

September 2026

Russia's Hybrid Pressure on Europe's Eastern Flank Since 2022



Executive Summary	2
Hybrid Pressure	5
Disrupting mobility and logistics	8
Cyber pressure on public services and infrastructure	11
Energy security, sanctions evasion and the shadow fleet	14
Critical infrastructure and undersea vulnerabilities	19
Information manipulation and psychological pressure	21
About us	25

Executive Summary

Jasmin Messaoudi

Russia's hybrid campaign against Europe's eastern flank has intensified since the full-scale invasion of Ukraine in February 2022. Hybrid pressure is not new in Russian statecraft, but its scale, frequency and operational reach have changed. Moscow has increasingly employed a combination of sabotage, cyber operations, electronic interference, energy coercion, maritime pressure and information manipulation to destabilise European states while staying below the threshold that would trigger a conventional military response. The campaign appears intended to impose costs, test NATO and EU resilience, and signal that support for Ukraine carries consequences inside Europe.

The central feature of this campaign is deniability. Many operations use proxies, criminal networks, commercial vessels, cyber actors or ambiguous technical disruptions, making attribution slow and politically difficult. This allows Russia to disrupt without accepting direct responsibility. The result is a grey-zone challenge for European governments: incidents are often serious enough to generate security, economic and political costs, but not always clear enough to justify a unified retaliatory response. This complicates deterrence and gives Russia room to sustain pressure over time.

Europe's eastern flank is especially exposed because it combines geographic proximity to Russia and Belarus with strategic infrastructure linked to Ukraine's defence. Finland, the Baltic states, Poland, Romania and Bulgaria sit across key land, air and maritime corridors. Their ports, railways, roads, undersea cables, energy infrastructure and logistics hubs connect civilian economies with military supply chains. The Baltic Sea has become a particularly sensitive area because it contains dense undersea infrastructure while also bordering Russian military facilities in Kaliningrad and St Petersburg. These structural vulnerabilities make the eastern flank a natural target for hybrid pressure.

Mobility and logistics have become a major pressure point. Russia-linked activity increasingly targets the systems that allow goods, people and military support to move. GPS jamming and spoofing affect aviation, shipping and navigation, especially around the Baltic Sea and Kaliningrad. These disruptions do not need to cause accidents to have a strategic effect. Rerouting, backup procedures, delays, reduced airspace capacity and uncertainty around maritime tracking already raise costs. Physical sabotage adds another layer. Self-igniting parcels, warehouse fires, railway attacks and attempted disruption of Ukraine-linked transport routes show how ordinary civilian logistics networks can be exploited. Together, electronic and physical disruption make Europe's transport systems less predictable and more expensive to secure.

Cyber pressure forms another core part of the campaign. Russian intelligence agencies and aligned cyber actors target governments, public services, transport systems, energy operators and private infrastructure. These operations range from espionage and data theft to destructive attacks designed to degrade services or disrupt critical sectors. Cyber operations are attractive to Russia because they are low-cost, difficult to attribute quickly and can be conducted through state-backed or proxy actors. Their effects extend beyond technical damage. Attacks on public registries, logistics providers, energy facilities and government systems can weaken trust in institutions, increase public anxiety and disrupt the services that societies rely on.

Critical infrastructure and undersea vulnerabilities represent a further risk. Since 2022, the Baltic Sea has seen repeated incidents involving damaged cables, pipelines and maritime infrastructure. These incidents have exposed weaknesses in surveillance, attribution and legal enforcement. NATO's Baltic Sentry and EU cable security initiatives show growing institutional recognition of the threat, but practical deterrence remains limited. Under existing maritime law, enforcement is difficult when suspicious vessels operate in international waters or under flags of convenience. Even when surveillance improves, prosecution and attribution often lag behind. This creates a gap between detecting suspicious behaviour and imposing meaningful consequences.

Energy remains one of Russia's most consequential tools of coercion. Before 2022, Moscow used long-term dependence on Russian oil and gas to create political leverage, especially in Central and Eastern Europe. After the invasion, this shifted into open pressure through supply cuts, rouble payment demands and gas disruption. The EU response has reduced Russian energy dependence through diversification, LNG infrastructure, renewables, interconnectors and regulatory phase-out measures. However, Russia has adapted by expanding the shadow fleet, using opaque ownership structures, flags of convenience, AIS blackouts and high-risk ship-to-ship transfers to sustain oil revenues and evade sanctions. Some governments and analysts increasingly warn that parts of the shadow fleet now function not only as an economic tool, but also as a maritime pressure instrument near sensitive infrastructure.

Information manipulation gives these physical, cyber and economic activities a wider psychological effect. Russian narratives seek to undermine support for Ukraine, portray NATO as aggressive, present EU policy as self-defeating and increase public doubt about democratic institutions. These campaigns rarely rely only on fabricated content. They mix facts, distortions and false claims to create uncertainty and reduce trust in reliable sources. Election interference in Romania, Moldova, Georgia and other states shows how information operations can shape the political environment without directly changing votes. Hybrid incidents themselves also create opportunities for psychological

pressure, as sabotage, drone incursions, GPS disruption and cable damage generate fear, speculation and pressure on governments to respond.

The cumulative effect is more important than any single incident. Russia's hybrid campaign works by creating repeated uncertainty across multiple systems at once: transport, energy, cyber, information, maritime security and public trust. Each incident may appear limited in isolation, but together they stretch police, intelligence, military, regulatory and communications capacity. They also force European governments to spend more on domestic security while sustaining military and financial support for Ukraine. This is the strategic purpose of the campaign: to make support for Ukraine politically, economically and socially harder to maintain.

European responses have expanded, but important gaps remain. NATO and the EU have improved monitoring, created new maritime security operations, strengthened cyber coordination and increased attention to foreign information manipulation. However, attribution delays, legal constraints, fragmented national responsibilities and uneven resilience continue to limit deterrence. The central challenge is no longer simply recognising Russia's hybrid campaign. It is building a response framework that can impose costs, protect critical systems and maintain public confidence without overreacting to every incident. Russia's hybrid pressure is likely to persist regardless of how the war in Ukraine evolves, making resilience on Europe's eastern flank a long-term security requirement rather than a temporary wartime concern.

