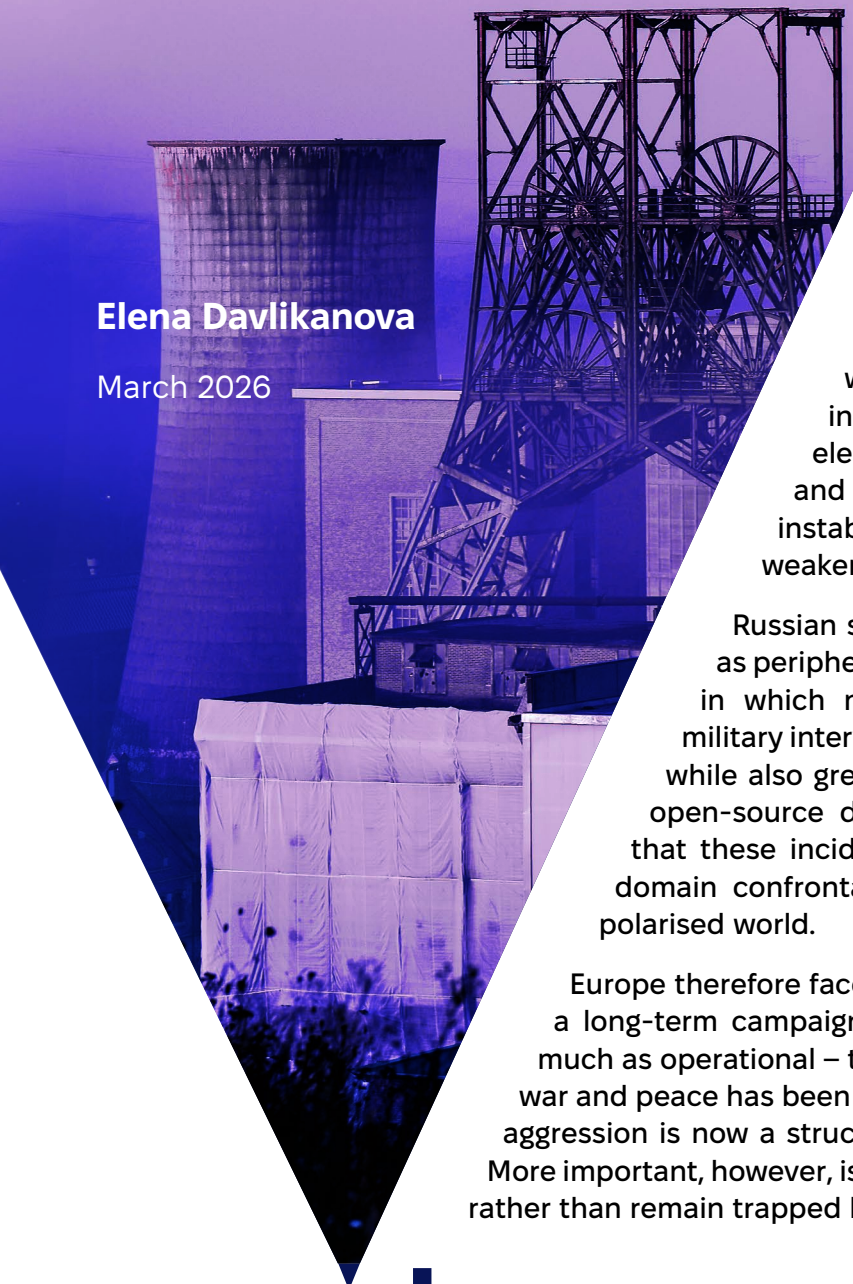
POLICY BRIEF

RUSSIA'S EVERYWHERE WAR AGAINST EUROPE



Elena Davlikanova

March 2026

Russia's campaign against Europe is now best understood not as episodic hybrid disruption, but as a sustained sub-threshold war conducted across the air, maritime, land, cyber and cognitive domains. The full-scale invasion of Ukraine – and especially the atrocities revealed in the de-occupied territories – has closed down much of Moscow's former space for soft power in Europe. The Kremlin has adapted by escalating deniable hostile activity below the threshold of open interstate war. Its actions involve sabotage, maritime incursions, GPS jamming, cyberattacks, election interference, weaponised migration and proxy operations designed to normalise instability, test democratic resilience and weaken European cohesion.

Russian strategic thought treats such methods not as peripheral tools, but as integral to modern conflict, in which non-military means can outweigh direct military intervention by as much as four to one in scope, while also greatly enhancing the effects. Evidence from open-source datasets and analytical trackers suggests that these incidents form a pattern of deliberate, multi-domain confrontation that is likely to persist in a highly polarised world.

Europe therefore faces not a temporary grey-zone problem but a long-term campaign. The central challenge is conceptual as much as operational – to recognise that the dividing line between war and peace has been eroded, and that persistent sub-threshold aggression is now a structural feature of the security environment. More important, however, is need to shift to "a doctrine of reciprocity", rather than remain trapped by the fear of escalation.

epik EUROPEAN POLICY INSTITUTE IN KYIV

Sahaidachnyi Security Center

epik.eu

INTRODUCTION

While much of Europe frames the current security environment as being not at war but no longer at peace with Russia, this characterisation obscures a harsher reality.[1] For more than two decades, Moscow has operated largely through non-kinetic instruments, leveraging energy partnerships, elite networks, media presence, think tank engagement, cultural exposure and covert political financing to preserve influence and shape the environment across the continent. Even after the 2014 annexation of Crimea, Russia retained significant access to European political, business, academic and cultural spheres.

That space narrowed dramatically after February 2022. The full-scale invasion of Ukraine – and particularly the detailed evidence of potential Russian war crimes revealed in Bucha and other de-occupied territories – have led to the collapse of any residual political room for manoeuvre in Europe. Moral and political shock have reshaped the landscape. Formal partnerships have been severed, economic ties are reduced and public tolerance for engagement with Moscow has sharply declined.

In modern conflict the ratio of non-military to military measures can be roughly four to one, making armed forces only one component of a broader strategic campaign, according to Russian General Valery Gerasimov.

In response to this strategic contraction, Russia has not scaled back, but escalated its ambitions – intensifying a blend of sharp and semi-hard power and effectively launching what could be described as an undeclared "everywhere war". This concept captures coordinated hostile actions across all domains – air, land, maritime, space, cyber and cognitive – that are carefully calibrated to remain below the threshold that would trigger NATO's Article 5 collective defence mechanism.

These activities range from sabotage of critical infrastructure and assets on land and at sea to violations of air, land, and sea borders; cyberattacks and elements of EW; hostile space surveillance; and proxy violence, as well as cognitive operations (FIMI), alongside the weaponization of migration. Individually, such incidents might appear ambiguous or isolated; collectively, they reveal a pattern of sustained, multi-domain confrontation.

There is no single consolidated database that captures the full scope of these events. Attribution is often complex, and many cases have been classified or deliberately under-publicised to avoid public panic or diplomatic escalation. Nonetheless, analytical tools – such the Everywhere War Tracker, open-source intelligence aggregation and assessments by institutions such as the International Institute for Strategic Studies (IISS) and Harvard – provide a strategic "helicopter view".[2] Taken together, they demonstrate that Europe is facing not episodic disruption, but a systemic campaign designed to normalise instability as a feature of the security environment and to undermine EU coherence through orchestrated chaos.

