CEPA

WAR WITHOUT END

Deterring Russia's Shadow War

ABOUT CEPA

The Center for European Policy Analysis (CEPA) is a nonprofit, nonpartisan, public policy institution headquartered in Washington, DC with hubs in London and Brussels, focused on strengthening the transatlantic alliance through cutting-edge research, analysis, and programs. CEPA provides innovative insight on trends affecting democracy, security, and defense to government officials and agencies; helps transatlantic businesses navigate changing strategic landscapes; and builds networks of future leaders versed in Atlanticism.

Cover art: Sara Boyer/Center for European Policy Anlaysis. Credits (Clockwis) Photo: Russian President Vladimir Putin, chairs a video conference meeting of government members from the Kremlin, October 29, 2025 in Moscow, Russia. Credit: Alexander Kazakov/Kremlin Pool/Alamy Live News; Photo: A firefighter works to extinguish fire following recent shelling at an oil storage in the course of Russia-Ukraine conflict in the town of Shakhtarsk (Shakhtyorsk) near Donetsk, Russian-controlled Ukraine, October 27, 2022. Credit: REUTERS/Alexander Ermochenko; Photo: The Internal Security Agency (ABW) officers escort a man arrested on suspicion of spying in front of the district court in Warsaw October 17, 2014. Two men arrested by Polish authorities on suspicion of spying were working for Russian intelligence, a member of the Polish parliament's intelligence committee said on Friday. Credit: REUTERS/Kacper Pempel; Photo: Russian hacking underground newsletter is seen in this illustration taken, December 19, 2022. Credit: REUTERS/Dado Ruvic/Illustration; Photo: A German Navy sailor aboard FGS Homburg Standing NATO Mine Counter Measure Group 1 (SNMG1) while leaving Bergen to participate in Trident Juncture exercise. Credit: WO Fran C.Valverde/NATO Flickr.

Contents

Toward Credible Deterrence of Russia's Shadow War

SAM GREENE

Europe is no longer merely a witness to Russian aggression. It is one of its principal targets. While Ukraine remains the most visible front in Russia's confrontation with the West — and while it is primarily Ukrainians who are suffering and dying under massive bombardment — it is no longer the only battlefield. Across Europe, Russian-linked actors have sabotaged critical infrastructure, disrupted aviation and energy systems, penetrated digital networks, surveilled military facilities, and targeted political opponents and defense officials, a reality long familiar to several front-line European states. These acts are rarely claimed by their perpetrators, often ambiguously attributed by their victims, and almost never met with decisive retaliation. Taken individually, each attack may appear manageable. Taken together, they constitute something more troubling: a sustained campaign of shadow warfare designed to degrade European security while remaining below the threshold that would trigger a military response.

Over the past year, the Center for European Policy Analysis (CEPA) has conducted a major study of the actors and tactics involved in Russia's shadow warfare, its strategic underpinnings and governance structures, and the processes and patterns of European response. Since 2022, these activities have become more tightly synchronized with Moscow's broader war aims in Ukraine. At its core, this research argues that Russia's shadow warfare is not a temporary or stop-gap expedient, nor a collection of opportunistic "hybrid" adaptations. Rather, it is a system of conflict rooted in ideology, embedded in institutions, and biased toward escalation. The danger it poses thus lies not in the limited damage it causes today, but in the potentially unlimited damage it could cause tomorrow as the risk of inadvertent escalation grows. As a result, deterrence is necessary both to secure Europe against ongoing attacks and to ward off potentially catastrophic eventualities. European states have begun to develop effective responses, and we can already draw valuable lessons from their experience. Troublingly, however, CEPA's research finds that Europe's failure to deter this campaign has less to do with a lack of awareness, which would be easily remedied, than with a persistent mismatch between how Russia fights and how the West responds. Overcoming this mismatch will require consistent structural and behavioral change.

Photo: The emblem of the FSB of Russia on the fence at the headquarters building, Nizhny Novgorod, Russia - September 14, 2019. Credit: Irina Rebrova/Alamy Live News.

Shadow Warfare as a System, Not a Tactic

At the heart of Russia's shadow warfare is a worldview that does not recognize clear boundaries between war and peace, or between domestic and foreign threats. In the Kremlin's eyes, the war in Ukraine, covert operations in Europe, and the repression of dissidents at home and abroad are not separate endeavors. Rather, they are fluid fronts in a single, existential struggle, the ultimate aim of which is regime survival. This outlook has deep roots in Soviet, and particularly Stalin-era, concepts of permanent confrontation, in which conflict is not an exception to normal politics, but its organizing principle.

Within this framework, shadow warfare is not a substitute for conventional force, deployed by the weak against the strong. Nor is it merely a means of avoiding escalation. Instead, it is one of several interchangeable tools available to the Russian state, alongside diplomacy, information operations, cyberattacks, and traditional warfare. What makes shadow aggression both attractive and dangerous is that it operates without clear benchmarks for success or failure. These operations

depend on a calibrated mix of deniability abroad and visibility at home, where the activity itself can be used to validate the regime's narrative of strength in the face of encirclement. Thus, for the Russians who perpetrate shadow warfare — and whose budgets and political positioning depend on its success — disruption is success, exposure can be framed as proof of relevance, and even failure can justify further investment and greater risk-taking.

This absence of internal discipline creates a powerful bias toward escalation. Russian intelligence and security services are rewarded for initiative rather than restraint. Operations need not achieve specific strategic objectives in order to be validated; they need only demonstrate action. In such a system, escalation is the natural outcome.

Western deterrence models, by contrast, presume an adversary that weighs risks carefully and adjusts in response to the risk of punishment. Against a system that converts pressure into confirmation and disruption into validation, these assumptions break down. The result is that Russian shadow warriors are constrained *neither* by internal governance structures, *nor* by external structures of deterrence. In the widening gap between Russian activity and Western response, Moscow has learned to act with increasing confidence.

Patterns of Shadow Warfare

The empirical record across Europe illustrates how this system operates in practice. Russia's shadow warfare spans multiple domains, but its effects are cumulative and mutually reinforcing.

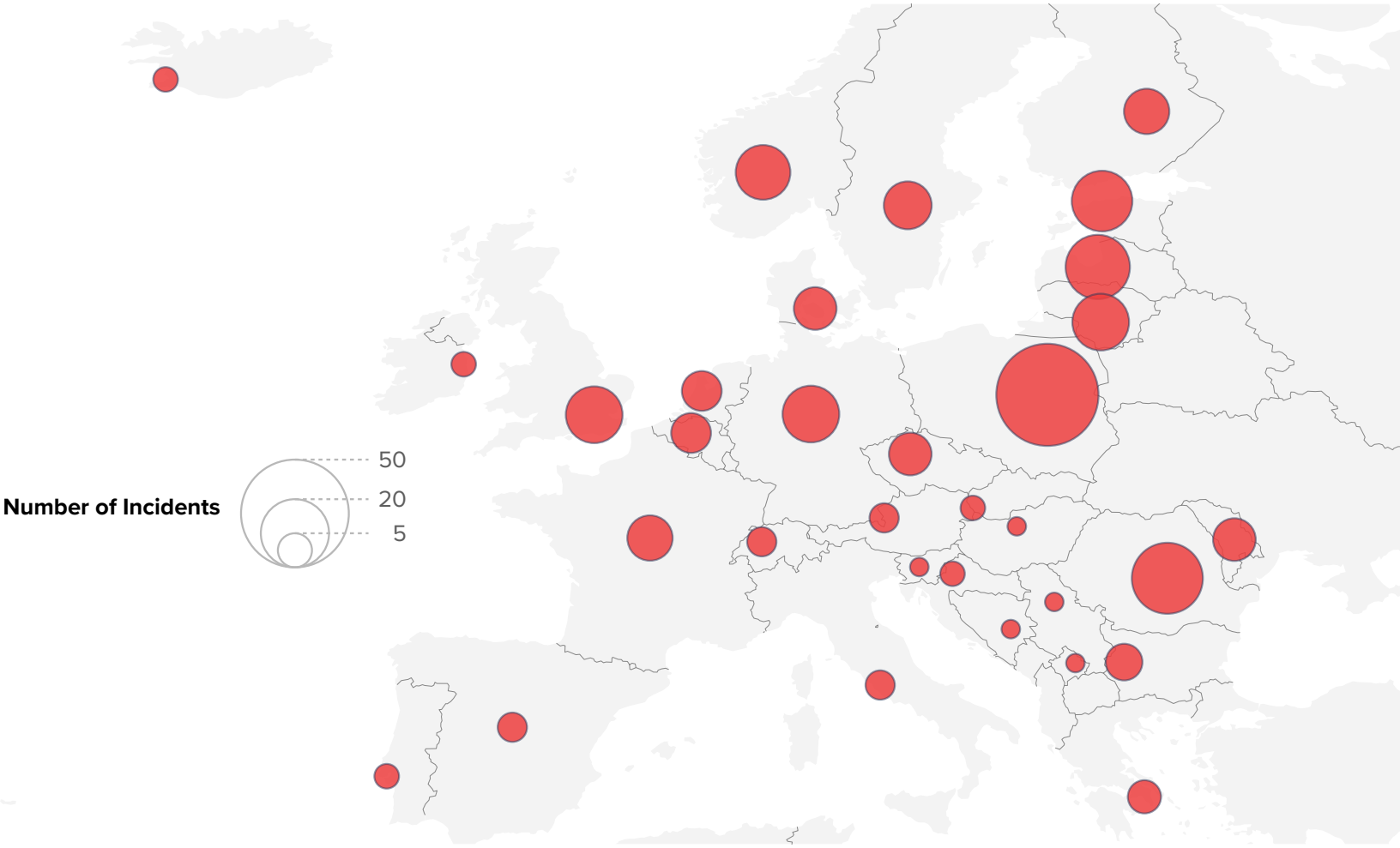
One prominent front is infiltration and the use of proxies. Russia routinely relies on criminal networks, loosely affiliated intermediaries, and ideologically flexible recruits to carry out arson, surveillance, intimidation, and sabotage. This "proxyization" serves several purposes at once: It reduces operational risk, blurs lines of responsibility, and stretches Western investigative and legal processes. Perhaps most importantly, it normalizes hostility. When such incidents are treated as isolated crimes rather than elements of a coordinated campaign, they fade into the background noise of daily security challenges — precisely the environment in which shadow warfare thrives.

A second front involves the sabotage and manipulation of critical infrastructure, particularly undersea cables and energy connections. These assets are both highly vulnerable and deeply integrated into civilian and military life. Disrupting them can degrade communications, strain energy markets, and complicate military command and control, all without firing a shot. The use of civilian and dual-use vessels, opaque ownership structures, and operations in contested legal spaces allows Russia to probe European defenses while exploiting gaps in jurisdiction and attribution, a

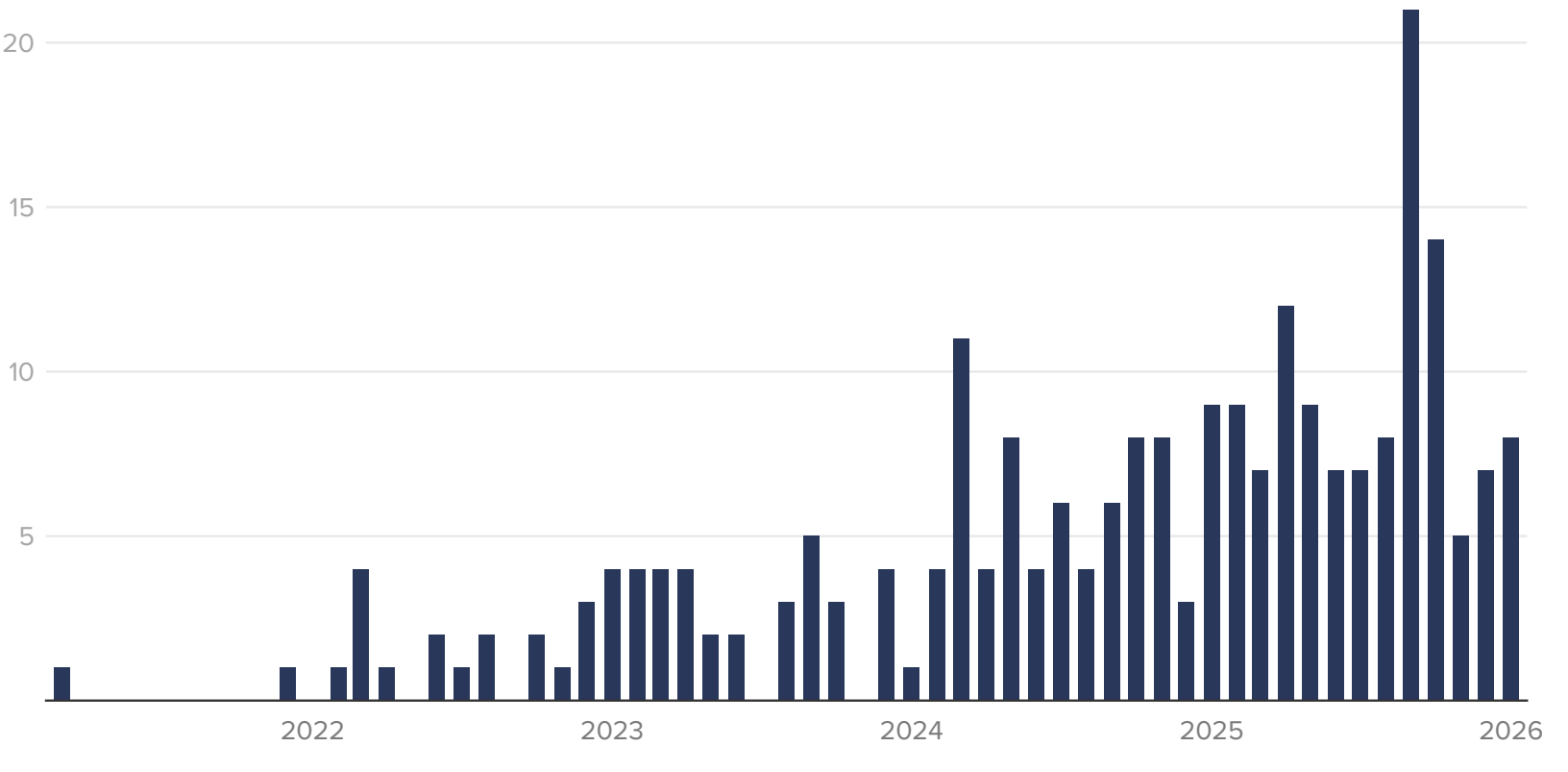
Opposite Map and Chart include confirmed and highly likely incidents of Russian Shadow Warfare. Confirmed incidents include those attributed by government and journalistic sources to Russia or Russian-supported perpetrators. Highly likely incidents include those that have been reported by government and journalistic sources with a high likelihood.of being attributable to Russia or Russian-supported perpetrators.

Graphics: Michael Newton/Isabella Nieminen/Katelynn Henics/Center for European Policy Analysis. Source: Emma Burrows et al.,"Russian Sabotage Across Europe," Associated Press News, December 18, 2025, https://apnews.com/projects/russian-europe-sabotage/; Sahaidachnyi Security Center, "The Everywhere War: Sub-Threshold Warfare Tracker,"https://sahasec.org/tracker/; Nichita Gurcov," ACLED data show at least 50 instances of airspace violations of countries on Ukraine's western borders since 2022 — Expert comment,» ACLED, September 11, 2025, https://acleddata.com/expert-comment/acled-data-show-least-50-instances-airspace-violations-countries-ukraines-western; Charlie Edwards and Nate Seidstein,"The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure." IISS, August 2025, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/08/pub25-095-the-scale-of-russian-sabotage-operations.pdf; and Open-Source Information gathered by CEPA staff.

Russia’s Shadow War Attacks by Country



Russia’s Shadow Warfare Attacks Over Time



challenge many Nordic and Baltic states have grappled with for years. Even when responsibility is widely understood, the lack of incontrovertible proof sufficient for legal proceedings often delays or dilutes political response.

Cyber operations form a third, closely linked front. Russian-aligned actors have moved beyond episodic disruption toward persistent campaigns that blend espionage, sabotage, and psychological pressure. Cyberattacks increasingly target not just information technology but operational systems — energy grids, transport networks, registries — multiplying the real-world impact of digital intrusion. These operations are designed to scale horizontally across societies, imposing costs on civilians, businesses, and governments alike. Their ambiguity complicates attribution and response, while their integration with other forms of pressure magnifies their strategic effect.

Across these domains, the pattern is consistent. Russia exploits ambiguity, institutional seams, and procedural caution. It probes, observes, and adjusts, confident that the cumulative effect of many small actions will outweigh the limited consequences imposed in response to any single one.

Why Deterrence Has Failed

Europe's difficulty in deterring Russian shadow warfare does not stem from a lack of awareness. In extensive interviews with European and transatlantic security officials, the pattern of Russian activity is understood both in its broad implications and in granular detail. Rather, the failure stems from the ways in which this pattern is assimilated by established European and NATO security structures and practices, and in the habits of response those structures and practices engender.

In particular, CEPA's research elucidates four critical bottlenecks:

- **Shadow warfare is persistently misclassified**. Existing institutional mandates lead sabotage to be processed primarily through criminal law and civilian enforcement frameworks. Cable disruptions are framed as maritime accidents. Cyber intrusions are managed as technical incidents. Each response may be reasonable on its own. Together, they fragment responsibility and signal restraint rather than resolve. A coordinated campaign of hostile state action is handled as a series of unrelated problems.
- **The tempo of response lags behind the tempo of attack**. Russian operations are fast, deniable, and iterative. Western responses are slow, deliberative, and consensus-bound. By the time attribution debates conclude and possible responses are weighed, the political urgency of the incident has often passed. Deterrence weakens when consequences arrive late, or not at all.

- **Fear of escalation has produced a reliance on ambiguity that favors the aggressor**. By avoiding clear thresholds and predictable consequences, European governments hope to avoid war. In practice, this restraint has raised Moscow's tolerance for risk. Each unpunished act widens the space for the next one.
- **Deterrence has been tethered to courtroom standards of proof**. Shadow warfare is designed precisely to frustrate legal certainty. Insisting on incontrovertible evidence for each incident before acting strategically leaves the initiative in Moscow's hands. This is particularly true when attribution rests on intelligence sources that cannot be made public. Deterrence in the shadow domain cannot rest on legal attribution alone; it must be informed by patterns, intent, and cumulative effect. This does not mean that evidentiary standards should be lowered, but governments must be enabled to act on confident intelligence assessments that cannot always be made public.

Toward Effective Deterrence

Given these challenges, deterring shadow warfare requires not more activity, but differently organized activity, and different priorities to motivate that activity. Correspondingly, it demands four shifts in how Europe thinks about escalation, responsibility, and risk.

- **Deterrence must move beyond punishment to constraint**. Symbolic sanctions and rhetorical condemnation may express disapproval, but they do little to change Moscow's calculations. What matters is degrading Russia's ability to operate in the shadow domain by disrupting the networks, assets, and enablers that make such operations possible.
- **Deterrence must replace ambiguity of response with ambiguity of means**. In order to impose discipline, thresholds for consultation and action should be clear to Moscow, even if the specific form of retaliation remains unpredictable. Strategic ambiguity should complicate Russian planning, not obscure European resolve.
- **Deterrence must restore causal clarity**. The link between action and consequence must be visible, timely, and undeniable. Delayed, inconsistent, or purely rhetorical responses sever that link, inviting further escalation.
- **Deterrence must accept managed escalation as unavoidable**. The choice is not between escalation and stability. It is between disciplined escalation now and uncontrolled escalation later. Facing a system biased toward risk-taking, persistent restraint increases — rather than reduces — the likelihood of a major crisis. The danger against which Europe must guard is not deliberate war by choice, but accidents, miscalculation, and unintended consequences.

Deterrence in Action: What Must Change

Finally, translating these principles of deterrence into practice requires a discrete set of four clear, durable, and consistent policy changes.

- First, collective consultation should become routine, not exceptional. European allies should normalize collective consultations in response to shadow aggression, using existing European mechanisms where available and creating new ones where necessary, including by building on flexible partnership formats already used effectively in the Baltic and Nordic regions. Patterns of activity, rather than isolated incidents, should trigger collective assessment and coordination.
- Second, responses should be anchored in national security institutions. Militaries and intelligence services, not law enforcement agencies, should lead the coordination of responses to concerted campaigns of shadow warfare. This does not imply abandoning collective frameworks or sidelining law enforcement. Criminal investigations remain necessary in order to impose consequences on individual actors, but they cannot be the primary framework for deterring a committed state actor. Rather, they should feed into political and security decision-making structures, acting at pace and in coordination with partners across Europe.
- Third, allies should maintain a standing menu of consequences. This menu should be designed for speed and predictability, and include cyber and intelligence operations, interdiction of vessels and other infrastructure supporting covert activity, and economic measures that directly constrain Russia's warfighting capacity, rather than merely signaling displeasure.
- And fourth, Europe should internalize that deterrence is created by consistency. Deterrence will not be restored through sharper or faster rhetoric or better exposure alone. It will be restored only when Russia learns that shadow warfare reliably produces consequences that outweigh its benefits.

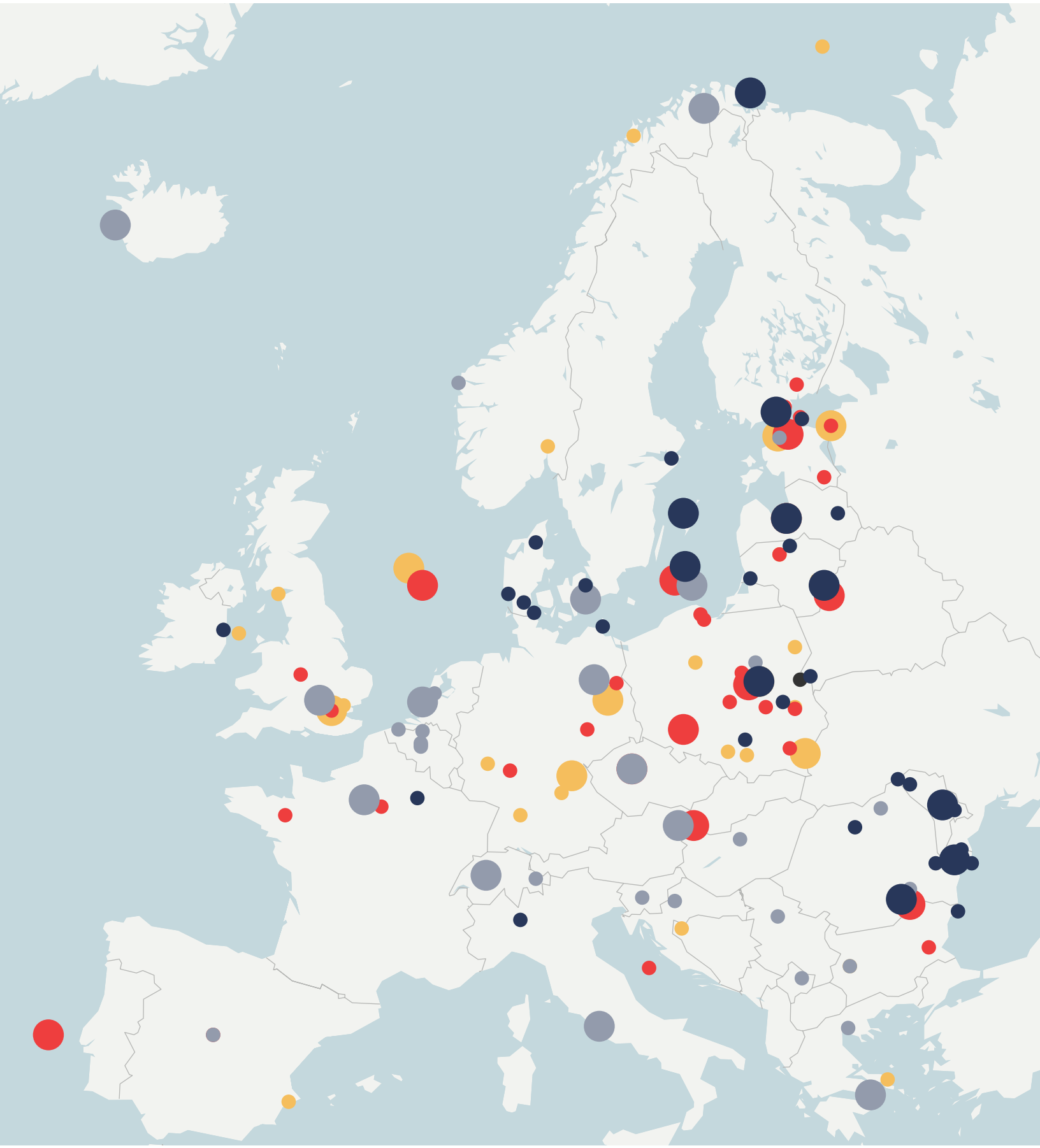
Russia's shadow warfare is not an aberration. It is a durable feature of how the Kremlin understands conflict and power. As long as it remains effective and low-cost, it will continue and likely intensify. Europe's task, then, is not simply to endure this campaign, nor to expose it for what it is. It is to impose limits. Other adversarial powers, including China, will also be watching how Europe responds. Deterrence will not be measured by the sharpness of condemnations or the ingenuity of defensive measures, but by the consistency with which aggression is met by consequence.