Hybrid Pressure

Edzhe Miteva

Hybrid pressure [refers](#) to the coordinated use of military and non-military tools, including cyber operations, informational manipulation, economic coercion, covert action and, in some cases, limited military measures to influence and destabilise an opponent. This is not a new concept for Russia. In a 2013 address, Chief of the General Staff Valery Gerasimov [argued](#) that non-military and informational tools could, in certain conditions, prove more effective than conventional weapons. Russian military thinking increasingly emphasised non-military means and so-called "non-contact" warfare. Rather, their scale and intensity have shifted since Russia's full-scale invasion of Ukraine in February 2022.

The defining feature of hybrid pressure is its deniability. Operations are designed in ways to ensure that NATO's Article 5 collective defence clause is not invoked. Article 5 [states](#) that "an armed attack against one NATO member shall be considered an attack against them all." In October 2024, Polish authorities and DHL confirmed that incendiary devices had been concealed in cargo shipments routed through logistics hubs in Germany, the UK, and Poland, linking this to Russian intelligence. If the devices had detonated mid-flight rather than at a warehouse, they could have brought down a civilian aircraft. This example illustrates the nature of Russia's hybrid pressure, where operations are severe enough to cause significant damage, yet deniable enough to avoid open conflict.

Since the onset of the war in 2022, the number of Russian attacks in Europe quadrupled between 2022 and 2023 and tripled again between 2023 and 2024. This [culminated](#) in a 246% increase in what the International Institute for Strategic Studies terms "escalatory covert incidents", noting that the surge correlates closely with the Western lifting of restrictions on Ukraine's use of advanced long-range weapons systems.

The prevalence of hybrid tactics foremost reflects an institutional shift within the Russian state. Over the past two decades, its primary security and intelligence agencies, have moved beyond intelligence collection into strategic decision-making. The shift towards intelligence agencies assuming a more prominent role in implementing Russian foreign and security policy has resulted in hybrid warfare becoming the default mode of Russian power projection.

The Kremlin frames the hybrid campaign within a broader civilisational narrative that frames the West as not just a geopolitical rival but a colonial aggressor. Drawing on longstanding intellectual traditions, like 19th-century Slavophile thought, Russia has

positioned itself as a counterweight against Western dominance. This framing, which intensified after 2022, serves to legitimise hybrid operations both domestically and internationally as acts of resistance and a defensive response to Western “aggression”, markedly the provision of military aid to Ukraine.

A significant proportion of hybrid operations since 2022 have directly targeted entities connected to Ukraine’s defence. The two largest European donors of military aid to Ukraine, Germany and the UK, experienced attacks on multiple defence manufacturing plants. In May 2024, Diehl Group [saw](#) a fire break out in one of its factories in Berlin, which manufactures IRIS-T surface-to-air missiles used in Ukraine. These incidents, whether confirmed as sabotage or not, carry a dual risk. Operationally, they threaten to disrupt the European defence supply chain at a moment when NATO allies are racing to scale up ammunition for Ukraine. Strategically, they send a signal to governments as well as private industry that supporting Ukraine carries domestic consequences, a strategy that could deter future investment in defence manufacturing or slow the expansion of production capacity that the NATO alliance [committed](#) to at the June 2025 Hague Summit.

The states along NATO's eastern border, from Finland in the north, through the Baltic states, Poland, and Romania, to Bulgaria on the Black Sea, bear a disproportionate share of hybrid pressure. This is not incidental; it reflects structural vulnerabilities that Russia is positioned to exploit.

The Eastern flank shares extensive land and maritime borders with Russia and Belarus. Finland’s 1,340km frontier with Russia, Poland’s border with Belarus, and the Baltic states’ proximity to Russia all provide spaces for physical infiltration and electronic interference. The Baltic Sea, bordered by multiple NATO members but also by Russian naval bases in Kaliningrad and St Petersburg, has emerged as a particularly acute vulnerability, with repeated incidents of damage to undersea cables and pipelines [prompting](#) NATO to launch Baltic Sentry in January 2025, a dedicated maritime operation to protect undersea infrastructure. By September 2025, following Russian drone incursions into Polish airspace, the alliance [formed](#) Eastern Sentry, a broader multi-domain activity extending vigilance from the High North to the Black Sea. The creation of these operations illustrates the scale of the threat that Europe’s Eastern flank faces.

Domestically, hybrid operations force European governments to divert resources towards domestic security. Weaponised migration alone, the deliberate channelling of third-country nationals towards EU borders by Russian and Belarusian authorities, cost the EU €36.4 billion (£31 billion) between 2022 and 2025, [according to the Foundation for Defense of Democracies](#). The European Commission [allocated](#) €170 million (£144.3 million) to support frontline states in December 2024. The risk is not just fiscal but also a

strategic calculation. The €170 million (£144.3 million) allocated by the Commission represents less than 0.5% of the estimated cost that frontline states endure, leaving national governments to absorb the remainder at a time when public spending is already under pressure.

This political fragility faced by several eastern flank states compounds this vulnerability. Several eastern flank states already face low public trust in institutions, entrenched corruption, and fragile governing coalitions. Romania's 2024 presidential election illustrates this. In November 2024, far-right candidate Călin Georgescu surged from single-digit polling to win the first round on a pro-Russian, eurosceptic campaign. After what Romanian intelligence services [identified](#) as a coordinated Russian-backed social media campaign to inflate his visibility, the Constitutional Court annulled the results. Romania sits directly on Russia's strategic periphery, hosts major NATO infrastructure, and borders Ukraine; had Georgescu won, it could have shifted a critical ally away from the Western bloc.

Russia's hybrid campaign is unlikely to diminish regardless of how the war in Ukraine evolves. The Dutch Military Intelligence and Security Service (MIVD) director [stated](#) that the Russian threat against Europe is increasing, despite a possible end to the war against Ukraine. For European decision makers, the central challenge involves developing a framework that imposes meaningful costs on Russia as opposed to just recognition of its campaign.