A WAR OF DEFINITIONS

While Russia sharpens and scales-up its performance across domains, the West remains absorbed in debates over terminology and in carefully calibrated, non-escalatory responses grounded primarily in deterrence by denial rather than retaliation against sub-threshold operations, especially when confronting a nuclear-armed adversary.

A brief review of the Russian military and strategic literature suggests that its current assault exceeds the conventional concept of hybrid warfare. What is commonly referred to in western discourse as the "hybrid war doctrine" is, in fact, an interpretation of a 2013 article by General Valery Gerasimov in which neither

1. *"Ukraine war briefing: Europe 'no longer at peace' with Russia, says German chancellor,"* The Guardian, September 30, 2025, https://www.theguardian.com/world/2025/sep/30/ukraine-war-briefing-europe-no-longer-at-peace-with-russia-says-german-chancellor

2. Sahaidachnyi Security Center, *"The Everywhere War: Sub-Threshold Warfare Tracker,"* https://sahasec.org/tracker/

"hybrid" nor "doctrine" appears.[3]

The text, presented as an analytical reflection on contemporary conflict, offers several forward-looking observations on the shift to high-precision strikes and the possible emergence of fully robotic military formations capable of conducting independent combat operations, including on the basis of AI. It argues that remote, non-contact engagement with the enemy is becoming the principal means of achieving tactical and operational objectives, striking enemy targets throughout the full depth of its territory.

Interestingly, it starts with a reference to the so-called colour revolutions, which Moscow regularly frames as externally orchestrated regime-change operations. The Arab Spring is interpreted as "a typical war of the 21st century" that demonstrates how externally influenced political movements can rapidly destabilise otherwise stable states, turning them into arenas of armed conflict, foreign intervention, humanitarian crises and civil war. The US-led operation in Libya is cited as another example.

Gerasimov argues that the line between war and peace has become increasingly blurred, as conflicts often unfold without a formal declaration. He emphasises the growing role of non-military means – using political, economic, informational, humanitarian and other instruments – that in some cases exceed the effectiveness of weapons. Direct military intervention tends to occur only at a later stage, frequently under the guise of peacekeeping or crisis management, to secure the final outcome. He suggests that in modern conflict the ratio of non-military to military measures can be roughly four to one, making armed forces only one component of a broader strategic campaign.

As part of its cognitive warfare, Russia continues to project the illusion of military invincibility to fuel fear and persuade the West to draw more self-inflicted red lines.

Particular attention is given to information confrontation, the manipulation of public opinion, the destabilisation of societies from within and exploitation of the "protest potential" of populations. Overt military force – frequently presented as peacekeeping or crisis response – is introduced only at a later stage, primarily to consolidate and finalise the desired outcome of the conflict.

When discussing new forms and methods of warfare, Gerasimov argues that Russia's own experience should not be forgotten, highlighting the use of partisan formations during World War II and counterinsurgency operations in Afghanistan and Chechnya, where tactics based on surprise, rapid manoeuvre and the effective use of tactical airborne assaults and flanking detachments were developed to pre-empt the enemy and inflict significant losses. The principles outlined in the article were later reflected in Russia's own operations in Crimea and the Donbas, where non-military pressure, information operations, proxy actors and conventional force were synchronised in a unified strategic approach.

Interestingly, during the Civil War of 1917–1922, Russia used similar methods to reassert control over newly independent states that had emerged after the October Revolution. Pro-communist uprisings were fomented, Moscow-backed alternative authorities were proclaimed and these bodies then formally requested Russian assistance. Intervention was framed as the defence of "working people" and legitimate governments against bourgeois nationalists, and this was accompanied by intensive ideological and information campaigns discrediting national and democratic movements.

European examples include Hungary in 1956 and Czechoslovakia in 1968, when pro-Soviet elements depicted reformist leaders as 'counter-revolutionaries' and, especially in the Czechoslovak case, helped Moscow frame the ensuing Warsaw Pact interventions as 'fraternal assistance' requested from within the ruling party. Intervention was thus framed not as an invasion, but as support for "legitimate

3. Academy of Military Sciences (Russia), "*Materials of the General Assembly of the Academy of Military Sciences, January 26, 2013,*" no. 1 (42), 2013, https://www.avnrf.ru/attachments/article/534/AVN-1(42)_maket_001-184.pdf

socialist authorities" defending socialism against bourgeois nationalism and western subversion.

By 1991, the Soviet Union was notorious for its hybrid and cognitive warfare, better known as 'active measures', albeit without modern technological tools.[4] Although the Soviet Union ultimately failed to outlast the West economically, the spirit of confrontation endured beyond an initial period of détente and persisted despite repeated efforts by successive US administrations and EU countries to normalise relations.

Modern Russia openly signals continuity with its security service lineage In September 2023, Sergei Naryshkin – Director of Russia's Foreign Intelligence Service (SVR) and former Speaker of the State Duma – oversaw the unveiling of a monument to Felix Dzerzhinsky, the founder of the Soviet secret police at SVR headquarters in Moscow. The monument faces north-west – symbolically towards Europe and the North Atlantic, reflecting the traditional focus of Soviet and Russian foreign intelligence on the western strategic direction.

Gerasomov only hints at regular western implementation of non-kinetic methods of warfare. However, in the same 2013 collection of materials where Gerasimov's article was published, Belarusian Major General Pavel Tikhonovsky argued that recent conflicts demonstrate how strategic objectives can be achieved through indirect actions that precede the use of force.[5] He framed this as the practical application of western concepts of "low-intensity conflict", interpreting political destabilisation, information campaigns and internal unrest – often associated with events like the Arab Spring – as preparatory phases of modern warfare.

While many Western analysts focus on the degradation of Russia's armed forces as a constraint on its ability to attack Europe, since early 2026, Russian information networks have been promoting the idea of a so called Narva People's Republic in Estonia's predominantly Russian speaking border city of Narva, echoing narratives used ahead of Russia's intervention in eastern Ukraine in 2014.[6] The campaign is centred on a small cluster of Telegram, VKontakte and TikTok channels created in 2025 but activated in February and March 2026. These call for the separation of Narva and Ida Virumaa from Estonia and the establishment of a "people's republic" under the slogan "We are waiting for Russia". These accounts circulate separatist symbols, "state flags" and military insignia, and urge supporters to distribute leaflets, carry out sabotage and arm themselves to resist the Estonian state, suggesting that Russian forces will come to their aid.

The scope of means applied in the conflict with Europe exceeds a conventional interpretation of hybrid war.[7] The Foreign Policy Research Institute introduced the term nontraditional warfare to emphasise the joint nature of the strategic methods of political warfare and irregular warfare, contrasting it with big or small conventional war. The issue here is the classical interpretation of irregular warfare understood as a fight by state and non-state actors. Moreover, the non-conventional dimension of war in these terms was explicitly articulated by Sun Tzu, making it less a novel innovation than a technologically upgraded continuation of a long-standing strategic tradition.

For the sake of analytical clarity, this paper uses the term sub-threshold warfare and the synonymous expression, everywhere war, to describe hostile, multi-domain activities that do not trigger a formal declaration of war and are often plausibly deniable, conducted by state or non-state actors below the threshold of conventional armed conflict. Related concepts include the "grey zone" between peace and war, "phase zero" operations and the notion of a "shadow war".[8] Hopefully, the academic debate over terminology will conclude before Russia's undeclared war on Europe enters its next phase.

