I"C"UV INTERNATIONAL CENTRE FOR UKRAINIAN VICTORY

RUSSIA'S UNDECLARED "PHASE ZERO WAR" AGAINST EUROPE

> We never intended to attack Europe, it sounds ridiculous to us.[1]

AUTHOR:

Iryna Krasnoshtan, Program Director, International Center for Ukrainian Victory

Funded by
the European Union

March 2026

SUMMARY

This paper analyses the evolving spectrum of Russia's hybrid warfare targeting European states, mainly focusing on the period following Russian full-scale invasion of Ukraine. It provides a comprehensive overview of Moscow's operations across multiple domains, including cyberattacks, sabotage and physical operations, espionage, disinformation and political influence, instrumentalised migration, GPS jamming, threats to undersea infrastructure, airspace violations and other military provocations.

The research demonstrates a significant intensification of these activities in scale, boldness and geographical reach. It shows that Russia increasingly combines multiple tools in coordinated hybrid campaigns designed to undermine European resilience and support for Ukraine, generate political pressure, and exploit institutional vulnerabilities. New operational patterns — particularly the use of drones and electronic warfare — highlight Moscow's focus on ambiguity, deniability, and psychological impact.

While these activities are often described as "hybrid", their cumulative scale and coordination indicate a more advanced stage of confrontation. Russia is progressively stretching the limits of what constitutes an "armed attack" while remaining formally below that threshold, effectively conducting a sustained "phase zero" war against Europe.

The final part of this paper distils practical recommendations to European countries, also drawing from Ukraine's experience of fighting with Russia. These insights aim to strengthen national preparedness, enhance cooperation, and improve Europe's collective ability to deter and respond to Russia's expanding hybrid toolkit.

INTRODUCTION

Russia's aggression against Ukraine since 2014 has been accompanied by a campaign of so-called "hybrid" activities targeting European states, which has evolved and intensified since the full-scale invasion in 2022. While commonly described as hybrid, this terminology increasingly understates both the scale and the strategic intent of these actions, giving the targets the illusion of safety.

In reality, Russia's ongoing attacks and operations against Europe are much better

[1] Vladimir Putin at the press-conference on 27 November 2025. Direct quote: "Because it's one thing, in general, to say that Russia has no plans to attack Europe, for us it sounds ridiculous, honestly. We never intended to, but if they want to hear it from us, well, sure, we'll put it on record. No problem."

understood through the concept of a "phase zero" war: a continuous, multi-domain campaign that has moved beyond isolated or merely "destabilising activities". Their cumulative scale, coordination and coercive impact indicate a deliberate effort to target the European security environment both from outside and from within, while progressively stretching the limits of what constitutes an act of war, yet remaining formally just below that threshold.

Despite this, these actions continue to be intentionally downplayed by some political leaders, contributing to a gradual expansion of what is considered tolerable.

A particularly illustrative example of this dynamic happened in the second half of 2025. An invisible "battle" took place in Brussels, in which Russia deployed a full spectrum of hybrid activities, combined with physical threats against the Belgian leadership, which have resulted in the blockade of a decision on using Russian frozen assets for the so-called "reparation loan" for Ukraine.

Russian intelligence have reportedly used direct threats and intimidation campaigns against Belgian political leaders, including the Prime Minister, and key executives of Euroclear depository holding the frozen assets, including its CEO. Investigators revealed "Bolshoi-loving bankers" working inside the Euroclear, like Olivier Huby, a French banker who had reportedly visited Russia 155 times over a decade and passed direct threats to Euroclear management.[2] Russian authorities also used "legal warfare", announcing legal action against Euroclear in the Moscow courts and European institutions. Simultaneously, multiple "unidentified drones" were reported flying over Belgium's nuclear power plants,[3] Belgian military facilities,[4] Brussels' key airport Zaventem, Liege airport, and other critical infrastructure. In the end, Belgian authorities blocked the decision, citing various economic, financial and other concerns. **Russia appears to have drawn a clear conclusion – its intimidation works and it can continue to rely on hybrid means to influence European decision-making.**

This paper examines how Russia applies its expanding hybrid toolkit across the European continent. It maps the principal domains in which these activities occur, identifies the patterns and actors involved, and highlights specific cases documented between 2022 and early 2026.

The research combines qualitative analysis, open-source intelligence (OSINT), and selected case studies to examine Russian hybrid activities across Europe.

---

2 https://euobserver.com/23635/bolshoi-loving-banker-threatened-euroclear-ceo-amid-eu-talks-on-russian-assets/
3 https://www.politico.eu/article/drones-spotted-belgium-nuclear-plant-doel-airspace-incursions/
4 https://www.bbc.com/news/articles/c20e8qzllewo

It draws on government statements, official reports, including from national intelligenceand law-enforcement authorities, media investigations and reporting, as well as NATO and EU assessments and statements.

The paper does not aim to provide an exhaustive record of all Russian hybrid activities in Europe. Instead, it focuses on representative cases that illustrate broader operational patterns, tactics, and strategic intent. Where possible, incidents are cross-referenced across multiple domains to reflect the increasingly interconnected nature of Russia's hybrid toolkit.
The analysis covers the period from February 2022 to early 2026, with earlier examples included when they highlight long-term trends. While the paper follows a domain-based structure, these activities perform specific functions within Russia's broader approach and are therefore grouped, based on hierarchy of functions – ranging from enabling access and intelligence collection (preparation layer), through direct disruption and coercion (core pressure layer), to influence operations (cognitive layer) and military signaling and threshold testing (escalation layer).

1. ENABLING ACCESS AND INTELLIGENCE COLLECTION OPERATIONS

ESPIONAGE

Recent developments suggest Russia's transition from traditional, diplomat-based espionage toward more diversified and resilient models. These include the increased use of "one-time agents," recruitment via digital platforms, and reliance on intermediaries operating across multiple jurisdictions ("travel operatives").
At the same time, espionage is becoming more closely integrated with other hybrid activities, including sabotage and disinformation, serving both intelligence-gathering and operational functions.

Espionage has long been an integral component of Russian operations abroad. However, both its intensity and methods have evolved significantly in recent years. At the same time, the efficiency of European counterintelligence has increased and counterintelligence services of Western countries are becoming more resolute in identifying and expelling spies operating under diplomatic cover.

Expelling the spies. Poland provides a notable example of this growing trend.[5] Between 2016 and 2023, Polish authorities arrested 46 individuals suspected of cooperating with Russian and Belarusian intelligence services,

[5] https://infosecurity24.pl/sluzby-specjalne/agencja-bezpieczenstwa-wewnetrznego/polski-kontrwywiad-w-liczbach-ile-osob-pracowalo-na-rzecz-rosji-i-bialorusi
[6] https://www.polskieradio.pl/395/7784/Artykul/3596320,55-people-arrested-in-poland-over-russianlinked-espionage

compared to only 11 arrestsduring 2008–2015. During the same 2016–2023 period, Polish services identified and expelled 55 Russian and Belarusian intelligence officers working under diplomatic status (compared to seven between 2008 and 2015), and denied accreditation to 13 diplomats suspected of intelligence links (only one such case in 2008–2015). Furthermore, 816 individuals were placed on the national entry blacklist for confirmed ties to Russian or Belarusian intelligence — a dramatic increase from 25 in the earlier period. In 2025, Polish security services publicly reported that they had arrested 55 individuals suspected of carrying out Russian-linked espionage,[6] underscoring that the trend continues to expand.