Disrupting mobility and logistics

Jasmin Messaoudi

Russia's hybrid campaign against Europe's eastern flank increasingly targets the systems that allow people, goods, and military support to move. Electronic interference with satellite-based positioning systems and physical sabotage against transport networks serve the same broader purpose: to make movement slower, less predictable, and more costly without triggering direct military confrontation. These activities also allow Russia to impose costs on countries supporting Ukraine while maintaining a degree of deniability. NATO has [identified](#) sabotage, electronic interference, and proxy activity as part of a broader pattern of Russian hybrid operations across the Euro-Atlantic area.

Mobility is particularly vulnerable because Europe's eastern flank combines civilian transport routes with strategic supply corridors. Poland, the Baltic states, Finland, and the Baltic Sea connect airports, ports, railways, roads, warehouses, and routes used to sustain support for Ukraine. Disrupting these systems can affect commercial activity and security planning at the same time. Centre for Strategic and International Studies (CSIS) data on Russian hybrid activity between 2022 and March 2025 [found](#) that suspected and confirmed Russia-linked hybrid incidents nearly tripled between 2023 and 2024. Transport targets, including trains, vehicles, and aircraft, accounted for around 27% of recorded attacks, and many targets were linked to Western assistance to Ukraine.

The electronic dimension of this interference is visible in GNSS interference. Jamming [weakens](#) or blocks satellite signals, while spoofing generates false position data. Both can affect aviation, shipping and land transport systems that rely on accurate positioning, timing and route information. The issue has moved from a technical concern to an operational resilience problem. On 3 July 2026, the European Union Aviation Safety Agency updated its Safety Information Bulletin on Global Navigation Satellite System (GNSS) outages and alterations after assessing recent jamming and spoofing cases. The update included new pilot-air traffic control phraseology, electronic flight bag integration, operational and training requirements, and guidance on air traffic control capacity.

The March 2026 EASA-Eurocontrol action plan shows that European authorities [expect](#) GNSS interference to remain a continuing operational problem. The plan followed a June 2025 letter from 13 member states asking the European Commission to address GNSS radio frequency interference. It aims to preserve aviation safety while reducing the impact on airspace capacity over the next three years. This matters because electronic interference does not need to cause an accident to create disruption. If pilots

and air traffic controllers need to rely on backup procedures, reroute aircraft, increase separation, or reduce capacity, the result is already higher cost, delay and uncertainty.

Kaliningrad is central to this risk. Lithuanian assessments from May 2026 [indicated](#) that GPS spoofing equipment in Kaliningrad had expanded from three antennas in early 2025 to 36, with a possible reach of up to 450 kilometres. These assessments suggest that interference could affect much of the Baltic region and parts of northern and central Europe, including the Baltic Sea. Russia denied the claims, so the figures should be treated as Lithuania's assessment rather than as an independently confirmed fact. Even with that caution, the reported scale is significant because it suggests a shift from sporadic interference to a more systematic capacity to distort positioning data across a wide area.

Shipping is also affected where satellite interference disrupts vessel movement, tracking and port coordination. Finland's Coast Guard [detected](#) constant satellite positioning interference in the Baltic Sea from April 2024, including jamming and spoofing affecting vessels. Finnish assessments linked the interference to cases where ships lost their way or were placed in danger, alongside disruptions to automatic identification system signals. For commercial shipping, this increases reliance on backup systems and manual checks. For ports and logistics operators, it creates uncertainty around vessel tracking, scheduling and safe movement in already crowded waters.

Physical sabotage creates a second form of disruption. Instead of interfering with positioning data, it targets the logistics systems that move goods, supplies, and military assistance. The strongest recent example is the investigation into self-igniting parcels. Eurojust's March 2026 statement [describes](#) a joint investigation team from Germany, Lithuania, the Netherlands, Poland, and the United Kingdom that exposed an operation involving parcels that ignited in Germany, Poland, and the UK. One parcel caught fire at Leipzig airport shortly before it was due to be loaded onto an aircraft, another caught fire in a UK warehouse, and one caught fire in a truck in Poland. Eurojust identified 22 suspects in Lithuania and Poland suspected of working on behalf of Russia's military intelligence service.

This case [shows](#) how sabotage can exploit ordinary civilian logistics networks. The alleged operation did not require a direct attack on a military facility. It used parcels, warehouses, trucks, sorting centres and air cargo routes. Eurojust's statement also describes suspects being recruited through an online messaging service, given separate tasks and sometimes paid in cryptocurrency. This points to a proxy model in which Russian-linked services can use local or vulnerable recruits to carry out disruptive actions while preserving deniability. It also increases the burden on European police, intelligence, and transport security authorities because the threat sits inside normal commercial flows.

Rail sabotage in Poland shows the same logic more directly. Polish authorities [linked](#) the November 2025 explosion on the Warsaw-Lublin railway route to two individuals assessed to have collaborated with Russian intelligence and later fled to Belarus. The line connects Warsaw to the Ukrainian border, and Poland has become a major hub for aid to Kyiv. Polish authorities assessed that the aim was to cause a railway traffic catastrophe. A second attempted incident involved a steel clamp placed on the track with the likely aim of derailing a train. This example shows how physical sabotage can target transport corridors that are central to sustaining support for Ukraine.

The risk remains current. In July 2026, Polish special services were [preparing](#) for possible Russian sabotage intended to exploit tensions between Poles and Ukrainians. Russian-linked interest had reportedly been observed around military facilities, infrastructure, aid organisations, and sites connected to Polish-Ukrainian cooperation. This should not be treated as evidence of a specific imminent operation, but it shows that logistics, aid networks, and transport corridors remain likely targets.

Russia's campaign on mobility and logistics therefore works through cumulative disruption rather than one decisive attack. GNSS interference can complicate aviation and shipping without physical damage. Parcel plots and railway sabotage test the vulnerability of civilian transport systems. Together, these actions raise costs, stretch security services, and signal that support for Ukraine can carry risks inside Europe. The strategic effect lies less in any single incident than in repeated uncertainty across the systems that keep Europe's eastern flank moving.