4. *Sovetskie aktivnye meropriyatiya: doklad ob aktivnykh meropriyatiyakh i propagande, 1986–1987* (New York: U.S. Department of State, 1987), https://vtoraya-literatura.com/pdf/sovetskie_aktivnye_meropriyatiya_ch1_1987__ocr.pdf

5. Academy of Military Sciences (Russia), *"Materials of the General Assembly of the Academy of Military Sciences, January 26, 2013,"* no. 1 (42), 2013, https://www.avnrf.ru/attachments/article/534/AVN-1(42)_maket_001-184.pdf

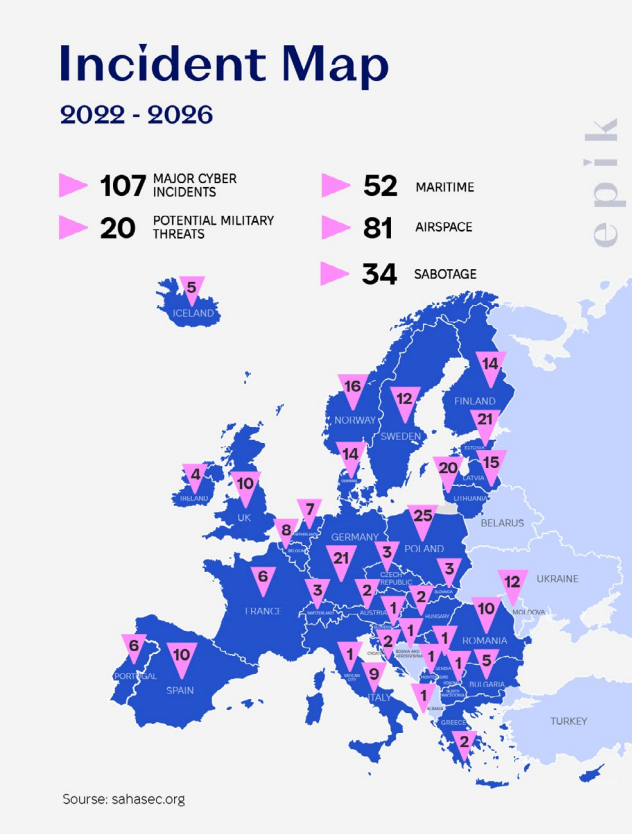
6. "Russia Begins Propaganda Campaign to Create a 'Narva People's Republic' in Estonia," Militarnyi, accessed March 16, 2026, https://militarnyi.com/en/news/propaganda-narva-people-s-republic-estonia/

7. Philip Wasielewski, *"The Constant Fight: Intelligence Activities, Irregular Warfare, and Political Warfare,"* Foreign Policy Research Institute, June 20, 2023, https://www.fpri.org/article/2023/06/the-constant-fight-intelligence-activities-irregular-warfare-and-political-warfare/

8. Sam Greene, Andrei Soldatov, and Irina Borogan, *War Without End: Russia's Shadow Warfare*, Center for European Policy Analysis, November 19, 2025, https://cepa.org/comprehensive-reports/war-without-end-russias-shadow-warfare/

DOCUMENTING THE UNDECLARED: MAPPING SUB-THRESHOLD WARFARE IN EUROPE

Many Russia-linked incidents are difficult to attribute in real time. Some go unreported or remain non-public for security and public order-related reasons. The diversity of categories makes comprehensive tracking inherently complex, while the volume of incidents in certain categories is so high that the authorities deprioritise them or cease systematic tracking altogether. This represents a key analytical challenge. In its report, "The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure", the International Institute for Strategic Studies documents about 100 incidents since 2018, showing a sharp increase that began in 2022 and peaked in 2024.[9]



According to reports on the Russian crime–terror nexus by the International Center for Counter-Terrorism (ICCT) and GLOBSEC, the number of recorded cases between February 2022 and February 2026 had reached 151.[10] Their report presents a dataset of kinetic activities from assassination attempts to assaults, abductions, arson and explosive attacks, acts of sabotage and vandalism, and public disturbances. The focus on Russia's "single-use" agents in Europe – often socially marginalised individuals with criminal backgrounds – shows how Moscow has made criminality a core pillar of its undeclared warfare.

An interactive tool by the Sahaidachnyi Security Center, The Everywhere War: Sub-Threshold Warfare Tracker, paints a detailed picture of Russia's activities since 2022 in five major categories: potential military threats, sabotage, maritime incidents, airspace violations and cyber operations.[11] Within these categories, the tracker records sub-categories such as border base construction, military drills, relocation of nuclear warheads and launchers, troop and weapon transfers; sabotage against critical infrastructure, industrial and economic facilities, and military targets; maritime intrusions by shadow fleet vessels, submarines and warships; and airspace violations involving aircraft, drones and missiles. There are 294 incidents listed in total.

The geography of recorded incidents extends beyond Europe to North America, underscoring the transatlantic scope of Russia's sub-threshold campaign and demonstrating deliberate diversification of efforts. Although this analysis does not extend beyond the transatlantic space, it is safe to say that Russia is also actively employing sub-threshold methods in Latin America, Africa and Asia. For example, Moscow is blending disinformation from state media and private military companies, cyber operations and arms deals to shape political outcomes, weaken western influence and secure access to resources and strategic footholds, while avoiding open interstate conflict.

According to the Tracker metrics, and in line with the findings of GLOBSEC and the ICCT report, Poland is the most affected country, followed

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

10. Kacper Rekawek et al., *Update of Russia's Crime-Terror Nexus: Criminality as a Tool of Hybrid Warfare in Europe*, GLOBSEC, February 24, 2026, https://www.globsec.org/publication/update-russia-crime-terror-nexus-hybrid-warfare-europe/

11. Sahaidachnyi Security Center, *"The Everywhere War: Sub-Threshold Warfare Tracker,"* https://sahasec.org/tracker/

by Germany, the USA and a selection of Nordic-Baltic Eight states. In the US case, cyberattacks are the most common. However, the kinetic component is significant in all countries, involving airspace and maritime space violations, as well as sabotage.

ELECTRONIC WARFARE

However, this is, unfortunately, only a glimpse through the keyhole. Finland documented nearly 2,800 GPS jamming incidents at airports in 2024, compared to only about 200 in the previous year.[12] Older, non-GPS based, radio navigation systems had to be installed at airports in eastern Finland in 2024, where flights had regularly had to be cancelled due to constant GPS jamming.[13]

Older, non-GPS based, navigation systems had to be installed at airports in eastern Finland, where flights had regularly had to be cancelled due to constant GPS jamming.

In northern Norway's Finnmark region, GPS signal jamming has become so frequent that the Norwegian Communications Authority (Nkom) no longer requires every incident to be recorded.[14] Disruption intensified after Russia's invasion of Ukraine and 294 days of interference were reported in 2023.

Since 2023, disruption of GPS and other global navigation satellite system (GNSS) signals has spiked throughout the Baltic Sea region. Between January and April 2025, nearly 123,000 flights over Poland, the Baltic states, Finland and Sweden were affected by Russian GPS jamming and spoofing from transmitters in Kaliningrad, St Petersburg, Smolensk and Rostov.[15] In 2025, the Estonian authorities reported the deployment of additional Russian signal-jamming systems near Kingisepp, just 20 kilometres from the Estonian border.