The German Military Counterintelligence Service (MAD) has likewise reported a sharp increase in espionage and destructive activities by Russia. According to MAD President Martina Rosenberg, Russian intelligence agencies are now operating "as they did during the Cold War." The agency noted that the number of related incidents in Germany has nearly doubled within a year and that Russian operatives enter the country through third states.[7]

According to October 2025 data from the Ukrainian Foreign Intelligence Service, since the beginning of Russia's full-scale invasion of Ukraine in 2022, European intelligence services have expelled around 700 Russian intelligence officers operating under diplomatic cover. The most extensive purges occurred in Bulgaria (82 expulsions), followed by Germany (65), Poland (58), Romania (52), Slovakia (39), the Netherlands and Slovenia (34 each), among others.[8]

As European counterintelligence became more effective against agents operating under diplomatic cover, **Russia began relying more heavily on social networks and travelling operatives**, according to Germany's 2024 report on the protection of the Constitution.[9] Consequently, in the 19th sanction package adopted in October 2025,[10] the EU governments agreed to restrict the movement of Russian diplomats within the Schengen Area, as intelligence agencies have linked several sabotage operations across Europe to Russian operatives posing as diplomats, officially accredited in a third country and travelling to conduct intelligence or sabotage activities.[11]

---

7 https://militarnyi.com/en/news/russian-espionage-and-sabotage-in-germany-have-doubled-over-the-past-year/

8 https://szru.gov.ua/en/news-media/news/700-expelled-diplomats-and-130-new-cases--europe-responds-to-moscows-espionage-expansion

9 https://verfassungsschutz.de/SharedDocs/publikationen/EN/reports-on-the-protection-of-the-constitution/2025-06-brief-summary-2024-report-on-the-protection-of-the-constitution.pdf?__blob=publicationFile&v=5

10 https://www.consilium.europa.eu/en/press/press-releases/2025/10/23/19th-package-of-sanctions-against-russia-eu-targets-russian-energy-third-country-banks-and-crypto-providers/

11 https://www.ft.com/content/bc1aeba0-d5f8-482e-b121-d71f8ceff23b

12 https://szru.gov.ua/en/news-media/news/700-expelled-diplomats-and-130-new-cases--europe-responds-to-moscows-espionage-expansion

13 https://szru.gov.ua/en/news-media/news/700-expelled-diplomats-and-130-new-cases--europe-responds-to-moscows-espionage-expansion

Since 2023–2024, Russia has also intensified **recruitment of so-called "one-time agents" or "low-level agents" from among European civilians** — using them both for intelligence gathering and implementing sabotage operations. According to data from the Ukrainian Foreign Intelligence Service,[12] 47 people have been charged with espionage for Russia in Poland, 20 in Estonia, 19 in Latvia, 12 in Germany, and 10 in the United Kingdom. In total, 130 individuals across 12 European countries have been suspected of working for Russian intelligence. Recruitment often occurs online — through social media platforms, particularly through Telegram, but also religious organisations, sports clubs, and public events.

These individuals are typically engaged only once, to collect specific information or perform limited tasks.[13] They usually do not have prior intelligence experience, and act for small sums of money, frequently unaware of the true identity of their handlers. They receive step-by-step instructions for carrying out their tasks, often also via Telegram. And payments are commonly made in cryptocurrency. Youngsters in vulnerable situations are often recruited for quick and easy money. Russian intelligence also often recruits Ukrainians, Belarusians, or Russians with European citizenships who reside in Europe. Some perpetrators have criminal backgrounds or drug addictions, as reported by the Swedish Security Police (Säpo).

Publicly available data on recent arrests shows that the tasks of such "spies" vary widely — from identifying potential saboteurs to spying on military training sites, defence facilities, and logistical hubs supporting Ukraine. Their assignments have included monitoring transport routes for weapons and humanitarian aid, gathering intelligence on military equipment destined for Ukraine, collecting data on the structure, locations, and capacities of armed forces, and surveilling former servicemen who fought in Ukraine.

A large espionage network was uncovered in Poland in 2024 following a series of arrests and court proceedings. The network comprised 16 individuals — including a 21-year-old Russian hockey player – who played for a Polish team since 2021 – recruited by the FSB, 13 Ukrainians, and two Belarusians.[14] Among the detainees were a lawyer, a political scientist, a French language teacher, a pharmacy technician, and a software engineer. The group operated in early 2023, conducting surveillance of Polish border checkpoints with Ukraine and major rail networks used for transferring weapons and humanitarian aid to Kyiv,

[14] https://wiadomosci.onet.pl/swiat/rosyjski-hokeista-skazany-w-polsce-za-szpiegostwo/5kjm2e7
[15] https://apnews.com/article/germany-russia-spying-military-officer-305ee23eb4677f3215c9e3560945a0d9
[16] https://www.dw.com/en/espionage-germany-cases/a-66496986
[17] https://www.reuters.com/world/germany-expel-russian-diplomat-over-espionage-accusations-2026-01-22/
[18] https://apnews.com/article/russia-germany-ukraine-taurus-missiles-recording-de408772f1edf3bd2f98fd5a3f64da3c

including by installing hidden video cameras along transport routes. Their additional tasks included distributing anti-Ukrainian propaganda materials and preparing for sabotage operations.

Russia also seeks to recruit or exploit serving and former officials and military personnel in Western countries. Germany has recorded a number of such cases. In spring 2024, a Bundeswehr officer was convicted of espionage and breach of official secrecy after voluntarily providing internal documents from the Federal Office of Bundeswehr Equipment to the Russian consulate in May 2023 to be forwarded to Russian intelligence, offering further cooperation.[15] Another officer of the Federal Intelligence Service (BND), head of the technical intelligence unit with access to highly classified documents, was accused of state treason for acting as a double agent for the FSB. His accomplice served as an intermediary between him and Russian handlers in 2022.[16] In January 2026, Germany expelled a Russian diplomat believed to be the handler of an alleged spy – German-Ukrainian woman – who had been arrested on espionage charges.[17]

Another major espionage incident occurred in February 2024, when a recording of internal discussions among senior German Air Force officers was intercepted [18] and released by Russian propagandist Margarita Simonyan. The recording, which covered hypothetical scenarios involving the transfer and use of Taurus missiles by Ukraine — including possible strikes on the Crimean Bridge — was disseminated publicly in an apparent attempt to discredit the German military and prevent such a decision.