The question is no longer whether Russia will continue to fight in the shadows. It is whether Europe will continue to allow those shadows to set the terms of escalation, or whether it will act now to prevent a larger war.

Opposite map includes approximate locations confirmed and highly likely incidents of Russian Shadow Warfare. Confirmed incidents include those attributed by government and journalistic sources to Russia or Russian-supported perpetrators. Highly likely incidents include those that have been reported by government and journalistic sources with a high likelihood of being attributable to Russia or Russian-supported perpetrators.

Opposite Map: Michael Newton/Isabella Nieminen/Katelynn Henics/Center for European Policy Analysis. Source: Emma Burrows et al.,"Russian Sabotage Across Europe," Associated Press News, December 18, 2025, https://apnews.com/projects/russian-europe-sabotage/; Sahaidachnyi Security Center, "The Everywhere War: Sub-Threshold Warfare Tracker,"https://sahasec.org/tracker/; Nichita Gurcov," ACLED data show at least 50 instances of airspace violations of countries on Ukraine's western borders since 2022 — Expert comment,» ACLED, September 11, 2025, https://acleddata.com/expert-comment/acled-data-show-least-50-instances-airspace-violations-countries-ukraines-western; Charlie Edwards and Nate Seidstein,"The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure." IISS, August 2025, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/08/pub25-095-the-scale-of-russian-sabotage-operations.pdf; and Open-Source Information gathered by CEPA staff.

Mapped: Russia's Shadow War



Cyberattacks, including electronic warfare.

Espionage, including assassinations and attempted killings.

Airspace incursions and malicious drone activity.

Sabotage, including arson and attacks on undersea infrastructure.

The Veiled Invasion: Deterring Russian Infiltration in Europe

DAVID KAGAN

Introduction

Over the last year, NATO has seen a dramatic surge in the number and severity of Russian shadow operations in its territory. Russia's full-scale invasion of Ukraine in 2022 ushered in a period of unprecedented brazenness from Moscow that has deepened as the Kremlin intensifies its war with the West. The airspace incursions, arson, and targeted violence that Europe has endured over the course of the last four years represent a bald-faced escalation of this war without end.

NATO has long struggled to produce an effective deterrence policy against Russian shadow war. Its dread of escalation with Russia since 2014 has so paralyzed the alliance that Vladimir Putin has been able to escalate his war with Ukraine and the broader conflict with NATO on his own terms with impunity. The challenge for NATO is both strategic and structural. NATO's deterrence posture depends on the consensus of more than 30 democracies constrained by disparate threat perceptions, polarized domestic public opinion, and varying risk tolerance levels and thresholds for escalation. Cognizant of these conditions, Moscow has learned to exploit them by operating its shadow war just below the level that would definitively compel collective action from NATO allies.

Another key challenge for allies that limits their ability to decisively respond to Russian shadow war is attribution. A defining feature of Russian shadow warfare is that it is designed to mask the Kremlin's involvement and blur clean lines of attribution that would normally trigger clear political or legal responses. Rather than relying on uniformed forces or overt state actors, Russian security services increasingly operate through layers of intermediaries — proxies, criminal facilitators, deniable contractors, and loosely affiliated third-country actors. By ensuring that individual incidents lack a "smoking gun" that could legally tie Moscow to its shadow operations, Russia has slowed decision-making, fractured consensus, and cultivated a propensity toward restraint among NATO allies.

Allied assessments of Russian responsibility must therefore rest not on isolated events or single strands of evidence, but on cumulative pattern recognition over time. Russian security services have demonstrated a consistent operational signature across Europe: the use of deniable intermediaries; targeting operations

aligned with Kremlin strategic objectives; and repetition of similar tactics across multiple allied states. In this environment, insisting on incontrovertible proof for each operation before responding leaves initiative in the hands of the Kremlin. Deterrence in the shadow domain will depend not on courtroom standards of evidence, but on strategic judgment informed by patterns, precedent, and intent.

As a result of these muddled attribution lines, the inherent structural challenges within the alliance, and Moscow's ability to manipulate those structural challenges, NATO has largely failed to deter Russian aggression in its territory over the last decade. The alliance has tolerated a much more aggressive posture from the Kremlin in years since the full-scale invasion of Ukraine and has set up little meaningful deterrence. Moscow, meanwhile, has enjoyed success exploiting divisions and uneven threat perceptions within the transatlantic alliance, conducting infiltration operations on European soil effectively at will without prompting a forceful response.

Thus, when NATO Secretary General Mark Rutte and NATO's supreme allied commander, Gen. Alexus Grynkewich, took the podium in Brussels on Sept. 12, 2025, just a couple days after more than 20 Russian drones were detected in Polish airspace, there was a palpable expectation for a big announcement detailing a new NATO posture for dealing with Russia's growing aggression. Seeing as the events from earlier in the week represented the largest drone incursion into allied airspace to date — a clear escalation in what should be perceived by allies as a direct confrontation with NATO's security apparatus — Rutte and Grynkewich's presser in Brussels carried a weight not unlike that of a head of state addressing their country on the precipice of war.

What came out of the press briefing, however, was not a distinct, new posture, but more of the same. Rutte and Grynkewich announced Operation Eastern Sentry, aimed at strengthening eastern flank surveillance and air defense response coordination. The operation expands NATO's air policing and early warning posture, deploying additional fighter aircraft and anti-drone capabilities to the alliance's eastern flank.[1] It also enhances real-time intelligence sharing between Allied Air Command and national defense agencies to improve detection and reaction times.[2] In concept, Eastern Sentry signals to Moscow that allied airspace is monitored and defended, and that NATO is united in the defense of its territory.

This is a good start. It acknowledges that Russian shadow warfare has breached acceptable boundaries and places additional capability where the threat is most acute. It serves an important reassurance function in that front-line allies now enjoy a more visible NATO presence overhead in the face of encroaching Russian aggression.

But deterrence requires more than increased surveillance and patrols. It requires consequences. Despite Eastern Sentry's deployment, Russia and its proxies have continued to probe allied airspace — flying drones deep into allied territory (as far west as Belgium and Ireland), drifting surveillance balloons from Belarus into Lithuanian skies, and conducting recurrent incursions across the eastern flank. The persistence of these operations demonstrates that Eastern Sentry has not changed Moscow's core strategic calculation that Russian hybrid violations remain a low-cost, low-risk method for eroding NATO cohesion.

In its current form, Eastern Sentry is a defensive posture, not a deterrent strategy. It helps NATO see more, but leaves unsettled what the alliance is willing to do about it. As long as allied responses remain confined to scrambling jets, finger-wagging, and urging restraint, Russia will continue to escalate, normalizing its presence in NATO skies and transforming the unacceptable into the routine.

What NATO lacks, and what the moment urgently demands, are clearly defined red lines and consequences. Deterrence does not function on ambiguity. It is most effective when an adversary believes two things simultaneously:

- **There are unmistakable red lines**
- **Crossing them will generate a response that outweighs any benefit**

Right now, Moscow sees neither. Russian decision-makers perceive NATO's fear of escalation as a vulnerability to be exploited. Every drone, jet, and balloon that crosses into sovereign airspace without serious repercussion reinforces the perception that Europe's political will is fragmented and that allies are reaction-averse.

Strength must be paired with predictability. The Kremlin must understand exactly when an intrusion becomes a strategic error. Absent that clarity, Russia will continue to dictate the tempo of escalation.

Part 1 — Defining Russian Infiltration

Russia's shadow war doctrine increasingly emphasizes infiltration — the deployment of indirect and deliberately ambiguous attacks that fall somewhere between normal criminality and full-out conventional war. The infiltration tactics used by the Kremlin offer Moscow lower-cost, deniable means to test allied resilience, undermine cohesion, and stretch thin the allied security apparatus.

These operations take many forms and test allies' political will and deterrence capabilities in a variety of ways. Inexpensive drone incursions on NATO's eastern flank oblige costly responses from allies like scrambling fighter jets and counter-drone systems (which thus far have accomplished little in the way of deterrence); sabotage operations on key infrastructure supporting Ukraine's defense (like the

Photo: Koleje Mazowieckie train sits on the track with police tape as Polish Prime Minister Donald Tusk visits the site of a blast on railway of the Warsaw-Lublin line in Mika, Poland, November 17, 2025. Credit: KPRM/Handout via REUTERS.

November 2025 explosion on the Warsaw-Lublin railway line or the plot to kill Rheinmetall CEO Armin Papperger) are routinely conducted by proxy networks and thus not easily attributable to Moscow; and non-kinetic operations like forced migration threaten the European Union's already fragile internal political unity. In the aggregate, these infiltration tactics collectively test the political will, coordination, and deterrence posture of NATO allies. Infiltration complements Russia's other hybrid tools by exploiting ambiguity, deniability, and legal asymmetry among allies.

This is Moscow's adaptation to an uncomfortable reality of its perpetual conflict with the West. Confronting the alliance conventionally is effectively out of the question for Russia. Its gross domestic product of roughly $2.54 trillion is dwarfed by the EU's $21.1 trillion,[3] and NATO's military expenditure is 10 times[4] what Moscow has been able to conjure up, even with the Kremlin having fully reoriented the Russian economy to a wartime posture.

Unable to carry out its war with the West in a conventionally kinetic manner, Moscow instead seeks to erode NATO political and societal cohesion from within by challenging the alliance through diffuse and hard-to-attribute disruptions. These tactics are relatively inexpensive and scalable — and their success hinges on a lack of European cohesion. For on-the-ground infiltration, Russian intelligence and affiliated networks employ overlapping ecosystems of criminal organizations and ideologically fluid local recruits. The Kremlin benefits from a middle ground between espionage and ordinary crime by non-state actors, enabling it to destabilize adversaries while maintaining plausible deniability to skirt formal responses.

Take as an example the 2024 arson attack on the Marywilska 44 shopping center in Warsaw: Even though local authorities ultimately traced the attack back to Russia through an expansive network of Kremlin proxies, the investigation took over a year and the Polish government still has taken no significant accountability measures. This event illustrates a key point outlined by Sam Greene in the introduction of this report: "While front lines progress or fail, and bombs hit or miss their targets, shadow warfare operations succeed when they disrupt, they succeed when they're exposed, and they succeed when they fail. As such, in Moscow's decision-making framework, shadow operations are always a viable option, and more operational risk-taking is always better than less."[5]

In the air, meanwhile, the Kremlin has benefitted the most from NATO's paralysis.

Russian infiltration operations serve several purposes:

- **Testing allied systems:** Repetitive, small probes allow Russia to map response timelines, interagency gaps, political will, and cross-border coordination.
- **Political weaponization:** Infiltration acts seldom aim for significant material damage; their utility lies in sowing fear, uncertainty, and division.
- **Normalization of hostility:** Persistent infiltration desensitizes publics and institutions, making subsequent escalations less shocking and thus less likely to elicit a response.
- **Ambiguity and plausible deniability:** By employing proxies with criminal profiles or third-country actors, Moscow makes attribution difficult and reduces the political cost of escalation.
- **Low unit cost, scalable operations:** Small-scale incidents (drone overflights, fires, migration surges) can multiply quickly, imposing cumulative stress on law enforcement.

Part 2 — Deterring Russia's Aerial Incursions

Eastern Sentry: What It Is and What It Isn't

Less than 24 hours after NATO announced Operation Eastern Sentry on Sept. 12, 2025, another Russian drone was detected in Romanian airspace.[6] Less than a week later, three Russian MiG-31 fighter jets violated Estonian airspace above the Gulf of Finland, where they loitered for 12 minutes with their transponders off under no flight plan.[7] Three days after that, sightings of suspected Russian drones over Copenhagen's airport halted take-offs and landings for over four hours.[8] Belarussian weather balloons over Lithuania;[9] more drone flights over a US Army base in Estonia;[10] another invasion of NATO airspace by Russian military aircraft over Lithuania that prompted the scrambling of NATO jets[11] — all occurred within weeks of NATO's announcement of its new defense posture.

These events demonstrate a Kremlin playbook that uses relatively inexpensive aerial probes to gather intelligence on allied reaction times, strain local air-defense resources, and provoke political division — all while avoiding the threshold that would compel an automatic allied military response.

Taking into account the acceleration of Russian airspace violations, the Kremlin appears little deterred by the early stages of Operation Eastern Sentry. But that doesn't mean it shouldn't be celebrated for improving allied defense posture. It augments NATO's air policing on the eastern flank by deploying additional fighter rotations, mobile radar and sensor assets, enhanced NATO/EU intelligence-sharing links, and counter-drone teams where feasible. These deployments help monitors more quickly spot intrusions and increase the proportion of incursions that are documented, tracked, and interdicted.

Allied Commitments to Eastern Sentry

Country	Assets Committed
France	3 Rafale fighter jets; 1 Airbus A400M military transport aircraft
United Kingdom	RAF Typhoon fighter jets
Germany	4 Eurofighter Typhoon jets
Italy	Fighter aircraft (type TBC, likely Eurofighter)
Denmark	F-16 fighter jets; 1 naval frigate
Spain	Air assets (fighters or support aircraft, TBC)
Sweden	Air assets (fighters/support aircraft, TBC)
Czech Republic	Special forces troops; 3 military helicopters

Addressing NATO's 'National Caveat' Gaps

One of the main benefits of Eastern Sentry is the discussion it is prompting over NATO's operational constraints — most notably the alliance's built-in "national caveats." NATO members still retain sovereignty over the deployment of military assets for NATO missions, which creates a patchwork of available forces and limits rapid, integrated responses. The US Ambassador to NATO, Matthew Whittaker, noted "It's no secret that the more 'national caveats' there are on — especially our fighter jet assets — the harder it is for [the supreme allied commander] to respond immediately."[12]

Eastern Sentry offers a new avenue for addressing these gaps. It can chip away at institutional barriers within NATO to establish pre-agreed commitments from member states. Under this framework, air, maritime, and counter-drone assets assigned to the eastern flank can be pledged in advance for NATO air-policing and counter-incursion duties. By binding contributors into a shared mission architecture and specifying zones of operation under a unified command, Eastern Sentry can limit discretion at a moment of crisis. The result should be faster decision-making, fewer obstacles, and more credible deterrence. The initiative would signal a meaningful shift toward collective rapid-reaction posture, signaling to Moscow that NATO force contributions are not merely symbolic, but operationally ready under shared rules.

Europe's Cost Asymmetry and Political Will Problem

Nevertheless, a recurrent problem facing NATO is that it costs allies more to manage Russian aerial incursions than it costs Russia to launch them. While the drones that traverse NATO airspace are relatively cheap to manufacture and deploy, allied responses — scrambling jets, diverting AWACS and tanker sortie hours, and activating air-defense batteries — are expensive.[13] Shooting down even a small, low-cost drone requires interceptors, rapid-response infrastructure, and politically delicate rules of engagement. Ukraine has excelled at neutralizing Russian drones with low-cost materiel, but NATO's response mechanisms to similar incursions are typically less cost-effective. For the attacker, the equation is simple: Expend a cheap asset, gather a multitude of data points, accomplish certain political goals, and force the defender to pay the price in resources and attention. Eastern Sentry is an important initial step toward a more integrated aerial defense posture within NATO, but there is still little discussion about asymmetry in costs. This issue risks metastasizing into more political dissonance among member states as the EU and NATO persist in the age-old debate of who will foot the bill of European deterrence and security. This is precisely the Kremlin's objective.

We see this internal political dissonance at play with one of the key allied strategies for addressing Russian incursions into NATO airspace. The idea of building a so-

called "drone wall" — a network of radars, sensors, jammers, and interceptors stretching along Europe's eastern flank — has generated strong support in Brussels and among front-line states, yet the initiative is running into two major constraints. First, the scale and cost of deploying a layered detection and defeat architecture across Russia's border with Europe is massive. The need for long-term funding, joint procurement, and ongoing sustainment makes the project both expensive and slow. EU Defense Commissioner Andrius Kubilius has admitted that the EU's "capabilities are really, for the time being, quite limited."[14]

Second, not all European capitals are sold on the idea. Eastern and Baltic states press hard for rapid deployment, while western and southern nations that are less exposed to the immediate threat question both the cost burden and what's in it for them. Italy's Georgia Meloni is a key skeptic of the program's utility for her country's security.[15] These dual pressures — high cost and split political will — mean that even as the concept of a drone wall resonates rhetorically, its implementation risks being delayed or deferred.

Changing Moscow's Calculus

The reality is that augmented detection systems and procedures change what NATO sees more than what NATO does. Eastern Sentry increases the alliance's situational awareness, which is necessary, but not sufficient, for deterrence. The Kremlin can and will continue to test the alliance as long as the act of being seen imposes no politically meaningful cost.

Surveillance and rapid reaction are necessary building blocks. They buy time and gather the evidence needed for attribution and targeted action. But the true test of deterrence will be whether allies transform that evidence into predictable, materially consequential outcomes that alter Russian cost-benefit calculations. The Kremlin has been able to escalate its probing exercises because the downside is low. The only way to change that arithmetic is to make the downside permanent, visible, and strategically costly.

A well-funded drone wall might reduce the frequency of incursions, but it will not by itself stop the strategic logic that drives them. Only a combined posture — augmented surveillance plus an unambiguous, public escalation ladder tying incursions to actionable responses (including accelerated support for Ukraine) — will make Moscow reconsider its aerial incursion strategy.

Taking into account their various challenges, allies should consider the following:

- Codify preauthorized decision pathways and operational assets pool. NATO's supreme allied commander should be granted standing authority to deploy fighters; intelligence, surveillance, and reconnaissance platforms; and counter-drone teams during hybrid attacks, with allies opting into asset pools ahead of time to prevent political delays

Photo: May 12, 2024, Warsaw, Masovian Voivodeship, Poland: A person looks at the burning Marywilska 44 shopping center in Warsaw. Massive fire at the Marywilska 44 shopping center in Warsaw's Białołęka district. Credit: Attila Husejnow/SOPA Images via ZUMA Press Wire

- Clarify burden-sharing for air defense to address the cost asymmetry created by Russia's low-cost aerial probes by:
  - Establishing an EU-NATO hybrid-defense fund
  - Reimbursing front-line states for sustained air-policing operations
  - Co-funding counter-drone and drone-wall components

To make deterrence credible, NATO must ensure that each aerial incursion carries a tangible and escalating consequence. There are several ways to do that, the most effective of which would be to link every violation of allied airspace directly to increased material support for Ukraine, including:

- Unlocking previously withheld long-range strike capabilities
- Expanding the delivery of existing materiel
- Accelerating joint EU-NATO efforts to train Ukrainian pilots and integrate Western aircraft

Allies could also tie increased sanctions to aerial infiltration and coordinate the gradual unfreezing and transfer of interest accrued on Russian sovereign assets

to Ukraine's defense fund. This would make clear that each new incursion hastens Moscow's financial losses.

These measures will invite louder nuclear rhetoric and threats from the Kremlin, but that escalation is inevitable. Tolerating it is part of restoring deterrence. For too long, NATO has allowed Moscow's bluster to define the boundaries of acceptable action. Deterrence cannot function if fear of rhetorical escalation outweighs the critical security imperatives.

Part 3 — Deterring Russian Proxy Activity

One of the more challenging infiltration methods for allied states to address is the use of proxy networks, nonprofessional actors, and criminal syndicates by Russian intelligence services and other state actors. These operatives carry out attacks on behalf of or in alignment with the Kremlin's strategic objectives while maintaining layers of deniability for the Russian state. The recruitment process typically targets individuals embedded in Europe who are nonprofessional, financially vulnerable, ideologically ambivalent, or located in jurisdictions with weaker law enforcement mechanisms. Many of these actors carry out operations unaware of their Russian sponsorship. These strategies are now well-known in Europe — German authorities in September 2025 began warning their citizens against becoming "disposable agents" in Russian proxy operations in Europe.[16]

Russian Intelligence Recruitment

A May 2024 arson attack on an Ikea store in Vilnius is a prime example of Russian intelligence services' recruitment practices. Investigators found that the perpetrators were two Ukrainian citizens, one under 20, the other under 18, who were offered 10,000 euros ($11,000) and a used BMW for undertaking this operation.[17] Arturas Urbelis from the Lithuanian prosecutor general's office said the attack was linked to Russian military intelligence via a chain of more than 20 intermediaries.[18]

Three days later, Marywilska 44 shopping center in Warsaw burned in a massive fire that destroyed one of Poland's largest retail complexes. The Polish prime minister announced after a yearlong investigation that Russian secret services were behind the attack.[19] Prosecutors charged two Ukrainian citizens who had cooperated with those who carried it out. Poland then ordered the closure of Russia's consulate in Kraków in response. Public statements framed the fire as part of a broader sabotage campaign targeting states that support Ukraine.[20] While officials have not released the same granular payment details as in Vilnius, the pattern they describe — local, nonprofessional recruits guided by handlers abroad who were, in some cases, unaware of the ultimate sponsor — aligns with the wider recruitment model seen across recent incidents.

The November 2025 sabotage of the Warsaw–Lublin railway line, which carries more than 100 trains daily and is used for transporting military assistance to Ukraine, appears to have followed the same proxy-recruitment model seen in other recent Russian-linked operations. Polish authorities indicated that the plot relied on locally present intermediaries rather than trained operatives, including foreign nationals (among them Ukrainian citizens) who were recruited through informal or criminal networks and directed remotely by handlers operating abroad.[21]

Taken together, these incidents reveal a consistent and deliberate recruitment strategy by Russian intelligence services — the use of young, economically vulnerable operatives as proxy saboteurs for deniable operations across NATO and the EU. The frequent use of susceptible Ukrainian nationals is strategically consequential as well. Beyond the primary goals of Russian shadow war, which aims to outsource operational risk to expendable actors while complicating political attribution and blurring the line between victim and perpetrator, the use of Ukrainian nationals seeks to weaponize sympathy for Ukraine.

Since the full-scale invasion of Ukraine, EU and NATO states have made extraordinary political, financial, and social commitments to support Ukrainians fleeing Russia's war, extending protection, residency, employment access, and social services on an unprecedented scale. By embedding sabotage operations within this population, Russian intelligence services seek to exploit that openness and transform humanitarian solidarity into a perceived security liability. Even isolated cases — magnified through media coverage and political debate — can fuel suspicion of refugees, harden public attitudes, and empower domestic actors arguing for restrictive migration or asylum policies. This dynamic forces democratic governments into a tricky bind: tighten controls and risk undermining their moral commitment to Ukraine or maintain openness and absorb the political fallout of security incidents.

Russia's use of proxy operatives extends beyond sabotage to include targeted killings and assassination attempts on dissidents, defectors, and individuals Moscow deems strategically threatening. While high-profile GRU poisonings like the Skripal attack in Salisbury involved trained intelligence operatives, European governments have increasingly identified amateur intermediaries and organized-crime facilitators within these networks. These proxies are recruited not for ideological loyalty but for proximity, pliability, and expendability.

The most notorious instance of this approach was the plot against Rheinmetall CEO Armin Papperger. In early 2024, thanks to alerts from US intelligence, German authorities foiled a plot to murder Papperger, whose company is one of Kyiv's most critical suppliers of armored vehicles and munitions. Western intelligence would later implicate an active Russian proxy network as the perpetrators, though there was insufficient evidence to make arrests.[22]

In the spring of 2025, German authorities charged three men with working with Russian intelligence services to spy on and potentially assassinate a German citizen who fought with Ukrainian forces against Russia's invasion. According to federal prosecutors, the suspects — an Armenian, a Ukrainian, and a Russian national — had been gathering intelligence on the intended target's location and movements in preparation for what investigators described as a possible killing mission. The men were allegedly directed by the FSB and received instructions to locate and surveil the target in western Germany.[23]

Kremlin Methodology

As Western security services have hardened against sophisticated GRU operations, the Kremlin has adapted by outsourcing violence to irregular networks whose criminality blurs attribution and complicates legal response. The intent is not only to neutralize individual targets but also to signal to Brussels and European capitals its reach and impunity. Critics of the Kremlin — whether journalists, exiled opposition figures, community organizers, or those aiding Ukraine — face a threat environment in which a neighbor, co-worker, or petty criminal may serve as the weapon of their adversary. These cases underscore a core feature of the Kremlin's infiltration strategy — outsourced coercion that exploits Europe's open societies, legal protections, and trust in public space while shielding Moscow behind layers of deniability.

Taken together, the cases illustrate a repeatable strategy: Recruiters approach opportunistic, low-skilled actors (often via intermediaries and cross-border meetings) offering modest but salient incentives, and task them with simple, high-impact actions such as arson. The design exploits Europe's legal and political constraints while maximizing psychological and diplomatic tumult (e.g., consulate closures, emergency statements, and heightened public anxiety).