On Lithuania's initiative, the transport and digital affairs ministers of 13 EU member states, including three Baltic and two Nordic states, sent a joint letter to the European Commission calling for immediate, coordinated action against GNSS interference originating from Russia and Belarus, while also urging faster deployment of interference-resistant services, stronger protection of critical infrastructure, and enhanced safety and security across Europe.[16]

Several affected states elevated the issue of persistent GNSS (GPS) interference to the United Nations system, where the International Civil Aviation Organisation (ICAO) formally addressed it at its 42nd Assembly in October 2025. Delegates adopted resolutions condemning repeated GNSS radio frequency interference originating from the territory of the Russian Federation (and North Korea) as violations of the 1944 Chicago Convention on International Civil Aviation and called on Russia to cease such actions, explicitly framing the disruptions as a safety and security threat to international civil aviation rather than a technical anomaly.[17]

AIRSPACE VIOLATIONS

Since 2024, suspected Russian drone operations have repeatedly paralysed European airports, causing temporary closures in Poland in response to a September 2025 violation of airspace by 23 reconnaissance and decoy drones, and lengthy shutdowns at major hubs such as Copenhagen,

12. Yle News, *"USU: GPS Interference Affecting Almost All Finnish Airports,"* January 14, 2025, https://yle.fi/a/74-20136751

13. Yle News, *"Eastern Finland Airports Bring Back Radio Navigation Systems Due to GPS Interference,"* November 7, 2024, https://yle.fi/a/74-20123117

14. Trine Jonassen and Birgitte Annie Hansen, *"Stops Registering GPS Disruptions in Finnmark, Northern Norway,"* *High North News*, September 27, 2024, https://en.highnorthnews.com/politics/stops-registering-gps-disruptions-in-finnmark-northern-norway/212107

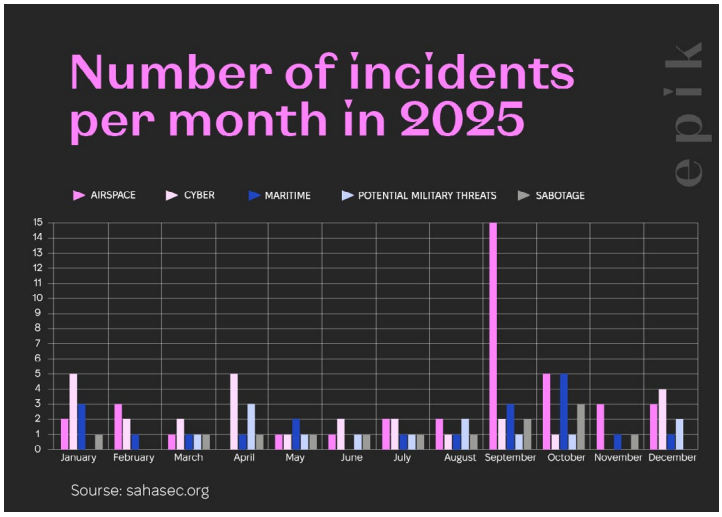
15. *"123,000 Flights Disrupted by Russian Signals – Threatening Aviation Safety,"* SVT News, September 5, 2025, https://www.svt.se/nyheter/inrikes/123-000-flyg-storda-av-ryska-signaler-hotar-flygsakerheten

16. *"13 Member States, Including Latvia, Call for EU Response to GNSS Interference,"* The Baltic Times, June 10, 2025, https://www.baltictimes.com/13_member_states__including_latvia__call_for_eu_response_to_gnss_interference/

17. International Civil Aviation Organization, *"ICAO Assembly Condemns GNSS Radio Frequency Interference Originating from the DPRK and the Russian Federation,"* October 3, 2025, https://www.icao.int/news/icao-assembly-condemns-gnss-radio-frequency-interference-originating-dprk-and-russian

Oslo, Munich and Liège, affecting tens of thousands of passengers.[18]

In most cases, the drones have not been officially attributed, but independent analysts see these incidents as probable elements of Russia's sub-threshold warfare, intended to test NATO air defences and normalise the use of drones to disrupt civil aviation.[19] These attacks have an immediate economic impact: a four-hour disruption at Copenhagen Airport costs €6.5 to €15 million.



Since September 2025, violations of European airspace by Russian aircraft have occurred on an almost monthly basis. Sweden, Norway, Moldova, Germany, all three Baltic states, Ireland, Poland and Denmark have reported drone-related incursions, while Romania recorded the highest number of such incidents in the past year. Since 2023, there have been at least eight cases of Russian missiles entering Polish or Moldovan airspace.

In late 2025, the Lithuanian authorities faced a wave of meteorological balloon incursions launched from neighbouring Belarus, used to transport contraband cigarettes into the country. These led to repeated temporary closures of airspace and of Vilnius Airport, and a declaration of a state of emergency amid significant disruption to civilian flights.[20] Lithuanian officials characterised the incidents as a hybrid security threat while Belarus declared that Europe was launching a hybrid war against it.

MARITIME SPACE VIOLATIONS

Between 2022 and 2025, the Russian Federation conducted more than 50 documented maritime incursions in European waters, primarily in the Baltic Sea, the North Sea and around the United Kingdom. Since mid-2024, violations of European maritime space by Russian warships, submarines and suspicious commercial vessels have been registered on an almost monthly basis.

These operations form part of a coordinated, multi-domain intelligence campaign targeting NATO's eastern flank and critical sea lines of communication. Commercial vessels are used as launch platforms for reconnaissance drones, which exploit gaps in coastal radar and electronic warfare coverage.[21] The Danish Straits are strategically central. Russian naval and submarine activity there functions as both surveillance and a rehearsal for potential breakout operations into the North Sea.

A central instrument in this campaign is Russia's "shadow fleet" – at least 1337 marine vessels – that European security authorities warn enable espionage/sabotage and other proximity operations near critical undersea infrastructure.[22] Of this broader fleet, 544 vessels had been sanctioned by the EU as of the end of 2025, but shadow fleet traffic continues to generate up to $100 billion in revenue each year in support of the Russian economy, which only prolongs the war of attrition against Ukraine.[23]

18. Hromadske, *"Poland Shoots Down Russian Drones, Closes Airports, Calls Up Reservists,"* September 10, 2025, https://hromadske.ua/en/war/251046-poland-shoots-down-russian-drones-closes-airports-calls-up-reservists

19. Maira Butt, *"Airspace Violations and Drone Incursions: How Putin Is Probing NATO's Defences,"* The Independent, October 31, 2025, https://www.independent.co.uk/news/world/europe/russia-fighter-jets-nato-airspace-ukraine-war-b2855852.html

20. Euronews, *"Lithuania Declares State of Emergency Over Balloon Incursions from Belarus,"* December 9, 2025, https://www.euronews.com/2025/12/09/lithuania-declares-state-of-emergency-over-balloon-incursions-from-belarus

21. *"The Flashing Red Threat from Russia's Dark Fleet,"* The Economist, September 30, 2025, https://www.economist.com/international/2025/09/30/the-flashing-red-threat-from-russias-dark-fleet

22. *"Shadow Fleet,"* War & Sanctions Portal (GUR), accessed March 19, 2026, https://war-sanctions.gur.gov.ua/en/transport/shadow-fleet

23. *"EU Sanction Designated Vessels,"* Danish Maritime Authority, last updated December 18, 2025, https://www.dma.dk/growth-and-framework-conditions/maritime-sanctions/sanctions-against-russia-and-belarus/eu-vessel-designations

"Ghost Busters: Options for Breaking Russia's Shadow Fleet," Center for Strategic and International Studies, December 15, 2025, https://www.csis.org/analysis/ghost-busters-options-breaking-russias-shadow-fleet

The response has been limited. Fewer than 100 vessels have been arrested since 2022.[24] Ukraine has had to resort to "kinetic sanctions".[25] According RUSI, Ukrainian operations sank or significantly damaged 11 vessels associated with Russia's shadow tanker fleet in 2025.