Moreover, there are suspicions that German right-wing party AfD uses its parliamentary responsibilities to collect information with potential further transfer to Russia. AfD members of Bundestag have regularly made requests about sensitive matters, such as military logistics, countering drones, cybersecurity and protection of critical infrastructure.[19]

Estonia has likewise faced high-level espionage cases. One of the most significant involved a Russian national and university professor who had taught for years

[19] https://www.spiegel.de/politik/deutschland/afd-spionagevorwuerfe-wegen-anfragen-zu-bundeswehr-faehigkeiten-a-04200ee6-4f2c-4c17-ba41-b1c17d63a90f
[20] https://apnews.com/article/russia-estonia-spying-morozov-b72c14d9bcc70ae8946ea4c1e0e13b76
[21] https://www.ukrinform.net/rubric-society/4056945-russian-opposition-figure-detained-in-poland-admits-to-cooperating-with-fsb.html
[22] https://news.liga.net/en/world/news/bild-536-unidentified-drones-spotted-over-important-sites-in-germany-in-three-months
[23] https://www.dw.com/en/germany-registers-over-1000-suspicious-drone-flights-in-2025/a-75261162
[24] https://www.spiegel.de/politik/deutschland/russisches-spionageflugzeug-bei-nato-uebung-in-litauen-a-af18c80f-45a6-4d44-a838-e2f152d0f8a4
[25] https://www.liga.net/en/world/articles/spies-undercover-why-vienna-became-a-hub-for-russian-intelligence-services

at a prestigious university in Tartu,including teaching Estonian diplomats and senior officials. He was convicted in January 2024 of spying for Russian military intelligence, having operated in Estonia for 14 years and severely undermined the country's security.[20]

There is also increased evidence that **Russia uses so-called "opposition figures" in the West in its espionage activities.** Recently, a Russian "opposition activist" arrested in Poland admitted to have been hired by Russian FSB as an agent to infiltrate into the "opposition forces" to collect and transfer information about Russian activists and other figures of interest in Poland and his wife was his accomplice.[21]

Russia increasingly employs drones as part of its hybrid operations, using them as a tool for intelligence gathering and surveillance. This has become particularly prominent in Germany, where Russian-operated drones are regularly observed flying over critical infrastructure and military sites. Targets have included military and training facilities — notably those hosting training for Ukrainian personnel — as well as energy installations, liquefied natural gas (LNG) terminals, defence manufacturers, airports, ports, railway stations, government buildings, and administrative facilities.

According to a report by the German Federal Criminal Police Office (BKA), cited by media,[22] between January and March 2025 there were 270 recorded incidents involving 536 drones. Most incidents occurred near military sites, with 117 cases documented, including ten over the naval base in Wilhelmshaven. Up to fifteen drones were detected flying in formation over the U.S. Ramstein Air Base and in Bremerhaven. Another 88 incidents involved flights over energy infrastructure, including near LNG terminals in Stade, Wilhelmshaven, and Brunsbüttel. By the end of 2025, BKA registered more than 1,000 of such suspicious drone flights.[23]

Russia has also employed other aerial surveillance means, including balloons and reconnaissance aircraft. For instance, in May 2025, a Russian surveillance aircraft was reported to have conducted observation missions from Belarusian airspace during NATO exercises held in Lithuania.[24] Moreover, experts believe that Russia is actively reviving its intelligence gathering hub in Vienna, Austria,[25] where numerous satellite dishes have appeared on the rooftops of Russian-owned buildings in the past few years.

2. DIRECT DISRUPTION AND COERCION OPERATIONS
CYBERATTACKS

The cases analysed below point to several recurring features of Russian cyber operations against Europe. First, attacks are increasingly synchronised with political or military developments, suggesting deliberate timing rather than opportunistic activity. Second, there is a growing focus on critical infrastructure and high-impact civilian systems, increasing potential societal disruption. Third, the use of proxy groups and hacktivist fronts continues to provide plausible deniability while enabling scalable operations. Finally, cyber activities are frequently combined with other hybrid instruments, reinforcing their strategic effect.

Russian hybrid activities increasingly focus on cyber operations aimed at disrupting critical infrastructure, such as energy, water and sewage systems, by exploiting vulnerabilities. State institutions are also frequent targets – including websites of national and local authorities, ministries, and online public services such as state registries.[26] Other high-value targets include airports, defence manufacturers (e.g. Rheinmetall [27]), and military sub-contractors. For instance, Russian hackers reportedly infiltrated a contractor of the UK Ministry of Defence, leaking data on eight British military bases to the darknet.[28]

Since 2022, numerous European countries — including Germany, France, Italy, Estonia, Czechia, Denmark, Finland, Belgium, and others — have reported a marked increase in cyberattacks originating from or attributed to Russian actors. Poland, which plays a central role as a logistical hub for assistance to Ukraine, has been particularly affected. In October 2025, the Polish Minister of Digital Affairs, Krzysztof Gawkowski, reported that in the first three quarters of the year, 170,000 cyber incidents had been identified, the majority attributed to Russian actors.

[26] https://www.rmf24.pl/fakty/polska/news-atak-hakerow-na-systemy-panstwowe-sprawdz-co-wiadomo-o-cyber,nId,7957688
[27] https://www.reuters.com/technology/cybersecurity/rheinmetalls-civil-unit-suffered-cyberattack-that-cost-10-million-2024-05-14/
[28] https://www.mirror.co.uk/news/uk-news/vladimir-putins-hackers-hit-eight-36093236
[29] https://www.reuters.com/technology/poland-says-cyberattacks-critical-infrastructure-rising-blames-russia-2025-10-10/
[30] https://tvn24.pl/tvn24-news-in-english/russia-is-no-longer-hiding-it-is-at-cyberwar-with-poland-says-digital-affairs-minister-st8201519
[31] https://www.polskieradio.pl/395/7786/Artykul/3632810,poland-saw-30%C2%A0rise-in-cyberattacks-in-2025-officials-say
[32] https://www.err.ee/1609445333/venemaa-sojavaeluure-pani-toime-kuberrundeid-eesti-ametiasutuste-vastu
[33] https://mzv.gov.cz/jnp/en/issues_and_press/press_releases/statement_of_the_mfa_on_the_cyberattacks.html
[34] https://crn.pl/aktualnosci/cyberpolicja-w-akcji-przeciwko-prorosyjskiej-grupie-hakerow-noname05716/

Poland, which plays a central role as a logistical hub for assistance to Ukraine, has been particularly affected. In October 2025, the Polish Minister of Digital Affairs, Krzysztof Gawkowski, reported that in the first three quarters of the year, 170,000 cyber incidents had been identified, the majority attributed to Russian actors. The number of attacks continues to rise annually: in 2024, Poland detected twice as many cyber attacks as in 2023, and three times more than in 2022. And 2025 saw another 30% increase compared with 2024.

Attribution often points to Russian state or state-affiliated entities, such as military unit 29155 of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (as confirmed by Estonia), the APT28 (Fancy Bear) group associated with the Russian GRU (as confirmed by Czechia and Germany), and the Russian hacker group NoName057(16) (as confirmed by Poland). Several of these actors have publicly claimed responsibility for their operations, directly linking them to specific national decisions to support Ukraine. In other cases the attacks were not clearly attributed, but they coincided with important decisions related to Russia's war against Ukraine or important events for the nations concerned.

