign Against Europe, 2026–2030." Euro-Atlantic Resilience Centre (E-ARC), September 1, 2026. <https://e-arc.ro/2026/09/01/everything-everywhere-all-at-once-russias-hybrid-campaign-against-europe-2026-2030/>.

Lithuanian Police. "Prevenčių reidų pasienio rajonuose rezultatai" [Results of Preventive Raids in Border Districts]. August 10, 2026. <https://policija.lrv.lt/lt/naujienos/reidu-pasienyje-rezultatai-kJ96/>.

Lithuanian State Border Guard Service. *2022 metų veiklos ataskaita* [2022 Annual Activity Report]. Vilnius, March 17, 2023. https://vsat.lrv.lt/uploads/vsat/documents/files/2022%20m_%20VSAT%20ATASKAITA.docx.pdf.

Lithuanian State Border Guard Service. "3 mln. eurų inovatyviems sprendimams: verslas kviečiamas kurti technologijas Lietuvos oro erdvės apsaugai" [€3 Million for Innovative Solutions: Businesses Invited to Develop Technologies for Protecting Lithuania's Airspace]. July 9, 2026. <https://vsat.lrv.lt/lt/naujienos/3-mln-euru-inovatyviems-sprendimams-verslas-kviečiamas-kurti-technologijas-lietuvos-oro-erdves-apsaugai-03x/>.

Lithuanian State Border Guard Service. "Antradienį pasieniečiai 4 kartus išbaidė fizinį barjerą gadinusius baltarusius" [Border Guards Scare Off Belarusians Damaging the Physical Barrier Four Times on Tuesday]. October 11, 2023. <https://vsat.lrv.lt/lt/naujienos/antradieni-pasienieciai-4-kartus-isbaide-fizini-barjera-gadinusius-baltarusius/>.

Lithuanian State Border Guard Service. "Neįleistų neteisėtų migrantų statistika" [Statistics on Irregular Migrants Prevented from Entering]. Updated September 7, 2026. <https://vsat.lrv.lt/lt/naujienos/neileistu-neteisetu-migrantu-statistika/>.

Lithuanian State Border Guard Service. "Pasieniečiai perėmė pirmą šiemet balionais iš Baltarusijos atskraidintą kontrabandos krovinį" [Border Guards Intercept the First Contraband Shipment of the Year Flown from Belarus by Balloons]. January 6, 2026. <https://vsat.lrv.lt/lt/naujienos/pasienieciai-pereme-pirma-siemet-balionais-is-baltarusijos-atskraidinta-kontrabandos-krovini-foto-Tm7/>.

Lithuanian State Border Guard Service. "Pernai sulaikytas rekordinis VSAT veiklos istorijoje cigarečių kontrabandos kiekis" [Record Amount of Cigarette Contraband Seized in VSAT History Last Year]. January 9, 2026. <https://vsat.lrv.lt/lt/naujienos/pernai-sulaikytas-rekordinis-vsateveiklos-istorijoje-cigareciu-kontrabandos-kiekis-foto-2P2/>.

Lithuanian State Border Guard Service. "Tranzitiniame traukinyje – 12 tūkst. pakelių paslėptų baltarusiškų cigarečių" [12,000 Packs of Hidden Belarusian Cigarettes Found on a Transit Train]. January 16, 2023. <https://vsat.lrv.lt/lt/naujienos/tranzitiniame-traukinyje-12-tukst-pakeliu-pasleptu-baltarusisku-cigareciu-foto>.

Lithuanian State Border Guard Service. "Varėnos pasieniečiai aptiko jau trečią iš Baltarusijos vedantį tunelį" [Varėna Border Guards Discover Third Tunnel Leading from Belarus]. August 5, 2026. <https://vsat.lrv.lt/lt/naujienos/varenos-pasienieciai-aptiko-jau-trecia-is-baltarusijos-vedanti-tuneli-foto-B2v/>.

LRT TV News Service. "Cigarette Smugglers May Double as Russian Spies, Lithuanian Border Guards Warn." LRT, June 11, 2019. <https://www.lrt.lt/en/news-in-english/19/1068201/cigarette-smugglers-may-double-as-russian-spies-lithuanian-border-guards-warn>.