Contextualizing and Responding

Russia's campaign of on-the-ground infiltration across Europe is not a separate phenomenon from its war in Ukraine but an extension of it. Each operation carried out on European soil, whether an arson in Warsaw or a foiled assassination in Germany, serves the same strategic purpose of weakening allied resolve, disrupting military supply routes, and imposing psychological costs on governments supporting Kyiv. The 2024 plot to assassinate Papperger is an apt example, as Rheinmetall has been one of Ukraine's principal defense suppliers, producing ammunition and armored vehicles critical to Ukraine's battlefield resilience. Targeting its leadership was not random. It was a calculated signal that European defense industries directly aiding Ukraine are now part of the battlefield.

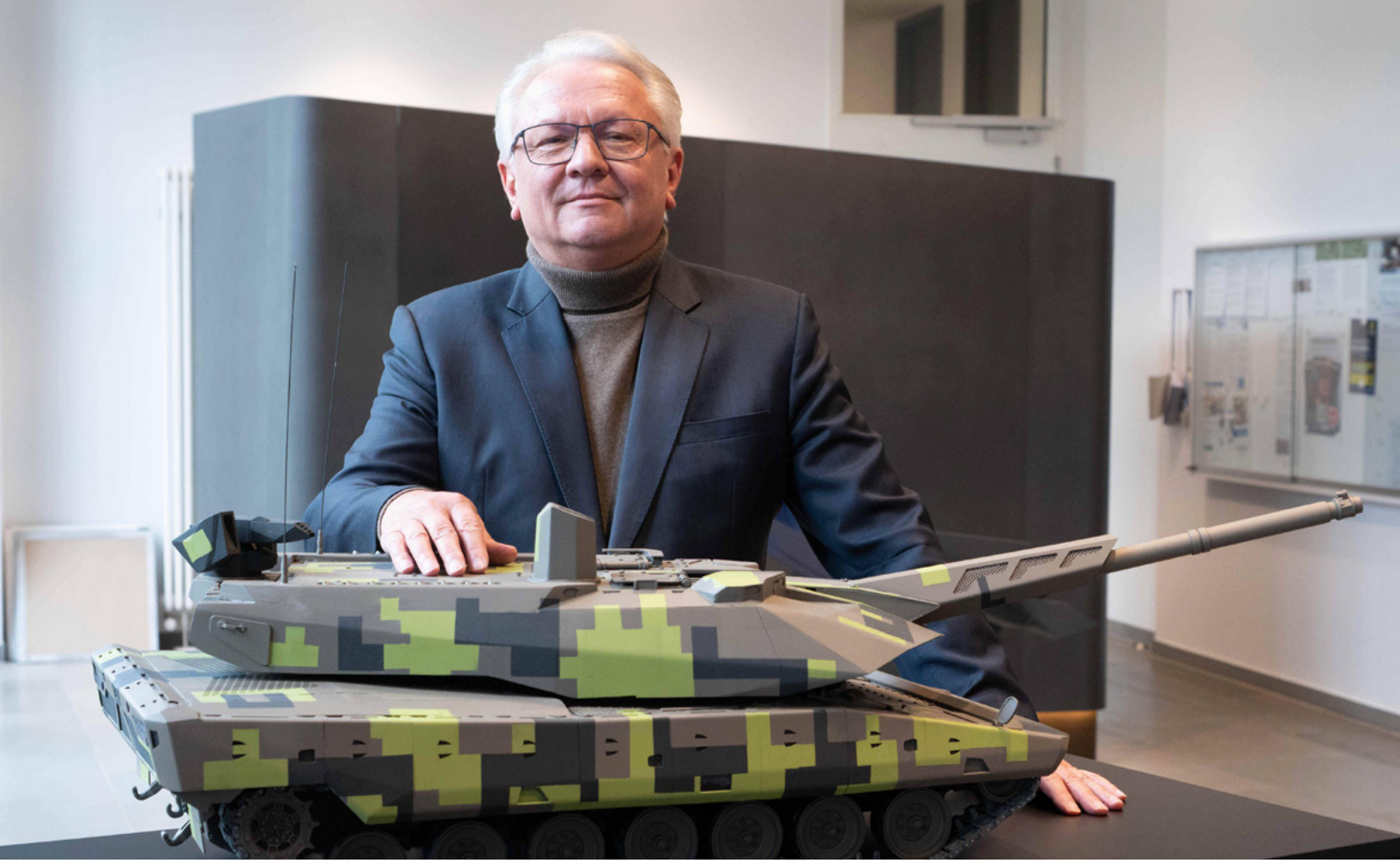


Photo: Armin PAPPERGER, Chairman of the Executive Board, CEO, at a model of the KF51 Panther main battle tank, which is produced by Rheinmetall, Balance Sheet Press Conference Balance Sheet PK, BPK of Rheinmetall AG on 11 03 2023 in Duesseldorf Germany. Credit: IMAGO/Malte Ossowski/ SVEN SIMON/Alamy Live News.

These operations illustrate how Moscow has expanded the geography of war to encompass Europe's interior. The Kremlin's method of using nonprofessional actors who can be plausibly disowned if exposed allows Russia to inflict political and economic disruption at minimal cost and with limited risk of escalation. It also enables Moscow to test NATO's internal cohesion by seeing whether acts of sabotage and intimidation on allied soil produce unified responses or disjointed national reactions. So far, it has largely been the latter.

Countering this strategy requires both defensive hardening and strategic signaling. The EU and NATO must first make proxy recruitment and sabotage more difficult. To this end, allied intelligence services should:

- **Expand joint task forces to monitor online recruitment networks on encrypted platforms**

  This could include the establishment of a dedicated NATO–EU attribution cell structured on the model of Europol's joint investigation teams, bringing together the full spectrum of evidence needed to pierce the layers of ambiguity Russia relies on. This unit would fuse:

  - Forensic material recovered from arson sites, sabotage attempts, or disrupted operations
  - Intelligence drawn from NATO's surveillance and reconnaissance platforms
  - Cyber forensics capable of mapping digital infrastructure, command nodes, and operational coordination behind each incident
- **Disrupt proxy financing by:**
  - Increasing monitoring and scrutiny of cross-border cash transfers and cryptocurrency exchanges, including crypto ATMs, prepaid phones, and anonymous remittance services
  - Requiring EU-wide ID verification for SIM card purchases
  - Using anti-money laundering and organized crime authorities to freeze assets of intermediaries without needing sanctions action
- **Strengthen cooperation with local law enforcement and Europol to identify financially vulnerable individuals susceptible to recruitment.**
- **Limit Russia's recruitment supply by:**
  - Expanding outreach in districts where patterns of recruitment have been detected
  - Increasing policing visibility in industrial zones and logistics hubs
  - Creating anonymous reporting channels for individuals approached by foreign-linked recruiters

The success of Russia's proxy campaigns depends on Europe's fragmented surveillance, inconsistent prosecutorial frameworks, and slow information-sharing among agencies. Closing those gaps will deprive Moscow of its low-cost, deniable manpower.

Yet even perfect prevention will not suffice for deterrence. What will alter Moscow's behavior is not restraint or episodic responses, but determined, consistent action over time that reshapes its cost-benefit calculations. Every attack or attempted attack on European soil should trigger a proportional increase in material support to Ukraine. Support for Ukraine is not a parallel effort to countering Russia's shadow war; it is its strategic center of gravity. Moscow's shadow war is designed to raise the perceived cost of sustaining Western support for Kyiv by testing allied resolve and exploiting political fatigue. These actions are not isolated provocations, but instruments intended to shape European and transatlantic decision-making on Ukraine. Any deterrence strategy that treats infiltration on NATO territory as separate from the war is a misreading of its purpose.

Aiding Ukraine represents the most direct and cost-effective means for the alliance to impose sustained pressure on Russia without entering a conventional conflict. Material support to Kyiv degrades Russian military capacity, strains its industrial

base, and consumes resources that might otherwise be directed toward hybrid operations against NATO members. In this way, reinforcing Ukraine's territorial integrity is not escalation by proxy, but a form of strategic containment — one that forces Moscow to confront the consequences of its actions on the battlefield.

NATO and the EU must make clear that Russian shadow war will not deter but will rather accelerate the very support that threatens Russia's war effort. Only by linking infiltration in Europe to punishment on the battlefield can the alliance transform Moscow's gray-zone strategy from a tool of coercion into a liability of its own making.

Part 4 — Forced Migration as a Tool of Undermining European Cohesion

One of the more subtle but effective infiltration tactics used by Russia and its allies is the weaponization of migration: the strategic use of migration flows, irregular border crossings, or facilitated transit to pressure allied states, undermine EU cohesion, amplify domestic political tensions, and test border and asylum systems. While Russia's war in Ukraine focuses attention on the battlefield, its parallel effort to destabilize Europe through the orchestration of migration flows represents an extension of the same strategic logic of fracturing allied unity and deepening domestic polarization.

Illustrative Examples

In 2021, Belarus launched a state-sponsored operation to channel migrants, primarily from the Middle East and North Africa, toward the borders of Lithuania, Poland, and Latvia. The move was retaliation for EU sanctions after the fraudulent 2020 Belarusian election and subsequent crackdown on protesters. Belarusian authorities, working with state-controlled travel agencies and Middle Eastern airlines, issued tourist visas and advertised easy access to the EU. Upon arrival, migrants were directed toward EU border zones, where many were supplied with tools to breach fences.[24] Those unable to cross were forced to remain in freezing conditions, while Belarus repeatedly refused Polish aid convoys.[25] At least 20 migrants died in the border area that winter.[26]

In 2023, Finland also saw a jump in attempted illegal crossings on its eastern border. Late that year, the Finnish border agency, Raja, said there were "clear indications that authorities of a foreign state or other operators have furthered the entry of those persons who illegally crossed the border into Finland."[27] This was likely a Russian response to Finland's NATO membership, which was a direct result of the full-scale invasion of Ukraine.

Photo: A soldier is on duty by the border wall in a forest in Podlasie, Poland, on June 8, 2024. Credit: Kamil Jasinski/NurPhoto

Allied Responses

In both instances, allied nations were forced to take extreme measures to protect their borders. Finland, newly admitted to NATO and directly confronting Russian hybrid tactics, closed all but one of its eastern crossings in late 2023. Helsinki also passed a temporary emergency law allowing border guards to reject asylum claims in specific national-security circumstances, citing the weaponization of migration by Russia.[28] The measure reflected the growing view among northern allies that hybrid border pressure required security-first responses.

Poland, Lithuania, and Latvia had already taken similar steps during the 2021-2022 Belarus-engineered migration crisis. Warsaw declared a state of emergency and constructed a 115-mile steel barrier along its border with Belarus, funded nationally after the European Commission refused to finance physical border walls.[29] Lithuania erected a comparable 300-mile fence and expanded surveillance capabilities.[30] Latvia followed suit by constructing its own fence across its 100-mile-plus border with Belarus.[31]

These measures collectively marked the emergence of a Baltic-Nordic security belt, a network of hardened frontiers designed to blunt Russia's and Belarus's attempts to use migration as a destabilizing tool. Yet the response also underscored a persistent tension within the EU: Front-line states prioritize deterrence and border control, while Brussels remains wary of breaching asylum and human rights norms. For Moscow and Minsk, that tension is itself a success in that it forces Europe to debate its values under pressure.

The weaponization of migration exposes a fundamental asymmetry between authoritarian and democratic systems. Moscow and Minsk operate without legal, humanitarian, or political constraints. They can manufacture crises, instrumentalize vulnerable populations, and escalate pressure at will, unconstrained by domestic accountability or international norms. Democratic states, by contrast, are bound by rule-of-law obligations, asylum frameworks, judicial oversight, and public scrutiny– constraints that are not weaknesses in peacetime but become exploitable vulnerabilities under deliberate pressure, as is the case today. Russian and Belarusian strategy is built precisely on this imbalance, forcing democracies to choose between acting decisively and upholding their own rules.

Russia's Objectives

There is a clear and consistent strategy at play for Russia and Belarus here:

- **Facilitated transit:** recruitment of migrants in one region, directed via Belarus (or Russia) to a targeted border
- **Amplified narrative:** use of Russian state media and proxies to brand the target country as cruel, illegitimate, or incapable of managing the influx, thereby undermining public trust and generating populist backlash
- **Resource strain and political polarization**: sudden migrant influxes create border pressures, humanitarian dilemmas, political disputes (particularly in EU states with migration-sensitive electorates)

The defensive steps taken by Finland, Lithuania, Latvia, and Poland triggered unease in Brussels. Critics, including the European Commission and human rights advocates, warned that these measures and laws enacted by border states risked breaching EU asylum standards and the bloc's broader human rights obligations. This underscores a recurring dilemma for the EU: Coercive migration pressures force front-line states to choose between upholding EU norms and defending their borders. Each new crisis exposes the political and legal asymmetries within the EU's migration system, in which the moral burden of protection falls disproportionately on states that border Russia and Belarus.

This is precisely the pressure Moscow seeks to generate. Weaponized migration creates both humanitarian and institutional crises. It strains the Schengen system, fuels far-right political movements across member states, and challenges the credibility of the EU's governance model. By forcing the bloc to debate whether security trumps legality, Russia achieves its central goal — not territorial gain, but political paralysis.

The pattern of state-orchestrated migration pressure is now well established. The EU and NATO should no longer treat future incidents as unforeseen humanitarian emergencies but as anticipated instruments of shadow aggression. Advance preparation — clear emergency legal authorities, predefined coordination among front-line allies, and standing mechanisms for rapid political attribution — allows democracies to respond firmly without improvisation or erosion of legitimacy. Preparedness is how democratic systems reclaim agency in a contest where authoritarian actors seek to weaponize restraint itself.

Deterrence Strategies

Deterring the weaponization of migration requires more than ad hoc national emergency measures. It demands a coherent EU-NATO framework that both denies Moscow operational leverage and imposes political costs when coercive tactics are used. Several strands are key:

Allies should establish an EU-NATO hybrid border mechanism that treats orchestrated migration flows as a persistent security challenge rather than a series of isolated humanitarian incidents. This should include:

- Sharing early-warning indicators, such as sudden changes in visa issuance, charter flight patterns, or third-country recruitment
- Making joint risk assessments and agreeing on triggers for deploying Frontex, Europol, and NATO liaison teams to affected borders
- Ensuring rapid situational awareness to reduce the shock value that Russia and Belarus seek

Europe must raise the cost for state and commercial enablers.

Airlines, travel agencies, and logistics firms that knowingly participate in artificially manufactured migration flows should face consequences, including:

- Targeted sanctions and flight bans
- Revocation of landing rights for airlines facilitating manufactured migration
- Bans on EU travel agencies partnering with Belarusian state operators
- Aviation-safety and anti-money-laundering audits on firms complicit in organizing coerced migrant flows

Strategic communications must expose manipulation while preserving Europe's humanitarian narrative.

Governments should publicly distinguish genuine asylum-seekers from the hostile state behavior that placed them at the border. Doing so blunts extremist exploitation at home and denies Moscow the ability to brand European responses as arbitrary cruelty.

Deterrence requires making clear that coercive migration will come at a high price.

Each documented episode of weaponized migration should be tied to concrete Western steps that Russia cares about, including:

- Tighter sanctions enforcement
- Reinforced forward presence
- Increased economic and materiel support to Ukraine

Conclusion: Toward Credible Deterrence

The challenge confronting NATO and the European Union today is not a lack of awareness of Russian aggression, but a lack of strategic follow-through. Over the past decade, and especially since 2022, Moscow has systematically expanded the geography of confrontation to encompass Europe's interior. From drone incursions and arson attacks to proxy assassinations and weaponized migration, these operations aim to make shadow war the new normal.

What is often missing in allied debates is a clear-eyed recognition of how profoundly the threat has evolved since the period before Russia's annexation of Crimea. A dozen years ago, Russian coercion largely operated at the margins, through influence campaigns, cyber probing, and episodic pressure on vulnerable neighbors. Today, Moscow is executing a far more integrated and operationally mature campaign that blends intelligence services, criminal networks, proxies, and emerging technologies into a continuous pressure strategy inside NATO territory. These are not sporadic provocations but a sustained and holistic campaign to normalize hostile action below the threshold of war and recalibrate what Europe comes to accept as routine. Treating today's shadow warfare as an extension of earlier hybrid activity underestimates both its scale and its intent. The Kremlin has moved from testing NATO's red lines to exploiting the assumption that red lines no longer exist. Russia has also learned that ambiguity and deniability is a cheaper and more effective tool than conventional escalation. Each operation that goes unanswered reinforces Moscow's perception that NATO will monitor and condemn but not retaliate.

To reverse this dynamic, deterrence must be restored as a perpetual, adaptive strategy rather than a static posture. To this end, allies should reorient their strategic thinking along the following lines:

1. **NATO and the EU must accept that Russia's shadow war in Europe is not peripheral to the war in Ukraine, but rather an extension of it.**
   - Every drone over NATO airspace or proxy sabotage in Europe is a means of shaping the battlefield in Ukraine by exhausting allies while testing their unity and stretching their resources.
   - Thus, deterrence cannot remain siloed by geography or domain. A strike in Vilnius must have consequences in Donetsk. Infiltration in Berlin must translate into sanctions or arms deliveries that erode Russia's capacity to wage war.
2. **Deterrence must move from reaction to preemption.**
   - The alliance's defensive mechanisms like Eastern Sentry, the prospective "drone wall," and the Baltic-Nordic security belt improve detection, but deterrence is measured by the adversary's restraint, not by allies' visibility.
   - To change Moscow's calculus, allies must create predictable, escalating consequences that both establish red lines and tie every act of shadow war aggression to a tangible cost. A holistic EU-NATO hybrid escalation ladder could resemble the following:
     - **Tier 1: Single Incursion or Border Probe**
       - Deploy intel, surveillance, reconnaissance assets to affected regions
       - Increase EU customs screening of high-risk goods
       - Activate rapid NATO-EU hybrid threat information-sharing
     - **Tier 2: Repeated Incursions or Proxy Sabotage Attempts**
       - Increase preauthorized ammunition and air-defense packages to Ukraine
       - Expand export controls on dual-use electronics and drone components
       - Issue mandatory public attribution within 72 hours
     - **Tier 3: Confirmed Proxy Sabotage or Assassination Plot**
       - Accelerate the delivery of previously withheld weapons systems
       - Launch joint NATO-EU cyber pressure on Russian military logistics
       - Freeze assets of implicated facilitators using criminal (nonsanctions) tools

Photo: Olgierd L., 47, was arrested in Gdańsk and was to be transferred to the Lower Silesian branch of the Department for Organized Crime and Corruption in Wrocław. The arrest is tied to an ongoing investigation into potential links to acts of sabotage and subversion, allegedly inspired by Russian interests. Credit: ZUMA Press/Alamy Live News.

- **Tier 4: Multistate Infiltration Campaign**
  - Expand NATO air-policing rotations and deploy additional fighter detachments
  - Restrict correspondent banking access for enabler jurisdictions
  - Surge EU-wide inspections of reexported electronics and transit goods
- **Tier 5: Mass Incursion or High-Impact Hybrid Attack**
  - Permanently base additional air-defense units in affected states
  - Transfer interest from frozen Russian sovereign assets to Ukraine's defense fund
  - Launch coordinated operations targeting Russian intelligence networks in Europe

3. **The EU and NATO must harmonize their readiness capabilities and political thresholds for action.**
   - Fragmented decision-making and national caveats have become the soft underbelly of European deterrence. A cohesive, preagreed escalation ladder — codified across both institutions — would deprive Russia of the political space it exploits between them. Hybrid defense must no longer be treated as a matter of national discretion but as a collective security mandate.
   - To avoid duplication and close exploitable gaps, allies should formalize a division of labor where:
     - NATO leads on detection, defense, and military response
     - The EU leads on financial pressure, border controls, law enforcement, and export controls
   - NATO and the EU should fuse their intelligence, border, financial, and aviation monitoring capabilities into a combined early-warning mechanism focused on detecting indicators of Russian shadow-warfare activity. Key signals could include:
     - Shifts in Belarusian or Russian visa-issuance patterns
     - Spikes in charter flights from Middle Eastern hubs associated with migration manipulation
     - Online chatter or encrypted messaging spikes on platforms known for proxy recruitment
     - Coordinated drone launches or anomalous airspace activity near NATO borders
     - Launch-pattern clustering from Russian or Belarusian border districts, suggesting coordinated flight paths
     - Unusual cash movements through high-risk money transfer operators or crypto platforms
4. **Deterrence must reassert the political will to tolerate rhetorical and psychological escalation.**
   - Russia's nuclear threats and intimidation campaigns are not signs of strength, but reflexive attempts to deter Western resolve.
   - Restoring deterrence means reclaiming the initiative by neither seeking nor avoiding confrontation, but above all by imposing consequences.

If NATO and the EU can unite in these principles — clear red lines, guaranteed response, and political endurance — they can finally move from being observers of Russian aggression to architects of its containment. Deterrence will not be restored through vigilance alone, but through conviction.

War Beneath the Waves: Deterring Russian Sabotage of Undersea Infrastructure

MINNA ÅLANDER AND MATHIEU BOULÈGUE

Introduction

Critical underwater infrastructure has become ever-more critical, especially in the Baltic Sea region. Recent damage to data cables has reminded policymakers across NATO nations that the alliance is highly vulnerable to disruption by nefarious state actors.[32]

Critical underwater infrastructure (CUI) generally includes surface and underwater energy infrastructure (pipelines, power cables, wind farms, etc.); fiber optic data and communication cables; and fishing and shipping infrastructure. Of these, fiber optic cables are the most vulnerable. While more resilient, data cables are nevertheless vulnerable to physical damage, with more than 200 reported incidents each year.[33] The vast majority of damage is due to human error (anchoring and trawling activities by fishing vessels and commercial shipping), structural issues (obsolescence of the cables), or natural occurrences (seabed movements and abrasion, earthquakes, etc.).[34]

In recent years, however, the Baltic Sea area has become a testbed for targeted disruption of such infrastructure, particularly data cables. Past cases[35] show how sabotage takes place and illustrate Moscow's (and Beijing's) likely involvement. Given the technical challenges associated with forensic investigations of offshore infrastructure sabotage forensic investigations, attribution can be difficult. Although littoral states have seldom been able to officially attribute damage to subsea infrastructure in the Baltic Sea since Russia's full-scale invasion began in 2022, evidence in most cases points toward Russian involvement.

The nature of the Russian shadow fleet in the Baltic Sea is also well known and has been widely studied.[36] This case study examines its use for the sabotage of critical infrastructure, as well as the national and multilateral policy responses to the threat from countries in the Baltic Sea area.

Photo Opposite: A Turkish naval aviator and Turkish sailors conduct helicopter-submarine winch exercise during NATO exercise Dynamic Manta 24. Credit: NATO Flickr.

Part 1 – Cable Sabotage, Disruption, and Seabed warfare

Nefarious activities by state and nonstate actors account for a small percentage of cable disruption,[37] though bad actors have a strong incentive to interfere with CUI: Such operations, especially close to coastlines, are low-effort and low-cost — they do not require significant specialized knowledge or skills beyond simple anchor dragging — but can have a cascading impact in the civilian and military realms.[38]

In peacetime, seabed warfare allows nefarious actors to potentially disrupt the flow of an adversary's information, financial operations, and energy networks. In cases of military escalation, such activities can function as a tactical enabler for battlefield preparation in conjunction with other coordinated attacks against critical national infrastructure (CNI). Sabotage activities have clear military implications: They can complicate or disable military and diplomatic communication and ultimately impact military command and control (C2) structures.

Seabed Warfare

Seabed warfare has become part and parcel of Russia's low-intensity and sub-threshold warfare operations across the European theater. CUI disruption is also multi-domain by nature: beyond the seabed infrastructure itself, damage can also occur onshore against littoral landing stations, in cyberspace, and recently through the use of ships as platforms to launch aerial drones.