For instance, a cyberattack from Russian hacker group on German government services, companies and airports occurred shortly after Berlin's decision to deliver Leopard-2 tanks to Ukraine.[35] Similarly, NoName057(16) targeted Dutch government websites just before the NATO Summit in The Hague.[36]

At the end of 2025, Poland reported a coordinated cyber attack against its energy infrastructure, with 30 targets, including renewable energy plans, a manufacturing company, and a large combined heat and power plant supplying heat to almost half a million customers.[37] Polish authorities later stated that Poland was on the brink of a blackout, and attributed this massive cyber attack to Russia.[38]

---

[35] https://brusselsreporter.com/europe/2023/russian-hackers-launch-cyberattack-on-germany-in-leopard-retaliation/
[36] https://www.telegraaf.nl/binnenland/pro-russische-hackers-claimen-ddos-aanval-sites-nederlandse-gemeenten-en-provincies-slecht-bereikbaar/73241912.html
[37] https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/
[38] https://www.euractiv.com/news/russia-attack-on-power-grid-brought-poland-to-brink-of-blackout-warsaw-says/
[39] https://www.rmf24.pl/fakty/polska/news-ogolnopolska-awaria-problemy-z-paszportami-i-dowodami-osobis,nId,8019961
[40] https://www.euronews.com/2025/09/20/cyberattack-causes-disruptions-at-major-european-airports
[41] https://www.err.ee/1609445333/venemaa-sojavaeluure-pani-toime-kuberrundeid-eesti-ametiasutuste-vastu
[42] https://www.rfi.fr/en/france/20250430-russia-accused-of-cyberattacks-on-paris-olympics-and-french-election_cyberattacks.html
[43] https://www.france24.com/en/live-news/20260204-italy-foils-russian-cyberattacks-targeting-olympics
[44] https://www.reuters.com/world/europe/russia-backed-hackers-breach-signal-whatsapp-accounts-officials-journalists-2026-03-09/

Cyber operations are often synchronised with other elements of Russia's hybrid toolkit. During the Russian drone attack on Poland on 10 September 2025, the country simultaneously experienced its largest cyberattack since 2022, accompanied by a coordinated disinformation campaign seeking to attribute the drone strike to Ukraine. In the subsequent days, Poland faced nationwide disruptions to its passport registry[39] and payment systems.[40] Although these incidents were not publicly attributed to Russia, their timing suggests a coordinated operation.

In September 2025, while unidentified drones disrupted airports across Europe, several major airports simultaneously suffered cyberattacks targeting their automated registration systems.[41] These attacks caused widespread delays and flight cancellations, most notably at Brussels Airport, with Berlin Brandenburg and London Heathrow also affected.

Russian cyber attacks also targeted the hosts of the Olympics games – France[42] in summer 2024 and Italy[43] in winter 2026 – both accompanied with the sabotage of the railway systems.

In March 2026, Dutch intelligence services warned of a Russian-linked campaign targeting Signal and WhatsApp accounts of officials, military personnel and journalists through phishing and account-takeover techniques,[44] illustrating the growing emphasis on human-targeted cyber espionage alongside infrastructure attacks.

These incidents demonstrate how cyber operations have become a central pillar of Russia's hybrid campaign against Europe, enabling disruption, signalling, and political coercion while remaining below the threshold of open military confrontation.

GPS JAMMING & ELECTRONIC WARFARE

Russian electronic warfare activities demonstrate a shift from geographically limited disruptions to broader, more persistent interference affecting multiple countries simultaneously. The growing scale and frequency of incidents indicate a systematic rather than incidental use of these capabilities. Moreover, the dual-use impact — affecting both civilian and military systems — amplifies uncertainty and risk, while maintaining ambiguity regarding intent.

Since the Russian full-scale invasion of Ukraine, Russia has actively employed GPS signal jamming, disrupting civilian and military aviation, navigation systems, satellite communications, and related technologies.

Initially, these disruptions primarily affected flights near the Russian enclave of Kaliningrad. For instance, Finnair flights were regularly impacted from March 2022, with several regional flights in Finland cancelled.[45] In March 2024, Russia was suspected of jamming the GPS signal of the UK Defence Minister's plane flying near Kaliningrad.[46] Similar incidents occurred in September 2025 with the Spanish Defence Minister's plane[47] and repeatedly affected the German Bundeswehr Inspector General's aircraft over the Baltic Sea and Lithuanian airspace.[48]

Over time, Russian GPS jamming expanded in scope, affecting broader regions including Poland, the Baltic and Nordic countries, and parts of Germany. This escalation became particularly pronounced after December 2023.[49] In August 2025, the plane carrying European Commission President Ursula von der Leyen lost its satellite GPS signal over Bulgaria, reportedly due to Russian interference,[50] forcing pilots to rely on paper maps to land safely at Plovdiv Airport.

GPS jamming and spoofing also affect maritime navigation and drone operations. In January 2024, Polish authorities reported that both large and small vessels in the Baltic Sea experienced navigation failures, posing significant safety risks.[51] Estonia and Finland similarly issued warnings to maritime traffic in June 2024, noting a steady increase in Global Navigation Satellite System (GNSS) disruptions.[52]

In January 2024, Estonia reported the loss of several dozen drones, attributing these losses to electronic interference originating near its eastern border.[53] Estonian officials explained that as Ukrainian drone capabilities expand and reach Russian infrastructure, Russia increasingly uses GPS jamming to counter these threats.[54] These Russian actions undermine the security of the neighboring countries. Estonian authorities have formally protested to Russian officials multiple times, emphasizing that such interference violates International Telecommunication Union (ITU) regulations, which prohibit deliberate disruption of radio communications.[55]

---

[45] https://wyborcza.pl/7,75399,28205180,w-okolicach-kaliningradu-pojawily-sie-zaklocenia-w-systemie.html
[46] https://www.reuters.com/world/uk/russia-believed-have-jammed-signal-uk-defence-ministers-plane-source-2024-03-14/
[47] https://www.euronews.com/2025/09/24/spanish-defence-ministers-plane-hit-by-gps-disturbance-near-russian-enclave
[48] https://english.nv.ua/nation/nato-chief-warns-of-growing-russian-threats-after-gps-jamming-of-von-der-leyen-s-flight-50541815.html
[49] https://wiadomosci.gazeta.pl/wiadomosci/7,114881,30611828,miales-problem-z-gps-to-mogli-byc-rosjanie-i-to-nie-jest-spiskowa.html
[50] https://www.dw.com/en/eu-chief-plane-hit-by-suspected-russian-gps-jamming/a-73832942
[51] https://www.rmf24.pl/fakty/polska/news-zaklocenia-sygnalu-gps-na-baltyku-rybacy-wracaja-do-nawigacj,nId,7884976#crp_state=1
[52] https://www.transpordiamet.ee/uudised/eesti-ja-soome-hoiatavad-laevu-soome-lahes-sagenenud-gnss-hairete-eest
[53] https://www.err.ee/1609589921/eesti-riik-on-gps-hairingute-tottu-kaotanud-juba-paarkummend-drooni

In 2025, media referenced an internal EU document in which a number of the EU states raised the alarm[56] on the dramatic increase in jamming and spoofing of GNSS signals for aircrafts and sea vessels. In Lithuania, cases increased from 556 in March 2024 to 890 in October 2024 and 1,185 in January 2025; in Latvia, from 790 in October 2024 to 1,288 in January 2025; in Poland, from 1,908 in October 2024 to 2,732 in January 2025.[57] Moreover, the document named it not random incidents, but "a systematic, deliberate action from Russia and Belarus".