LRT. "Lithuanian Startup Develops Night-Vision Camera to Track Smuggling Balloons." February 9, 2026. <https://www.lrt.lt/en/news-in-english/19/2830544/lithuanian-startup-develops-night-vision-camera-to-track-smuggling-balloons>.

LRT. "Tobacco Giant Philip Morris Donates Drones to Lithuania to Help Combat Cigarette Smuggling." March 17, 2026. <https://www.lrt.lt/en/news-in-english/19/2870160/tobacco-giant-philip-morris-do>.

LRT.lt and BNS. "Smugglers' Balloons Deliberately Launched into Aviation Danger Zones – Lithuanian Official." LRT, December 1, 2025. <https://archyvai.lrt.lt/en/news-in-english/19/2762185/smugglers-balloons-deliberately-launched-into-aviation-danger-zones-lithuanian-official>.

Ministry of the Interior of the Republic of Latvia. "Austrumu robežas infrastruktūras izbūve tuvojas noslēgumam" [Construction of the Eastern Border Infrastructure Nears Completion]. July 28, 2026. <https://www.iem.gov.lv/lv/jaunums/austrumu-robezas-infrastrukturas-izbuve-tuvojas-noslegumam>.

Ministry of the Interior of the Republic of Lithuania. "Frequently Asked Questions about Irregular Migrants Detained at the Border with Belarus." Last updated September 20, 2023. <https://vrm.lrv.lt/en/information-on-irregular-migration/>.

National Crime Agency. "Investigating Russian-Speaking Money Launderers." In *National Strategic Assessment 2026 of Serious and Organised Crime*. 2026. <https://www.nationalcrimeagency.gov.uk/nsa-domains-2026/nsa-soc-finance-2026>.

National Crime Agency. "Operation Destabilise: NCA Disrupts \$Multi-Billion Russian Money Laundering Networks with Links to Drugs, Ransomware and Espionage, Resulting in 84 Arrests." December 4, 2024. <https://www.nationalcrimeagency.gov.uk/news/operation-destabilise-nca-disrupts-multi-billion-russian-money-laundering-networks-with-links-to-drugs-ransomware-and-espionage-resulting-in-84-arrests>.

North Atlantic Treaty Organization (NATO). "Countering Hybrid Threats." Updated January 29, 2026. <https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats>.

North Atlantic Treaty Organization (NATO). *Defence Investment of NATO Countries (2014–2026)*. July 3, 2026. <https://www.nato.int/content/dam/nato/webready/documents/finance/def-exp-2026-en.pdf>.

North Atlantic Treaty Organization (NATO). *NATO 2022 Strategic Concept*. Brussels: NATO, 2022. <https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf>.

North Atlantic Treaty Organization (NATO). "Statement by the North Atlantic Council on the Situation at the Poland-Belarus Border." November 12, 2021. <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2021/11/12/statement-by-the-north-atlantic-council-on-the-situation-at-the-poland-belarus-border>.

North Atlantic Treaty Organization (NATO). "The Ankara Summit Declaration." July 8, 2026. <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/07/08/the-ankara-summit-declaration>.

North Atlantic Treaty Organization (NATO). "Washington Summit Declaration." July 10, 2024. <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/washington-summit-declaration>.

Office of the Director of National Intelligence. *Annual Threat Assessment of the U.S. Intelligence Community*. Washington, DC: Office of the Director of National Intelligence, March 2026. <https://archive.dni.gov/files/ODNI/documents/assessments/ATA-2026-Unclassified-Report.pdf>.

Philip Morris International. "The First Investor's Recipe for Change: 30 Years of Growth, €400 Million Investment, and Exceptional Focus on Employees." September 21, 2023. <https://www.pmi.com/markets/lithuania/en/overview/the-first-investor-s-recipe-for-change-30-years-of-growth-400-million-investment-and-exceptional-focus-on-employees>.

Police of the Republic of Moldova. "46 de percheziții în dosarul privind coruperea electorală, finanțarea ilegală a partidelor politice și spălarea banilor" [46 Searches in the Case Concerning Electoral Corruption, Illegal Financing of Political Parties, and Money Laundering]. September 18, 2025. <https://igp.gov.md/en/node/1373>.

Police of the Republic of Moldova. "Percheziții în dosarul privind coruperea alegătorilor, finanțarea ilegală a partidelor și spălarea banilor" [Searches in the Case Concerning Electoral Corruption, Illegal Party Financing, and Money Laundering]. September 11, 2025. <https://igp.gov.md/en/node/1265>.