CYBER OPERATIONS

Russia is host to a complex and dynamic cyber ecosystem made up of formal military and intelligence units, state-aligned cybercriminal networks, coerced or state-encouraged technology developers, patriotic hacker groups (both state-linked and independent) and private military companies that offer offensive cyber, signals intelligence (SIGINT) and related digital capabilities, all of which operate with varying degrees of Kremlin influence.[26] This environment enables large-scale cybercrime to originate from Russian territory and allows the state to mobilise or tolerate specific actors that serve strategic objectives in hybrid conflict.

European intelligence agencies warn that Russian services are acquiring property near military bases, ports, and critical infrastructure across at least 12 European countries, creating "Trojan horse" assets for surveillance, sabotage, and covert operations.

Russian cyberattacks against NATO countries have increased by about 25% in the past year.[27] While Ukraine is the most targeted, 20% of attacks were directed at the United States, 12% at the United Kingdom and 6% at Germany. Belgium, Italy, Estonia, France, the Netherlands and Poland each accounted for a smaller but significant share of Russian cyber operations.

Sweden, which is not a primary focus of Russian cyber efforts, experienced one of its most severe cyberattacks in recent memory in August 2025. The centralised IT service provider Miljödata was hit by a targeted ransomware assault, disrupting digital operations in about 80% of the country's municipal administrations.

Earlier the same year, pro-Russian hackers breached the control system of the Risevatnet dam in Bremanger, Norway, manipulating water flow valves for several hours.[28] This low-tech attack, which targeted a public-facing interface, was confirmed by Norwegian intelligence as a deliberate, politically motivated act by Russian-affiliated actors to create fear.

Europol's 2025 EU Serious and Organised Crime Threat Assessment highlights that criminal networks are highly active in the cyber domain and increasingly entangled with externally driven hybrid threats, carrying out a broad spectrum of illicit activities and tactics, often acting as proxies.[29] Although financial profit remains their primary incentive, their operations frequently advance, directly or indirectly, the geopolitical objectives of the actors behind these hybrid campaigns.

WEAPONISED MIGRATION, COGNITIVE WARFARE AND ELECTION INTERFERENCE

All three Baltic states, Finland and Norway have faced weaponised migration since 2021.

24. *"Ukraine Has Arrested 68 Vessels of the Russian Shadow Fleet in the Last Five Years,"* USM Media, December 2025, https://en.usm.media/ukraine-has-arrested-68-vessels-of-the-russian-shadow-fleet-in-the-last-five-years/

25. *"Ukraine's 'Kinetic Sanctions' Change the Game,"* Royal United Services Institute (RUSI), January 29, 2026, https://www.rusi.org/explore-our-research/publications/commentary/ukraines-kinetic-sanctions-change-game

26. *"Confronting Russia's Cyber Power: Reassessing Assumptions, Sizing Up the Threat, and Building a Proactive Response,"* Atlantic Council, May 2, 2025, https://www.atlanticcouncil.org/wp-content/uploads/2025/05/Confronting-Russias-Cyber-Power.pdf

27. *"Russian Cyber-Attacks Against Nato States Up by 25% in a Year, Analysis Finds,"* The Guardian, October 16, 2025, https://www.theguardian.com/world/2025/oct/16/russian-cyber-attacks-against-nato-states-up-by-25-in-a-year-analysis-finds

28. *"Russian Cyberattack Opens Floodgates of Dam in Norway,"* EU News, August 14, 2025, https://www.eunews.it/en/2025/08/14/russian-cyberattack-opens-floodgates-of-dam-in-norway/

29. *"The Changing DNA of Serious and Organised Crime: EU Serious and Organised Crime Threat Assessment (EU SOCTA) 2025,"* Europol, March 24, 2025, https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

Approximately 1,300 undocumented migrants, primarily from the Middle East and Africa, entered Finland between September 2023 and January 2024.[30] Since August 2021, Lithuania has prevented 24,508 illegal crossings and Latvia 39,724, often involving repeated attempts facilitated by the Belarusian authorities and affiliated travel agencies. In 2025, Poland faced 150 to 170 migrant-smuggling incidents per day along its border, many of which the authorities believe were organised by foreign state authorities in cooperation with criminal networks operating in the Middle East and Turkey.[31] Four tunnels from Belarus into EU territory, probably used for migrant smuggling, were discovered in 2025, underscoring the operational dimension of the pressure campaign.[32]

The effects extend beyond border security into domestic politics. Ahead of Poland's May 2025 presidential election, social media outlets were flooded with disinformation amplifying the migration issue, including fabricated videos of migrants entering Kraków at night and false claims that Germany was relocating migrants into Poland for financial reasons. Major anti-migrant messages focused on aid to Ukraine, the negative impact of Ukrainian migrants on Polish budget allocations and the well-being of Polish families, and the overall threat to the Polish economy, especially the agricultural sector, should Ukraine join the EU.

In April 2022, during France's presidential election, the authorities and cybersecurity firms identified coordinated disinformation networks to amplify pro-Kremlin narratives.[33] In 2023–2024, the "Doppelgänger" operation cloned major European media outlets to influence public debate ahead of the June 2024 elections to the European Parliament, leading to EU sanctions in July 2024 against individuals and entities linked to the campaign.[34] Both operations were coordinated by John Mark Dougan – a key architect of Kremlin campaigns in Europe.[35]

In March–April 2024, the Czech authorities dismantled the "Voice of Europe" network in Prague, alleging that it channelled Russian funds to influence politicians in several EU member states ahead of the European elections.[36] In January 2024, Germany attributed cyberattacks on SPD infrastructure to the Russia-linked APT28 group, months before key regional and European elections.[37]

Continuously playing defence is an almost guaranteed path to defeat, especially amid rapid technological change and increasingly sophisticated cognitive warfare.

Since 2022, Moldova has faced repeated, documented attempts at electoral interference attributed to Russia-linked actors. Ahead of the November 2023 local elections and the October 2024 presidential election and EU accession referendum, the authorities uncovered voter-bribery schemes, illicit financing networks connected to fugitive oligarch Ilan Shor, coordinated disinformation campaigns and organised efforts to mobilise

30. *"Finland Investigates Illegal Migrant Crossings from Russia,"* Odessa Journal, November 20, 2023, https://odessa-journal.com/finland-investigates-illegal-migrant-crossings-from-russia

31. *"Russia Using Criminal Networks to Drive Increase in Sabotage Acts, Says Europol,"* The Guardian, March 18, 2025, https://www.theguardian.com/technology/2025/mar/18/russia-criminal-networks-drive-increase-sabotage-europol

32. *"Weaponized Mass Migration: A Security Risk to Europe and the United States,"* Foundation for Defense of Democracies, February 10, 2026, https://www.fdd.org/analysis/2026/02/10/weaponized-mass-migration/

33. *"Russian Disinformation Network Intensifies in France,"* Center for Countering Disinformation (CPD), December 4, 2025, https://cpd.gov.ua/en/international-threats-en/europe/russian-disinformation-network-intensifies-in-france/

34. *"Russia's Doppelgänger: The Secret Operation That Cloned Europe's Biggest News Brands to Wage a Disinformation War,"* The Geopolitics Report (Medium), February 16, 2026, https://medium.com/the-geopolitics-report/russias-doppelg%C3%A4nger-the-secret-operation-that-cloned-europe-s-biggest-news-brands-to-wage-a-5b16a6539239

35. *"EU Sanctions Tracker – Subject 180200,"* European Commission (data.europa.eu), accessed March 19, 2026, https://data.europa.eu/apps/eusanctionstracker/subjects/180200

36. *"A Spate of Scandals: Europe's Response to Foreign Interference,"* German Marshall Fund of the United States, May 8, 2024, https://www.gmfus.org/news/spate-scandals-europes-response-foreign-interference

37. *"Cyber Attacks Traced to Russian Military Intelligence Agency,"* *Federal Ministry of the Interior and Community*, May 3, 2024, https://www.bmi.bund.de/SharedDocs/kurzmeldungen/EN/2024/05/schutzmassnahmen-cyberangriffe-en.html

unrest.[38] In 2025, the security services conducted further raids targeting what they described as Russia-backed destabilisation plots ahead of parliamentary elections.