SABOTAGE AND PHYSICAL ATTACKS

Acts of sabotage across Europe reveal increasing operational tempo, geographic spread, and target diversity. A notable trend is the reliance on low-level, locally recruited operatives, enabling scalability and deniability at relatively low cost. Many attacks target symbolic or civilian infrastructure, amplifying psychological impact beyond their immediate physical damage. The integration of sabotage with broader campaigns — particularly cyber operations and disinformation — further enhances its destabilising effect.

Since the onset of Russia's full-scale invasion of Ukraine in 2022, the number of acts of sabotage and physical attacks across European countries has grown significantly. According to the International Center for Counter-Terrorism report, [58] there were 151 cases of sabotage in Europe identified between February 2022 and February 2026. Poland – key logistical hub of provision of Western support for Ukraine – was identified by the report as the most targeted country (31 cases – 21%).

The incidents include arsons of symbolic civilian targets – shopping centres (Marywilska Centre in Warsaw in May 2024,[59] an IKEA store in Vilnius in May 2024,[60]

[54] https://www.err.ee/1609589921/eesti-riik-on-gps-hairingute-tottu-kaotanud-juba-paarkummend-drooni
[55] https://rus.err.ee/1609336152/mid-jestonii-iz-za-sboev-v-rabote-gps-vyzval-vremennogo-poverennogo-v-delah-rossii
[56] https://www.theguardian.com/world/2025/sep/01/russia-suspected-jamming-gps-plane-carrying-ursula-von-der-leyen-eu
[57] https://data.consilium.europa.eu/doc/document/ST-9198-2025-INIT/en/pdf
[58] https://icct.nl/publication/more-same-russias-crime-terror-nexus-criminality-tool-hybrid-warfare-revisited
[59] https://apnews.com/article/poland-russia-420187f5755036f6f61c65122c11348f
[60] https://apnews.com/article/lithuania-russia-intelligence-arson-attack-ikea-vilnius-b7f915c6376c0711b852657d17a30c0d
[61] https://www.gov.pl/web/prokuratura-krajowa/zarzut-wobec-stepana-k
[62] https://www.polskieradio.pl/395/7784/Artykul/3438168,russian-gru-behind-arsons-in-wroclaw-confirms-polish-foreign-ministry
[63] https://www.rmf24.pl/fakty/polska/news-dzialal-na-zlecenie-rosji-wiadomo-kto-stoi-za-podpaleniami,nId,8004549
[64] https://securingdemocracy.gmfus.org/incident/russia-behind-attempted-arson-on-prague-bus-depot/

construction market in Warsaw in April 2024),[61] factories (an attempted arson at a paint factory in Wrocław in January 2024[62]), depots (Warsaw and Radom in May 2024[63]), bus stations (Prague in 2024[64]), waste disposal sites (near Lublin in 2025[65]) and restaurants (Ukrainian restaurant in Estonia in early 2025[66]).

Military and defence-related facilities have also been targeted, with specific targets to disrupt the aid to Ukraine. Examples include the arson of a depot storing military aid for Ukraine in the United Kingdom (March 2024[67]); the burning of Bundeswehr Rheinmetall army trucks at a military facility in Erfurt (June 2025)[68]; sabotage attempts against weapons facilities in Sweden[69]; and attempted sabotage of the German navy corvette Emden (late 2024)[70] or the navy frigate Hessen (February 2025).[71]

Attacks have also targeted transport and logistics infrastructure. There has been a notable increase in sabotage and arson incidents affecting railway systems in Germany, as well as similar cases in Czechia and France, including acts of sabotage just before the official opening of the Olympic Games. Some incidents directly targeted the transportation of military and humanitarian aid to Ukraine in Poland.[72] In November 2025, a major sabotage case in Poland involved blowing up a railway segment between Warsaw and Lublin, which is used for logistics into Ukraine.[73]

---

[65] https://wiadomosci.gazeta.pl/polska/7%2C198072%2C32218705%2Cogromny-pozar-pod-lublinem-w-akcji-ponad-100-strazakow-sytuacja.html
[66] https://www.postimees.ee/8279658/video-ukraina-restorani-ja-toidukaupluse-suudanud-moldova-kodanikud-tegid-gru-tellimustood
[67] https://apnews.com/article/russia-ukraine-london-arson-warehouse-intelligence-a00f7429e0688731ff1718d2c3bb855f
[68] https://militarnyi.com/en/news/russians-publish-footage-of-arson-of-military-equipment-in-germany/#google_vignette
[69] https://www.theguardian.com/world/article/2024/aug/29/sweden-warns-of-heightened-risk-of-russian-sabotage
[70] https://militarnyi.com/en/news/sabotage-on-emden-corvette-foiled-in-germany/
[71] https://www.tagesschau.de/investigativ/marine-kriegsschiff-sabotageverdacht-100.html
[72] https://www.gazetapolska.pl/30717-mieli-wysadzac-pociagi-w-polsce-kulisy-zatrzymania-rosyjskich-szpiegow-moskwa-placila-w-bitcoinach
[73] https://x.com/donaldtusk/status/1990328246848909536?s=20
[74] https://www.gov.pl/web/prokuratura-krajowa/akt-oskarzenia-wobec-dwoch-obywateli-rosji-za-szpiegostwo-na-rzecz-rosyjskiego-wywiadu
[75] https://www.gov.pl/web/prokuratura-krajowa/wszczecie-sledztwa-w-sprawie-dzialalnosci-obcego-wywiadu-i-przygotowan-do-aktow-sabotazu
[76] https://www.dw.com/en/germany-more-bomb-threats-against-schools-and-public-sites/a-67236957
[77] https://www.msn.com/en-gb/news/world/police-receive-hundreds-of-calls-over-threat-to-berlin-schools/ar-AA1QA0rK
[78] https://news.err.ee/1609258853/iss-russian-special-services-behind-attack-on-estonian-minister-s-car
[79] https://www.reuters.com/world/europe/threat-plot-murder-rheinmetall-ceo-was-part-sabotage-campaign-nato-says-2025-01-28/
[80] https://www.eurointegration.com.ua/news/2024/04/18/7184138/

Other operations have included the dispatch of packages containing explosive devices [74] and flammable materials [75], waves of fake bomb threats — for instance, multiple threats against public institutions and schools in Germany in autumn 2023 [76] and again in Berlin in autumn 2025 [77] — and vandalism of vehicles and monuments, including attacks against the car of the Estonian Minister of the Interior and against journalists.[78] Physical assaults and assassination attempts have also been recorded, including the failed attempt on Rheinmetall CEO Armin Papperger [79] and the foiled plot to assassinate Ukrainian President Volodymyr Zelenskyy.[80]

By now, most of these acts have been officially and publicly attributed to Russia, particularly to the Russian military intelligence service (GRU), by security agencies in various European states. In several cases foreign involvement was initially denied, however, subsequent investigations confirmed that Russian intelligence services had orchestrated the attacks. One notable example is the arson of the large shopping centre "Marywilska 44" in Warsaw on 12 May 2024: although officials at first dismissed the possibility of Russian involvement [81], further investigation conclusively established it.[82]

In July 2024, one of the largest sabotage operations to date took place across Europe, when an organised terrorist network supported by Russia used international parcel delivery and transport services of major companies — DHL and DPD — to send parcels containing improvised explosive devices from Vilnius to multiple destinations. Two parcels were addressed and dispatched by DHL cargo aircraft to the United Kingdom: one detonated at Leipzig Airport in Germany just before being loaded onto a connecting flight, while the second exploded at a DHL warehouse in Birmingham. Two more parcels were sent by DPD trucks to Poland: one detonated en route, and the other failed to explode due to a technical malfunction.