Polish Border Guard. "Podziemne przejście pod polsko-białoruską granicą" [Underground Passage under the Polish-Belarusian Border]. December 12, 2025. <https://strazgraniczna.pl/pl/aktualnosci/15117,Podziemne-przejscie-pod-polsko-bialoruska-granica.html>.

Progni, Loneta, and Vytautas Leškevičius. "Civilian Infrastructure Is Now a Strategic Target. NATO Must Adapt to Protect It." Atlantic Council, July 2, 2026. <https://www.atlanticcouncil.org/dispatches/civilian-infrastructure-is-now-a-strategic-target-nato-must-adapt-to-protect-it/>.

Prosecutor General's Office of the Republic of Latvia. "Ģenerālprokuratūrā uzsākts kriminālprocess par Baltkrievijas Republikas robežsardzes struktūru amatpersonu noziedzīgajām darbībām" [Criminal Proceedings Initiated concerning Criminal Activities of Officials of the Border Guard Structures of the Republic of Belarus]. July 15, 2026. <https://www.prokuratūra.lv/lv/aktualitates/2026/aktualitates/generalprokuratura-uzsakts-kriminalprocess-par-baltkrievijas-republikas-robezsardzes-strukturu-amatpersonu-noziedzigajam-darbibam-3809>.

Prosecutor General's Office of the Republic of Lithuania and Lithuanian Criminal Police Bureau. "Case on Terror Acts Organised and Planned in Different Countries Referred to Court." March 6, 2026. <https://www.prokuraturos.lt/lt/teismui-perduota-byla-del-skirtingose-valstybese-organizuotu-ir-planuotu-ivykdyti-teroro-aktu-with-text-in-english/12174>.

Prosecutor General's Office of the Republic of Lithuania and Lithuanian Criminal Police Bureau. "Plataus masto policijos ir prokuratūros operacija: ardomi „balionų“ kontrabandos nusikalstami tinklai" [Large-Scale Police and Prosecutor's Office Operation: Criminal Balloon-Smuggling Networks Dismantled]. May 22, 2026. <https://www.prokuraturos.lt/lt/plataus-masto-policijos-ir-prokuraturos-operacija-ardomi-balionu-kontrabandos-nusikalstami-tinklai/12449>.

Prosecutor's Office of Estonia. "The Court Convicted a Resident of Narva of an Offence against the State." February 20, 2026. <https://www.prokuratuur.ee/en/news/court-convicted-resident-narva-offence-against-state>.

Republic of Lithuania. *Law No. XV-1002 Amending the Law on Crisis Management and Civil Protection No. VIII-971*. June 11, 2026. *Register of Legal Acts (TAR)*, June 26, 2026, no. 11088. <https://e-tar.lt/portal/lt/legalAct/86c35e02715711f1b53dfa020e517810>.

Roonemaa, Holger. "How Smuggler Helped Russia to Catch Estonian Officer." Re:Baltica/Postimees, September 13, 2017. <https://en.rebaltica.lv/2017/09/how-smuggler-helped-russia-to-catch-estonian-officer/>.

Roonemaa, Holger. "These Cigarette Smugglers Are on the Frontlines of Russia's Spy Wars." BuzzFeed News, September 13, 2017. <https://www.buzzfeed.com/holgerroonemaa/these-cigarette-smugglers-are-on-the-frontlines-of-russias>.

Rutte, Mark. "To Prevent War, NATO Must Spend More." Speech at Carnegie Europe, December 12, 2024. NATO. <https://www.nato.int/en/news-and-events/events/transcripts/2024/12/12/to-prevent-war-nato-must-spend-more>.

Semjonova, Ella. "«De facto»: Latvijas uzņēmumi sankcijas pret Krieviju šogad apiet vairāk; tiesas pagaidām netiek galā" [Latvian Companies Are Circumventing Sanctions against Russia More Often This Year; Courts Are Not Yet Keeping Up]. LSM, November 24, 2024. <https://www.lsm.lv/raksts/zinas/latvija/24.11.2024-de-facto-latvijas-uznemumi-sankcijas-pret-krieviju-sogad-apiet-vairak-tiesas-pagaidam-netiek-gala.a577607/>.