Seabed warfare and CUI disruption generally take the form of two different but self-reinforcing activities:

- **Intelligence gathering and seabed infrastructure mapping** in preparation for acts of sabotage. These operations can be carried out by dedicated military assets or by "shadow fleets" of dual-use and civilian commercial vessels.[39]
- **Physical destruction or tampering with CUI** in a coordinated action of sabotage. Perpetrators use various methods, from simple anchor dragging to more sophisticated use of dedicated uncrewed underwater vehicles or undersea explosives.[40]

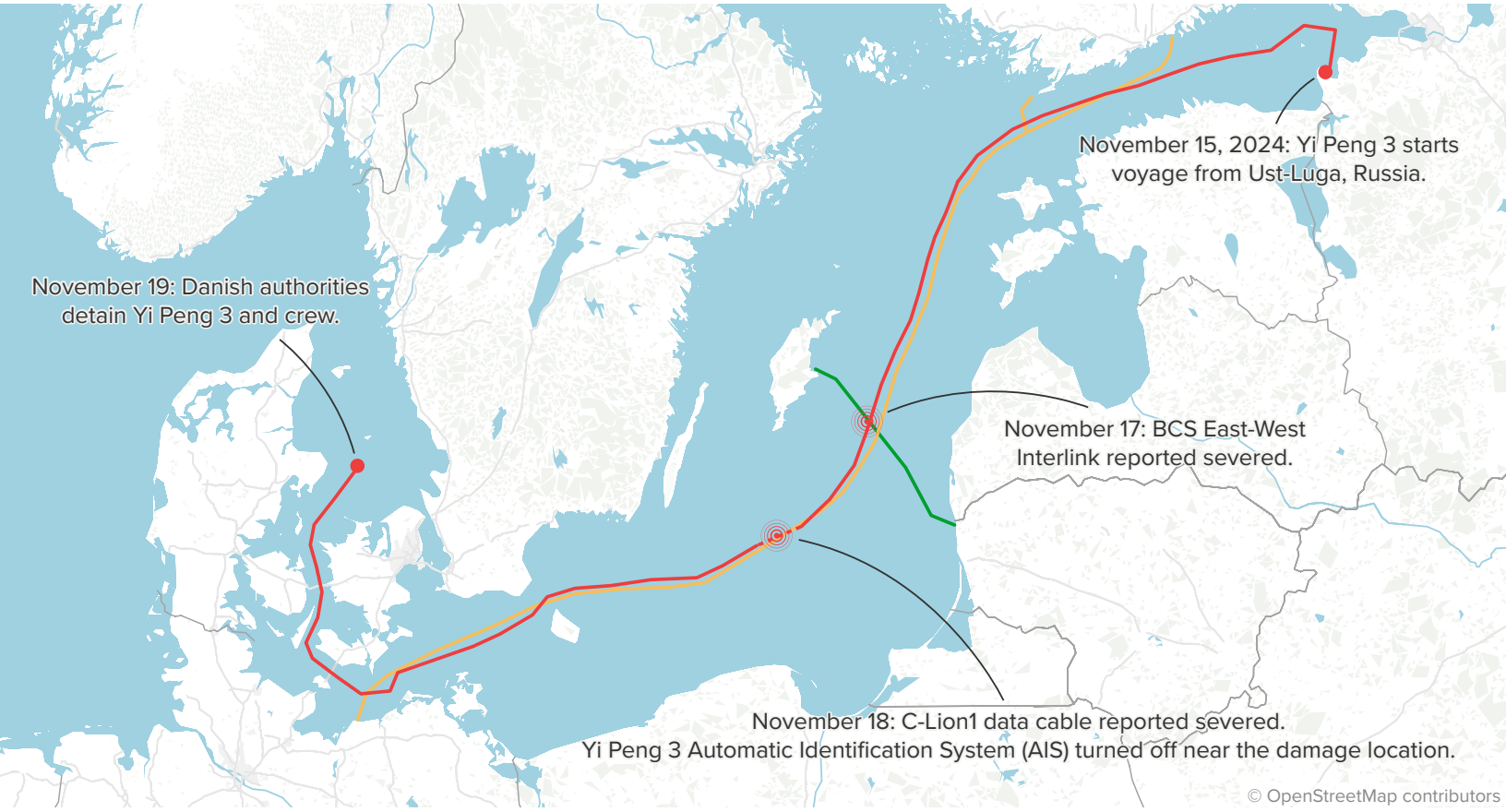
The situation is compounded by a paradox inherent to data cable placement and security. Near coastlines and in shallower waters, hostile states can carry out low-cost, low-tech sabotage using dual-use surface vessels with relative ease, while running a higher risk of detection and direct attribution. In contrast, operations that are less traceable and more difficult to attribute are conducted in deeper waters, where cables are less protected but far more challenging to access without specialized submersible assets.

Photo: A view shows the Chinese ship, the bulk carrier Yi Peng 3, mid-sea in the Kattegat, Denmark, November 20, 2024. Credit: Ritzau Scanpix/Mikkel Berg Pedersen via REUTERS

Cable sabotage is a long-standing component of Russia's gray-zone warfare, meaning operations that remain below the threshold of open warfare and allow for plausible deniability.[41] For Moscow, interfering with undersea cables serves as an asymmetric tool useful during escalation or in the early phases of conflict, enabling faster decision-making and potentially outpacing any responses.[42] Cable sabotage is an important aspect of Russia's informational and psychological preparation of the battlespace,[43] allowing it to probe Western and NATO reactions.

To support this strategy, Russia has invested time and effort in developing military structures and acquiring capabilities to conduct seabed warfare.[44] Among other structures, the Defense Ministry's main directorate of deep-sea research (GUGI) plays a central role in coordinating military activities around seabed warfare.[45] Its responsibilities encompass naval and seabed intelligence as well as managing specialized surface and subsurface assets conducting seabed operations.[46]

Yi Peng 3: Sabotage Voyage November 15-19, 2024



Source: Benjamin L. Schmitt, UNDERWATER MAYHEM Project - University of Pennsylvania, Department of Physics and Astronomy, Kleinman Center for Energy Policy, Perry World House (Penn Global). Map: Michael Newton/Center for European Policy Analysis.

For intelligence mapping, Moscow relies on a vast network of civilian and dual-use vessels. Using plausible deniability,[47] the odd fleet of fishing trawlers, cargo carriers, tankers, research vessels, and even private yachts is enabled to conduct intelligence gathering operations, conduct surface reconnaissance, and map the seabed. The practice is deep-rooted: Since Soviet times, Russia's Northern and Pacific fleets have overseen an auxiliary fleet of dual-use ships operating in far sea areas.[48] In particular, Russia has long operated a fleet of vessels whose publicly stated mission is scientific research, though many of these vessels have long been suspected of conducting clandestine maritime intelligence-gathering operations. A notable suspect among this fleet is the Yantar, which regularly loiters in European waters.[49]

Civilian vessels like these are equipped with inconspicuous monitoring devices, covert listening apparatus attached to the deck or hidden within fishing gear, and other instruments carrying out seabed sensing/mapping. Seafloor mapping is particularly valuable, as equipment aboard these vessels can produce 3D models of the seabed and gather environmental data like salinity and temperature (information that is crucial for submarine operations), as well as hydrographic measurements and information on water depths and undersea topography. Vessels can also track foreign surface and subsurface naval activity and deployments. Another form of intelligence operation is the use of drone overflights to map CUI and CNI onshore.[50]

The weaponization of civilian and dual-use vessels allows Moscow to discreetly conduct cable layout mapping in preparation for acts of sabotage. In the case of suspicious behavior or reported cable damage, the "civilian" nature of the vessels helps conceal their true purpose and gives cover for any disruptions of CUI as accidental. Overall, all surface vessels linked to Russia are technically able to conduct intelligence-gathering operations.

Russia's 'Shadow Fleet'

Since its full-scale invasion of Ukraine and the subsequent Western sanctions on Russian oil, Russia increasingly relies on the so-called "shadow fleet" for its global oil exports. This is a loosely connected network of vessels with obscure and frequently changing ownership structures and legally flexible flag states – referred to as "flags of convenience" due to the minimal requirements they impose on the vessels and their owners.[51]

Other internationally sanctioned countries such as Iran and Venezuela have also used the shadow fleet (often also called "dark fleet") to circumvent sanctions.[52] Their various and often changing flags are meant to complicate legal attribution.

Shadow fleet vessels often obfuscate their position, either by sailing with their Automatic Identification System (AIS) and Vessel Monitoring System (VMS) transponders switched off or by spoofing their location with different geolocation data.[53] The resulting fleet of "ghost ships" makes their detection complex and increases the potential for accidents and incidents at sea.[54] Crews on these ships are often expected to host military surveillance equipment, with collected data transferred to dedicated intelligence structures once the vessel returns to port. In some cases, military operatives may be embedded directly within the civilian crew to manage the devices.

The growing use of the shadow fleet also strains coast guard and naval resources by forcing more search-and-rescue operations and surveillance operations. For instance, the reconnaissance and surveillance vessels Yantar and Yuri Ivanov routinely loiter inside Britain's exclusive economic zone (EEZ), forcing the Royal Navy to dispatch military assets to shadow it.[55]

The Issue with Attribution

A key issue in attribution is the ability to gather sufficiently irrefutable technical evidence with existing technology, from remote sensing to domain awareness capabilities. In other words, limiting adversarial activities against critical underwater infrastructure entails having more eyes and ears, across from the seabed to outer space.

Attribution includes three crucial elements:

- **Technical attribution:** the ability to gather enough irrefutable technical evidence through the use of technology (domain awareness, sensing capabilities, etc.)
- **Legal attribution:** a legal framework that allows states and cable operators alike to prosecute
- **Political attribution:** the national and multilateral willingness to call out the responsible party based on the evidence, while managing the risk of escalation

The stars rarely align to make attribution irrefutable. Cable disruption always holds a dose of technical uncertainty and is often blocked by tepid political responses. NATO countries also have diverse approaches to attribution. Western European nations tend to assume innocence until proven guilty, while Eastern European and Nordic members take a more direct approach, assuming guilt until proven otherwise. This case study seeks to bridge the knowledge gap and provide policymakers with policy pathways to prevent and deter disruptions in the Baltic Sea and beyond.

Part 2 – Technical Attribution: Technology, Domain Awareness, and Deterrence by Presence for CUI Protection

Technical investigations of suspicious behavior and damage to CUI are generally the first step to attribution. Investigators must trace the breadcrumbs of evidence pointing toward a responsible party. Thorough investigation and confidence in attribution are even more crucial, as they help maintain confidence in national authorities. Technical attribution raises policy questions about the role and place of autonomous systems and uncrewed platforms to monitor CUI networks.

NATO and Multinational Responses

In the wake of the 2022 Nord Stream pipeline damage and the 2023 NewNew Polar Bear/Balticconnector incidents, NATO began placing CUI protection at the center of its activities in the Baltic Sea area. The alliance created a Critical Undersea Infrastructure Coordination Cell (CUICC) in February 2023 as part of NATO HQ to help "map vulnerabilities and coordinate efforts among NATO allies, partners, and the private sector."[56] The cell marked an important first step toward increased information sharing and streamlined political responses.

During the Vilnius summit in 2023, NATO's Maritime Command (MARCOM) launched a NATO Maritime Center for the Security of Critical Undersea Infrastructure

(MCSCUI),[57] which acts as an operational hub to coordinate intelligence sharing, threat detection, and incident response. [58]

The alliance also set up a new tactical maritime headquarters, the Commander Task Force Baltic, in October 2024. Placed under MARCOM, it coordinates naval activities and efforts to grasp all maritime activity and potential threats, or maritime-domain awareness, among other tasks.[59]

In addition, NATO established the Digital Ocean Initiative under the Defense Investment Division in October 2023 and the Critical Undersea Infrastructure Network in May 2024[60] to promote technological innovation and interoperability.[61]

By the time a Hong Kong-registered ship damaged the Balticconnector gas pipeline between Finland and Estonia in October 2023, NATO had already increased surveillance in the Baltic Sea area.[62] But it was the damage to the Estlink 2 power cable and the Eagle S case, also between Finland and Estonia, in December 2024 that supercharged efforts by NATO and its individual members to increase domain awareness, launching several operations and task forces in the following months.

Baltic Sentry

The largest NATO response so far has been the Baltic Sentry operation, initiated in January 2025 to increase naval and aerial patrols in the region to protect CUI through monitoring, deterrence, and rapid response.[63] Baltic Sentry strengthens the logic of deterrence by presence in the Baltic Sea through increased patrols and technological enablers, allowing for faster threat detection. Russian operators were made aware that they are being observed.

Baltic Sentry emphasizes integrated presence by rapidly deploying pre-existing naval groups (for instance, the Standing NATO Maritime Group 1 - SNMG1 and the Standing NATO Mine Counter Measures Group 1 – SNMCMG1), maritime patrol aircrafts, as well as aerial and underwater drones alongside remote sensing capabilities (maritime and space-based). Baltic Sentry is managed through NATO Maritime Command (MARCOM) and the new Centre for Critical Undersea Infrastructure (*see below*), while fully integrating the two new Allies, Finland and Sweden.

Task Force X

NATO has also been experimenting with domain awareness technology with the creation of the Task Force X (TFX) in early 2025. TFX aims to conduct fast experimentation and rapid deployment of an integrated suite of uncrewed maritime

Photo: The Royal Netherlands Navy survey ship HNLMS Luymes, flagship of Standing NATO Mine Countermeasures Group One, pulls away from its slip in Malmö, Sweden, to take part in Baltic Sentry, a maritime patrol activity intended to deter attacks on Allied critical underwater infrastructure. Credit: NATO Flickr.

systems, data fusion, and AI-enabled systems and sensors.[64] TFX focuses on the surveillance and safeguard of CUI through early threat detection with the help of the most advanced technologies.[65]

TFX is a 'sensor first' operation that puts autonomous and uncrewed intelligence, surveillance, and reconnaissance (ISR) capabilities at its center. Remote presence is crucial to filling gaps in conventional surveillance.[66] Instead of a top down, heavy structure, TFX has a minimal human footprint and approaches domain awareness by "machining the front" instead of "manning" it. In this sense, TFX enables NATO's preemptive denial by tracking the shadow fleets and vessels sailing with their AIS/VMS transponders off in order to preempt CUI disruption.

The task force addresses the need for round-the-clock intelligence, surveillance, and reconnaissance activity, which is possible only through autonomy and uncrewed systems. The next step for TFX will be to create an interoperable network where

allies can "plug and play" their national capabilities individually across the Baltic Sea area and potentially beyond.

Joint Expeditionary Force and Nordic Warden

The United Kingdom-led Joint Expeditionary Force (JEF) has extended its core mission to surveillance and protection of CUI through dedicated investments for ISR and rapid incident responses.[67] One week after the Eagle S/Estlink 2 cable-cutting incident, the JEF launched Nordic Warden in January 2024, a rapid-response effort across the North Atlantic, Baltic, and Nordic Area of Responsibility (AoR). Nordic Warden also enhances domain awareness through data fusion and AI-enabled systems for vessel tracking and activity monitoring.[68]

As an operational tripwire, JEF should continue tailoring its procurement choices towards the mission imperative of rapid response against CUI disruption. It should also integrate itself more deliberately into the newly created NATO structures responsible for CUI management, notably the Maritime Centre for the Security of Critical Undersea Infrastructure. [69]

Toward Seabed to Space Awareness and 'Transparent Oceans'

These and other NATO and national responses point to a new approach for deterring nefarious activities: deterrence by presence. With the activation of Baltic Sentry and other operations in the Baltic Sea area, noncompliant vessels sailing with transponders turned off, unseaworthy ships sailing with no flags and/or displaying unusual behavior will be pressed hard for identification and proof of ownership. Denmark, for instance, has ramped up inspections of vessels carrying Russian oil through the Danish straits.[70] Denmark has also increased inspections of "old and worthless" vessels navigating critical chokepoints of the Baltic Sea.[71]

Greater maritime domain awareness (MDA) through modern technology also allows for faster detection and reconnaissance of shadow fleet vessels. Greater presence at sea also allows NATO countries to board and inspect conspicuous vessels much more quickly than before.

Maritime tracking and shadowing of suspicious assets is also key to deterrence, as in the Royal Navy's constant deployments against Russian assets violating the UK's exclusive economic zone.[72] Constant naval and aerial deployments increase the operational tempo for the Royal Navy but act as a deterrent by presence and patrol.

Moving forward, two concepts help guide NATO toward a comprehensive view of the maritime and aerial environments for the protection of subsea infrastructure:

- **Seabed-to-space situational awareness (S3A):** [73] as part of NATO's 2023 Digital Ocean Initiative. This includes working with the Defense Innovation Accelerator for the North Atlantic (DIANA) network.
- **'Transparent Oceans':**[74] this refers to the effort to make oceans "transparent" by 2050, through the proliferation of uncrewed underwater vehicles, big-data analysis and machine learning, and aerial reconnaissance through drones and space-based sensing.

The development and acquisition of seabed sensing, monitoring technology and detection tools that span multiple domains, from space to the seabed, will boost efforts to track and deter undersea-infrastructure disruptions. The technology needed for complete situational awareness is maturing, but it must be scaled up and integrated within NATO structures across the Baltic Sea theater and beyond.

These technologies pertain to:

- **Layered sensing and seabed monitoring**. Advancements in fixed sonar and acoustic sensing technology must go hand in hand with more advanced capabilities, such as hydrophones and distributed acoustic sensing. This enables early warning and threat detection in the case of anchor impact, dragging, and direct cutting. Industry players, especially from Nordic countries, are also integrating new fiber sensing technologies.[75]
- A breakthrough in layered sensing took place in July 2025, when the NATO Research Vessel (NRV) Alliance detected the underwater acoustic signature of a ship's anchor hitting the seabed, which data infusion ensured by the dedicated ship tracking tool Mainsail.[76]
- **Uncrewed underwater vehicles (UUVs)**: The use of UUVs and semi-autonomous submersibles is key to remote sensing and inspection. Task Force X has become the ideal place to experiment with such systems and integrate them into commercial and military systems.[77]
- **AI-enabled data fusion and intelligence gathering for increased domain awareness.** Progress in AI-enabled technology, big data analytics, and quantum sensing paves the way for better data fusion, together with advances in satellite reconnaissance technology. Another pathway for data cables is to use sensors directly in the fiber optic.[78]
- **Special operations:** Protection of underwater infrastructure depends on the use of special operations forces (SOF), divers, and mine countermeasures units trained to foil sabotage and clandestine operations. Recent NATO exercises have been testing such a range of missions.[79]
- **Rapid response and repair capabilities:** When infrastructure is damaged, repair capabilities must be streamlined between private operators and governments. Infrastructure resilience heavily depends on the maintenance of repair ship fleets, for instance the US Cable Security Fleet implemented in 2021.[80] Repair times vary greatly depending on the type of infrastructure and geophysical constraints on the seabed.[81]

Photo: A sign points to an undersea power cable in Scarden, 09 03 2026 Scarden Ireland. Credit: Florian Gaertner/IMAGO/ via Reuters Connect

Crucially, dialogue has improved between public authorities and private companies. Despite their responsibility to inform authorities of disruptions, private companies have often lacked the capability to be present on the seabed.

When and what to report is not straightforward, as most companies lack the means to categorize the cause of damage (natural or sabotage). Government authorities can help determine the cause with their more advanced surveillance capabilities. Information sharing and cooperation between public authorities and private companies is therefore of mutual interest and benefit.

The extent of such public-private communication varies greatly across countries of the Baltic Sea region. For example, Lithuania established a national security standard for private companies after 2014 to harmonize preparedness measures. In 2022, private companies approached the government to better understand threats to critical infrastructure. The explosion of the Nord Stream gas pipelines in September 2022 led to another push for private companies to seek consultations with the Lithuanian government on methods of undersea monitoring.

In Finland, information sharing and consultation occurs via informal networks and was not legally required until recently. A 2025 law[82] mandates that private companies operating critical national infrastructure "assess risks, develop resilience plans, and notify authorities of incidents to strengthen infrastructure resilience against disruptive events."

In Sweden, on the other hand, strict laws on information sharing and regulations vary even among authorities, which often hampers consultation. To overcome these issues, Sweden is now making public-private interaction and industry reporting mandatory by law.[83]

In the Baltic states, Finland, Sweden, and Denmark, critical infrastructure companies are also subject to a European Union requirement ensuring entities providing essential services can maintain uninterrupted operations despite natural or man-made threats. Critical entities must be officially identified by July 17, 2026, with their owners then having nine months to conduct their own risk assessments and 10 months to fully comply with all resilience requirements.

Of the Baltic Sea countries, only Estonia has transposed the directive to national law within the timeline set by the EU in 2024. By 2025, most of these countries had adopted the directive's requirements in national regulation, but technical parameters of implementation were still being set.[84] How extensively the resulting regulations specifically deal with ways to prevent or deter acts of sabotage of critical services is likely to differ from country to country.

Part 3 – Legal Attribution and 'Deterrence by Accountability'

Across NATO and European nations, not all states have experienced a similar 'wakeup call' to undersea infrastructure sabotage as countries around the Baltic Sea. If there are now solid baselines of an international framework for legally assigning blame, it has not yet been transferred into national policies.

An Insufficient International Legal Framework

Several international conventions touch upon the protection of CUI, from the 1958 Geneva Conventions of the Continental Shelf and High Seas, as well as the 1884 International Convention for the Protection of Submarine Cables.

But the primary body of international law on the issue remains the 1982 United Nations Convention on the Law of the Sea (UNCLOS), and more specifically Articles 113 to 115. Article 113, which addresses the "breaking or damaging of submarine cables or pipelines," requires states to criminalize any harm caused to CUI by vessels flying a national flag.

Under UNCLOS, legal safeguards for undersea cables vary according to their location, whether inside territorial waters (up to 12 nautical miles), in contiguous zones (up to 24 nautical miles), within an EEZ (up to 200 nautical miles), or in international waters and the high seas beyond national jurisdictions.[85]

But the Law of the Sea offers little guidance for EEZs and high seas, where states lack both the authority and freedom of action to adequately protect cables. In these areas, it does not grant sufficient jurisdiction to secure seabed cables or stop nefarious activities by suspect vessels. In this, it does not grant states the authority to enforce these rules beyond their own jurisdiction, nor does it allow them to board or detain suspect ships operating in international waters.[86]

The weakness of the current legal framework is exacerbated by the absence of clear rules distinguishing between peacetime and wartime. Existing wartime provisions are outdated and fail to clarify whether damaging a cable constitutes an armed attack under international law or how cables should be treated during armed conflicts.[87] UNCLOS and the 1884 Cable Convention explicitly exclude armed conflict, while NATO's guide to international law on cyber operations, the Tallinn Manual 2.0, suggests that undersea cable systems might be considered legitimate military targets.[88]

Legal attribution is further complicated by the use of foreign flags and layered ownership structures to mask ships' true operators. This challenge is intensified by the multi-domain character of cable sabotage, which can include cyberattacks on onshore landing stations.[89]

The International Cable Protection Committee has produced a guide for governments on best practices for protecting and promoting resilience of submarine telecommunications cables. The ICPC, the UN, and the International Telecommunication Union also created an International Advisory Body for Submarine Cable Resilience in 2024[90] to improve resilience and best practices across industrial players and states.

Further guidelines such as the San Remo Manual on International Law Applicable to Armed Conflicts at Sea[91] and the Tallinn Manual 2.0 on cyber operations give states additional guidance on CUI protection.

Still, as risks to undersea cables expand, international legal protections remain fragmented and outdated. International law restrains national law enforcement's ability to criminally investigate suspicious vessels, posing a major challenge to attribution. This is exemplified by the case of the Yi Peng 3, a Chinese carrier suspected of cutting two undersea cables in the Baltic Sea in 2024. The vessel was released after a brief detention by a NATO member state. It is generally up to each

country to establish or strengthen its own legal frameworks, but that remains an insufficient measure, as the vessels rarely come into littoral states' national waters.

Toward National Enforcement and Accountability

In response to the inherent limitations of customary international law, Baltic Sea countries have begun reinforcing and/or developing stronger national legal frameworks to both attribute damage and seek reparation for damage done.

At the 2023 UN General Assembly, Resolution 78/69 urged states to improve CUI security and implement legal obligations provided by UNCLOS (under Articles 113 to 115), rendering disruption a punishable offense if done 'willfully or through culpable negligence'.[92] The provision empowered national jurisdictions to move from tedious legal attribution to seeking penalty enforcement and looking specifically for responsibility and accountability for damage done.[93]

A groundbreaking prosecution attempt took place in 2025, when the Prosecutor General of Finland opened a court case against key officers of the Eagle S, part of Russia's shadow fleet, after its anchor damaged power and data cables in the Baltic Sea. While being investigated for "aggravated sabotage and aggravated interference with telecommunications",[94] the court ruled that the disruption was not severe enough to justify criminal charges and simply identified the Eagle S as the technical cause of the disruption.

The Finnish court ultimately dismissed the case on the ground that the state lacked jurisdiction in international waters. The crux of the matter was that intentionality was impossible to prove. As a result, the court ruled according to maritime laws on international seafaring accidents.[95] The charges against the captain and two officers were dropped, leaving Finland responsible for their legal expenses.

The verdict highlights the 'resilience dilemma': countries' efforts to protect and harden their undersea infrastructure, and to build in redundancy, can make it harder to make a case against bad actors.[96]

The threshold for follow-on kinetic response after undersea sabotage is extremely high. It would be imaginable only if the technical and legal evidence irrefutably linked the damage to the death of individuals or the destruction of other infrastructure. More resilience leads to fewer disruptions, pushing the threshold for stronger responses.