On 17 September 2025, the Prosecutor General's Office of the Republic of Lithuania and the Lithuanian Criminal Police Bureau confirmed [83] attribution to the citizens of the Russian Federation with links to Russian military intelligence services. Fifteen suspects — citizens of the Russian Federation, Lithuania, Latvia, Estonia, and Ukraine — were charged with organising and carrying out the attacks. Investigators further concluded that several of the coordinators were also directly linked to the attempted terrorist attack in Vilnius on 9 May 2024, when the IKEA shopping centre was set on fire.

[81] https://tvn24.pl/polska/tusk-zabral-glos-w-sprawie-pozarow-st7915989
[82] https://www.politico.eu/article/russia-warsaw-poland-fire-donald-tusk/
[83] https://www.prokuraturos.lt/lt/isaiskinta-ir-sulaikyta-asmenu-grupe-organizavusi-ir-planavusi-ivykdyti-keturis-teroro-aktus-turincius-hibridiniu-tikslu-with-english-translation/11619

ATTACKS ON UNDERWATER INFRASTRUCTURE

Incidents affecting undersea infrastructure highlight the vulnerability of critical maritime assets and the challenges of attribution in this domain. The cumulative nature of disruptions suggests probing and testing behaviour rather than isolated accidents. The gap between growing threats and limited enforcement capacity remains a key structural weakness, especially in what concerns the Russian "shadow fleet".

After Finland and Sweden joined NATO in 2023 and 2024, there was hope that the Baltic sea would become a so-called "NATO lake." Instead, following the Russian full-scale invasion of Ukraine, the Baltic Sea has become a zone of rising tension and a testing ground for Russian hybrid operations against the EU and NATO.

The region hosts rich critical infrastructure, including undersea cables, pipelines, extraction platforms, and wind power plants. Since 2023, undersea infrastructure has been increasingly targeted by Russian—and sometimes Chinese—malign activities. Notable incidents include:

- October 2023: Damage to the Balticconnector pipeline and undersea communication cable connecting Estonia and Finland, believed to have been caused by the anchor of a Chinese vessel.[84]

- November 2024: Two undersea cables—connecting Finland–Germany and Sweden–Lithuania—were damaged [85] and another Chinese ship was suspected.[86]

- December 2024: Multiple undersea cables, including the Estlink 2 power cable (Finland–Estonia), were damaged, potentially by Russian "shadow fleet" vessels.[87]

- January 2025: The fiber-optic telecommunication cable linking Latvia and the Swedish island Gotland was damaged, [88] and a Norwegian ship with a Russian crew was arrested under suspicion of involvement.[89]

- September 2025: the Finnish operator Fingrid informed of the disturbance with undersea power cable Estlink 1 connecting Estonia and Finland.[90]

Related to that is the use of the so-called Russian "shadow fleet" – the fleet of aging tankers with obscure ownership and flags of third countries, which pass through the Baltic Sea transporting Russian oil and evading Western sanctions against Russian oil exports. In addition to sanction evasion and obvious environmental risks related to their poor condition, these vessels are linked to damaging undersea infrastructure, intelligence gathering and sabotage activities. Moreover, they were also suspected to serve as platforms to launch and control drone operations against a number of European states.[91]

In response, NATO littoral states increased their presence, patrolling and monitoring in the Baltic Sea, conducted exercises [92] to increase abilities to protect the undersea infrastructure. In May 2024, NATO launched a new Maritime Center for Security of Critical Undersea Infrastructure in British Northwood. [93] In October 2024, Germany inaugurated a new multinational naval tactical headquarters for the Baltic Sea in its port of Rostock. [94] And in January 2026, Finland's Border Guard Service announced plans to establish a maritime surveillance centre to prevent damage to critical undersea infrastructure in the Gulf of Finland. [95]

In January 2025, leaders of NATO littoral states agreed the action plan to respond to the damages of the undersea infrastructure [96], and NATO announced the start of the "Baltic Sentry" mission to enhance vigilance, improve the ability to protect critical undersea infrastructure of the Baltic Sea and respond if required [97]. In October 2025, the EU High Representative and Vice-President Kaja Kallas appointed a special envoy for the "shadow fleet". [98]

In January 2026, a group of 14 European coastal states issued a joint declaration on the growing risks for maritime safety [99], warning that tankers from Russia's shadow fleet with dubious flag registrations or documentation would be subject to closer legal scrutiny and enforcement under international maritime law. Over the years, the EU has also sanctioned hundreds of vessels in the "shadow fleet." However, the enforcement actions often stop at inspection rather than seizure.

Several countries have taken actions to detain the vessels of the Russian shadow fleet, however, some of them discovered they do not have the necessary legislative basis in place to proceed with the seizure. Thus, in January 2026, French naval forces intercepted a Russian shadow fleet tanker, detained it for several weeks, but later released it upon a fine payment.[100]

---

[84] https://www.eurointegration.com.ua/news/2023/11/10/7173302/
[85] https://www.bbc.com/news/articles/c9dl4vxw501o
[86] https://www.npr.org/2024/11/21/nx-s1-5198511/two-undersea-data-cables-damaged-in-the-baltic-sea
[87] https://apnews.com/article/eu-finland-estonia-baltic-sea-power-cable-6741ef1ce9130602abac6214d7297717
[88] https://p.dw.com/p/4pegY
[89] https://www.eurointegration.com.ua/news/2025/01/31/7203873/
[90] https://yle.fi/a/74-20180367?utm_medium=social&utm_source=copy-link-share
[91] https://nv.ua/ukr/world/geopolitics/rosiya-zapuskaye-droni-po-yevropeyskih-krajinah-z-tankeriv-zayaviv-zelenskiy-50548585.html
[92] https://www.bundeswehr.de/en/organization/navy/news/northern-coasts-germany-baltic-sea-exercise
[93] https://mc.nato.int/media-centre/news/2024/nato-officially-launches-new-nmcscui#:~:text=Northwood%2C%20UK%20%E2%80%93%20NATO%20has%20established%20a%20new,disrupting%20energy%20supply%2C%20global%20communications%20and%20economic%20activity.
[94] https://www.dw.com/en/germany-inaugurates-new-naval-hq-on-the-baltic-sea/a-70553331
Finland hopes to prevent cable damage with new surveillance centre | Reuters
[95] https://www.presidentti.fi/en/joint-statement-of-the-baltic-sea-nato-allies-summit/

The first precedent of the confiscation happened in March 2025, when Germany's customs detained the tanker Eventin, confiscated its cargo and replaced its crew.[101] In March 2026, Belgian special forces assisted by the French Navy boarded and detained another "shadow fleet" tanker Ethera, and the authorities started procedures to confiscate it.[102]

The response to the Russian shadow fleet has gradually become more determined, but the institutional and legal frameworks are still not at the level required by the threat. Moreover, Russia has also responded by increasing security for these tankers, including occasional military escorts.