In 2023, Bucharest expelled Russian diplomats over espionage allegations, while the intelligence services reported intensified disinformation campaigns aimed at eroding public trust in NATO membership, EU alignment and Romania's support for Ukraine. Russian interference in the 2024 presidential race led Romania's Constitutional Court to annul the results of the first round and cancel the planned second-round runoff, forcing the entire election to be rerun.

These are just few examples of everyday cognitive offense, orchestrated by Russia to influence the West through its own and foreign television channels, online platforms and messengers, as well as cultural events, academic cooperation, branches of the Russian Orthodox Church, gamification and AI fake videos, among other things.

Moreover, as part of its cognitive warfare, Russia continues to project the illusion of military invincibility to fuel fear and persuade the West to draw more self-inflicted red lines. Since 2022, Russia has intensified the reconstruction and expansion of its military infrastructure along its borders with EU and NATO member states. Satellite imagery and open-source reporting highlight renewed activity at Soviet-era garrisons in Petrozavodsk and new construction in Kandalaksha near Finland, as well as upgrades to missile and radar facilities in Kaliningrad, and infrastructure reconstitution near Pskov and Luga close to the Baltic states.

SABOTAGE

A survey of European security experts conducted by the European Union Institute for Security Studies (EUISS) and the European University Institute identified a disruptive hybrid attack on EU critical infrastructure as the single most likely high-impact security risk for 2026.[39] Experts ranked scenarios such as subsea cable sabotage, power grid disruptions or similar attacks on critical systems above conventional military escalation, reflecting growing concern that Europe's most serious vulnerabilities lie in interconnected infrastructure rather than traditional battlefield threats.

This trend has been clear since 2023, which marked an increase in suspected Russian sabotage operations and preparatory activities targeting critical infrastructure, military logistics and politically sensitive targets. While the EUISS report identified about 100 sabotage incidents since 2018, the German authorities registered approximately 320 suspected sabotage incidents in 2025.[40] Meanwhile, the total number could be in the thousands according to sources.

Critical infrastructure has been the primary focus, particularly rail networks, ports, energy grids, telecommunications cables and facilities connected to military logistics. Documented incidents range from cable cutting along Deutsche Bahn rail lines and arson attacks on depots to suspected tampering with railway signalling systems. Operations frequently rely on third country nationals or locally recruited operatives, enabling plausible deniability and sometimes allowing disinformation narratives to emerge around the identity of the perpetrators.

The pattern of incidents is uneven across Europe. Poland appears to be the most frequently targeted country, followed by France, Lithuania, Germany, the United Kingdom and Estonia – a distribution broadly aligned with the level of political and military support these states provide to Ukraine.

Transport infrastructure has been a regular target. In July 2024, coordinated arson attacks disrupted sections of France's high-speed rail network hours before the opening ceremony of the Paris Olympic Games, paralysing key routes and highlighting vulnerabilities in critical event security planning. In Poland, the authorities dismantled networks suspected of planning sabotage and installing surveillance devices along railway lines used to transport military equipment to Ukraine, demonstrating how

38. *"How Moldova's Democracy Succeeded Against Russian Interference,"* Atlantic Council, October 23, 2025, https://www.atlanticcouncil.org/blogs/new-atlanticist/how-moldovas-democracy-succeeded-against-russian-interference/

39. *"Global Risks to the EU in 2026: What Are the Main Conflict Threats for Europe?"*, European Union Institute for Security Studies, January 20, 2026, https://www.iss.europa.eu/publications/commentary/global-risks-eu-2026-what-are-main-conflict-threats-europe

40. *"Russia Linked to 151 Hybrid Warfare Operations in Europe Since 2022, Dutch Think Tank Says,"* The Moscow Times, February 26, 2026, https://www.themoscowtimes.com/2026/02/26/russia-linked-to-151-hybrid-warfare-operations-in-europe-since-2022-dutch-think-tank-says-a92065

disruption of a single rail node could affect logistical flows to NATO's eastern flank.

Utilities and military infrastructure have also been tested. In August 2024, the German authorities temporarily sealed off a Bundeswehr base near Cologne Bonn Airport after detecting a possible attempt to contaminate the water supply. Days earlier, a similar investigation took place at the NATO base in Geilenkirchen, which hosts the AWACS airborne surveillance fleet and serves as an important logistics hub for training Ukrainian personnel.

European intelligence agencies have warned that Russian special services are actively acquiring residential and commercial property near military bases, ports and critical infrastructure in at least 12 European countries, turning these properties into a network of so-called Trojan horses intended to support surveillance, sabotage and covert operations in the event of a geopolitical escalation.[41]

Russia's grey-zone strategy relies precisely on Europe's tendency to deliberate endlessly about thresholds rather than establish and, most importantly, implement operational rules of response.

DEMOCRACIES' DILEMMAS VS SURVIVAL INSTINCT

Much of the European debate about Russia's sub-threshold warfare is framed around "dilemmas": escalation versus restraint, deterrence versus stability, attribution versus response. In reality, however, many of these dilemmas are overstated and self-restraining. Russia's grey-zone strategy relies precisely on Europe's tendency to deliberate endlessly about thresholds rather than establish and, most importantly, implement operational rules of response.

Airspace violations are a case in point. Russian drones, reconnaissance platforms and, occasionally, missiles have regularly crossed NATO airspace since 2022. The debate often centres on whether shooting down such objects might escalate tensions, even though no pilot casualties would be involved. Destroying drones that violate airspace should be treated as routine air defence, not escalation. Moreover, the precedent of Turkey shooting down a Russian Su-24 in 2015 demonstrates that Moscow ultimately understands the language of force more clearly than expressions of 'deep concern'.

Electronic warfare presents a similar challenge. NATO member states should assume persistent Russian jamming and GPS spoofing in regions adjacent to Russian military hubs, particularly around Kaliningrad and the Kola Peninsula, where such disruption already affects civil aviation and maritime navigation across the Baltic and High North. Rather than treating these incidents as anomalies, Europe should harden its systems and respond in kind – using calibrated jamming and spoofing in these regions to impose reciprocal costs and deny Russia uncontested dominance of the electromagnetic spectrum.

Maritime sabotage requires a denial strategy. Repeated incidents involving undersea cables, pipelines and suspicious vessels in the Baltic Sea illustrate the vulnerability of European infrastructure. Europe should move to access-denial measures: tighter monitoring of suspicious vessels, interception authorisation for coastguards and exclusion zones around critical infrastructure.