The Eagle S precedent failed to establish a case for countries to move from attribution to accountability. Legal 'deterrence by accountability' or 'deterrence by resilience' does not work, as the attacks are designed to evade the jurisdiction of

countries adhering to the rule of law. On the other hand, resilience is a defensive strategy, but it does not deter Russia from exploring new attack vectors. As Elisabeth Braw cogently argued, the failure to convict the Russian crew and to attribute the case creates a dangerous precedent for the Kremlin to exploit, as Moscow will feel vindicated in continuing its seabed warfare activities.[97]

After the Eagle S incident in 2024, Finland held a meeting of NATO member states from the Baltic Sea in 2025.[98] Among other pledges, the group (comprised of the Baltic States, Finland, Sweden, Denmark, Poland, and Germany) announced its intention to "identify further measures in accordance with international law of the sea, including the freedom of navigation, to prevent and effectively respond to willful damage to critical undersea infrastructure or irresponsible behavior."

One year later, in January 2026, a broader group of Baltic and North Sea countries released a statement clearly identifying Russia as the source of new maritime hazards and calling for the recognition of Global Navigation Satellite System (GNSS) interference and AIS manipulation as threats to maritime safety and security.[99] The statement also introduced 13 legal measures to address the use of the shadow fleet, based on different aspects of international law "whether customary international law or as contracting parties to international conventions." These include the use of so-called flags of convenience, insufficient insurance and vessel condition, increased flag state responsibility, ship identification and tracking, and reporting and carrying out ship-to-ship transfers.

The statement does not promise the use of specific measures in cases of a violation, but it provides a legal basis for future interceptions of shadow fleet vessels and juridical proceedings against their crews.

Part 4 – Political responses: Shedding Light on the 'Shadow Fleet' and Deterrence by Resilience

Recent cases of CUI disruption in the Baltic Sea area have prompted swift responses from national governments, NATO, and private companies. Robust multilateral engagement and support for the integrity of CUI pave the way to better policy response and political attribution. Ultimately, the goal is to create a deterrence framework "denying deniability" for nefarious acts.[100]

Public and Private Responses to CUI Disruption

European Union Responses

The EU quickly adapted to the threat presented by Russia's intensified sub-threshold warfare activities. In 2023, the Directive on the Resilience of Critical Entities mandated that member states "develop a national strategy and carry out regular risk

Photo: Rohuneeme. Estonian authorities detained an oil tanker which forms part of Russia's «shadow fleet» and which had been sailing through Estonian waters in the Gulf of Finland. The vessel Kiwala is not permitted to sail on the open seas. Credit: Photo Eero Vabamägi, Postimees via Reuters

assessments to identify entities that are considered critical or vital for society and the economy."[101] Meanwhile, the European Commission's 2024 Recommendation on the Security and Resilience of Submarine Cable Infrastructures gives members incentives to improve coordination, governance, and protection of CNI.[102] NATO and the EU also launched a NATO-EU Task Force on Resilience of Critical Infrastructure in January 2023 to enhance coordination, preparedness, and overall resilience against CNI disruption.[103]

In 2024, the commission joined with the United States and 16 other countries in a statement that encouraged closer public-private cooperation on "responsible undersea cable deployment, maintenance, and repair according to established international industry norms."[104]

The following year, the Commission also released a Joint Communication detailing an "Action Plan on Cable Security" to protect undersea data cables by "fostering 'cable diplomacy' with global partners."[105] In October 2025, an informal expert group tasked by the EU followed up with a report on "Security and Resilience of

EU Submarine Cable Infrastructures," that included guidance for mapping and stress tests, as well as a recommendation for the EU to establish a cable security toolbox.[106] In early 2026, The EU implemented the Cable Security Toolbox of risk-mitigating measures and a list of Cable Projects of European Interest (CPEIs) in early 2026 and allocated €347 million to strategic submarine cable projects, including a €20 million call to enhance Europe's repair capacities.[107]

National and Multinational Initiatives

At the national level, countries across the Baltic Sea area have taken the lead in setting up individual and joint political responses to the threat against CUI. Regional states have all increased their presence at sea and in the air and strengthened their legal frameworks and cooperation with each other. Baltic Sea countries have also understood the need for streamlined regional cooperation, information sharing, and incident response.[108] For instance, as an immediate response to Russia's deliberate violation of Polish airspace with drones in September 2025, Sweden and Poland launched the Gotland Sentry short-notice military exercise for the Baltic Sea area.[109]

This regional 'coalition of the willing' approach holds promise as cooperation in sensitive areas like intelligence data sharing is partially inhibited by the lack of trust among political actors. Hungary's defense of Russia's interests in the EU and, to a lesser extent, past leaks of EU intelligence discussions to Russia, are the primary reason why more extensive intelligence sharing may not be considered by decision-makers across the EU. But within a Baltic-Nordic framework (along with the cooperation of Poland, Germany, and North Sea partners), enhanced data fusion could become the blueprint for strengthened protection of civilian and military infrastructure such as offshore windfarms, not only undersea assets.

CUI protection is also becoming a priority in other regional theaters. In 2024, Norway and Germany proposed the creation of CUI Hubs for the European Arctic and for the Baltic Sea.[81] Furthermore, Belgium, Denmark, Germany, the Netherlands, Norway, and the United Kingdom signed a North Sea Agreement in 2024, increasing information sharing linked to CUI protection.[110]

On the national level, CUI protection and threat responses usually fall to law enforcement – typically coast guards and ministries of interior or justice – with militaries and defense ministries in a supporting role, and ministries of foreign affairs responsible for facilitating international coordination. Finland and Estonia are exceptions: the Estonian navy is tasked with law enforcement, and the Finnish coast guard is a law enforcement authority with military capabilities.

Intelligence and security services play an important role in CUI threat monitoring for all the Baltic Sea countries and assist law enforcement authorities with collecting

evidence. Some foreign ministries in the region have also established the position of a special representative or coordinator for hybrid threats, reflecting heightened threat perception and a high priority on sub-threshold attacks.

Industry and Private Sector Endeavors

Private companies, from fiber optic cable hyperscalers to multinational energy consortia, own most underwater infrastructure and are generally responsible for laying, operating, maintaining, and repairing it. The private sector has tremendous responsibility for monitoring its assets and reporting incidents, especially when intentional damage is suspected. While private companies have less capability than governments to be physically present on the seabed, they nevertheless have the responsibility to be aware of the state of their infrastructure, in line with incident reporting.

For the past few years, companies have built closer ties with public authorities.[111] Major energy firms have embedded a liaison officer from relevant state institutions and/or Ministries to ensure optimal incident reporting, information sharing, and overall public-private collaboration for crisis response. Private operators have also been engaged in discussions with NATO MARCOM and EU structures for the same reason.

National and multilateral strategies on the protection, defense, and resilience of CUI are rapidly developing, but much remains to be done. Indeed, national agencies and multilateral organizations are still going through a steep learning curve on best practices, responses, and coordination mechanisms.

Toward an Integrated Deterrence Framework Against CUI Disruption

As an integral part of sub-threshold destabilization activities, Russian seabed warfare and the disruption of CUI will continue to intensify in the Baltic Sea area. As outlined in this case study, a better deterrence framework is necessary to properly attribute the disruption of CUI moving forward.

From a political perspective, direct and unequivocal attribution will allow Baltic Sea area countries and NATO to "deny deniability."[112] States must be empowered to use all available political, legal, and technical tools to shed light on the shadows, calling out and attributing disruption to bad actors. But naming and shaming alone does not deter Russia, as the Kremlin seems impervious to reputational costs.

From a military perspective, the protection and defense of CUI must become an integral part of NATO planning against gray-zone activities to protect lines of communication in the Baltic Sea and to ensure unhampered access to a potentially contested operational environment. Cooperation among various levels – national,

Photo: A Royal Danish Navy crew member on board the HDMS Triton looks through binoculars. Credit: NATO Flickr.

regional, or small coalitions – or between institutions such as NATO and the EU must be further improved to predetermine jurisdiction questions and enable faster responses.

Through collective action and response, individual countries will feel less self-deterred against Russia's propensity to use plausible deniability and to escalate. This is particularly important for the small Baltic nations that rely on multinational cooperation for their security, such as the Baltic Air Policing that NATO allies provide, and have limited national capacity to keep up with the Russian "whack-a-mole" strategy designed to overwhelm authorities. Escalation control is also key to managing the potential for miscalculation provoked by acts of disruption and sabotage. While resilience is not a deterrent, it is an essential starting point for an effective defense against accelerating hybrid attacks.

A key element of defending against and deterring hybrid attacks will be deciding whether to recognize CUI as a full-fledged operational domain of war.[113] To do

so would allow NATO and individual nations to integrate CUI protection into military doctrine and develop more effective deterrence strategies. Innovation is required, as Poland and Estonia's recent invocations of NATO's consultative Article 4 (citing threats to their territorial integrity) only exposed disunity. Invoking Article 5 is also unrealistic, as sub-threshold warfare is specifically designed to stay below that threshold.

Conclusion

The case study established that CUI disruptions lead to various forms of attribution.

- **Detection leads to technical attribution** through multidomain monitoring, remote sensing, early warning systems, and overall use of modern technology. This situation brings a form of deterrence by presence as a form of deterrence by denial.
- **Evidence leads to legal attribution** by streamlining legal frameworks and national jurisdiction to prosecute responsible parties. This evolution leads to 'deterrence by accountability' as a form of deterrence by punishment.
- **Impact leads to political willingness to attribute and counterattack** through multilateral cooperation, cohesion, solidarity and ultimately deterrence by punishment in form of united responses and contributions from multiple NATO allies, regardless of the geographical location of the attack.

Ongoing endeavors, from a military, legal, and technological point of view are all going in the right direction, whether nationally or multilaterally. Yet the deterrence of seabed and maritime warfare must become a strategic defense priority for Baltic Sea area countries and NATO.

Deterrence by presence will allow Baltic Sea countries to move from technical attribution towards damage preemption. Then, if CUI disruption occurs, states must go from legal attribution to legal responsibility/accountability for the damage done. In both cases, these developments will ensure better political attribution and ultimately deterrence by punishment against Russia's sub-threshold warfare activities on the seabed and above water.

Policy recommendations

Technical attribution and technological responses

- **Broaden the depth and scope of operations to protect underwater infrastructure during NATO and multinational military exercises.** Rehearsing MDA activities in various domains and counter-sabotage operations is key to operational readiness. More operational planning and exercises, such as the

2023 Dynamic Messenger[114], which featured CUI protection missions, should regularly take place. Meanwhile, NATO must systemically communicate around such exercises and demonstrate readiness.

- **Increase the availability of open-source and commercial geospatial imagery data**. Commercial space actors possess a multitude of unclassified satellite imagery data that can support European law enforcement, coast guard, and naval investigative teams, allowing for this data to be integrated into investigations and then rapidly released to the public.
- **Integrate technology seamlessly with a "sensor first" approach**. Like any other maritime area, the Baltic Sea theater is diverse and vast, with no 'one size fits all' approach to technology. Yet NATO and its members should consider harmonizing their multi-domain awareness efforts to ensure seamless integration of assets, technology, and data management.
- **Ensure smart procurement**. Continued investments and procurement can ultimately achieve a form of intelligence and capacity 'overkill' against nefarious activities by using remote sensing, early warning, and incident response technology.
- **Find the balance between direct human presence and indirect, remote presence** through uncrewed systems, autonomous platforms, and remote sensing capabilities.[115] This will drive future capability requirements across the range of missions necessary to deter CUI disruption.
- **Embed data fusion in national and EU regulation for protection and resilience of civilian critical infrastructure**, where, at the moment, only data sharing is mandated. This would require a much broader political mandate for responsible national and EU agencies to share data for real-time processing with their EU and NATO counterparts. However, this would also enable more up-to-date protection of critical infrastructure and deterrence of malign actors.

Legal attribution

- **Amend the Law of the Sea.** International discussions should focus on potentially amending UNCLOS to clarify the 'rules of the road' on cable disruption during peacetime and wartime.[116]
- **Strengthen national jurisdiction to foster legal deterrence.** National legal frameworks across Baltic Sea countries must evolve to continue 'reflecting the criticality of the infrastructure.'[117] States must also consider strengthening criminal jurisdiction to increase penalties against CUI disruption, create a more stringent inspection regime, identify vessel ownership, and overall raise the cost of nefarious activities.
- **Criminalize noncompliance.** International and national legal frameworks must adapt to ensure criminal prosecution when vessels sail with their

AIS/VMS transponders switched off. Similarly, there should be more legal emphasis on criminalizing suspicious and unusual patterns of behavior by surface vessels (and especially commercial and fishing boats). Reporting, investigating, and prosecuting suspicious activity before any damage is done will help strengthen legal deterrence.

- **Ensure proper insurance disclosure.** Illegal vessels should not be able to pass through the shadows because of leniency. Similar to compliance with International Maritime Organization (IMO) regulations and AIS/VMS tracking, national authorities should request mandatory insurance disclosure at port and when inspecting any vessel sailing the Baltic Sea. Enforcement mechanisms must also be created to heavily sanction violations from a financial perspective, but also through diplomatic retribution. It should be costly to be non-compliant.[118] Such controls, however, must walk a thin line to avoid disrupting innocent passage under UNCLOS.
- **Harmonize regulatory and legal provisions between countries**. At the EU and NATO levels, member states must strengthen regulatory harmonization regarding CUI legal frameworks. Previous research identified that NATO could also work more closely with the ICPC to increase standards for cable security.[119] The EU could, for example, enable intervention by national authorities in EEZs in cases of suspected criminal activity by sharpening EU regulation on threats to critical infrastructure. Such legislation could also enable swifter identification of vessels suspected of functioning as drone launch pads.
- **Learn from other legal frameworks.** Future legal discussions can draw valuable insights from the legal and normative frameworks already developed regarding cyberwarfare and space, for instance, responsible state behavior. The legal regime regulating cyberspace should also include the protection of CUI, as they can – and often are – also be targeted by cyberattacks.

Political responses

- **Adapt NATO's Article 4.** The Alliance should not hesitate to invoke an Article 4 collective consultation in the event of offshore (and onshore) infrastructure sabotage and where attribution is possible.[120] While not resulting in an Article 5 collective military response, the aim is to increase operational support for counter-sabotage operations as well as unlock resources for CUI protection initiatives and endeavors across NATO structures. The recent activation of Baltic Sentry in response to Russian sub-threshold warfare activities is an example to follow to quickly set up monitoring capacity and to deter future incidents.
- **Deepen information sharing between key stakeholders and organizations.** Existing information-sharing structures and organizations should systematically establish institutional linkages to enhance intelligence and information sharing at the multinational and multilateral levels, whether at

the EU or NATO levels.[121] Within the EU, data fusion should be encouraged for intelligence and situational awareness.[122]

- **Streamline institutional cooperation.** Information sharing and cooperation can always be improved, especially civilian-military relations between NATO and EU structures. This is paramount for achieving optimal domain awareness in the Baltic Sea area. Ultimately, cooperation should lead to the creation of collective frameworks and standards for regulations, incident response, and repair capacity.[123]
- **Unify multilateral incident reporting and response schemes.** When an incident happens in the Baltic Sea, private companies and the public sphere already have many reporting channels (national, multinational, minilateral/regional, EU, NATO, etc.). Yet a multitude of reporting mechanisms and the number of stakeholders involved tend to duplicate efforts, fragment information sharing, and ultimately dilute the speed and effectiveness of response. To avoid these issues, a single, centralized, multilateral point of entry should be created to unify incident reporting and response.[124] Determining the appropriate format and the lead agency, however, might prove complicated and would require reaching a political agreement between EU and NATO member states.
- **Build strong and systematic public-private ties.** It is the public sector that responds to disruptions against privately-owned CUI. Deeper cooperation between the private CUI industry and governments and multilateral fora is therefore the only way to ensure full domain awareness, threat identification, incident reporting, and comprehensive response.
- It is also important to keep in mind that private sector technology and response often outpace public endeavors and legal adaptations.[125] Conversely, there should be greater public oversight about corporate responsibility in the use of technology of foreign companies whose governments are known to disrupt CUI – namely China and Russia.
- **Ask for transparency and accountability from the fishing industry.** A large part of human-made, accidental damage against CUI (and particularly data cables) stems from fishing vessels sailing with transponders off for competitive intelligence reasons. Addressing this issue would allow the private industry and the public sector to focus solely on the remaining cases of accidents and intentional, nefarious attacks. The way forward is to foster cross-industry discussions with fishing industry representatives, CUI operators, and public institutions at the EU level.

Photo: A German Navy sailor aboard FGS Homburg Standing NATO Mine Counter Measure Group 1 (SNMG1) while leaving Bergen to participate in Trident Juncture exercise. Credit: WO Fran C.Valverde/NATO Flickr.

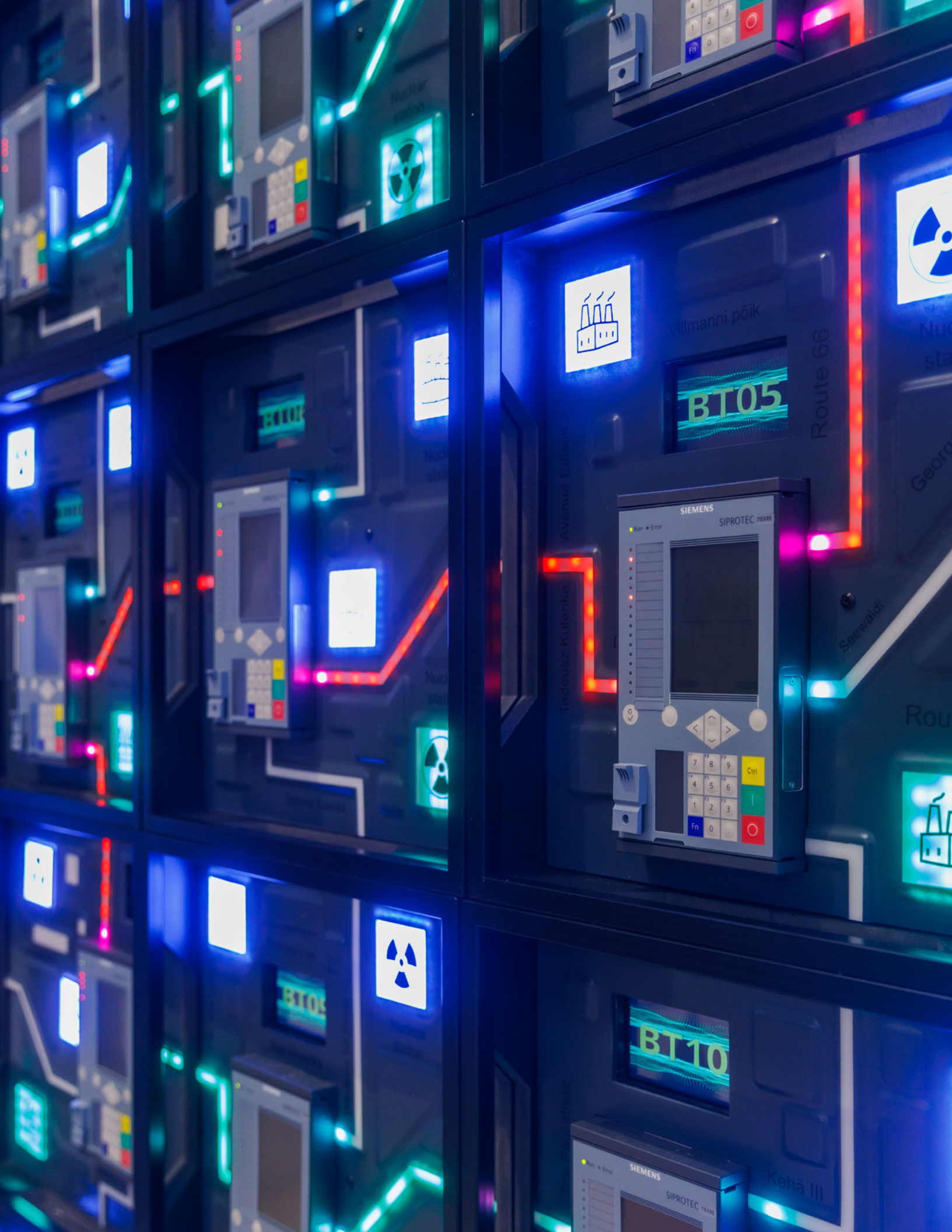
Defending against hybrid attacks

- **Build resilient repair and maintenance capabilities.** CUI repair capabilities often rely on private fleets of maintenance ships and are often limited. As outlined by the 2025 EU Action Plan,[126] building a fleet of reserve and emergency repair ships for the Baltic Sea would create better resilience for the network and further reduce the likelihood of large-scale disruptions. Pooling resources across Baltic Sea countries would also offer greater flexibility in terms of response and be more cost-efficient.
- **Conduct national vulnerability audits and risk assessments**. Baltic Sea area countries should work nationally and regionally to carry out cable infrastructure risk assessments, vulnerability mapping, and maritime chokepoint identification in low-redundancy areas in order to strengthen network resilience.[127]

- **Maintain and further increase presence and monitoring.** While the jury is still out, so far NATO's enhanced vigilance activities seem to be the most promising way to deter by 'denying deniability'. Monitoring capacity that is visible to Russian operators is needed both on the seabed and above water, as the latest drone sightings suspected to originate from Russian-linked ships indicate.

Deterrence by punishment

- **Identify asymmetric response options.** Since the kinetic threshold stemming from CUI disruption is high, Baltic Sea area countries should collectively determine what the proverbial redlines are, regardless of direct physical effect or cascading impact. Instead of remaining purely defensive in their responses, NATO countries should incur costs on Russia in asymmetric ways, including interfering with Russian operations in other theatres, further limiting Russian nationals' access to the Schengen area, using Russian frozen assets (currently a work in progress),[128] and lifting any remaining restraint on Ukrainian operations in Russia.
- **Use more covert action.** While European responses to Russian hybrid attacks should and cannot be fully symmetric, European intelligence and secret services can design and conduct operations against Russia that make the costs of continued hybrid aggression more evident. This should be combined with robust public communication, while respecting the covert nature of the operations.


BT05
SIEMENS
SIPROTEC
Run
Error
Ctrl
Fn
BT10
SIEMENS
SIPROTEC
Villmanni põik
Route 66
Avenue Edison
Tadeusz Kulenka
Seewaldi
Kehä III

The Digital Front: Deterring Russia's Cyber-Kinetic War

DOUGLAS WHITE

Introduction

Cyber operations are no longer a niche or episodic risk: They are a central theater of modern geopolitical competition and a direct instrument of statecraft.[129] Since 2014, and accelerating through the 2022 full-scale invasion of Ukraine, Russian-aligned actors have shifted from opportunistic disruption to persistent, strategic campaigns that blend espionage, sabotage, supply chain penetration, and information operations. These campaigns are designed not only to collect intelligence or degrade systems, but also to impose political costs, shake public confidence, and shape battlefield conditions. Cyberattacks now routinely sit alongside kinetic operations as synchronized elements of multidomain campaigns[130]; their effects cascade across military readiness, economic activity, civil governance, and diplomatic posture.

Cyber effects compound across modern, integrated societies. A single successful intrusion into a telecom, cloud provider, or registry can degrade emergency communications, disrupt commerce, halt cross-border transactions, and freeze supply chains that span allied economies. NotPetya (2017) and more recent destructive wipers deployed by Russian state-aligned actors against Ukraine are not merely IT incidents: They have destroyed business records, interrupted logistics, and produced multibillion-dollar economic losses[131] for neutral and allied companies alike. In wartime, targeted attacks on energy or transport assets multiply the humanitarian and military effects of kinetic strikes, rendering cyber a force multiplier for adversary aims. At the same time, espionage campaigns erode strategic advantage by draining proprietary industrial information, defense planning data, and political intelligence — upending competitive balances in commerce, trade, and technology.

The threat surface is vast and growing exponentially with each new app released, each new router deployed, each new internet-of-things-enabled (IoT) device sold to consumers, and each new endpoint added to networks. Modern states and societies operate on complex, interconnected ecosystems of information and communication technology, from national certificate authorities and cloud control planes to municipal water agencies' supervision and monitoring systems and consumer-grade IoT devices. Adversaries can exploit this heterogeneity: Supply-chain compromises give access to thousands of otherwise well-defended networks.

Photo Opposite: Photo: An dynamic display during at the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE) annual cyber defence exercise Locked Shields 2025 in Tallinn, Estonia. Credit: Arno Mikkor/NATO CCDCOE Flickr.

Social engineering and messaging-app remote-access trojans (RATs) turn individual devices into beachheads. Legacy systems with poor patching become access points into sensitive domains. The civilian sector, including telecoms, finance, health care, transportation, legal registries, and commercial cloud platforms, often holds the same or higher systemic risk than government networks because of sheer scale, high interdependence, and sometimes lower cyber maturity. Attacks on private sector targets rapidly produce public policy consequences, undermining trust in government, triggering market shocks, and presenting diplomatic dilemmas about attribution and response.