3. COGNITIVE INFLUENCE AND DESTABILISATION

DISINFORMATION, ELECTION AND POLITICAL INTERFERENCE

Russian information operations increasingly combine traditional propaganda with digitally enabled manipulation and covert influence networks. A key feature is the alignment of narratives with ongoing events, including crises and political processes, allowing rapid exploitation of emerging vulnerabilities. The integration of disinformation with cyber operations and real-world incidents reinforces its credibility and impact, while amplifying societal divisions.

Russia continues to use both traditional media and social media not only to spread disinformation and propaganda, but also to conduct Foreign Information Manipulation and Interference (FIMI).[103] Through intentional manipulation and coordinated activities, Moscow seeks to shape the information environment in a deceptive and coercive manner. Its objectives are to undermine public trust in national institutions, weaken democratic processes in European states, amplify existing social divisions, and exploit sensitive topics such as migration. Crucially, these operations aim to influence public perceptions of Ukraine and erode European support for Kyiv in the context of Russia's war of aggression.

[97] https://www.nato.int/cps/en/natohq/news_232122.htm
[98] https://www.eeas.europa.eu/delegations/ukraine/high-representative-kaja-kallas-%E2%80%9Cafter-19th-package-sanctions-eu-should-work-next-package-which-will_en?s=176
[99] https://www.gov.uk/government/publications/the-growing-risks-to-maritime-safety/the-growing-risks-to-maritime-safety
[100] https://apnews.com/article/russia-shadow-fleet-tanker-grinch-france-bc3031812f1ffcde8705af80c1cb23fd
[101] https://www.bloomberg.com/news/articles/2025-03-28/germany-takes-control-and-replaces-crew-of-seized-oil-tanker?srnd=homepage-europe
[102] https://www.theguardian.com/world/2026/mar/01/suspected-russian-shadow-fleet-tanker-seized-north-sea

Since the ban in March 2022 on Russian state propaganda broadcasting of Russia Today (RT) and Sputnik[104], many European authorities — including Germany's Federal Ministry of the Interior — have observed a sharp increase in Russia's use of social media platforms to promote its narratives to the broadest possible audience. In particular, Telegram has become a central platform for the distribution of disinformation, serving as an alternative channel to previously banned or restricted media outlets.[105]

Russian-affiliated cultural and religious institutions – most notably linked to "Russkiy Mir Foundation" and Russian Orthodox church – also continue to serve as an influence tool abroad. Across various countries, in particular, Germany, Finland, Estonia, Bulgaria, the Western Balkans they engage in dissemination of pro-Kremlin messages.

A number of recent examples illustrate the scope and variety of Russian FIMI operations. When in September 2025 dozens of Russian drones violated Polish airspace, Russia pushed disinformation claiming that Ukraine was responsible for the attacks. Polish officials underlined that Moscow deliberately exploited public fears and emotions to spread pro-Russian and anti-Ukrainian sentiments.[106] In November 2025, the major sabotage operation on the Polish railways – attributed to Russia – has also immediately seen the rise of disinformation narratives in Polish and Russian information space redirecting responsibility for the sabotage onto the Ukrainian side and discrediting the actions taken by the Polish security services.[107]

Russia's psychological operations in Poland further aim to create an atmosphere of fear and a sense of threat, inciting anti-Ukrainian sentiments among the Polish people.[108] According to the services, these narratives are combined with kinetic activities, such as arson of Ukrainian cars, or covering of anti-war murals.

Russia also exploits natural disasters and domestic challenges to undermine citizens' trust in their own governments. For example, during flooding in southwestern Poland in September 2024, Russian-linked networks disseminated manipulative content designed to evoke fear and helplessness among the citizens.[109]

[103] https://www.disinformation.ch/EU_Foreign_Information_Manipulation_and_Interference_(FIMI).html
[104] https://www.consilium.europa.eu/en/press/press-releases/2022/03/02/eu-imposes-sanctions-on-state-owned-outlets-rtrussia-today-and-sputnik-s-broadcasting-in-the-eu/
[105] https://www.verfassungsschutz.de/SharedDocs/publikationen/EN/reports-on-the-protection-of-the-constitution/2024-06-brief-summary-2023-report-on-the-protection-of-the-constitution.pdf?__blob=publicationFile&v=4
[106] https://x.com/donaldtusk/status/1967176203447701546
[107] https://www.gov.pl/web/cyfryzacja/narracje-dezinformacyjne-na-temat-sabotazu-polskich-linii-kolejowych
[108] https://x.com/SztabGenWP/status/1985279185200316761?s=20
[109] https://x.com/CyberWojska/status/1837842277781094752

During farmers' protests in Poland and Belgium in January and February 2024, pro-Russian banners and messages were identified among demonstrators.[110] In France, at the end of 2023, authorities detected a "Russian footprint" behind an artificially generated panic over alleged bedbug infestations, which led to the temporary closure of several schools.[111] Moscow also carried out a campaign to discredit France, its president, and the International Olympic Committee [112] by spreading narratives about France's alleged inability to guarantee safety during the Paris 2024 Olympic Games — aiming to discourage attendance and erode confidence in French authorities.

Russian information operations often include direct falsification and fake news through cyber-enabled disinformation. In June 2024, Russian hackers breached the website of Poland's state news agency PAP, publishing a fake report announcing a "partial mobilisation" of 200,000 Polish citizens to fight in Ukraine.[113] In April 2024, France's agency for countering foreign influence, Viginum, published a report exposing a Russian operation codenamed Portal Kombat, involving at least 193 websites disseminating Kremlin propaganda about the war in Ukraine.[114] Earlier, in June 2023, Viginum had revealed another major operation, Doppelgänger, which cloned prominent Western media websites.[115] Between June 2022 and May 2023, 355 domain names impersonated outlets such as France's 20 Minutes, Le Monde, Le Parisien, and Le Figaro, as well as Germany's Frankfurter Allgemeine Zeitung, Der Spiegel, Bild, and Die Welt. In France, these clones also targeted government sites — including that of the French Foreign Ministry — through typosquatting of domain names.[116] The fake content was then amplified by Russian embassies and cultural centres.