Recent investigations have linked damage to the Estlink 2 power cable and several telecom cables between Finland and Estonia to suspected anchor-dragging by Russia-linked "shadow fleet" tankers, while other disruptions are officially unattributed, underscoring the ambiguity that attackers exploit.[42] The legal response has been

41. *"The Kremlin's Spies Are Buying Homes Near Military Sites Across Europe,"* The Telegraph, February 23, 2026, https://www.telegraph.co.uk/world-news/2026/02/23/russian-spies-buy-homes-close-military-sites-europe-kremlin/

42. *"Finland Dismisses Case Over Baltic Cable Cuts,"* Euractiv, October 3, 2025, https://www.euractiv.com/news/finland-dismisses-case-over-baltic-cable-cuts/

weak. Charges against the tanker Eagle S and the related claim for damages were dismissed after the Helsinki District Court found that Finnish criminal law could not be applied, as the anchor dragging and cable damage in Finland's exclusive economic zone were legally classified as a maritime incident rather than a prosecutable offence under Finnish jurisdiction.[43] In the Fitburg case of telecommunications cable damage between Finland and Estonia, Finland detained the ship and 14-person crew, then released the vessel under escort once onboard investigations had been completed.[44] One crew member remains in custody and several are subject to travel bans in Finland.

At the same time, NATO's "Baltic Sentry" mission, launched in January 2025, and national actions, such as the Polish Navy's interception of a sanctioned Russian tanker near a power cable, show that interception, attribution and the prospect of legal and sanctions consequences can increase the cost of sabotage.[45] What is missing is not capability in principle, but a consistently applied, coordinated denial posture.

Cyber operations raise another persistent debate about retaliation. European policy still leans heavily towards defensive resilience, but deterrence in cyberspace requires credible retaliation. Responses need not mirror Russian tactics directly, but could involve disruptive operations against hostile infrastructure, potentially conducted through proxies, or coordinated law enforcement and intelligence channels.

Democracies are constrained by legislation, morality, rule-of-law norms, transparency and the public debate, while Russia operates with few such limits. Russia is of course acutely aware of these self-imposed limitations. This does not mean that Europe should abandon its principles; but it does mean that purely defensive strategies are insufficient against an adversary that treats hybrid operations as an integrated form of warfare. Retaliation is not the same as deliberate aggression. Protracted deliberations and weak responses are a sign that Europe is already losing the cognitive dimension of this conflict. Russia is a non-democratic state that has little regard for democratic debate.

CONCLUSIONS

Continuously playing defence is an almost guaranteed path to defeat, especially amid rapid technological change and increasingly sophisticated cognitive warfare. The West's primary task is therefore to reshape its strategic mindset now that its "holiday from history" has definitively ended.

Europe must move beyond the deterrence logic of the past, which relied primarily on economic pressure, sanctions and legal instruments. While financial restrictions, maritime monitoring, cyber defences, intelligence cooperation and law-enforcement measures are still important, they are no longer sufficient to alter the Kremlin's calculus. Russia has adapted to sanctions regimes and continues to operate hybrid campaigns through shadow fleets, sanctions-evasion logistics, front companies and proxy infrastructure.[46] These networks must be systematically targeted, disrupted and denied access to the financial and logistical systems that enable them.

Defensive measures alone rarely impose meaningful costs on the attacker and therefore do little to change behaviour. Europe should be guided by the calibrated policy of reciprocity and develop a framework that combines economic pressure with proportionate operational responses – including cyber counter operations, disruption of hostile networks and other measures that directly increase the cost of hybrid activity.

43. *"Finland Dismisses Case Over Baltic Cable Cuts,"* The Moscow Times, October 3, 2025, https://www.themoscowtimes.com/2025/10/03/finland-dismisses-case-over-baltic-cable-cuts-a90705

44. *"Ship Suspected of Severing Cable Between Finland and Estonia Released, However One Crew Member Was Detained,"* Babel, January 12, 2026, https://babel.ua/en/news/124254-ship-suspected-of-severing-cable-between-finland-and-estonia-released-however-one-crew-member-was-detained

45. *"NATO Launches 'Baltic Sentry' to Increase Critical Infrastructure Security,"* NATO, January 14, 2025, https://www.nato.int/en/news-and-events/articles/news/2025/01/14/nato-launches-baltic-sentry-to-increase-critical-infrastructure-security

"Poland Intervenes as Russian Shadow Fleet Ship Spotted Near Power Cable," The Moscow Times, May 21, 2025, https://www.themoscowtimes.com/2025/05/21/poland-intervenes-as-russian-shadow-fleet-ship-spotted-near-power-cable-a89160

46. Elena Davlikanova, et al. *"Russia's War Network: Military-Political Enablers of Aggression Against Ukraine and the West,"* NAKO, 2026, https://www.researchgate.net/publication/401805747_RUSSIA'S_WAR_NETWORK_Military-Political_Enablers_of_Aggression_Against_Ukraine_and_the_West

Cyberattacks should trigger cyber counter-operations. Any jamming attempts should trigger reciprocal EW measures on Russian territory in line with a reciprocity principle. Persistent violations of airspace by unmanned systems should result in their interception or equivalent reciprocal actions. This is not escalation but the establishment of predictable costs for hostile activity below the threshold of open war.

More broadly, European strategy must move away from binary thinking that separates "war" from "peace". Competition below the threshold of open conflict is here to stay. The focus must shift from deliberating on political vocabulary to shaping the operational environment in advance.

The first step for democratic nations is acknowledgement and openness in public debate. The prevailing "let's not worry the public" approach risks repeating the mistake of the Ukrainian leadership's reassurances in February 2022, when attempts to preserve calm obscured the scale of the looming threat. Such communication might temporarily reduce anxiety but ultimately weakens preparedness. National resilience begins with realism and honesty, not with toxic optimism or self-delusion.

Faster intelligence sharing, coordinated declassification mechanisms and synchronised public messaging among NATO, the EU and key national capitals would significantly reduce the attacker's ability to exploit informational uncertainty. Rapid, evidence-based attribution should become a routine feature of western responses rather than an exceptional step taken months after an incident. Hybrid operations are implemented across domains and jurisdictions. Responses must therefore do the same. Europe has become a bit better at this recently due to better synchronisation of efforts across actors and collaboration between the EU and NATO.

The EU Hybrid Toolbox is a detailed roadmap for coordinating responses to hybrid attacks by combining diplomatic, economic, cyber and CSDP instruments. A complementary foreign information manipulation and interference (FIMI) Toolbox provides graduated options, such as sanctions, content restrictions, public attribution, and so on, for countering Russian information operations. If implemented in full, they could significantly enhance European response to Russia's undeclared war.

NATO's current approach to hybrid warfare, which is built around the principles of preparation, deterrence and defence, should evolve to better reflect the realities of sub-threshold conflict. Given the ambiguous and deniable nature of many hybrid operations, NATO should shift its strategic emphasis to preparation, denial and retaliation. Strengthening resilience and early detection is still essential, but must be complemented by measures that deny adversaries operational space and impose tangible costs when hybrid attacks occur.

Moreover, defence and denial tools should be cost-effective. The 'Drone Wall' initiative is an essential shift in paradigm, but requires Ukraine's expertise and territory to give NATO's eastern flank strategic depth and relatively cheap technological solutions.[47] In addition, intercepting unmanned systems should not be viewed as escalation, as no pilots are directly at risk.