Cyber pressure on public services and infrastructure

Rita Fernández Pérez

In recent years, malicious Russian cyber activity has become an increasingly prominent security, economic and political concern across Europe. Intelligence reports suggest Russian cyberattacks and electronic sabotage complement other offensive instruments as part of a broader hybrid campaign against adversarial states. These cyberattacks aim to undermine the resilience of targeted states through different offensive operations, such as mobility and transport disruption, critical infrastructure sabotage, energy supply interruptions and information manipulation within the wider campaign.

Reports from Western intelligence agencies indicate that the main institutions involved in offensive cyber activity include the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU), the Federal Security Service (FSB) or the Foreign Intelligence Service (SVR). These agencies [conduct](#) operations involving cyber-espionage campaigns, sabotage, mass disinformation campaigns, sensitive information exfiltration and data destruction operations, amongst others.

Additionally, Russian cyber operations are supported by a vast network of state-sponsored cyber operators and cybercriminals who operate outside Russia's formal institutions yet remain broadly aligned with Moscow's strategic objectives. The participation of these proxy actors potentially [provides](#) Russian authorities with plausible deniability while simultaneously advancing the Kremlin's strategic interests. These kinds of offensive operations constitute a relatively inexpensive and discreet instrument for Russian authorities, as they can be conducted from Russian territory, third countries, or virtual networks that conceal the origin of the attack. Cyber-operations thus offer a more cost-effective and lower-risk alternative to conventional forms of aggression.

Russian cyberattacks on Europe's Eastern flank have [affected](#) several sectors across countries, primarily affecting governments, public services, transportation networks, energy facilities and other critical infrastructure. These campaigns produce widespread effects across society, as they impose a cost on civilians, businesses, and governments alike.

Cyber operations take place in various forms, and oftentimes do not result in the physical destruction of infrastructure. Instead, they often seek to collect intelligence and strategic information on a target state's government institutions and population, including sensitive information relating to political decision-making and national

security. For instance, the Finnish Security and Intelligence Service (FSIS) [identifies](#) Russian cyber espionage targeting Finland's governmental institutions, critical infrastructure and defence industry as one of the most persistent threats. Through these operations, Russia seeks to collect sensitive information on Finland's political decision-making and its foreign and security policy, particularly information that could potentially support its war of aggression in Ukraine.

Russian cyberattacks on public institutions, such as government agencies, state registries or electoral apparatus, have also become increasingly common. They potentially undermine the resilience of public services and democratic institutions across the affected countries. The 2024 Ukrainian public registry [attacks](#), which resulted in the violation of sensitive data of thousands of Ukrainian citizens, serve as a recent example of Russian activities designed to exfiltrate private information of citizens for political gain. Attacks on public institutions not only result in the collection of strategic intelligence and sensitive information, but also contribute to raising civil mistrust in public services, undermining public legitimacy of governmental authorities and institutions.

In addition to covert cyber operations aimed at gathering sensitive information, Russian cyberattacks designed to disrupt, degrade, or destroy the critical infrastructure of logistics providers and technology companies have multiplied in recent years. For one, Russian cyberattacks increasingly target logistics providers and technology infrastructure. A recent example is the state-sponsored Russian cyber campaign [targeting](#) several European logistics entities and technology companies involved in the delivery of foreign assistance to Ukraine, which targeted several European states, such as Moldova, as well as NATO member states, such as Poland, Slovakia, Bulgaria, Romania or Ukraine.

Other operational systems targeted by Russian hostile cyber operations include critical infrastructure such as energy grids and transport networks. The effects of these attacks often generate energy outages that result in the disruption of supply chains, causing financial losses in the manufacturing, retail, and IT sectors. Nonetheless, the effects of malicious cyber activity on energy and transport infrastructure are not limited to economic disruptions and potentially undermine public institutions such as healthcare services, water supply or communication systems, and energy supply to private households and businesses. The recent cyberattacks on Polish renewable energy facilities, for instance, [compromised](#) the energy distribution of nearly 500,000 citizens in a campaign deemed by Polish authorities as "purely destructive in nature". Similar Russian cyberattacks in Poland [increased](#) by 30% in 2025, often targeting the country's critical transport and energy infrastructure.

In the context of Russia's war of aggression in Ukraine, malicious cyber activities also complement and reinforce Russia's military activities. Cyberattacks against critical infrastructure are often designed to degrade military preparedness through the disruption of logistics, command systems or supplier networks. Prior to the 2022 conflict, Ukraine had been at the centre of Russian cyber aggressions, particularly after the start of the 2014 conflict. Even so, cyberattacks have increased significantly during the course of the war: according to the Centre for European Policy Analysis (CEPA), Ukraine has [faced](#) over 10,000 cyber incidents since the start of the 2022 full-scale Russian invasion, demonstrating the increasingly prominent role of cyberattacks within Russia's warfare strategy.

Overall, malicious cyber operations constitute a central part of Russia's foreign and security strategy, and are now consolidated as a core component of its foreign policy. In the last two decades, they have become a key part of Russian hybrid activities, making its cyber activity a latent threat for the political, economic and social stability of targeted states. Their low cost and difficult traceability make cyberattacks an attractive means of pursuing strategic military, political and economic objectives, while offering perpetrators a degree of plausible deniability, complicating attribution and the execution of an effective response. As Russian war efforts continue to evolve in Europe's Eastern flank, they are likely to remain an essential component of Russia's broader geopolitical strategy. The increase in cyber incidents underscores the importance of strengthening cyber resilience mechanisms to counter future threats.