Cyberattacks' impact across domains takes various formats:

- **Military readiness:** Compromised or disrupted logistics, command and control systems, or supplier networks complicate efforts to sustain forces and maintain visibility; wipers and long-term espionage degrade preparedness and can leave field commanders blind to current battlefield status.
- **Civil governance and public confidence:** Assaults on state registries, electoral apparatus, and public services undermine legitimacy and civic trust, an explicit goal of active-measures doctrine.
- **Commerce and trade:** Supply-chain intrusions and destructive malware create direct financial losses, interrupt cross-border commerce, and raise insurance and compliance costs. NotPetya illustrated how collateral economic damage can dwarf the local theater of operations.
- **Political and diplomatic effects:** Cyber operations cover their tracks, giving the culprits plausible deniability that complicates allied response, fractures international consensus, and sows political polarization domestically.
- **Economic coercion and resilience costs:** The requirement to harden, segment, migrate to cloud, and sustain long-tail detection consumes public budgets and private capital, shifting investment away from growth toward resilience and creating an attritional economic burden.

Collectively, these dynamics make cybersecurity a strategic vulnerability. It is not ancillary to defense or commerce but central to allied deterrence and economic security. Effective policy must therefore treat cyber as a cross-cutting national/transnational priority; one that is resourced, legally prepared, and institutionally coordinated between public and private actors.

Photo Opposite: Photo: In this photo illustration, a warning message in Ukrainian, Russian and Polish languages is displayed on a smartphone screen and in the background. Credit: Photo by Pavlo Gonchar / SOPA Images/Sipa USA.

Part 1 — Russian-Aligned Cyber Operations Timeline and Key Campaigns (2007-2025)

Over three-plus years of full-scale war, Russia's cyber strategy has evolved from brute-force disruption, defacement, and destruction campaigns to more persistent, espionage-focused operations, marked by an increased use of automation, supply chain exploitation, and social engineering.

Over the course of Russia's full-scale war against Ukraine, cyber operations have mirrored and augmented kinetic warfare in sophistication and persistence. From widespread disruption to advanced sabotage attempts, Ukraine has faced more than 10,000 cyber incidents, countered primarily by the Computer Emergency Response Team of Ukraine (CERT-UA), a unit of the country's cyber defense center, and by the Service for Special Communications and Information Protection (SSSCIP), within which it sits. Their adaptive defenses have reduced the number of critical cyber incidents, even as attacks increased. The following pages examine key trends, evolutions in attacker tactics, and successful mitigation strategies that hold lessons for allied nations.

Recent interviews with allied cyber practitioners emphasize an operational shift: Russian intelligence services increasingly rely on outsourced, deniable actors to conduct cyber and cross-domain activity. These criminal groups tend to be poorly trained contractors and volunteers recruited via messaging apps. This "proxyization" allows for more attacks and muddies attribution, as operations blend state direction with plausible deniability and commercial or criminal stovepipes.

KEY RUSSIAN-ALIGNED CYBER OPERATIONS

OPERATIONS

2007 | ESTONIA

Government, media, and banking infrastructure suffer coordinated denial-of-service (DDoS) attacks; no attribution initially, but widely linked to Russian state proxies.

2008 | GEORGIA

Cyberattacks, including website defacements and disruption of communications, are synchronized with kinetic invasion.

2014 | UKRAINE

BlackEnergy malware emerges. Cyber espionage and sabotage begin targeting Ukraine's government and critical infrastructure.

2015-2016 | UKRAINE

Sandworm attacks power grids using BlackEnergy and Industroyer malware, triggering the first-ever confirmed hacker-induced blackouts.

2017 | GLOBAL

NotPetya malware, attributed to Sandworm, uses a Ukrainian software update as a supply chain vector, causing $10 billion-plus in damage globally.

2018 | UNITED KINGDOM/OPCW

GRU officers use Novichok nerve agent to target ex-spy Sergei Skripal, then attempt to hack the Organisation for the Prohibition of Chemical Weapons (OPCW) to access and undermine the investigation, exposing Russia's integration of chemical weapons, cyber intrusion, and disinformation in hybrid operations.

2019-2021 | UNITED STATES

The SolarWinds Orion platform is compromised via supply chain intrusion. Attackers insert the SUNBURST backdoor into software updates, enabling espionage across US federal agencies and Fortune 500 firms. Widely attributed to Russia's foreign intelligence service, the SVR.

2022 | UKRAINE

Russia's full-scale invasion triggers waves of wiper malware (e.g., HermeticWiper, CaddyWiper). Cyberattacks attempt to disrupt command and communications, and weaken civilian morale.

2022 | GLOBAL

Cyclops Blink botnet is discovered, showing Sandworm's infiltration of firewall and router infrastructure, forming a botnet of compromised network appliances.

2023-2024

Sandworm and affiliated actors target industrial control systems and operational technology across NATO countries. Cybersecurity firm Dragos uncovers FrostyGoop, malware designed to cut heating in Lviv.

2024

Coordinated cyberattacks on Ukraine's state registries aim to paralyze digital governance and shake public trust. Systems are disrupted but recovered through cloud failover and pre-positioned backups.

2025 | WESTERN PIVOT

Microsoft attributes global intrusions to BadPilot, a Sandworm subunit conducting initial access operations in the US, UK, Canada, and Australia.

2007-2025

Part 2 — Tactical Evolution Since 2022

OT-Targeted Cyber-Physical Attacks

Russian-aligned advanced persistent threats (APTs), particularly Sandworm, have increasingly targeted operational technology (OT) to inflict kinetic consequences through digital means. Beginning with the 2015 and 2016 Ukrainian power grid attacks, Russian state-aligned actors, particularly Sandworm, pioneered malware tailored to industrial control systems to trigger real-world disruption. These attacks, using BlackEnergy and Industroyer, marked the first known use of cyber operations to cause blackouts. The trend deepened in 2022 with Industroyer2[132] and custom malware like Loadgrip, which exemplify this shift from IT to OT environments. Unlike earlier incidents that relied on spear phishing or lateral movement through IT environments, these attacks directly manipulate or disable critical infrastructure such as power substations. They do so by exploiting industrial control protocols that lack authentication, encryption, and basic integrity checks. Industroyer2 in particular was designed to automate circuit breaker manipulation by taking advantage of these protocol-level weaknesses.

By 2024, malware targeted at industrial control systems had become modular and tailored to specific grid configurations, often synchronized with kinetic strikes or timed for maximum civilian impact. Although Ukraine's improved segmentation of its operational technologies and protocol monitoring helped blunt later waves of such malware, the malware's sophistication demonstrated deep knowledge of Ukraine's grid. These attacks underscore GRU adversaries' capacity to translate cyber operations into physical outcomes, in a dangerous evolution in cyber warfare that effectively bridges digital disruption and battlefield objectives. As tactics continue to evolve and improve, we can expect to see attacks at great scale and greater "combined arms" approaches: more frequent and more effective synchronization of cyber and kinetic strikes on critical infrastructure, particularly the energy sector.

Hybrid Warfare Integration

Russia's 2008 invasion of Georgia revealed its blueprint for blending cyber and kinetic warfare. Website defacements, communications disruptions, and DDoS attacks occurred in parallel with ground invasions. This model was expanded in Ukraine, where cyberattacks frequently support kinetic objectives or undermine civic resilience, particularly the 2022 deployment of wipers alongside missile strikes. The April 2022 Industroyer2 campaign was launched when many civilians were returning to work following air raids, maximizing potential harm. By merging physical and digital domains, adversaries hope to overload national defense and emergency systems.

Core to Russian cyber doctrine are the psychological and logistical effects of paralyzing infrastructure, undermining trust, and impeding recovery. Over time, operations have shifted from one-off events to carefully sequenced campaigns integrated into strategic military planning. The strategic timing of cyberattacks alongside kinetic campaigns requires defenders to integrate cyber risk modeling into physical threat response planning. Ukraine's experience demonstrates that cyber operations should be viewed not in isolation, but as synchronized components of broader geopolitical aggression.

Persistence via Prior Access

Russia's cyber campaigns since 2007 initially relied on transient access via phishing or basic exploits, but by the late 2010s, GRU-linked actors began reusing infrastructure and reactivating old infections. Since 2022 in particular, Russian threat actors are increasingly using prior compromises to regain control of systems. Persistence is now an operational doctrine. Attackers routinely reuse earlier footholds and infrastructure (domains, loaders, IPs) to regain access months later. For example, UAC-0006, a financially motivated actor, resurfaced in 2024 using SmokeLoader malware that victims had previously downloaded in widespread phishing campaigns. This tactic, referred to by analysts as "victim once = victim always," exposes shortcomings in long-term monitoring and post-infection remediation.

Repeated access to previously infected endpoints represents a pivot from "break in and break things" to "stay hidden, return later." For attackers, it enables efficient operations with minimal new exposure, but for defenders, it demands long-term surveillance on attacker infrastructure, even after an apparent remediation. The implication is clear: One-time cleanup is insufficient. Defenders require long-retention telemetry, routine re-validation of endpoints, and active threat-hunting campaigns focused on long-tail infection vectors and legacy command and control signals. Comprehensive decontamination and continuous threat hunting and endpoint revalidation are crucial, even after apparent resolution of incidents. Such persistence strategies demonstrate an evolution from opportunistic compromises to strategic intrusions.

Use of Wipers and Killware

While data-destroying malware was seen in 2007-2008 defacements and DDoS attacks, Russia's shift to full-spectrum digital sabotage began with NotPetya in 2017. Disguised as ransomware, NotPetya was a wiper targeting Ukrainian infrastructure and spreading globally through M.E.Doc, a Ukrainian tax accounting software suite. One of the most devastating malware incidents in history, the NotPetya cyberattack cost companies around the globe up to an estimated $10 billion. Some of the hardest-hit organizations included Maersk, which lost between $250 million and $300 million, and FedEx, which suffered $300 million in losses. Other affected

companies included Merck, Mondelez International, and Reckitt Benckiser, all of which reported significant financial impacts. This Sandworm GRU-led attack ushered in the era of "killware" — code designed purely for destruction.

The 2022 invasion of Ukraine was preceded by a barrage of wiper malware, including HermeticWiper, CaddyWiper, and AcidRain.[133] These tools masqueraded as ransomware but had no recovery function, serving only to destroy. Their deployment targeted government systems, telecommunications, and even Viasat satellite modems. Notably, AcidRain disabled critical infrastructure by overwriting modems used by both military and civilian organizations. Wipers are intended to paralyze logistics and communications while sowing fear. Ukraine's growing use of cloud-based backups and data replication mitigated the worst of the early 2022 outcomes, but the tactic demonstrated the scale and immediacy of modern destructive cyber capabilities. Such malware reflects a doctrinal shift toward cyber "killware," code designed not to extort, but to annihilate.

Social Engineering + RATs

Human-centric attack methods remain a constant in Russian cyber operations. Early Russian cyber operations, for example the Estonia and Georgia campaigns, leaned heavily on phishing and spam to gain access. By the 2020s, these methods had evolved to exploit mobile apps, messaging platforms, and context-aware bait.

In 2024, Ukraine reported a surge in Signal and Telegram-based phishing. Threat actors posed as trusted sources to distribute malicious Android Package Kits (APKs) — the file format used to distribute and install Android software — embedded with remote access trojans (RATs). Hacking groups UAC-0184 and UAC-0195 were prominent actors in this space, launching campaigns that exploited emotional triggers, such as fake military petitions or humanitarian relief links.[134] These attacks blur technical and psychological lines, combining deception with surveillance. This tactic combines social engineering with lightweight malware to bypass traditional perimeter defenses. The shift from targeting organizational IT to exploiting individuals' digital trust and habits makes education and cybersecurity hygiene critical layers of defense. Ukrainian cyber defenders responded by releasing public advisories and blocking malicious infrastructure, but the tactic's effectiveness reinforced the importance of multifactor authentication and user awareness.

These human-centric techniques are not limited to wartime or regional operations. Similar social engineering methods underpinned Russian interference efforts in Western democratic processes, most notably the 2016 US presidential election. In that case, Russian state-linked actors combined phishing, credential harvesting, and persona-based deception with broader influence operations to exploit trust, amplify divisive narratives, and manipulate information environments rather than directly compromise technical systems.

"Proxyization: Recruiting Untrained Actors via Messaging Platforms

Since 2022, Russian-aligned operations have overwhelmed targets with proxy attacks on top of traditional APT tradecraft. Operators post tasking and recruitment calls on encrypted/messaging platforms (notably Telegram), offering small sums to carry out sabotage or intelligence collection, or to act as footholds for follow-on access.[135] Interviewed security experts described two cardinal consequences: (1) a sharp rise in the number of low-sophistication incidents, which in turn consume responder resources, and (2) more difficulty in tracing the culprits, as proxies are motivated by pay rather than clear chain-of-command orders.

Common Tactics of Russian-Aligned Threat Actors

Tactic	Description	Example(s)
OT-targeted Cyber-Physical Attacks	Use of malware targeted at industrial control systems to disable substations or relays	Industroyer2 (April 2022); Loadgrip/Biasboat (Oct. 2022)
Hybrid Warfare Integration	Synchronization of cyberattacks with missile strikes or military operations	Power grid attacks timed with civilian return to work (April 2022)
Persistence via Old Access	Reactivation of previously infected endpoints using legacy command infrastructure	UAC-0006 resurgence (2024), exploiting earlier SmokeLoader implants
Use of Wipers and Killware	Destructive malware used to erase data and disrupt recovery processes	HermeticWiper (2022), wipers used in parallel with attacks on operational technologies
Social Engineering + RATs	Use of fake software, phishing, and Signal/Telegram lures to install remote access trojans	UAC-0184/0195 campaigns via Signal-based APKs (2024)

Part 3 — Mitigation Strategies — Successful

Ukraine's successful mitigation techniques have evolved rapidly in response to the increasing sophistication of Russian cyber operations. Ukraine's defenders have steadily improved their detection, response, and resilience, cutting critical incident rates by over 80% (according to the country's information-security service) even as the number of incidents surged. Ukraine's experience offers a live model of adaptive, layered cyber defense under persistent nation-state attack. In particular, successful mitigation efforts include the following:

Photo: A participant at NATO CCDCOE's 2024 Crossed Swords exercise. Credit: Kristi Sits/NATO CCDCOE Flickr.

Endpoint Defense

Following widespread use of wipers like HermeticWiper and AcidRain in early 2022, Ukrainian agencies implemented aggressive endpoint hardening measures. Notably, CERT-UA issued advisories for blocking the use of vulnerable Windows system tools (e.g., mshta.exe, powershell.exe) that were frequently abused for malware execution. This strategy helped prevent the reactivation of dormant payloads like those seen in the UAC-0006 resurgence in 2024. Additionally, state and private sector organizations rolled out advanced endpoint detection and response (EDR) solutions to monitor the countless devices connected to their networks, enabling real-time behavioral analysis and threat containment. These tools played a key role in detecting lateral movement attempts and containing infections before they spread across networks, especially during high-risk incidents like the 2023 breach of the Kyivstar telecoms provider and a December 2022 phishing campaign against users of the DELTA battlefield monitoring and intelligence platform.

Threat Intelligence Integration

Through partnerships with Google's Threat Analysis Group (TAG), Microsoft, and the ESET cybersecurity firm, Ukraine was able to detect and neutralize the Industroyer2 malware in April 2022 before it could disrupt the power grid. Real-time threat sharing and regional CERT channels allowed defenders to act before the malware was executed. This is a textbook case of proactive intelligence-led defense.

Cloud Migration

A cyberattack on Ukraine's Ministry of Justice registry in 2022 prompted an aggressive cloud migration campaign. By 2023, more than 10 million GB of critical government data had been moved to cloud platforms like Amazon Web Services (AWS) and Azure.[136] During a December 2024 attack on state registries, this migration proved vital, enabling rapid recovery through cloud failover mechanisms.

OT Segmentation

After the 2015 and 2016 grid attacks and later the 2022 Loadgrip campaign, Ukraine implemented stricter segmentation between IT and operating technologies. When Sandworm deployed new malware against industrial control systems in late 2022, these defensive boundaries helped contain the impact, limiting access to certain industrial protocols.

Multistakeholder Coordination

During the 2023 Kyivstar breach, joint response efforts from Ukraine's telecom CERT, international telecom experts, and major cloud vendors helped stabilize services. Lessons from this incident informed broader public-private contingency planning, which proved effective in blunting attacks on digital state services in December 2024.

Part 4 — Mitigation Strategies — Unsuccessful

Despite numerous advances in cyber defense, some of Ukraine's efforts at mitigation have been insufficient or delayed. These instances underscore the necessity for continuous improvement and investment in cybersecurity resilience.

Justice Registry Breach (2022)

Prior to Ukraine's full cloud transition, attackers compromised portions of the Ministry of Justice's registry services, causing significant delays in legal and administrative functions.[137] The breach exposed weaknesses in legacy system security, insufficient redundancy, and a lack of immutable backups. The experience catalyzed the eventual cloud migration, but not before demonstrating the operational risks of outdated digital infrastructure.

Kyivstar Attack (December 2023)

One of Ukraine's largest telecom providers suffered a severe breach attributed to Sandworm-affiliated actors[138]. The attackers maintained undetected access for months, ultimately deploying scripts that disrupted mobile, internet, and emergency communication services nationwide. Post-incident analysis revealed a lack of internal segmentation and limited anomaly detection at the domain controller level. The attack highlighted gaps in telecom sector readiness and emphasized the need for endpoint detection and response integration at infrastructure scale.

UAC-0006 Resurgence (2024)

The reactivation of previously dormant infections using old command and control domains revealed that defenders had not fully eradicated malware from earlier phases of compromise. This incident illuminated shortcomings in persistent threat monitoring, particularly regarding legacy infrastructure and long-tail infection vectors.

Each of these cases serves as a reminder that cyber defense is a continuous process. Even with advanced tools and partnerships, effective mitigation requires constant reevaluation of assumptions, infrastructure, and adversary behavior.

Part 5 — Why Attribution Fails — Technical, Analytic, and Political Dimensions

Investigators' failure to identify attackers is seldom due to purely technical reasons.[139] Three recurrent constraints emerge from practitioner discussions:

- **Technical complexity:** Cross-border infrastructure, proxies, and shell companies thwart clean forensic chains and forensic determinations.
- **Analytic capacity erosion:** Several experts flagged reduced institutional analytic benches and significant personnel turnover as major constraints — meaning national centers sometimes lack the depth or time to develop stand-alone public attributions.
- **Political risk-aversion:** Governments often weigh escalation risk and public reaction, choosing to make cautious public statements even when classified intelligence is stronger.

A graded attribution pipeline, separating technical analysis, policy messaging, and legal evidence production can serve to preserve analytic credibility; allow calibrated, coordinated political action based on graded confidence; and create the legal basis for punitive measures where prosecutable evidence exists. This concept is expanded upon in the Policy Recommendations section.

Photo: A dynmaic display at NATO CCDCOE's 2024 Crossed Swords exercise. Credit: Kristi Sits/ NATO CCDCOE Flickr.

Part 6 — Lessons for Allies: Strategic Takeaways

Invest Early in OT Monitoring and Threat Detection

Ukraine's experience underscores the critical need for early deployment of staff and tools to monitor operational technologies. In 2015 and 2016, Russian-linked actors executed blackout-inducing cyberattacks using BlackEnergy and Industroyer, exploiting unmonitored industrial protocols. In response, Ukraine introduced segmentation, logging, and specialized detection systems across its energy infrastructure. By the time Industroyer2 and Loadgrip emerged in 2022, defenders had learned to identify abnormal traffic patterns, detect logic manipulation, and shut down intrusions before impact. Allies must prioritize deployment of detection tools that understand open platform communications technologies, which help hub-and-spoke systems to communicate, and other traffic specific to operations technology. These tools must be paired with cybersecurity training tailored to engineers and

grid operators in charge of supervision and monitoring systems. Without proactive visibility into the environments where operations technologies function, defenders will miss the earliest signs of adversarial reconnaissance and manipulation.

Assume Persistence, Not One-Off Attacks

Russian threat actors increasingly demonstrate long-term persistence strategies. Rather than compromising, executing, and retreating, groups like UAC-0006 reuse infrastructure and malware implants over time. This persistence reflects an operational doctrine that treats infection as long-term infrastructure. Defenders must respond by keeping watch even after a compromise appears to be remediated. Endpoint logs should be retained for months, not weeks. Indicators of compromise must include DNS and domain registrations, not just file hashes. Network defenders should expect adversaries to return months later, often with upgraded payloads and enhanced targeting. "Cleanup" must be followed by surveillance and validation.

Synchronized Cyber-Kinetic Campaigns Are a Norm

Several major Russian cyberattacks have been timed to amplify the effects of kinetic warfare. During the April 2022 attempt to trigger widespread blackouts, the Industroyer2 malware was deployed when workers were returning to their jobs after a weekend and following air raid alerts. This timing was designed to maximize confusion and delay restoration. The attack on Ukraine's heating infrastructure in late 2022 occurred during freezing temperatures, aiming to deepen civilian hardship. These patterns illustrate that cyber operations are increasingly integrated into military doctrine. Allies must build cyber risk modeling into physical security scenarios and war-gaming exercises. Civil defense systems must include cyber disruption as a component of mass casualty and humanitarian response planning. If adversaries blend digital and kinetic attacks, defenders must integrate cyber-physical coordination across sectors.

Rapid Response and Pre-Positioned Partnerships Matter

Ukraine's relatively rapid recovery from high-impact cyberattacks — especially Industroyer2 and the December 2024 state registry attacks — was made possible by early, trusted partnerships. Prior to the invasion, Ukraine had collaborated with Microsoft, Google TAG, and ESET on malware analysis and joint detection frameworks. CERT-UA's integration with NATO-aligned CERTs and the EU's cyber response teams also enabled faster information sharing and coordinated countermeasures. At the national level, Ukrainian government information-security principals had already exercised interagency and public-private response procedures through repeated tabletop exercises covering a range of cyber compromise scenarios. These practical and practiced relationships have meant that when attacks occur,

analysts and decisionmakers know whom to call and have workflows in place. Allies should preestablish incident response partnerships with both public and private sector organizations. Cyber diplomacy should extend beyond memorandums of understanding to include technical integration, joint exercises, and shared forensic capabilities. Waiting until after a breach to build relationships reduces effectiveness and delays recovery.

Cloud Migration Is a Defensive Asset

Ukraine's migration to cloud infrastructure has proved critical in ensuring the resilience of government operations amid intense cyberattacks. Following the 2022 attack on the Ministry of Justice's registry system, more than 10 million GB of state data were transitioned to secure cloud platforms like AWS and Azure. By December 2024, when attackers targeted Ukraine's state registries again, cloud failover protocols enabled continuity of operations with minimal data loss. Well-architected cloud environments offer geographic redundancy, rapid patching, version control, and scalable incident containment. However, they also demand rigorous management of users' identity and access, zero trust principles that apply security protocols to each connection in a network, and continuous security assessment. Allies should not only migrate core functions to the cloud but also build the institutional skills and budgets necessary to secure and audit those environments over time. Done well, cloud migration is not just a cost-saving measure, it is a strategic pillar of cyber resilience.

Prepare Legal and Institutional Frameworks for Cyber-Physical Attribution

In the aftermath of attacks on Ukraine's power grid and state infrastructure, Ukrainian leaders moved to define such operations as potential war crimes under international law. This advocacy gained traction following filings with the International Criminal Court that linked cyberattacks on civilian infrastructure to violations of the Geneva Conventions. The challenge for many allied nations is the lack of codified legal doctrine addressing attribution, proportionality, and sovereignty in cyberspace. To prepare for future attacks, governments must clarify what constitutes a cyber-physical attack on national infrastructure, when state attribution is valid, and how proportional responses will be coordinated across agencies and allies. Legal preparedness must also include the ability to preserve digital forensics for evidentiary use. Establishing norms now will prevent legal and diplomatic paralysis during the next major cyber-kinetic campaign.

Part 7 — Policy Recommendations

Recommendation	Projected Cost	Strategic Benefit	Priority
Graded attribution pipeline	Medium	High (enables coordinated response and raises costs of deniable operations)	High
Binding public-private reporting and telemetry sharing	High	Very High (massively reduces detection time, which is a core bottleneck today)	High
Joint allied cyber rapid-response and forensic surge	High	High (reduces impact of destructive attacks)	Medium
Monitoring and segmentation of operational technologies and industrial control systems	Medium	Very High (prevents blackouts; largest return on investment)	Very High
Evidence harmonization and legal frameworks	Low	Medium (enables prosecution and strengthens deterrence)	Medium

Establish a Graded Attribution Pipeline

Allies should adopt a three-track attribution architecture that is analytically rigorous but enables timely political and legal action.

- The first track is a classified technical assessment stream. It consists of rapid, high-confidence analyses shared among vetted allied analysts over secure channels, including full tactics, techniques, procedures and raw telemetry.
- The second track is a concise, jointly issued public attribution statement designed for policymakers and the public that expresses confidence in graded terms (for example: "highly likely," "probable," or "inconclusive").
- The third track is a separately compiled, court-grade evidentiary package with preserved logs, chain-of-custody documentation, and forensic reports suitable for domestic prosecutions or sanctions processes.

This separation prevents premature politicization of sensitive technical findings, makes potential prosecutions more viable, and ensures that technical, diplomatic, and legal actors can act from a common, defensible, factual basis. NATO should convene the initial design and interoperability work, with national CERTs, the NATO cyber defense hub, intelligence services, and EU cyber agencies supplying technical inputs and operating the assessment channels.