As warfare shifts towards semi-autonomous and autonomous systems, this transformation will increasingly affect not only conventional combat, but also sub-threshold capabilities such as surveillance, electronic warfare, targeting and unmanned operations. Artificial intelligence trained on high-quality operational data is becoming a critical strategic resource in this environment.[48]

Ukraine's wartime experience represents a unique asset in this domain. During its war with Russia, Ukraine has accumulated extensive battlefield datasets derived from real combat operations involving unmanned systems. In March 2026, the Ministry of Defence in Ukraine announced a framework for allowing international partners to train artificial intelligence models on real combat datasets gathered during the war. The initiative does not transfer the battlefield database itself. Instead, developers are given controlled access to train algorithms on datasets tailored to their needs while the data remains under the supervision of the defence ministry. This approach uses millions of annotated combat frames collected during tens of thousands of operational missions

47. Elena Davlikanova and Lesia Orobets, *"A Drone Wall Without Ukraine? A Barricade Lacking Bricks,"* Center for European Policy Analysis, December 4, 2025, https://cepa.org/article/a-drone-wall-without-ukraine-a-barricade-lacking-bricks/

48. Elena Davlikanova, *"Ukraine's World-Beating Combat Library Opens for Business,"* Center for European Policy Analysis, March 20, 2026, https://cepa.org/article/ukraines-world-beating-combat-library-opens-for-business/

to significantly improve the performance of autonomous systems. Structured cooperation with Ukraine in this field should become part of Europe's strategy to accelerate the development of AI-enabled defence capabilities. As a country that understands Russian tactics, culture and language, Ukraine can also provide detailed expertise on countering Russian cyber and cognitive warfare and serve as a forward platform for calibrated retaliatory measures.

Despite improvements, Europe still lacks a fully integrated, real-time picture of sub-threshold activity across domains and jurisdictions. The Sahaidachnyi Security Center's Everywhere War tracker could serve as a shared platform that European think tanks and official agencies can join as partners in a coalition to gather, share and analyse incident data on Russian operations.

The evolving strategic environment further reinforces the need for Europe to rethink its posture. As the United States increasingly shifts from its role as a predictable security guarantor to a 'security merchant', European states face growing pressure to accelerate the strengthening of their own defence capabilities. One reason why neither Moscow nor Washington consistently treats Europe as a negotiating party in discussions on a potential settlement of the war in Ukraine is the perceived fragility of Europe's military power.[49] Should the United States either formally or informally reduce or end its role within NATO, difficult questions would quickly arise regarding cohesion, the number of the remaining allies, their willingness to maintain collective defence commitments and the capabilities they could bring to bear.

The fading centrality of the United States in European security makes deeper integration with Ukraine not just desirable, but strategically necessary. Ukraine already possesses unmatched operational experience in countering Russian military, cyber and cognitive warfare. Its integration into European economic and security structures would strengthen both sides. EU membership would anchor Ukraine economically within Europe's defence-industrial ecosystem, while deeper security arrangements among the states of Eastern, Northern and Central Europe most exposed to Russian pressure could form the nucleus of a more robust regional defence architecture – and possibly even an alternative security alliance, should NATO's 'identity crisis' prove terminal.[50]

Russia's current hostile attitude to the West is not a glitch and is not going away. Sam Greene argues that Russia's shadow warfare is a continuation of Stalin's view of war as the natural, permanent condition of the state, fusing domestic and foreign enemies into a single, continuous battlespace in which everything and everyone is a potential target.[51]

In today's context of renewed great-power competition and "new generation" warfare, where kinetic, cyber, economic and cognitive tools have been fused, this logic makes Russia's undeclared war a long-term, methodical campaign that will persist as long as Russian imperial ambitions endure and, if left unchecked, could ultimately fracture the project of a democratic, united Europe.

Thus, a weak response to sub-threshold incidents and unassertive moves to prepare to retaliate constitute a strategic defeat today and an invitation to a larger kinetic war in the future. While most regional experts agree that Moscow is unlikely to open up a full-scale second front against NATO while the war in Ukraine continues, the pattern of incidents since 2022 demonstrates that sub-threshold warfare against Europe is already ongoing at scale.

49. *"'Go F*** Yourselves': The Kremlin Obscenely Responded to France's Proposal to Involve the EU in Peace Talks,"* Nasha Niva, March 15, 2026, https://nashaniva.com/en/390432

50. *"NATO, Iran, Israel and the U.S.: What the War Means for the Alliance,"* CBC News, March 2026, https://www.cbc.ca/news/politics/nato-iran-israel-us-war-9.7127634

51. Sam Greene, Andrei Soldatov, and Irina Borogan, *War Without End: Russia's Shadow Warfare*, Center for European Policy Analysis, November 19, 2025, https://cepa.org/comprehensive-reports/war-without-end-russias-shadow-warfare/

RECOMMENDATIONS

- **Recognise that Europe is already in Phase Zero of war and adopt "a doctrine of reciprocity".** This will require a shift in strategic mentality as continuously playing defence can only result in defeat. Hybrid actions should trigger proportionate responses – cyberattacks should be met with reciprocal cyber operations, GPS jamming with reciprocal jamming on Russian territory, and UAV incursions with reciprocal UAV incursions—establishing a clear quid pro quo. At the same time, European governments must maintain an honest dialogue with their populations. Realistic communication and resilience planning should replace attempts to preserve calm through strategic ambiguity.
- **Institutionalise rapid attribution and build a shared European picture of hybrid activity.** Develop integrated monitoring platforms – such as expanding the Everywhere War tracker – that link think tanks, governments and security institutions. Fully operationalise the EU Hybrid Toolbox and the FIMI Toolbox by applying sanctions, regulatory measures and information responses systematically against hostile networks. NATO and the EU should strengthen mechanisms for rapid intelligence sharing, coordinated declassification and timely public attribution of hybrid attacks.
- **Close legal loopholes.** Revisit interpretation of the freedom of maritime navigation. The current interpretation of freedom of navigation creates impunity for shadow fleet operations and must be narrowed for high-risk vessels engaged in sanctions evasion. Detaining sabotage ships without consequences dissipates efforts expended on their detention and spreads the feeling of impunity.
- **Develop cost-effective denial capabilities.** Expand initiatives such as the "Drone Wall", normalise the interception of unmanned systems and integrate Ukraine's operational experience. Accelerate AI-enabled defence through cooperation with Ukraine by using real combat datasets and battlefield expertise to improve autonomous systems. Invest in the Ukrainian military-industrial complex to win the war economy calculus.
- **Integrate Ukraine formally into Europe's security architecture.** Ukraine's extensive operational experience in countering Russian cyber, cognitive and drone warfare should be treated as a strategic asset for strengthening Europe's defence posture. At the same time, Ukraine should not remain permanently outside the perimeter of the collective European security architecture. Its formal integration – either as a member of NATO or, should it fracture, within a new European military alliance – would serve not just Ukraine's interests, but those of Europe as a whole.

Elena Davlikanova

Senior Fellow with Sahaidachnyi Security Center (Kyiv) and Center for European Policy Analysis (DC)

The European Policy Institute in Kyiv (EPIK) is a newly established think tank with a mission to inform policymaking by providing rigorous analysis, strategic insight, and forward-leaning policy ideas that contribute to Ukraine's European integration and regional security.

EPIK aims to be an independent, trusted, and influential voice in both Ukraine and the EU — a go-to platform for policymakers, experts, and international partners seeking clarity in complex policy environments.

EPIK was established by the Swedish Institute of International Affairs (UI) through its Stockholm Centre for Eastern European Studies (SCEEUS). It is co-funded by the European Union and the Swedish International Development Cooperation Agency (SIDA).

The contents of this publication are the sole responsibility of the author and do not necessarily reflect the views of the European Union or the Government of Sweden.

Cover photo: © Freepik

epik EUROPEAN POLICY INSTITUTE IN KYIV