Energy security, sanctions evasion and the shadow fleet

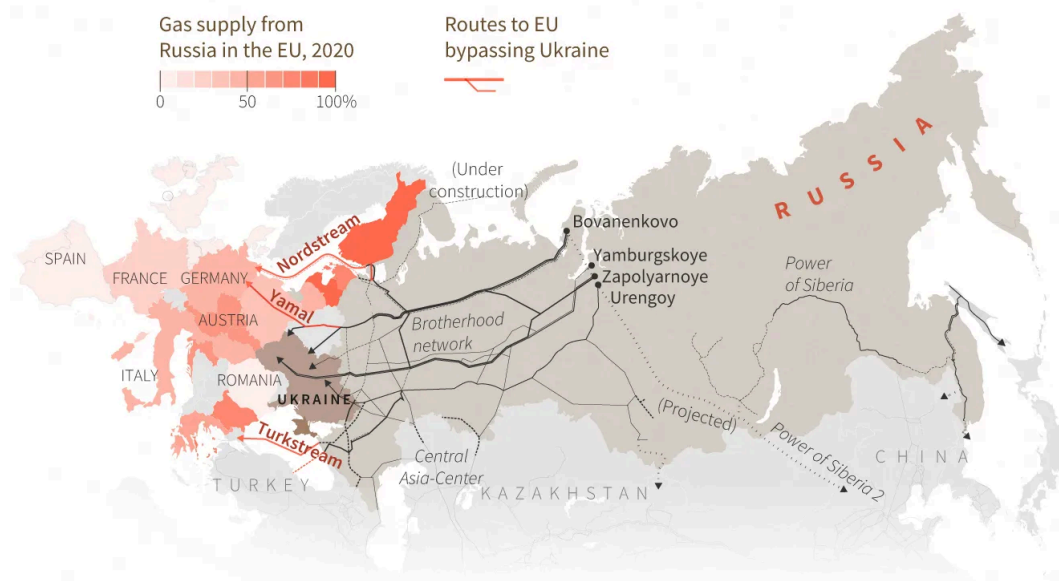
Cristina De Masi

Pre-2022 Energy weaponisation

Among Moscow's non-kinetic instruments against NATO's eastern flank, the weaponisation of energy has been one of its most consequential tools of coercion. For decades, Russia's large share of European oil and gas markets gave it substantial economic and political leverage. This strategy succeeded primarily in Central and Eastern Europe, where Soviet-era infrastructure integrated regional energy systems directly into Russian-controlled supply networks, including the Druzhba and Yamal-Europe pipelines and the Ukrainian transit corridor, although dependence also extended to major Western European economies. Limited regional liquefied natural gas (LNG) import capacity, insufficient alternative interconnectors, and the geographical isolation of these markets further constrained diversification, leaving many eastern flank states highly vulnerable to supply manipulation.

Main routes for Russian gas into Europe

Gas and oil-rich Russia is linked to European energy markets through a series of critical pipelines, the biggest flowing through Ukraine.



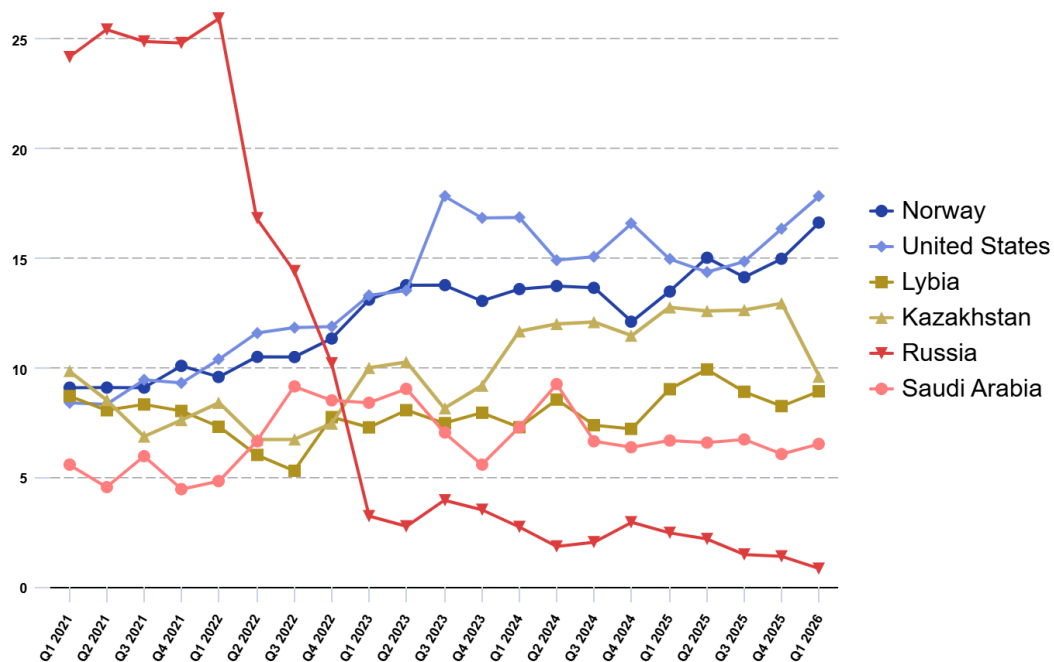
Routes of Russian Gas into Europe,
Source: CEPA 2022

Before 2022, the Kremlin's energy strategy relied on deepening economic interdependence, while maintaining the ability to weaponise energy exports when politically expedient. The gas transit disputes with Ukraine in 2006 and 2009 demonstrated the Kremlin's willingness to interrupt supplies to extract political concessions despite the wider disruption to European consumers. At the same time, the construction of the Nord Stream pipelines [bypassed](#) traditional transit states and strengthened direct energy ties with major Western European economies. These developments weakened EU policy cohesion, delayed diversification efforts, and reinforced the perception that Russian energy was economically indispensable.

Towards Energy Decoupling

Russia's full-scale invasion of Ukraine in 2022 marked a shift from cultivating long-term dependence to openly exploiting it. Deliberate reductions in gas supplies during late 2021 and early 2022 contributed to severe market volatility and soaring wholesale energy prices across Europe. Moscow subsequently demanded payments in rubles, suspended gas deliveries to Poland and Bulgaria, and ultimately halted Nord Stream 1 flows. These measures sought not only to impose economic costs but also to fracture European unity by increasing domestic political pressure on governments supporting Ukraine. Energy represented an overt instrument of coercion directed at undermining NATO and EU solidarity.

However, this coercion accelerated a fundamental restructuring of the continent's energy architecture. The Versailles Declaration [established](#) the political mandate to eliminate reliance on Russian fossil fuels, while the REPowerEU Plan translated this commitment into a strategy centred on supply diversification, renewable energy expansion, and improved energy efficiency. This political commitment later evolved into a binding regulatory framework providing for the phased elimination of Russian hydrocarbon imports, with the final restrictions scheduled to take effect by the end of 2027. By 2025, these interventions successfully [reduced](#) Russian gas from 45% of total EU imports before the war to approximately 12%.