Sheely, Zach. "Where the State Partnership Program Began: National Guard Leaders Visit Baltics." National Guard Bureau, June 11, 2026. <https://www.ang.af.mil/Media/Article-Display/Article/4514311/where-the-state-partnership-program-began-national-guard-leaders-visit-baltics/>.

State Border Guard of Latvia. "Border Guards Detect 15 Persons Who Illegally Crossed the State Border through an Underground Tunnel." August 11, 2026. <https://www.rs.gov.lv/en/article/border-guards-detect-15-persons-who-illegally-crossed-state-border-through-underground-tunnel>.

State Border Guard of Latvia. "Border Guards Detected 28 Persons Who Illegally Crossed the State Border through a Dug Underground Tunnel." August 21, 2026. <https://www.rs.gov.lv/en/article/border-guards-detected-28-persons-who-illegally-crossed-state-border-through-dug-underground-tunnel>.

State Border Guard of Latvia. "Latvijā fiksēti vairāki kontrabandistu baloni no Baltkrievijas" [Several Smugglers' Balloons from Belarus Detected in Latvia]. November 24, 2025. <https://www.rs.gov.lv/lv/jaunums/latvija-fikseti-vairaki-kontrabandistu-baloni-no-baltkrievijas>.

State Revenue Service of the Republic of Latvia. "Pagājušajā gadā muitas kontroles pasākumu rezultātā novērsti vairāk nekā 14 500 pārkāpumi" [More than 14,500 Violations Prevented as a Result of Customs Control Measures Last Year]. January 26, 2024. <https://www.vid.gov.lv/lv/jaunums/pagajusaja-gada-muitas-kontroles-pasakumu-rezultata-novers-ti-vairak-neka-14-500-parkapumi>.

State Revenue Service of the Republic of Latvia. *Valsts ieņēmumu dienesta Publiskais pārskats 2024* [State Revenue Service Public Report 2024]. <https://www.vid.gov.lv/lv/media/30752/download?attachment=>.

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

Stoltenberg, Jens. "Doorstep Statement." NATO, November 16, 2021. <https://www.nato.int/en/news-and-events/events/transcripts/2021/11/16/doorstep-statement>.

The White House. *National Security Strategy of the United States of America*. Washington, DC: The White House, November 2025. <https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf>.

U.S. Centers for Disease Control and Prevention, National Center for Health Statistics. "U.S. Overdose Deaths Decrease for Third Consecutive Year in 2025." May 13, 2026. <https://www.cdc.gov/nchs/pressroom/releases/20260513.html>.

U.S. Department of Justice. "Asset Forfeiture Program." <https://www.justice.gov/afp>.

U.S. Department of Justice. "Suspected Russian Intelligence Operative Extradited from Estonia to Face Charges Related to Providing American-Made Electronics and Ammunition to Russian Military." July 14, 2023. <https://www.justice.gov/usao-edny/pr/suspected-russian-intelligence-operative-extradited-estonia-face-charges-related>.

U.S. Department of Justice. "The Department of Justice Announces Significant Enforcement and Expansion Efforts to Dismantle Transnational Human Smuggling and Trafficking Networks." September 4, 2025. <https://www.justice.gov/opa/pr/departement-justice-announces-significant-enforcement-and-expansion-efforts-dismantle>.

U.S. Department of State, Office of the Spokesperson. "Joint Statement on the PSI Baltics Workshop and Tabletop Exercise." June 6, 2024. <https://2021-2025.state.gov/joint-statement-on-the-psi-baltics-workshop-and-tabletop-exercise/>.

U.S. Department of State. "U.S. and Lithuania Sign Agreement on Countering Nuclear Smuggling." Atlantic Council, April 23, 2013. <https://www.atlanticcouncil.org/blogs/natosource/us-and-lithuania-sign-agreement-on-countering-nuclear-smuggling/>.

U.S. Department of the Treasury. *2026 National Money Laundering Risk Assessment*. Washington, DC: U.S. Department of the Treasury, March 2026. <https://home.treasury.gov/system/files/246/2026-NMLRA.pdf>.

U.S. Department of the Treasury. "Treasury Exposes Money Laundering Network Using Digital Assets to Evade Sanctions." December 4, 2024. <https://home.treasury.gov/news/press-releases/jy2735>.

