POLICY BRIEF

# Transatlantic Security Institutions and Hybrid Threats: Adaptation, Gaps, and Policy Imperatives

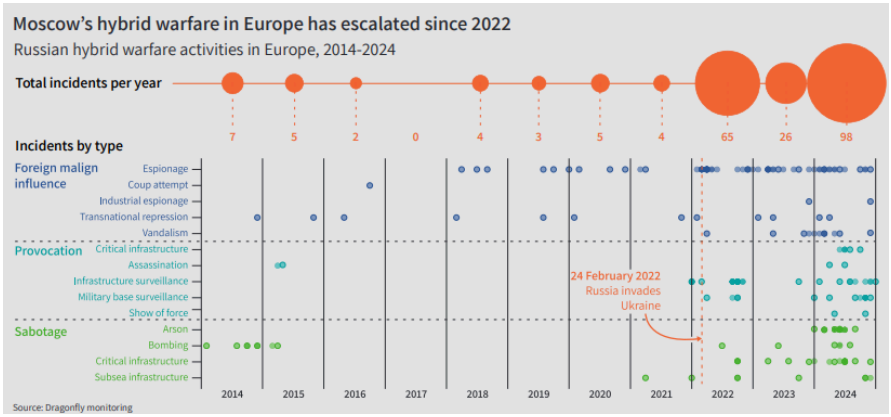
Dr. Mikhail A. Polianskii, Peace Research Institute Frankfurt (PRIF) and Carleton University

November 26, 2025

Russia has significantly escalated its hybrid warfare operations against countries of the political West since 2022. While the North Atlantic Treaty Organization (NATO) and the European Union (EU) have implemented new sanctions regimes, doctrinal frameworks acknowledging hybrid attacks as collective defense triggers, and operational capabilities including rapid response teams, critical gaps persist that undermine institutional effectiveness. Legal ambiguities, attribution challenges, investment imbalances favouring military over resilience spending, fragmented coordination mechanisms, and accelerating disinformation outpace European adaptive capacity. NATO and EU policymakers should work towards adopting a unified doctrine that tackles every operational domain of hybrid warfare, rebalancing defense investment toward societal and infrastructure resilience, and establishing clear operational emergency protocols to address the growing threat.

## Introduction

Europe faces an unprecedented security challenge. Russia no longer relies solely on direct military confrontation but wages systematic war against the continent through hybrid tactics that exploit democratic openness, legal ambiguities, and interconnected vulnerabilities. These attacks – ranging from critical infrastructure sabotage to weaponized migration to coordinated disinformation – operate deliberately below traditional warfare thresholds, complicating collective response and testing institutional cohesion. Understanding the scope and character of these threats, evaluating Europe's adaptive responses, and identifying remaining vulnerabilities is essential for policymakers tasked with defending democratic institutions and critical infrastructure.




Source: https://publications.dragonflyintelligence.com/the-hybrid-war

The scale of escalation is striking. Intelligence assessments document over 200 Russian hybrid attacks between 2014 and 2024, but the pace has dramatically increased: before 2022, Russia targeted an average of three European countries annually; since 2022, that number has climbed to twenty countries per year. The manifestations are concrete and costly.

In October 2023, the Balticonnector gas pipeline connecting Finland and Estonia was severed by a Chinese-flagged vessel with a Russian crew, disrupting energy security for NATO members. In November 2024, two critical undersea communication cables were cut within 24 hours – one linking Finland to Germany, the other Lithuania to Sweden. In 2024, Russian intelligence recruited arsonists online to set fire to a London warehouse storing humanitarian aid for Ukraine. Since 2021, Belarus – acting as Russian proxy – has facilitated thousands of migrants from Iraq, Syria, and Yemen to Poland's border in orchestrated destabilization campaigns.

Russia employs this strategy deliberately. First, hybrid operations provide plausible deniability – severed cables can be attributed to accidental anchor dragging, recruited arsonists to common crime, and damaged railways to general claims of Russophobia. Second, these attacks exploit democratic openness: free movement of people, interconnected infrastructure, civil liberties, and transparent governance create inherent vulnerabilities that authoritarian states weaponize systematically. Third, hybrid attacks operate deliberately below the threshold of traditional warfare. NATO's Article 5, designed in 1949 for Soviet tank formations, was never meant to address disinformation campaigns or cyber operations. Russia exploits this legal and doctrinal gap with precision.