Source: Eurostat database (Comext) and Eurostat estimates

eurostat 

EU imports of energy products from 2021-2026 by main partners

Source: Eurostat

Across NATO's eastern flank, decoupling proceeded through a combination of regional integration and national infrastructure investment. The Baltic states pursued one of the most comprehensive reductions in Russian energy dependence, culminating in their February 2025 desynchronisation from the Russian-controlled BRELL electricity system and synchronisation with the Continental European grid. This was paired with targeted national initiatives: Lithuania expanded the capacity of its Klaipėda LNG terminal, Estonia accelerated renewable generation, and Latvia enhanced its hydropower reserves. Simultaneously, Poland consolidated the expansion of the Świnoujście LNG terminal and the operationalisation of the Baltic Pipe, securing direct access to Norwegian shelf gas. Although landlocked states such as Hungary and Slovakia continued to face greater supply constraints, new regional infrastructure, including the Poland-Ukraine energy corridor and the Southern Vertical Corridor connecting Greek LNG facilities with Balkan and Central European markets, began reducing reliance on traditional Russian transit routes.

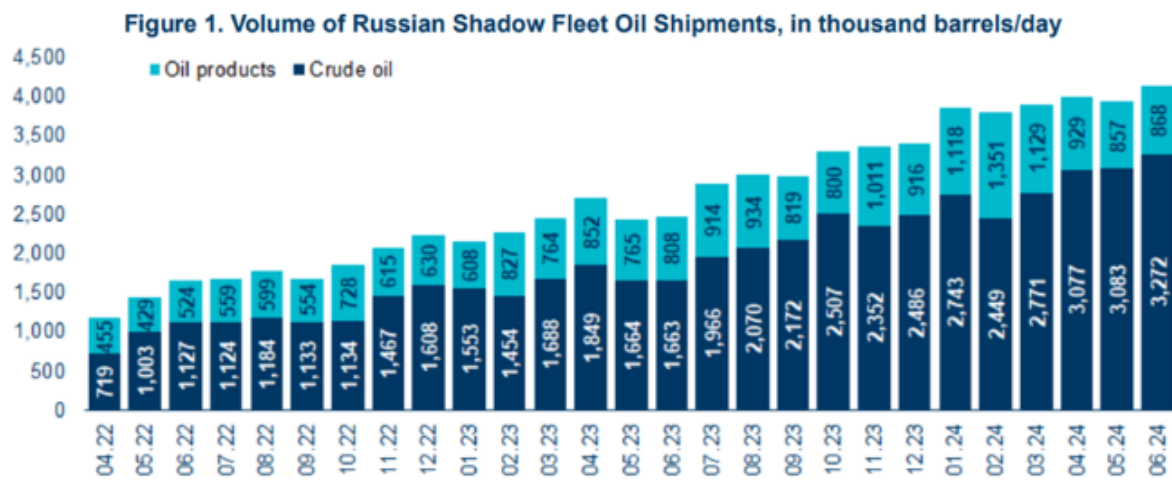
The 'Shadow Fleet' beyond sanction evasion

As European states reduced their dependence on Russian hydrocarbons, Moscow also faced mounting constraints from Western sanctions targeting its energy sector. The most significant measure was the December 2022 G7 and EU oil price cap, which [prohibited](#) Western shipping, insurance, financing, and other maritime services from transporting Russian crude sold above the established price threshold. The measure sought to reduce the Kremlin's oil revenues while maintaining sufficient Russian exports to avoid major disruptions to global energy markets. Combined with the EU embargo on seaborne Russian crude and petroleum products, these restrictions significantly reduced Russia's access to its most profitable European markets and increased the costs and complexity of exporting oil to alternative buyers.

To mitigate these losses, Russia rapidly expanded a "shadow fleet" of ageing tankers operating through opaque ownership structures, flags of convenience, and non-Western insurers. By circumventing Western maritime services and concealing the origin and sale price of Russian oil through Automatic Identification System (AIS) blackouts and high-risk ship-to-ship transfers, this parallel shipping network enabled Moscow to sustain exports to Asian markets, particularly China and India, preserving a critical source of state revenue despite sanctions.

The shadow fleet has, however, evolved beyond a mechanism for sanctions evasion into an instrument of hybrid warfare that continues to exert pressure on NATO's eastern flank. Exploiting the right of innocent passage under the United Nations Convention on the Law of the Sea (UNCLOS), these vessels can [transit](#) the territorial waters of littoral states while limiting opportunities for interdiction. Their frequent AIS blackouts and operations near critical maritime infrastructure simultaneously reduce maritime domain awareness and complicate attribution of suspicious activity.

This opaque maritime presence has become particularly significant in the Baltic Sea due to its dense concentration of critical underwater infrastructure, including the Estlink cables, regional gas interconnectors, and sensitive military data links. Repeated patterns of shadow fleet vessels drifting over critical nodes, coupled with calculated AIS blackouts, mirror the grey-zone sabotage patterns that disrupted Baltic subsea infrastructure across 2024 and 2025. By fusing sanctions evasion, critical infrastructure reconnaissance, and intentional legal exploitation, the shadow fleet has evolved beyond sanctions evasion. It is now fully integrated into Russia's hybrid warfare tactics, extending the Kremlin's energy strategy from market manipulation into the physical security architecture of NATO's eastern flank. Consequently, as Russia's ability to exert pressure through direct energy dependence has diminished, it has increasingly shifted towards protecting hydrocarbon revenues while employing the shadow fleet as a tool of intimidation, intelligence collection, and hybrid coercion.



Source: Equasis, the International Group of P&I Clubs, Kpler, and the KSE Institute

Critical infrastructure and undersea vulnerabilities

Yassine Battah

The Baltic Incident Timeline (2022–2026)

Maritime infrastructure has become an increasingly prominent target for hybrid pressure: disrupting the essential services it provides can cause significant economic, financial, and societal harm. Russia's campaign against it has diversified since 2022, combining physical sabotage with Automatic Identification System (AIS) spoofing and, as early as 2017, the NotPetya cyberattack that [crippled](#) Maersk's global shipping operations.