U.S. Department of War. *2026 National Defense Strategy*. Washington, DC: U.S. Department of War, January 23, 2026. <https://media.defense.gov/2026/Jan/23/2003864773/-1/-1/0/2026-NATIONAL-DEFENSESTRATEGY.PDF>.

U.S. Drug Enforcement Administration. *2025 National Drug Threat Assessment*. Washington, DC: U.S. Department of Justice, May 2025. <https://www.dea.gov/sites/default/files/2025-07/2025NationalDrugThreatAssessment.pdf>.

Vilnius County Police. "Šalčininkų rajone užkardytas stambus kontrabandos kanalas – sulaikyti trys asmenys" [Major Smuggling Channel Disrupted in Šalčininkai District – Three People Detained]. May 29, 2026. <https://vilnius.policija.lrv.lt/lt/naujienos/salcininku-rajone-uzkardytas-stambus-kontrabandos-kanalas-sulaikyti-trys-asmenys-cigaretes-gabentos-meteorologiniaiis-balionais-video-Pw6Q/>.



Vytautas Leškevičius

Vytautas Leškevičius is a Lithuanian security and defence policy expert and analyst with 30 years of experience in international security, defence, transatlantic relations, NATO and EU affairs. His professional experience spans senior roles across security policy, international affairs, and strategic analysis, including service as Lithuania's Permanent Representative to NATO and Deputy Foreign minister in charge of coordinating Lithuania's first-ever Presidency of the Council of the European Union. Throughout his career, he has been involved in major negotiations and policy processes related to NATO and EU security and defence policies, resilience and crisis management. Ambassador Leškevičius currently serves as Chief Foreign Policy Advisor at the Geopolitics and Security Studies Center, a Vilnius-based think tank. He is also a non-resident senior fellow at the Atlantic Council.



Žydrūnas Bartkus

Žydrūnas Bartkus is a former Director of Lithuania's Special Investigation Service (STT), the country's main specialised anti-corruption law-enforcement institution, and a former President of EPAC/EACN, the European network bringing together anti-corruption authorities and police oversight bodies. He has more than two decades of experience in law enforcement, institutional reform and international cooperation. In his current international advisory work, he advises public institutions and international partners on anti-corruption, anti-money laundering, asset recovery and financial investigations, including in the context of Moldova's and Ukraine's European integration processes. His recent work has focused on strengthening institutional capacity, aligning national frameworks with EU standards, and addressing the links between corruption, illicit finance, organised crime and national security.



Eitvydas Bajarūnas

Ambassador Eitvydas Bajarūnas is a Lithuanian diplomat and international security expert with more than three decades of experience in foreign policy, NATO and EU affairs, hybrid threats, defence, and geopolitics. He currently represents the Lithuanian Confederation of Industrialists at the European Economic and Social Committee (EESC) in Brussels and serves as a non-resident Senior Fellow at CEPA and an Associated Expert at the Geopolitics and Security Studies Center in Vilnius. His senior diplomatic assignments include serving as Lithuania's Ambassador to the UK, Russia, and Sweden, as well as Political Director at the Ministry of Foreign Affairs and Ambassador-at-Large for Hybrid Threats. He writes extensively on NATO, Russia, hybrid threats, and Baltic-Nordic security and holds degrees from Vilnius University and King's College London.



Henrik Praks

Henrik Praks is a research fellow with the Security & Resilience Programme at the International Centre for Defence and Security (ICDS) in Tallinn, Estonia. His main areas of expertise include hybrid warfare, influence activities, Baltic Sea regional security and comprehensive security. Before joining ICDS he worked as a Senior Analyst at the European Centre of Excellence for Countering Hybrid Threats in Helsinki. Earlier in his career he held various positions within the Estonian Ministry of Defence, focusing on defence and security policy, regional security, NATO, and EU defence issues; and worked at the Baltic Defence College (BALTDEFCOL) as a Lecturer in Strategic Studies.



Beāte Livdanska

Beāte Livdanska is a researcher and project leader at the Latvian Institute of International Affairs, where she leads the *Belarus Research Network for Neighbourhood Policy*. She is also a lecturer and researcher at Rīga Stradiņš University, where she is a PhD candidate in political science. Her research focuses on Belarusian foreign and domestic policy, Belarus's relations with the Baltic states and the European Union, and the role of small states in shaping EU policy.