## Institutional Adaptations

---

European institutions have responded with notable innovation, yet critical gaps persist that constrain effectiveness and create exploitable vulnerabilities.

To begin with, NATO's 2024 Washington Summit represented a significant doctrinal moment. The Alliance formally acknowledged that hybrid attacks – including cyber operations and infrastructure sabotage – can trigger Article 5 collective defence, expanding the definition of armed attack from physical invasion to sophisticated coordinated operations across cyber, physical, and information domains.

Operationally, NATO launched two significant missions. Operation Eastern Sentry deployed fighters from Denmark, Germany, and France to Poland and Romania after repeated Russian airspace violations. Baltic

Sentry, launched in January 2025, maintains continuous naval presence with eight NATO member states rotating daily maritime patrols to protect undersea infrastructure critical for energy security and communications. NATO's Cyber Defence Pledge 2.0 mandates that Allies substantially increase cyber capabilities spending and integrate cyber resilience into national defence planning.

The EU, in its turn, established an entirely new sanctions regime in October 2024 specifically targeting hybrid threats, enabling asset freezes and travel bans for actors involved in sabotage, election interference, cyber-attacks, or weaponized migration regardless of whether these constitute traditional warfare. In December 2024, the EU imposed first-ever designations under this regime, sanctioning GRU Unit 29155 and affiliated organizations that were responsible for sabotage and assassinations in Europe.

The EU also operationalized the so-called Hybrid Toolbox, a coordinated response framework encompassing preventive, cooperative, stability, restrictive, and recovery measures. The Hybrid Rapid Response Teams, formally approved in May 2024, deploy civilian experts in cyber defense, critical infrastructure protection, and disinformation detection within days to EU member states or partner countries facing hybrid attack. The first operational deployment occurred from April-May 2025, when teams deployed to Moldova in the run-up to its parliamentary elections.

Finland exemplifies comprehensive adaptation. After the aforementioned Balticonnector sabotage, Finland became the first country to activate the EU Hybrid Toolbox and published a crisis preparedness guide that was downloaded by nearly 500,000 Finnish citizens, amounting to roughly 10 percent of its population. Finland's "total defence" or "comprehensive security" model integrates military, civilian, economic, and psychological resilience with mandatory public preparedness training, where every citizen understands crisis protocols and their specific role in national defense. This comprehensive approach has become a reference point for other European states.

## Persistent Gaps

---

Despite these advances, critical vulnerabilities undermine institutional effectiveness. The legal grey zone remains fundamentally unresolved. When does sabotage constitute an act of war? How many attacks justify Article 5 invocation? What evidence thresholds suffice for attribution? Poland's border crisis illustrates the dilemma: Poland's exclusion zone and pushbacks as a response to Belarussian instrumentalization of migration technically violate EU asylum law and international human rights law. Yet Polish policymakers rightly argue that defensive necessity against a hostile neighbour weaponizing humanitarian crisis justifies exceptional measures. This legal ambiguity creates paralysis precisely when decisive action is needed.

Second, attribution remains persistently difficult. When Chinese-flagged vessels with Russian crews damage Baltic cables, responsibility becomes legally and practically complex. Which actor – China, Russia, or a rogue captain – does one sanction when arresting such a ship? Russia and other malign actors deliberately exploit this ambiguity, recruiting untrained saboteurs via encrypted communications, paying in almost untraceable cryptocurrency, and distancing itself from its "throwaway" operatives. Even though attribution in some cases remains problematic, intelligence assessments can and do identify Russian direction behind such acts with high confidence. Yet, classified intelligence cannot always serve as basis for public sanctions or military response in democracies constrained by rule of law. Russia weaponizes this asymmetry deliberately.