The most recent case came on 31 December 2025, when Finnish police [seized](#) the cargo vessel Fitburg for allegedly dragging its anchor across a Helsinki-Tallinn telecoms cable, its multinational crew holding Russian, Georgian, Kazakh and Azerbaijani nationalities. Days later, Latvian authorities [boarded](#) a second vessel suspected of damaging a Latvia-Lithuania link, though initial investigations found no evidence linking the ship to the damage. A year earlier, on 25 December 2024, the tanker Eagle S severed the EstLink-2 power cable and four telecoms lines between Finland and Estonia; despite Finland linking the ship to Russia's sanctions-evading "shadow fleet," a Finnish court [dismissed](#) the case in October 2025 for lack of jurisdiction, ruling the incident fell outside Finland's territorial waters, meaning that any claims would have to go through the ship's flag country, a ruling now central to debates over the adequacy of maritime law. One month before that, the Chinese-flagged Yi Peng 3 was [tracked](#) at the precise time and location of two further cable breaches within 24 hours, severing links between Sweden-Lithuania and Finland-Germany.

The pattern traces back to October 2023, when the Balticconnector pipeline and an adjacent Estonia-Finland cable were [damaged](#) by the Newnew Polar Bear, and to September 2022, when explosive charges destroyed sections of Nord Stream. In total, roughly 10 incidents of cable or pipeline damage have been recorded since 2022, with seven concentrated in the three months between November 2024 and January 2025 alone.

EU and NATO Responses

Institutional recognition of the threat has been swift, if still maturing. NATO launched [Baltic Sentry](#) on 14 January 2025, a multi-domain mission combining frigates, maritime patrol aircraft and naval drones to strengthen surveillance and response around critical

undersea infrastructure. The UK-led Joint Expeditionary Force complemented this with [Nordic Warden](#), an AI-driven system that assesses vessel risk in real time using AIS data.

The European Commission moved in parallel. On 21 February 2025, the Commission and the EU's High Representative [adopted](#) the EU Action Plan on Cable Security, structured around four priorities: prevention, detection, response and repair, and deterrence. This culminated on 5 February 2026 with a [€347 million](#) (£297.2 million) Cable Security Toolbox and a list of 13 Cable Projects of European Interest, though the underlying legal constraint remains unresolved: under the UN Convention on the Law of the Sea (UNCLOS), vessels on the high seas generally fall under the exclusive jurisdiction of their flag state, leaving coastal states with limited boarding powers unless a recognised legal exception applies.

Policy Gaps, Preparedness and Where Things Stand Today

Despite this institutional response, the practical record remains mixed. Every prosecution attempted so far under existing maritime law has [collapsed or stalled](#): the Eagle S case was dismissed for lack of jurisdiction, the Vezhen incident was ruled accidental, and the Newnew Polar Bear and Yi Peng 3 cases have not resulted in confirmed state attribution more than a year on. Repair timelines compound the problem; the global median for fixing a submarine cable fault is around 40 days, a window during which affected states have limited alternative capacity.

Analysts increasingly frame the core weakness as legal rather than technical: [UNCLOS](#) constrains what coastal states can do against a vessel in international waters, even with strong circumstantial evidence, and enforcement still depends on a ship's flag state cooperating, something Russia-linked shadow fleet vessels are structurally designed to avoid. A small set of concrete measures recur across expert assessments of where this gap should close next:

Different approaches have been proposed to strengthen the protection of critical undersea infrastructure. [RAND Europe](#) has argued that private cable operators should adopt a formal duty of care and act as the first line of defence, rather than relying primarily on state naval patrols. Additionally, [CEPA](#) has recommended a shared Baltic registry of pipelines, data cables and offshore energy assets to close early-warning gaps and feed NATO's Seabed Warfare initiative. On the other hand, [CSIS](#) has proposed reforming maritime jurisdiction so that prosecution no longer depends on a vessel's flag state, directly addressing the accountability gap exposed by the Eagle S dismissal.

Until prosecution keeps pace with surveillance, deterrence in the Baltic may remain aspirational rather than operational, and the pattern of incidents recorded since 2022 suggests that this calculus has yet to change for Moscow.

Information manipulation and psychological pressure

Nana Katsia

Russia's use of information manipulation as an [instrument](#) of state power long predates its full-scale invasion of Ukraine. Disinformation, propaganda and influence operations have for decades formed an integral part of the Kremlin's broader approach to conflict, accompanying diplomatic pressure, cyber operations and, where necessary, military force. This pattern was familiar to countries on Europe's eastern flank, particularly [Georgia](#), [Ukraine](#) and the [Baltic](#) states, which repeatedly warned that Russian information campaigns should be regarded as a security challenge rather than merely a media phenomenon. The 1992-1993 and 2008 wars in Georgia and the annexation of Crimea in 2014 illustrated that military action was accompanied by coordinated efforts to shape domestic and international perceptions, discredit national governments and justify Russian actions through carefully constructed narratives.

The full-scale invasion of Ukraine therefore greatly increased the scale, visibility and political importance of these operations across Europe. As military confrontation intensified, information operations increasingly complemented cyberattacks, sabotage and other forms of hybrid activity, seeking to influence how events were interpreted rather than simply how they unfolded. They have sought to exploit existing political divisions, increase uncertainty and weaken confidence in democratic institutions, making collective decision-making within the European Union and NATO more difficult. The European External Action Service now treats these activities as Foreign Information Manipulation and Interference ([FIMI](#)), recognising them as a coordinated security threat rather than isolated incidents of disinformation.

The invasion of Ukraine illustrates that major military campaigns are rarely prepared through military means alone. Long before Russian troops crossed the border in February 2022, the Kremlin had spent years [promoting narratives](#) questioning Ukraine's sovereignty, portraying NATO as an existential threat to Russia and presenting the Ukrainian government as illegitimate.

These narratives were gradually embedded through state media, diplomatic messaging and coordinated online influence campaigns, helping to establish an informational environment in which military action could later be justified to domestic audiences and defended internationally.