Make Public-Private Cooperation Binding and Operational

National governments must move beyond voluntary engagement and put in place binding, operational mechanisms that get telemetry and expertise flowing in real time between critical providers and state responders. Require mandatory incident reporting by defined critical sectors — energy, telecoms, finance, transportation, health, and core government registries — into protected national reporting channels, with statutory confidentiality and whistleblower/disclosure protections to safeguard sensitive telemetry and sources. Standardize technical threat-intelligence exchange and operationalize it through pre-positioned integration points: liaison teams of government analysts embedded inside the security operations centers of major telecoms companies and cloud services providers, and industry liaison officers assigned to national CERTs to enable near-real-time correlation and joint triage. Finally, sustainable multiyear funding mechanisms (grants, matched incentives, or tax credits) must underwrite long-term investments in endpoint detection and response, identity/zero-trust practices, segmentation of operation technologies, and forensic readiness rather than one-off patches. These measures address the most persistent operational gap raised by practitioners: private underinvestment and fragmented reporting. These efforts can be modeled on Finland's high-trust, civic-literacy approach. National ministries of interior/ICT and regulators should lead, with national CERTs implementing integration and the EU Commission coordinating cross-border harmonization.

Harmonize Legal and Evidentiary Standards for Cyber-Physical Attribution

Technical attribution matters most when it can be translated into legal accountability and coordinated allied action. States should standardize forensic formats, logging retention policies and chain-of-custody procedures to ensure digital artifacts are admissible and portable across jurisdictions. At the same time, updated mutual-assistance mechanisms such as treaties or agreements, an EU rapid e-evidence pathway, and preapproved disclosure clauses with major cloud providers would speed cross-border evidence transfers. Legal architecture should also codify thresholds and procedures that distinguish criminal attribution from political attribution and explicitly criminalize state-directed cyber-physical harms where national jurisdiction applies. These measures reduce procedural friction that currently stalls prosecutions and allied decision-making. Justice ministries should lead drafting and coordination with national prosecutors, cyber-forensics labs, EU legal services, and NATO legal advisers.

Photo: Participants at NATO CCDCOE's 2024 Crossed Swords exercise. Credit: Kristi Sits/NATO CCDCOE Flickr.

Stand up a Joint Allied Cyber Rapid Response and Forensics Capability

Allies should establish a rostered, multinational surge capability that can be rapidly mobilized to provide forensic surge capacity, coordinated containment, and delivery of the graded attribution products described above. This capability, combining national responders, vendor partners, and deployable mobile forensic labs, must operate under prenegotiated agreements with major cloud and security vendors and be supported by expedited, preauthorized legal tasking frameworks to clear cross-border constraints. By pre-positioning relationships, playbooks, and interoperable toolkits, the alliance can more quickly detect, attribute, and remediate incidents; the Ukraine experience makes clear that these preexisting partnerships are a decisive advantage. NATO should host and coordinate the capability while national CERTs, NATO's cyber defense hub, and commercial partners populate the roster and provide operational build-out.

Align Investment Priorities and Create Sustained Funding Vehicles

Durable cyber resilience requires predictable, multiyear investment focused on a clear set of technical priorities: operations technology/industrial control systems monitoring and protocol-aware detection and segmentation; enterprise endpoint detection and response with long-tail endpoint analytics and extended log retention; robust identity and zero-trust controls; standardized telemetry and threat-intelligence integration; cloud resilience with immutable backups and tested failover; and forensic readiness with secure archives and sandboxing. Rather than episodic or emergency funding, these capabilities should be financed through a mix of multiyear grants, matched national contributions, and pooled allied procurement for shared capabilities and forensic nodes. Ministries of finance and defense should marshal the funds, with EU and NATO investment instruments coordinating cross-border financing, and national regulators and industry partners ensuring eligibility and technical alignment. Sustained financing removes the chronic short-termism that undercuts remediation and allows allied governments and private operators to harden systems to withstand persistent, state-level cyber campaigns.

Conclusion

Cyber operations are no longer peripheral. They are a central domain of warfare and a primary theater of statecraft that routinely amplifies kinetic violence, corrodes public trust, and inflicts multibillion-dollar economic damage. Russian-aligned campaigns have evolved from episodic disruption to persistent, synchronized cyber-kinetic campaigns that exploit supply chains, long-tail persistence, social engineering, and outsourced, deniable actors. Ukraine's experience proves defenders can blunt the worst effects through operations technology segmentation, cloud failover, sustained threat intelligence partnerships, and practiced incident playbooks and tabletop drills. Ukraine's experience also exposes persistent gaps: fragmented public-private collaboration and reporting, uneven legal frameworks for cyber-physical attribution, and chronic underinvestment in long-term detection and forensics. Allies must treat cyber as a cross-cutting strategic priority: Adopt a graded attribution pipeline, bind public-private telemetry and liaison mechanisms into law, harmonize evidentiary standards, stand up an allied rapid-response forensics capability, and fund multiyear resilience programs that prioritize operations technology monitoring, endpoint detection and response, identity/zero-trust practices, and forensic readiness. Doing so converts experience into deterrence: faster detection, credible attribution, and consequences that raise the cost of persistent state-level cyber aggression.

Glossary of terms

APT	Advanced Persistent Threat
AWS	Amazon Web Services
APK	Android Package Kit; file format used to distribute and install applications on Android devices
C2	Command and Control
CERT	Computer Emergency Response Team
CERT-UA	Computer Emergency Response Team of Ukraine
DDoS	Distributed Denial of Service
DELTA	DELTA battlefield management platform; Ukraine's digital command and control system
DNS	Domain Name System
DNP3	Distributed Network Protocol version 3
EDR	Endpoint Detection and Response
GB	Gigabyte
GRU	Main Directorate of the General Staff of the Armed Forces of the Russian Federation
ICS	Industrial Control System; a subset of OT
ICT	Information and Communication Technology
IEC-104	International Electrotechnical Commission 60870-5-104 telecontrol protocol
IoT	Internet of Things
Loadgrip / Industroyer2:	ICS malware used to disrupt the Ukrainian power grid
Not Petya	2017 destructive wiper disguised as ransomware
OT	Operational Technology; physical process control systems
RAT	Remote Access Trojan; used for surveillance and access
Sandworm	GRU Unit 74455; conducts OT blackouts and destructive wipers
SSSCIP	State Service of Special Communications and Information Protection of Ukraine
SVR	Foreign Intelligence Service of the Russian Federation
TAG	Threat Analysis Group; Google's threat intelligence center
UAC-0006	Ukrainian cyber threat group designation 0006 (CERT-UA classification)
UAC-0184	Ukrainian cyber threat group designation 0184 (CERT-UA classification)
UAC-0195	Ukrainian cyber threat group designation 0195 (CERT-UA classification)
Wiper	Malware designed to permanently delete or corrupt data on targeted systems

Key Recommendations

The recommendations below represent the central findings of CEPA's research for core policy priorities for transatlantic decision-makers. They are not exhaustive but rather represent the most critical steps required to restore credible deterrence against Russia's shadow war.

Why Deterrence Has Failed

- **Shadow warfare is persistently misclassified.**
  - Existing institutional mandates lead sabotage, for example, to be processed primarily through criminal law and civilian enforcement frameworks. Cable disruptions are framed as maritime accidents. Cyber intrusions are managed as technical incidents. Each response may be reasonable on its own. Together, however, they fragment responsibility and signal restraint rather than resolve. A coordinated campaign of hostile state action is handled as a series of unrelated problems.
- **The tempo of response lags behind the tempo of attack.**
  - Russian operations are fast, deniable, and iterative. Western responses are slow, deliberative, and consensus-bound. By the time attribution debates conclude and response options are weighed, the political urgency of the incident has often passed. Deterrence weakens when consequences arrive late, or not at all.
- **Fear of escalation has produced a reliance on ambiguity that favors the aggressor.**
  - By avoiding clear thresholds and predictable consequences, European governments hope to avoid war. In practice, this restraint has raised Moscow's tolerance for risk. Each unpunished act widens the space for the next one.
- **Deterrence has been tethered to courtroom standards of proof.**
  - Shadow warfare is designed precisely to frustrate legal certainty. Insisting on incontrovertible evidence for each incident before acting strategically leaves initiative in Moscow's hands. This is particularly true when attribution rests on intelligence sources that cannot be made public. Deterrence in the shadow domain cannot rest on legal attribution alone; it must be informed by patterns, intent, and cumulative effect. This does not mean that evidentiary standards should be lowered, but governments must be enabled to act on confident intelligence assessments that cannot always be made public.

What Must Change

- **Deterrence should be based on cumulative pattern recognition, not isolated proof**
  - Russian shadow warfare relies on deniability. Allied responses should rest on repeated operational signatures (methods, targets, timing, and intent) rather than treating each incident as a standalone criminal act.
- **Collective consultation should become routine, not exceptional**
  - European allies should normalize collective consultations in response to shadow aggression. Patterns of activity, rather than isolated incidents, should trigger collective assessment and coordination.
- **Hybrid threats should be integrated into a single deterrence framework**
  - Cyber attacks, critical undersea infrastructure disruption, drone incursions, and proxy violence are not separate challenges. They are mutually reinforcing elements of a unified Russian strategy. Allies should treat hybrid warfare as a continuous campaign, aligning maritime, cyber, legal, intelligence, and military tools under a shared escalation logic.
- **Allies should maintain a standing menu of consequences**
  - This menu should be designed for speed and predictability, and include cyber and intelligence operations, interdiction of vessels and proxy networks and other infrastructure supporting covert activity, economic measures that directly constrain Russia's warfighting capacity, and direct support for Ukraine's defense, rather than merely signaling displeasure.

TIER	ATTACK	RESPONSE
TIER 1	SINGLE INCURSION OR BORDER PROBE	Deploy additional ISR (intelligence, surveillance, reconnaissance) assets to affected regions; Increase EU customs screening of high-risk goods; Activate rapid NATO–EU hybrid threat information-sharing mechanisms.
TIER 2	REPEATED INCURSIONS OR PROXY SABOTAGE ATTEMPTS	Increase preauthorized ammunition and air-defense packages to Ukraine; Expand export controls on dual-use electronics and drone components; Issue mandatory public attribution within 72 hours.
TIER 3	CONFIRMED PROXY SABOTAGE OR ASSASSINATION PLOT	Accelerate delivery of previously withheld weapons systems to Ukraine; Launch joint NATO–EU cyber pressure targeting Russian military logistics; Freeze assets of implicated facilitators using criminal (non-sanctions) tools.
TIER 4	MULTISTATE INFILTRATION CAMPAIGN	Expand NATO air-policing rotations and deploy additional fighter detachments; Restrict correspondent banking access for enabler jurisdictions; Surge EU-wide inspections of reexported electronics and transit goods.
TIER 5	MASS INCURSION OR HIGH-IMPACT HYBRID ATTACK	Expand NATO air-policing rotations and deploy additional fighter detachments; Restrict correspondent banking access for enabler jurisdictions; Surge EU-wide inspections of reexported electronics and transit goods.

- **The EU and NATO should harmonize readiness capabilities and political thresholds for action.**
  - Fragmented decision-making and national caveats have become the soft underbelly of European deterrence. To avoid duplication and close exploitable gaps, allies should formalize a division of labor where NATO leads on detection, defense, and military response, and the EU leads on financial pressure, border controls, law enforcement, and export controls.
- **Responses should be anchored in national security institutions**
  - Militaries and intelligence services—not law enforcement agencies—should lead the coordination of responses to concerted campaigns of shadow warfare. This does not imply abandoning collective frameworks or sidelining law enforcement. Criminal investigations remain necessary, in order to impose consequences on individual actors, but they cannot be the primary framework for deterrence of a committed state actor. Rather, they should feed into political and security decision-making structures, acting at pace and in coordination with partners across Europe.
- **Allies should institutionalize public–private coordination as a permanent pillar of hybrid deterrence**
  - Across seabed infrastructure protection, cyber-kinetic defense, and counter-infiltration efforts, the frontline of Russia's shadow war consistently runs through privately owned systems and civilian spaces—undersea cables, energy grids, telecom networks, cloud platforms, shipping, and local communities. Allied governments should move beyond ad hoc information sharing toward formal, legally mandated public–private security partnerships that integrate industry into threat detection, attribution, incident response, and resilience planning.
- **Allies should reassert political durability in the face of Russian escalatory rhetoric**
  - Strong allied deterrence policy, as outlined in this report, will undoubtedly invite louder escalatory rhetoric from Moscow. This strategic intimidation is designed to paralyze allied decision-making before policies are implemented. Restoring credible deterrence requires the political will to tolerate intimidation without allowing it to dictate thresholds or timelines for action. Clear red lines, predictable consequences, and collective resolve must hold even when Moscow responds with saber rattling. The objective is neither to seek confrontation nor to avoid it reflexively, but to impose consequences consistently.

About the Authors

Sam Greene

Sam Greene is a Nonresident Senior Fellow for the Democratic Resilience program at the Center for European Policy Analysis (CEPA) and Professor of Russian Politics at King's College London (KCL).

David Kagan

David Kagan serves as a Senior Program Officer with the Democratic Resilience program at the Center for European Policy Analysis (CEPA).

Mathieu Boulègue

Mathieu Boulègue is a Senior Fellow with the Transatlantic Defense and Security Program at the Center for European Policy Analysis (CEPA).

Minna Ålander

Minna Ålander is a Fellow with the Transatlantic Defense and Security Program at the Center for European Policy Analysis (CEPA), an Associate Fellow at Chatham House Europe Programme, and a Senior Fellow at the Stockholm Free World Forum.

Douglas White

Douglas White is a Senior Fellow with the Democratic Resilience Program at the Center for European Policy Analysis (CEPA).

Acknowledgments

This report was generously supported by the Smith Richardson Foundation. The authors are grateful to CEPA staff members Christopher Walker, Michael Newton, Isabella Nieminen, David Kagan, SaraJane Rzegocki, Katelynn Henics, and Gabriel Goldberg, whose editorial and production support were invaluable elements of the release of this report. The authors would also like to thank the members of CEPA's Shadow War Working Group – Aaron Allen, Eitvydas Bajarūnas, Ben Dubow, Marija Golubeva, Olga Lautman, Edward Lucas, and Ben Schmitt – for their essential advice and expertise throughout the project.

Endnotes

1 Jozwiak, Rikard."NATO Launches Eastern Sentry Drills as Russian Drones Enter Polish Airspace." Radio Free Europe/Radio Liberty, December 5, 2024, https://www.rferl.org/a/nato-eastern-sentry-russia-drones-poland/33536306.html.

2 "Eastern Sentry to Enhance NATO's Presence Along Its Eastern Flank." NATO Shape, September 12, 2025. https://shape.nato.int/news-releases/eastern-sentry-to-enhance-natos-presence-along-its-eastern-flank.

3 World Economic Outlook Database: Gross Domestic Product, Current Prices (NGDPD). International Monetary Fund, accessed December 31, 2025. https://www.imf.org/external/datamapper/NGDPD@WEO/OEMDC/ADVEC/WEOWORLD.

4 Lopes da Silva, Diego, Nan Tian, and Alexandra Marksteiner. "Trends in World Military Expenditure, 2024." SIPRI Fact Sheet-Solna: Stockholm International Peace Research Institute, April 2025. https://www.sipri.org/sites/default/files/2025-04/2504_fs_milex_2024.pdf.

5 Green, Sam, Andrei Soldatov, Irina Borogan. "War Without End: Russia's Shadow Warfare." Center for European Policy Analysis, 2024. https://cepa.org/comprehensive-reports/war-without-end-russias-shadow-warfare/.

6 Dragusin, Alina and Adrian Dumitru. "Pericol de prăbușire a dronelor rusești în Tulcea, la câteva zile de la incidentul din Polonia. RO-Alert a transmis mesaj de avertizare." Antena 3 CNN, September 13, 2025. https://www.antena3.ro/actualitate/pericol-de-prabusire-a-dronelor-rusesti-in-tulcea-la-cateva-zile-de-la-incidentul-din-polonia-ro-alert-a-transmis-mesaj-de-avertizare-759501.html.

7 "Chart Shows Russian Jets' 12-Minute Violation of Estonian Airspace." Estonian World, September 30, 2025. https://estonianworld.com/security/chart-shows-russian-jets-12-minute-violation-of-estonian-airspace/.

8 Kilander, Gustaf and Alexander Marrow. "Drones That Shut Copenhagen Airport Flown by Capable Operator, Danish Police Say." Reuters, September 23, 2025. https://www.reuters.com/world/europe/drones-that-shut-copenhagen-airport-flown-by-capable-operator-danish-police-say-2025-09-23/.

9 Jordan, Dearbail. "Drone Incidents: Copenhagen Airport Closure and Broader Europe Security Concerns." BBC News, October 23, 2025. https://www.bbc.com/news/articles/c0r0ezjzwpno.

10 Vandiver, John. "Estonia Shoots Down Russian Drone as Tensions Escalate in the Baltics." *Stars and Stripes*, October 29, 2025. https://www.stripes.com/theaters/europe/2025-10-29/estonia-drone-shotdown-19584290.html.

11 Blackburn, Gavin. "Two Russian Military Aircraft Enter NATO Member Lithuania's Airspace, Military Says." Euronews, October 23, 2025. https://www.euronews.com/2025/10/23/two-russian-military-aircraft-enter-nato-member-lithuanias-airspace-military-says.

12 Espinoza, Javier and Matthew Karnitschnig. "NATO Weighs Options to Sew Up Patchwork Air Defenses." Politico, December 4, 2025. https://www.politico.eu/article/nato-weighs-options-to-sew-up-patchwork-air-defenses/.

13 Edwards, Charlie. "The Paradox of Russian Escalation and NATO's Response." IISS Online Analysis, September 2025. https://www.iiss.org/online-analysis/online-analysis/2025/09/the-paradox-of-russian-escalation-and-natos-response/

14 Pullella, Philip and Sabine Siebold. "EU Scramble to Build Anti-Russia 'Drone Wall' Hits Political, Technical Hurdles." Reuters, October 15, 2025. https://www.reuters.com/business/aerospace-defense/eu-scramble-anti-russia-drone-wall-hits-political-technical-hurdles-2025-10-15/.

15 Wilson, Joseph and Kate Abnett. "Ursula von der Leyen's 'Drone Wall' Plan Hits Crash-to-Reality." Politico, October 15, 2025. https://www.politico.eu/article/ursula-von-der-leyen-drone-wall-plan-crash-eu-reality/.

16 Jordans, Frank. "Germany Accuses Russia of Running Spying, Social Media Campaign to Undermine Support for Ukraine," AP News, May 15, 2025. https://apnews.com/article/germany-russia-spying-social-media-campaign-4ffac951b38a2092e159993998df77b4.

17 Higgins, Andrew. "Lithuania Investigates IKEA Fire as Possible Russian Sabotage." The New York Times, April 10, 2025. https://www.nytimes.com/2025/04/10/world/europe/lithuania-ikea-fire-russia-sabotage.html.

18 Sytas, Andrius. "Lithuania Says Russian Military Intelligence Was Behind IKEA Arson Last Year." Reuters, March 17, 2025. https://www.reuters.com/world/europe/lithuania-says-russian-military-intelligence-was-behind-ikea-arson-last-year-2025-03-17/.

19 Tusk, Donald (@donaldtusk). "Poland will not be intimidated...," X (formerly Twitter). October 27, 2025, 6:42 p.m. https://x.com/donaldtusk/status/1921629800730382832.

20 Associated Press. "Poland Blames Russian Intelligence for Fire at Shopping Center," CNN, May 11, 2025. https://www.cnn.com/2025/05/11/europe/poland-blames-russian-intelligence-fire-shopping-center-latam-intl.

21 Burke, Jason. "Ukrainians Working for Russia Behind Rail Blasts, Says Poland Prime Minister Donald Tusk," The Guardian, November 18, 2025. https://www.theguardian.com/world/2025/nov/18/ukrainians-working-for-russia-rail-blasts-says-poland-prime-minister-donald-tusk.

22 Agence France-Presse. "Kremlin Dismisses Reports of Assassination Plot Against German Arms Maker." Kyiv Post, July 12, 2024. https://www.kyivpost.com/post/35747

23 Moulson, Geir. "Russia Used Spies in Germany to Target Ukraine Supporters and Sabotage Infrastructure, Prosecutors Say." AP News, August 22, 2025. https://apnews.com/article/russia-germany-ukraine-spying-sabotage-frankfurt-db05e9d4f0c625b927f1f6670eda1bfb.

24 Arraf, Jane and Elian Peltier. "Caught in Belarus, Exiled in Iraq: Migrants Who Risked All Find Themselves Back Home." The New York Times, November 13, 2021.https://www.nytimes.com/2021/11/13/world/middleeast/belarus-migrants-iraq-kurds.html.

25 "Konwój z pomocą humanitarną na granicy Polska–Białoruś," Gazeta Prawna, September 24, 2025. https://www.gazetaprawna.pl/wiadomosci/kraj/artykuly/8232938,konwoj-z-pomoca-humanitarna-granica-polska-bialorus.html.

26 Gera, Vanessa. "Poland Says Russia Tried to Recruit Migrants in Africa and the Middle East to Set Fires in Its Forests," AP News, June 20, 2025. https://apnews.com/article/russia-ukraine-africa-poland-forests-middle-east-443c8068ea7b5d1d8f6980da6e3879af.

27 "Phenomenon of Illegal Entry in the Area of Southeast Finland Border Guard District." Finnish Border Guard, November 16, 2023. https://raja.fi/en/-/phenomenon-of-illegal-entry-in-the-area-of-southeast-finland-border-guard-district.

28 Higgins, Andrew. "Finland Closes Border with Russia Over Suspected Weaponization of Asylum Seekers." The New York Times, July 12, 2024. https://www.nytimes.com/2024/07/12/world/europe/finland-asylum-russia-border.html.

29 "Belarus Protesters and Migrants: The Crisis at the Poland Border." BBC News, September 5, 2021. https://www.bbc.com/news/world-europe-58474475.

30 Sytas, Andrius. "Lithuania Starts Building First European Wall to Ward Off Migrants from Belarus." Reuters, November 4, 2021. https://www.reuters.com/world/europe/lithuania-starts-building-first-european-wall-ward-off-migrants-belarus-2021-11-04/.

31 LSM English. "Latvian-Belarusian Border Fence Project Completed." Public Broadcasting of Latvia (LSM), July 31, 2024. https://eng.lsm.lv/article/society/defense/31.07.2024-latvian-belarusian-border-fence-project-completed.a563367/.

32 Boulègue, Mathieu. "Arctic Seabed Warfare Against Data Cables: Risks and Impact for US Critical Undersea Infrastructure." Wilson Center, July 30, 2024. https://www.wilsoncenter.org/publication/arctic-seabed-warfare-against-data-cables-risks-and-impact-us-critical-undersea.

33 Hillman, Jonathan E. Securing the Subsea Network A Primer for Policymakers Center for SIS, March 9, 2021. https://www.csis.org/analysis/securing-subsea-network-primer-policymakers

34 Sunak, Undersea Cables: Indispensable, Insecure, 2017.; International Cable Protection Committee, Submarine Cable Protection and the Environment, Issue no. 2, March, 2021.

35 See an overview of recent events impacting regional CUI, see Rickard Lindholm, "Mapping Undersea Infrastructure Attacks in the Baltic Sea," Wilson Center, March 24, 2025, and Heather A. Conley, Sophie Arts, Kristine Berzina, and Frida Rintakumpu, "Protecting Undersea Infrastructure in the North American Arctic: Lessons from Incidents in the Baltic Sea and High North," German Marshall Fund of the United States, October 3, 2024. There are other cases of Russia involvement in cable disruption in the Arctic: against the Lofoten-Vesterålen (LoVe) Ocean Observatory case in 20221, the Svalbard Undersea Cable System case in 2022, and the SHEFA-2 data cable in the Shetland Islands in 2022. In the Baltic Sea, the explosion of the Nord Stream 2 pipeline in 2022 represents a major case study, although without clarity on the responsible party.

36 Schmitt, Benjamin, Alan Riley and Michał Kurtyka. "Underwater Mayhem: Countering Threats to Energy and Critical Infrastructure Across the NATO Alliance and Beyond." Vol. 01. Philadelphia: Kleinman Center for Energy Policy, University of Pennsylvania, 2025.; Hilgenstock, Benjamin and Oleksii Hrybanovskii, and Anatoliy Kravtsev. Assessing Russia's Shadow Fleet: Initial Build-Up, Links to the Global Shadow Fleet, and Future Prospects (KSE Institute, June 2024). https://kse.ua/wp-content/uploads/2024/06/Global-Shadow-Fleet-June-2024.pdf; Caprile, Anna and Gabija Leclerc, "Russia's 'Shadow Fleet': Bringing the Threat to Light." European Parliament, November 2024. https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766242/EPRS_BRI(2024)766242_EN.pdf .