Third, investment imbalance remains problematic. NATO's 2025 Hague Summit mandated 5 percent of GDP defense spending by 2035, but only 1.5 percent targets non-military capabilities – cyber defense, infrastructure protection, societal resilience – while 3.5 per cent funds military hardware. This 3:1 ratio reflects a long-entrenched institutional bias toward kinetic solutions, yet Russia's strategy exploits precisely those domains where military force proves least effective. Most European countries lack comprehensive crisis preparedness frameworks comparable to Finland's model. Few have mandatory preparedness training or public education on disinformation identification. Financing these programs should take precedence over financing conventional weapon systems in the long term, the domain in which NATO is and likely will remain significantly more superior vis-à-vis Russia.

Fourth, coordination mechanisms remain fragmented. The EU Hybrid Toolbox, NATO Counter Hybrid Support Teams, Cyber Diplomacy Toolbox, NIS2 and CER Directives, bilateral defense treaties, national mechanisms and other frameworks are juxtaposed without clear sequencing, responsibility assignment, or coordination procedures. Even though all of these individual measures are of value, more often than not they also overlap or even conflict with each other. Moreover, practical experience remains limited – the EU deployed its first Hybrid Rapid Response Team to Moldova only in 2025; NATO's Counter Hybrid Support Teams have deployed to only two countries since 2019. During actual crisis, institutional confusion could delay response critically. If Canadian critical infrastructure faces a coordinated cyber campaign tomorrow, which mechanism activates first? Who's in charge? How do EU and NATO coordinate? There must be concrete emergency plans that can be pulled out of the shelf in a case like this

Lastly, the information battlefield poses perhaps the most asymmetric challenge. Russia doesn't just sabotage infrastructure. Russia sabotages truth, both domestically and internationally. Moscow's disinformation exploits algorithmic amplification, artificial intelligence deepfakes, and micro-targeted campaigns while operating 24/7 across dozens of languages through thousands of social media accounts. As a response, the EU established and promoted FIMI monitoring mechanisms and strengthened platform obligations through the Digital Services Act, which are now also being prominently used across all European countries. Yet, Russian adaptability consistently outpaces European countermeasures. Russian state actors adjust narratives rapidly without democratic constraints, while European fact-checking operates within legal frameworks protecting free speech and requiring transparent methods. This creates structural advantage for the aggressor. Banning false information and the agencies spreading it risks democracies becoming more authoritarian themselves, creating genuine value conflict with no clear resolution.

## Conclusion

---

The adaptation of transatlantic security institutions demonstrates institutional capacity for rapid innovation when political will exists. NATO's Article 5 evolution, EU sanctions regime establishment, and Hybrid Rapid Response Team deployment prove speed is achievable. Yet gaps remain that Russia deliberately exploits.

Three imperatives demand immediate action.

First, NATO and the EU must jointly develop a unified hybrid warfare doctrine which would include every domain of hybrid warfare – modelled on the Tallinn Manual for cyber operations but integrated across physical, cyber, information, and economic domains – establishing clear collective defense triggers,

evidence thresholds for attribution, and proportional response guidelines. This doctrine should clarify when NATO Allies and EU member states can activate different response mechanisms and establish unified command structures.

Second, NATO Allies and EU member states must rebalance defense investment from the current 3:1 military-to-resilience ratio, targeting at least 2.5 percent of GDP for non-military security capabilities by 2030, with explicit mandates for public preparedness campaigns, critical infrastructure redundancy, mandatory civic education, and public-private threat intelligence sharing. Every European country should develop crisis preparedness frameworks equivalent to Finland's model, ensuring public awareness, individual preparedness training, and institutional coordination.

Third, NATO and the EU must conduct comprehensive audits of overlapping mechanisms and establish unified crisis response frameworks specifying primary responder roles, escalation procedures, mandatory information sharing, and joint annual exercises. These frameworks should create clear decision trees for policymakers during hybrid attacks, eliminating confusion about which institution acts first and how different mechanisms coordinate.

Russia is in a de facto state of war over Ukraine and beyond and its leaders have committed to permanent hybrid warfare. Europe must commit to permanent readiness. The question facing policymakers is not whether adaptation is possible – clearly it is – but whether adaptation can proceed quickly enough. Evolution is slow; hybrid attacks are fast. Closing these gaps through concrete policy action offers realistic path to security in an era of unconventional threats. Without urgent action, the window for effective institutional adaptation will continue to narrow.