Disinformation, propaganda and false narratives around Ukraine

Rather than relying solely on fabricated stories, Russian information campaigns combine factual information, misleading interpretations and false claims to create competing versions of reality. This makes them more difficult to identify and allows different narratives to resonate with different audiences. State-controlled media (such as TASS, RIA Novosti, RT), proxy websites, social media platforms and networks of coordinated online accounts are used simultaneously to amplify these messages across multiple information environments, increasing their reach and credibility. According to the European External Action Service (EEAS), such campaigns are rarely isolated incidents but form coordinated efforts to manipulate public discourse and influence political decision-making across Europe.

Since 2022, these efforts have centred on sustaining support for Russia's strategic objectives by undermining public backing for Ukraine. Common narratives have [portrayed](#) sanctions as harming European economies more than Russia, claimed that Western military assistance merely prolongs the war, or questioned the legitimacy of the Ukrainian government. For example, pro-Kremlin outlets repeatedly attributed Europe's energy crisis exclusively to EU sanctions rather than Russia's deliberate reduction of gas supplies, while false claims alleging widespread misuse of Western military aid by Ukraine have circulated across social media despite repeated fact-checking by independent organisations.

Similarly, following the Bucha massacre in April 2022, Russian state media sought to [discredit](#) evidence of civilian killings by presenting contradictory explanations and alleging that the events had been staged, despite extensive investigations reaching the opposite conclusion. Rather than persuading audiences to accept a single version of events, these campaigns aim to generate uncertainty, exploit existing political grievances and erode confidence in reliable sources of information, making consensus within democratic societies increasingly difficult.

Election interference

Russian election interference is often less about changing votes directly than about shaping the political atmosphere in which elections take place. By amplifying fear, polarisation and distrust, these campaigns can influence public debate without formally interfering with the electoral process itself.

Recent elections illustrate this evolving approach. During Romania's 2024 presidential election, [Romanian](#) intelligence services identified a coordinated online campaign, particularly on TikTok, that artificially amplified content supporting candidate Călin Georgescu, leading the Constitutional Court to annul the first round of voting over

concerns of foreign interference. In [Moldova](#), authorities accused Russia-linked actors of conducting coordinated disinformation campaigns and large-scale vote-buying schemes ahead of the 2024 presidential election and referendum on European Union membership. [Georgia's](#) 2024 parliamentary elections also unfolded amid allegations of Russian influence and widespread information campaigns portraying closer Western integration as a threat to peace and stability, while promoting narratives favourable to closer relations with Moscow. Similar influence efforts have been observed in the wider eastern neighbourhood. In [Armenia](#), pro-Kremlin information campaigns have sought to exploit public dissatisfaction following the loss of Nagorno-Karabakh, undermine confidence in Prime Minister Nikol Pashinyan's government and portray closer cooperation with the European Union as a threat to Armenia's security. At the same time, Russian officials have repeatedly argued that Ukraine should hold presidential elections despite the country's constitutional prohibition on elections under martial law, using this narrative to question the legitimacy of President Volodymyr [Zelenskyy's](#) government. Together, these examples demonstrate that contemporary election interference extends beyond the electoral process itself, seeking instead to shape the political and informational environment in which democratic choices are made.

Panic after hybrid incidents

[Hybrid](#) incidents also create opportunities for psychological pressure. Suspected sabotage of undersea cables in the Baltic Sea, drone incursions into NATO airspace, GPS jamming affecting aviation and maritime traffic, arson attacks and drone sightings are not only physical or technical disruptions; they also generate uncertainty about the scale of the threat and the adequacy of the state response. This was visible in September 2025, when NATO said numerous Russian drones violated Polish airspace and Allied air defences were activated to protect NATO territory. [NATO](#) has described recent cyberattacks, sabotage and possible attacks on undersea cables as part of a broader campaign to destabilise Allied societies. Even when attribution remains difficult, the informational effect can be immediate: speculation spreads quickly, media attention increases and governments are forced to respond under conditions of public anxiety. In this sense, the political and psychological effects of hybrid incidents may exceed the direct material damage, especially when the objective is to make European societies feel vulnerable and permanently exposed.

Attempts to weaken trust in the EU and NATO

The broader [strategic](#) objective is to weaken trust in the institutions that organise Europe's collective response. Russian narratives repeatedly portray NATO as an aggressor, the EU as divided or undemocratic, and Western support for Ukraine as economically destructive or strategically pointless. The EEAS has noted that Russian FIMI actors seek to mobilise anti-establishment sentiment by undermining trust in the EU,

while earlier EU reporting also identified Kremlin efforts to erode international support for Ukraine by blaming NATO and the West for the war. These messages do not need to create majority support for Russia to be effective. It is enough to increase doubt, fatigue and suspicion, making it harder for democratic governments to sustain sanctions, military assistance and long-term political unity.

Russian information manipulation is widely regarded by European institutions as a long-term instrument of pressure rather than a set of isolated false stories. Its purpose is to prepare narratives, exploit crises, intensify fear and weaken public trust in collective institutions. Europe has become more aware of this threat since 2022, but resilience still depends on maintaining public confidence, credible communication and political unity.

About us

Polis Analysis is a provider of high quality, succinct analysis of international political developments with teams in London, Brussels, Berlin, Paris, Rome, Washington D.C., Abu Dhabi and Hong Kong. We have a global community of thousands of readers based in over 100 countries.

What we believe

In an era of twenty-four-hour news, complex political developments and disinformation, we believe individuals deserve access to fact-based, free and easy to understand analysis of the events shaping their lives.

That is our mission at **Polis Analysis**.

Follow us on social media

LinkedIn: Polis Analysis (<https://linkedin.com/company/polis-analysis>)

Instagram: Polis Analysis (<https://www.instagram.com/polisanalysis/>)

Twitter: Polis Analysis (https://x.com/polis_analysis)

Contact us

For business inquiries and more information, reach out to us via:

Email: hello@polisanalysis.com

Website: <https://www.polisanalysis.com/>

Rights & Content

All content provided by Polis Analysis Limited is for informational purposes only and is not meant to represent political recommendations or influence political decision-making. © 2026 Polis Analysis Limited.