37 Russia, but also China in the South China Sea and towards the Taiwan Strait, and even Houthi rebels in the Red Sea now have a track record of sabotage.

38 Boulègue, Mathieu. "Arctic Seabed Warfare Against Data Cables: Risks and Impact for US Critical Undersea Infrastructure." Wilson Center, July 30, 2024.

39 Kertysova, Katarina and Gabriella Gricius. "Countering Russia's Hybrid Threats in the Arctic." European Leadership Network, August 2023.; NATO Parliamentary Assembly, 2023.

40 It must be noted that nefarious actors can also target CUI support infrastructure such as landing stations as well as carry out cyberattacks against the later.

41 Stensrud, C.J. and A. Østhagen. "Hybrid Warfare at Sea? Russia, Svalbard and the Arctic." Scandinavian Journal of Military Studies 7. No. 1, 2024: 111–130.

42 EU Parliament. 2022.; Wall, Colin and Pierre Morcos. "Invisible and Vital: Undersea Cables and Transatlantic Security." Center for Strategic International Studies, June 11, 2021. https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security

43 Kaushal, Sidharth. "Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure," Royal United Services Institute (RUSI). May 2023. https://www.wilsoncenter.org/publication/arctic-seabed-warfare-against-data-cables-risks-and-impact-us-critical-undersea.

44 Kaushal, Sidharth. "Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure." Royal United Services Institute (RUSI). May 2023. https://www.wilsoncenter.org/publication/arctic-seabed-warfare-against-data-cables-risks-and-impact-us-critical-undersea.

45 Sidharth Kaushal."Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure," Royal United Services Institute (RUSI), May 2023, https://www.wilsoncenter.org/publication/arctic-seabed-warfare-against-data-cables-risks-and-impact-us-critical-undersea; French Ministry of Defense. "Seabed Warfare Strategy.", February 2022.; Kofman, Michael. "Fire aboard AS-31 Losharik: Brief Overview." Russia Military Analysis, July 3, 2019.

46 French Ministry of Defense. "Seabed Warfare Strategy.", February 2022.

47 Jensen, Benjamin. "How to Exorcise Russia's 'Ghost Fleet." Center for Strategic and International Studies (CSIS), January 7,2025. https://www.csis.org/analysis/how-exorcise-russias-ghost-fleet; Nakamura, Hotaka. "The Enemy Below: Fighting against Russia's Hybrid Underwater Warfare." Center for Maritime Strategy, June 29, 2023. https://centerformaritimestrategy.org/publications/the-enemy-below-fighting-against-russias-hybrid-underwater-warfare/ ; Sanger, David E. and Eric Schmitt. "Russian Ships Near Data Cables Are Too Close for U.S. Comfort." The New York Times, October 25, 2015. https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html

48 Kim, Byung Ki. "Moscow's South Pacific Fishing Fleet Is Much More Than It Seems." Heritage Foundation, September 1988.

49 Gardner, Frank. "How Serious is the Russian spy ship move?" BBC News, November 19, 2025. https://www.bbc.com/news/articles/c4gpgj6d4e6o

50 House of Lords International Relations and Defence Committee, "Corrected Oral Evidence: The Arctic." testimony by Dr. Sidharth Kaushal and Dr. Lee Willett, July 5, 2023.

51 Ekwall, Daniel and Thomas Ekström. "The Global Shadow Fleet: Circumventing the Tools of Geoeconomics." Royal Swedish Academy of War Sciences Blog, September 17, 2025. https://kkrva.se/the-global-shadow-fleet-circumventing-the-tools-of-geoeconomics/

52 Saul, Jonathan. "Shadow Tanker Fleet Grows More Slowly as Western Sanctions Target Russian Oil." Reuters, August 13, 2025. https://www.reuters.com/business/energy/shadow-tanker-fleet-grows-more-slowly-western-sanctions-target-russian-oil-2025-08-13/.

53 Walters, Tiara. "Russia's Spoofing Karpinsky: The Ship That Tried to Dock in Estonia Without Leaving St. Petersburg." Daily Maverick, September 23, 2024. https://www.dailymaverick.co.za/article/2024-09-23-russias-spoofing-karpinsky-the-ship-that-tried-to-dock-in-estonia-without-leaving-st-petersburg/.

54 "Putin's Shadow War," documentary series, directed by Boris Benjamin Bertram, produced by DR, NRK, SVT & YLE, 2023. https://www.drsales.dk/programmes/putin-s-shadow-war/.

55 Yorke, Harry. "Revealed: Russia's Secret War in UK Waters." The Times, April 5, 2025. https://www.thetimes.com/uk/defence/article/russia-secret-war-uk-waters-submarines-dpbzphfx5?gaa_at=eafs&gaa_n=AWEtsqcIeHAXGt8YBD2L40tqf2v8MyvW-Alde3ao14y2Gllzqgd_KxORYYMY-QT8V9g%3D&gaa_ts=69a0a7d7&gaa_sig=_BafruB7mEKYtrlbWHnwCRjCQe9gWyYYcRgaZ5g34KfqK-mvm5V1rviNMLrtX52KJshdk9r51G3veogehRH1Tg%3D%3D ; "Royal Navy Monitors Russian Spy Ship Loitering Near NATO Exercise." The Maritime Executive, May 30, 2025.

56 McNamara, Eoin Micheál. "Reinforcing Resilience: NATO's Role in Enhanced Security for Critical Undersea Infrastructure." NATO Review, August 28, 2024. https://www.nato.int/docu/review/articles/2024/08/28/reinforcing-resilience-natos-role-in-enhanced-security-for-critical-undersea-infrastructure/; NATO. "NATO stands up undersea infrastructure coordination cell." February 15, 2023.

57 NATO MARCOM. "NATO focus is on Critical Undersea Infrastructure during series of multidomain exercises with latest autonomous vehicles in Portugal." October 4, 2023.

58 NATO MARCOM. "NATO focus is on Critical Undersea Infrastructure during series of multidomain exercises with latest autonomous vehicles in Portugal." October 4, 2023.

59 NATO. "Commander Task Force Baltic Established." October 22, 2024. https://mc.nato.int/media-centre/news/2024/Commander-Task-Force-Baltic-Established.

60 NATO. "NATO holds first meeting of Critical Undersea Infrastructure Network." May, 23, 2024. https://www.nato.int/cps/en/natohq/news_225582.htm.

61 NATO. "NATO holds first meeting of Critical Undersea Infrastructure Network." May, 23, 2024. https://www.nato.int/cps/en/natohq/news_225582.htm.; McNamara, Eoin Micheál. "Reinforcing Resilience: NATO's Role in Enhanced Security for Critical Undersea Infrastructure." NATO Review, August 28, 2024. https://www.nato.int/docu/review/articles/2024/08/28/reinforcing-resilience-natos-role-in-enhanced-security-for-critical-undersea-infrastructure/

62 "NATO steps up Baltic Sea patrols after subsea infrastructure damage." Naval News, October 19, 2023. https://www.navalnews.com/naval-news/2023/10/nato-steps-up-baltic-sea-patrols-after-subsea-infrastructure-damage/

63 NATO. "NATO launches 'Baltic Sentry' to increase critical infrastructure security." January 14, 2025. https://www.nato.int/cps/en/natohq/news_232122.htm.

64 Willett, Lee. "NATO's Task Force X Baltic Demonstrates Multi-Domain Response to Seabed and Wider Maritime Threats." Naval News, June 19, 2025. https://www.navalnews.com/naval-news/2025/06/natos-task-force-x-baltic-demonstrates-multi-domain-response-to-seabed-and-wider-maritime-threats/.

65 NATO. "NATO TASK FORCE X: Deterring Today and Protecting Tomorrow." January 31, 2025. https://www.act.nato.int/article/nato-task-force-x.

66 NATO. "NATO Conducts Unmanned Surface Vehicle Demonstration in Baltic Sea." February 20, 2025. https://mc.nato.int/media-centre/news/2025/page228602539.

67 Ministry of National Defense of Lithuania, "JEF Response Option activated to address regional critical infrastructure security." November 28, 2023.

68 Ruitenber, Rudy. "British-led force to use AI in tracking Russia's shadow fleet." Defense News, January 7, 2025, https://www.defensenews.com/global/europe/2025/01/07/british-led-force-to-use-ai-in-tracking-russias-shadow-fleet/; Ministry of Defence & Foreign, Commonwealth & Development Office. "Joint Expeditionary Force Activates UK-Led Reaction System to Track Threats to Undersea Infrastructure and Monitor Russian Shadow Fleet." January 6, 2025. https://www.gov.uk/government/news/joint-expeditionary-force-activates-uk-led-reaction-system-to-track-threats-to-undersea-infrastructure-and-monitor-russian-shadow-fleet.

69 van Soest, Henri, James Black, Harper Fine, and Lucia Retter. "Evolving Threats to Critical Undersea Infrastructure: Implications for European Security and Resilience." RAND Corporation, 2025.

70 "Denmark to Intensify Scrutiny of Russia's 'Shadow Fleet' Tankers," Bloomberg, February 5, 2025, https://www.bloomberg.com/news/articles/2025-02-05/denmark-to-intensify-scrutiny-of-russia-s-shadow-fleet-tankers

71 "Denmark Increases Inspections of Shadow Fleet's "Old and Worthless" Ships," The Maritime Executive, October 6, 2025, https://maritime-executive.com/article/denmark-increases-inspections-of-shadow-fleet-s-old-and-worthless-ships.

72 Ministry of Defence and The Rt Hon John Healey MP. "Royal Navy tracking Russian spy vessel in the Channel to keep UK safe." January 22, 2025. https://www.gov.uk/government/news/royal-navy-tracking-russian-spy-vessel-in-the-channel-to-keep-uk-safe; Sabbagh, Dan. "Britain's response to Russian 'spy ship' is game of political messaging - for now." The Guardian, January 24, 2025. https://www.theguardian.com/politics/2025/jan/24/britain-russian-spy-ship-response-political-messaging; "Royal Navy Monitors Russian Spy Ship Loitering Near NATO Exercise." The Maritime Executive, May 30, 2025. https://www.maritime-executive.com/article/royal-navy-monitors-russian-spy-ship-loitering-near-nato-exercise.

73 NATO. "NATO Defence Ministers launch initiative to enhance maritime surveillance capabilities." October 12, 2023.; Braca, Paolo. "Multi-Domain Situational Awareness: Seabed to Space Situational Awareness (S3A)." NATO Science and Technology Organization, Centre for Maritime Research & Experimentation, March 2023.

74 Paul van Hooft, Davis Ellison and Frederik Mertens. "Maritime Security in a Time of Renewed Interstate Competition: Navigating the Royal Netherlands Navy through the Geopolitical and Technological Challenges and Threats in the Euro-Atlantic and Indo-Pacific Regions." The Hague Center for Strategic Studies, January 2024.

75 For instance, AI-enabled fiber sensing solutions are now increasingly able to detect and identify the signature of vessels sailing with their AIS transponders switched off.

76 NATO. "NRV Alliance Detects Undersea Threats in Baltic First." July 9, 2025. https://www.cmre.nato.int/anchor-alert-nrv-alliance-detects-undersea-threats-in-baltic-first/.

77 "Baltic Sea Demonstration Showcases Saildrone Capabilities for NATO Task Force X Baltic." SailDrone, July 7, 2025. https://www.saildrone.com/media-room/press-releases/nato-task-force-x-baltic-sea-demonstration-complete.

78 Kavanagh, C., Franken, J. and He, W, "Achieving Depth: Subsea Telecommunications Cables as Critical Infrastructure." United Nations Institute for Disarmament (UNIDIR), April 23, 2025.

79 Gosselin-Malo, Elisabeth. "NATO drill sends divers, drones to sneak by underwater alarm sensors." Defense News, November 15, 2024. https://www.defensenews.com/global/europe/2024/11/15/nato-drill-sends-divers-drones-to-sneak-by-underwater-alarm-sensors/.

80 Runde, D.F., E.L. Murphy, and T. Bryja. "Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition." Centre for Strategic and International Studies, August 16, 2024.

81 van Soest, Henri, James Black, Harper Fine, and Lucia Retter. "Evolving Threats to Critical Undersea Infrastructure: Implications for European Security and Resilience." RAND Corporation, 2025.

82 Ministry of the Interior Finland, "New legislation to strengthen protection of critical infrastructure and resilience of society," June 12, 2025, https://intermin.fi/en/-/new-legislation-to-strengthen-protection-of-critical-infrastructure-and-resilience-of-society.

83 C. Kavanagh, J. Franken, and J. He, Achieving Depth: Subsea Telecommunications Cables as Critical Infrastructure, (UNIDIR, April 23, 2025).

84 KPMG (2025) Critical Entities Resilience Directive. Compliance insights on ensuring resilience for critical infrastructure. https://assets.kpmg.com/content/dam/kpmg/nl/pdf/2025/services/cer-whitepaper-may-2025.pdf

85 Soldi et al. (2023), op. cit.; EU Parliament (2022), op. cit.

86 C. Kavanagh, J. Franken, and J. He. "Achieving Depth: Subsea Telecommunications Cables as Critical Infrastructure." UNIDIR, April 23, 2025.

87 Ryan (2023), op. cit.; C. Kavanagh. "Wading Murky Waters: Subsea Communications Cables and Responsible State Behaviour." UNIDIR, 2023.

88 Sarah Kuszynski, "The Geopolitics of Undersea Cables: Underappreciated and Under Threat," London Politica, December 2022. C. Kavanagh. "Wading Murky Waters: Subsea Communications Cables and Responsible State Behaviour." UNIDIR, 2023.

89 Trausti Fridbertsson, Njall. "Protecting Critical Maritime Infrastructure – The Role Of Technology, General Report." NATO Parliamentary Assembly, October 7, 2023.

90 International Telecommunication Union (ITU). "International Advisory Body for Submarine Cable Resilience." November 2024. https://www.itu.int/digital-resilience/submarine-cables/advisory-body/,

91 For more information, see Kavanagh (2023)

92 United Nations General Assembly. "Oceans and the Law of the Sea." December 11, 2023. https://docs.un.org/en/a/res/78/69; Kavanagh, C., Franken, J. and He, W. "Achieving Depth: Subsea Telecommunications Cables as Critical Infrastructure." United Nations Institute for Disarmament (UNIDIR), April 23, 2025.

93 Kavanagh, C., Franken, J. and He, W,. "Achieving Depth: Subsea Telecommunications Cables as Critical Infrastructure." United Nations Institute for Disarmament (UNIDIR), April 23, 2025.

94 Milne, (2025), op.cit.; Bryant, (2025), op.cit.; Minchin, (2025), op.cit.

95 Giordano, Elena. "Finnish court dismisses case against crew accused of cutting undersea cables." Politico, October 3, 2025. https://www.politico.eu/article/finnish-court-dismisses-eagle-s-cable-cutting-case/.

96 Helsinki District Court. "District Court Judgment in the Criminal Case Involving the Tanker." October 3, 2025. https://tuomioistuimet.fi/material/sites/oikeus_karajaoikeudet_helsinginkarajaoikeus/tiedotteet/spinbijpv/ratkaisutiedote_R_706-2025-12270_EN.pdf

97 Braw, Elisabeth, "Anchors Away." Foreign Policy, October 10, 2025. https://foreignpolicy.com/2025/10/10/finland-cable-cuting-russian-sabotage/

98 President of the Republic of Finland. "Joint Statement of the Baltic Sea NATO Allies Summit." January 14, 2025. https://www.presidentti.fi/en/joint-statement-of-the-baltic-sea-nato-allies-summit/

99 Department for Transport. "Correspondence: The growing risks to maritime safety." January 26, 2026. https://www.gov.uk/government/publications/the-growing-risks-to-maritime-safety/the-growing-risks-to-maritime-safety

100 NATO. "NATO officially launches new Maritime Centre for Security of Critical Undersea Infrastructure." May 28, 2024. https://mc.nato.int/media-centre/news/2024/nato-officially-launches-new-nmcscui.

101 Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, (Official Journal of the European Union, Dec ember 27, 2022). https://eur-lex.europa.eu/eli/dir/2022/2557/oj,

102 "Commission Recommendation (EU) 2024/779 of 26 February 2024 on Secure and Resilient Submarine Cable Infrastructures." Official Journal of the European Union, March 8, 2024. https://eur-lex.europa.eu/eli/reco/2024/779/oj/eng.

103 European Commission. "EU-NATO Task Force: Final assessment report on strengthening our resilience and protection of critical infrastructure." June 29, 2023.

104 European Union. "The New York Join Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World." September 26, 2024, https://digital-strategy.ec.europa.eu/en/library/new-york-joint-statement-security-and-resilience-undersea-cables-globally-digitalized-world.

105 European Union. "Commission and the High Representative present strong actions to enhance security of submarine cables." February 20, 2025.

106 European Union. "Report on Security and Resilience of EU Submarine Cable Infrastructures, October 23, 2025. https://digital-strategy.ec.europa.eu/en/library/report-security-and-resilience-eu-submarine-cable-infrastructures

107 European Union. "Commission increases submarine cable security with 347 Million Euro investment and new toolbox ." February 5, 2025. https://digital-strategy.ec.europa.eu/en/news/commission-increases-submarine-cable-security-eu347-million-investment-and-new-toolbox

108 Liebetrau, Tobias and Christian Bueger. "Advancing coordination in critical maritime infrastructure protection: Lessons from maritime piracy and cybersecurity." International Journal of Critical Infrastructure Protection, Volume 46, 2024.

109 "Poland and Sweden hold first bilateral military drills in Baltic." Notes from Poland, September 22, 2025. https://notesfrompoland.com/2025/09/22/poland-and-sweden-hold-first-bilateral-military-drills-in-baltic/.

110 Danish Ministry of Climate, Energy and Utilities, "New Cooperation to Strengthen Security Around Critical Infrastructure in the North Sea," April 9, 2024, https://www.kefm.dk/aktuelt/nyheder/2024/apr/nyt-samarbejde-skal-styrke-sikkerheden-omkring-kritisk-infrastruktur-i-nordsoeen-.

111 Sophia Besch and Erik Brown, Securing Europe's Subsea Data Cables, (Carnegie Endowment for International Peace, December 16, 2024), https://carnegieendowment.org/research/2024/12/securing-europes-subsea-data-cables.

112 NATO, "NATO officially launches new Maritime Centre for Security of Critical Undersea Infrastructure," May 28, 2024, https://mc.nato.int/media-centre/news/2024/nato-officially-launches-new-nmcscui.

113 Boulègue, (2024), op. cit.;

114 NATO. "NATO focus is on Critical Undersea Infrastructure during series of multi-domain exercises with latest autonomous vehicles in Portugal." October 4, 2023.

115 Boulègue, Mathieu, Minna Ålander, Charlotta Collén, Edward Lucas, Catherine Sendak, and Krista Viksnins. "Up North: Confronting Artic Insecurity Implications for the United States and NATO." Center for European Policy Analysis, December 5, 2024. https://cepa.org/comprehensive-reports/up-north-confronting-arctic-insecurity-implications-for-the-united-states-and-nato/.

116 Boulègue, Mathieu. "Arctic Seabed Warfare Against Data Cables: Risks and Impact for US Critical Undersea Infrastructure." Wilson Center, July 30, 2024. https://www.wilsoncenter.org/publication/arctic-seabed-warfare-against-data-cables-risks-and-impact-us-critical-undersea.

117 Kavanagh, C., Franken, J. and He, W, "Achieving Depth: Subsea Telecommunications Cables as Critical Infrastructure." United Nations Institute for Disarmament (UNIDIR), April 23, 2025.

118 Hilgenstock, Benjamin, Oleksii Hrybanovskii, and Anatoliy Kravtsev. "Assessing Russia's Shadow Fleet: Initial Build-Up, Links to the Global Shadow Fleet, and Future Prospects." KSE Institute, June, 2024. https://kse.ua/wp-content/uploads/2024/06/Global-Shadow-Fleet-June-2024.pdf; Hilgenstock, Benjamin, Anatoliy Kravtsev, Yuliia Pavytska, and Anna Vlaysuk. "Creating "Shadow-Free" Zones, KSE Institute, October, 2024. https://kse.ua/wp-content/uploads/2024/10/Shadow_free_zones_October_2024_final.pdf; Andrius, Sytas. "Russian 'shadow fleet' to be boarded or sanctioned if it refuses to provide insurance." Reuters, December 17, 2024. https://www.reuters.com/world/europe/russian-shadow-fleet-be-boarded-or-sanctioned-if-it-refuses-prove-insurance-2024-12-17.

119 Petit, Zelie. "Beneath NATO's Radars: Unaddressed Threats to Subsea Cables." Center for Strategic International Studies, December 2, 2024. https://www.csis.org/blogs/strategic-technologies-blog/beneath-natos-radars-unaddressed-threats-subsea-cables

120 Schmitt, Benjamin, Alan Riley and Michał Kurtyka. "Underwater Mayhem: Countering Threats to Energy and Critical Infrastructure Across the NATO Alliance and Beyond." Vol. 01. Philadelphia: Kleinman Center for Energy Policy, University of Pennsylvania, 2025.

121 van Soest, Black, Fine, and Retter (2025), op. cit.

122 At the moment, only cybersecurity-related data sharing in the EU is sufficiently mandated by regulation (The NIS2 Directive (Directive (EU) 2022/2555) to enable real-time monitoring of threats and attacks.

123 Petit, Zelie. "Beneath NATO's Radars: Unaddressed Threats to Subsea Cables." Center for Strategic International Studies (CSIS), December 2, 2024.https://www.csis.org/blogs/strategic-technologies-blog/beneath-natos-radars-unaddressed-threats-subsea-cables; Kavanagh, C., Franken, J. and He, W, "Achieving Depth: Subsea Telecommunications Cables as Critical Infrastructure." United Nations Institute for Disarmament (UNIDIR), April 23, 2025.

124 ICPC, op.cit.

125 van Hooft, Paul, Davis Ellison and Frederik Mertens. "Maritime Security in a Time of Renewed Interstate Competition: Navigating the Royal Netherlands Navy through the Geopolitical and Technological Challenges and Threats in the Euro-Atlantic and Indo-Pacific Regions." The Hague Center for Strategic Studies, January 2024.

126 European Commission and Council of the European Union. "EU Action Plan on Cable Security." Joint Communication, February 21, 2025. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52025JC0009.

127 Wall, Colin and Pierre Morcos. "Invisible and Vital: Undersea Cables and Transatlantic Security." Center for Strategic International Studies, June 11, 2021. https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security

128 Sorgi, Gregorio and Antonia Zimmermann. "Germany backs EU's 'creative' plan to send frozen Russian cash to Ukraine." Politico, September 25, 2025. https://www.politico.eu/article/germany-back-eu-creative-plan-send-frozen-russia-cash-ukraine/.

129 NATO Strategic Communications Centre of Excellence. "*Russia's Strategy in Cyberspace*." (Riga: NATO StratCom COE, 2021), https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf

130 FP Analytics. "*Digital Front Lines: Cross-Cutting Responses to Strengthen Ukraine's Digital Resilience*." Digital Front Lines, 2023, https://digitalfrontlines.io

131 Greenberg, Andy. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *WIRED*, June 28, 2022. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

132 Google Threat Analysis Group. "Sandworm Disrupts Power in Ukraine Using OT Malware." 2023. https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology.

133 CERT-UA. "*APT Activity Report H1 2023*."(Kyiv: State Service of Special Communications and Information Protection of Ukraine, 2023). https://cip.gov.ua/en/news/yak-zminyuyutsya-taktiki-cili-i-spromozhnosti-khakerskikh-grup-uryadu-rf-ta-kontrolovanikh-nim-ugrupovan-zvit

134 Morphisec. "Unveiling UAC-0184: The Remcos RAT Steganography Saga." February 22, 2024. https://www.morphisec.com/blog/unveiling-uac-0184-the-remcos-rat-steganography-saga/.

135 NATO StratCom COE. "*Russia's Strategy in Cyberspace*." (Riga: NATO StratCom COE, 2021). https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf

136 CERT-UA. "*APT Activity Report H1 2024*" (SSSCIP, 2024). https://cip.gov.ua/en/news/sektor-bezpeki-i-oboroni-derzhavni-ta-miscevi-organi-vladi-u-fokusi-uvagi-vorozhikh-khakeriv-kilkist-kiberincidentiv-zrostaye

137 Kramarenko, Danylo and Daria Dmytriieva. "Ukraine Suffers Largest Cyberattack Since Full-Scale Invasion." RBC Ukraine, January 2024. https://newsukraine.rbc.ua/news/ukraine-suffers-largest-cyberattack-since-1734704699.html.

138 Balmforth, Tom. "Russian Hackers Were Inside Ukraine Telecoms Giant for Months, Cyber Spy Chief Says." Reuters, January 4, 2024. https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/.

139 NATO StratCom COE. "*Russia's Strategy in Cyberspace*."

Center for European Policy Analysis HQ
1275 Pennsylvania Ave NW, Suite 400
Washington, DC 20004

info@cepa.org | www.cepa.org