---

110 https://www.rmf24.pl/regiony/lublin/news-proputinowskie-banery-na-kolejnym-rolniczym-protescie,nId,7351860

111 https://www.lemonde.fr/en/france/article/2024/03/01/bedbug-panic-was-stoked-by-russia-says-france_6575870_7.html

112 https://apnews.com/article/france-election-disinformation-russia-olympics-be18d688677240686df200096018f221

113 https://www.onet.pl/informacje/onetwiadomosci/falszywa-depesza-w-serwisie-pap-to-prawdopodobnie-atak-hakerski/bljf2f6,79cfc278

114 https://www.sgdsn.gouv.fr/files/files/Publications/20240428_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK-REPORT_NEW%20DOMAIN%20NAME_%28PART3%29_ENG_VF.pdf

115 https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/news/2023/article/statement-by-ms-catherine-colonna-foreign-digital-interference-france-s

116 Typosquatting also known as cybersquatting is the abusive practice of registering and using an internet domain name with a small change/typo almost identical to trademarks, service marks, personal names or company names with the bad faith intent

117 https://www.reuters.com/world/europe/poland-says-russia-is-trying-interfere-presidential-election-2025-05-06/

118 https://www.eurointegration.com.ua/eng/news/2023/12/7/7175106/

119 https://www.independent.co.uk/news/world/europe/russian-interference-disinformation-elections-moldova-uk-b2836457.html

120 https://www.voanews.com/a/russia-sustains-influence-operation-to-undermine-integrity-of-european-elections-/7654747.html

Election and political interference remain central components of Russian disinformation and FIMI strategies. Russia frequently supports far-right groups and actors promoting pro-Russian and anti-EU and anti-NATO narratives. Through coordinated networks of websites, proxy organisations, and covert agents, Moscow spreads false narratives, fake or manipulated content ahead of the elections, and manipulates public discourse, by aggravating the internal divisions and undermining electoral integrity.

Multiple European states – including Poland,[117] United Kingdom [118], Germany, France, Moldova [119] – have reported unprecedented levels of Russian interference, in some cases directly linked to the Russian FSB. A particularly large and multi-faceted operation targeted the European Parliament elections in June 2024.[120] European security agencies exposed a pro-Russian network responsible for orchestrating influence campaigns and media operations against EU institutions and Ukraine. Central to this network was the international website voice-of-europe.eu, which published fake or biased articles, comments, and interviews. It is believed to have been financed by pro-Russian Ukrainian politician and oligarch Viktor Medvedchuk.[121]

Beyond spreading disinformation, the network also engaged in bribery of politicians across Europe — including in Poland, Hungary, Germany, France, Belgium, and the Netherlands.[122] In September 2025, former UK Member of the European Parliament Nathan Gill pleaded guilty to accepting payments in exchange for making statements supportive of pro-Russian media operating in Ukraine between 2018 and 2020.[123]

INSTRUMENTALISED MIGRATION

The use of migration as a pressure tool reflects a deliberate strategy of exploiting legal, humanitarian, and political constraints within the EU. These operations are state-coordinated, sustained over time, and adaptable to changing political conditions. Their effectiveness lies not only in physical border pressure but also in their capacity to generate internal political tensions within targeted states.

121 https://www.bbc.com/news/world-europe-68685604
122 https://ua.korrespondent.net/world/4674743-rosiiska-merezha-nove-vykryttia-u-yevropi
123 https://www.counterterrorism.police.uk/former-mep-pleads-guilty-to-bribery-following-investigation/
124 https://foreignpolicy.com/2021/09/18/russia-belarus-poland-lithuania-migrants-eu-weapon/
125 https://news.sky.com/story/eu-threatens-belarus-sanctions-as-it-rejects-election-result-12052472
126 https://theweek.com/news/world-news/europe/952979/belarus-dictator-threatens-flood-eu-with-drugs-migrants-avoid-sanctions
127 https://www.dw.com/en/poland-baltics-step-up-border-controls-amid-migrant-crisis/a-69350351

Russia and Belarus deliberately orchestrated migration flows as a hybrid pressure instrument against the EU. In 2021 "migration crisis"[124] was first created as the tool of pressure on Poland and other neighbouring countries. It followed the European Union refusal to recognise the results of the 2020 Belarusian presidential elections and the imposition of sanctions in response to electoral fraud and the use of force against protestors. Additional sanctions were imposed after the May 2021 forced landing of a civilian plane in Belarus and the arrest of two passengers.[125] Lukashenko publicly threatened to "flood Europe with migrants and drugs"[126] and a sudden surge in irregular border crossings was immediately observed. Belarusian border guards directly facilitated the movement of migrants from the Middle East and Africa toward the borders of Poland, Lithuania, and Latvia, with other state authorities supporting their transit.

Since Russia's full-scale invasion of Ukraine, this tactic has intensified again. According to DW,[127] citing the statistics of the relevant border guard services, between 2021 and mid-2024, migrants made nearly 150,000 attempts to illegally cross into Poland, Lithuania, or Latvia, with Poland experiencing the highest number of incidents. In 2021, illegal crossings at these borders peaked at 52,151, while in 2022, decreased to 31,497 attempts. In 2023, crossings rose again to 43,005 attempts overall, including 26,500 at the Polish border and 13,863 at the Latvian border.

In 2025, irregular migration pressure has primarily targeted the Polish border, although flows at the Latvian and Lithuanian borders have also increased since April 2025.[128] By October 2025, there had already been 28,000 attempted illegal crossings at the Polish-Belarusian border.[129]

Weaponised migration has forced Poland and Baltic states to significantly reinforce the security of their eastern borders, deploying additional personnel and resources. In June 2022, Poland constructed a five-meter metal barrier on its border with Belarus,[130] complemented by electronic surveillance systems and an increased presence of Border Guard and Armed Forces personnel.

128 https://valtioneuvosto.fi/en/-/1410869/eu-external-border-countries-face-common-security-challenges-both-on-land-borders-and-in-the-baltic-sea
129 https://www.facebook.com/share/r/1BV5CEhJFH/
130 https://x.com/Straz_Graniczna/status/1542403492102414338
131 https://x.com/KosiniakKamysz/status/1798710293935083856
132 https://tvpworld.com/78042420/poland-reintroduces-buffer-zone-at-belarus-border-to-curb-migration
133 https://www.rmf24.pl/fakty/polska/news-prawo-do-skladania-wnioskow-o-azyl-zawieszone,nId,7938595#crp_state=1
134 https://www.rmf24.pl/fakty/polska/news-o-polnocy-granica-z-bialorusia-zostala-calkowicie-zamknieta,nId,8019545
135 https://www.mod.gov.lv/en/news/baltic-defence-ministers-agree-baltic-defence-line
136 https://tarczawschod.wp.mil.pl/en/
137 https://www.cbc.ca/news/world/poland-ottawa-convention-landmines-9.7098794
138 https://www.hs.fi/politiikka/art-2000010336512.html
139 https://valtioneuvosto.fi/en/situation-at-finlands-eastern-border
140 https://www.eurointegration.com.ua/news/2024/03/14/7181733/

Following a violent attack on Polish border patrols in May 2024, which included the deadly stabbing of a Polish soldier, [131] Poland reintroduced a temporary "buffer zone" along the border with Belarus.[132] In place since June 2024, its duration has been extended multiple times and is currently in effect. In March 2025, the Polish government restricted the right to submit applications for asylum at the Polish-Belarusian border.[133] And in September 2025, Poland temporarily closed the border entirely due to the Russian-Belarusian military drills "Zapad-2025" coinciding with an increased flow of migrants.[134]

Beyond immediate border-control measures, several countries have also launched broader military-defence initiatives. In January 2024, the Baltic states ministers agreed to begin construction of a common Baltic Defence Line to strengthen their borders with Russia and Belarus, incorporating physical barriers to slow or block potential aggressors. [135] Poland also announced a massive project called "East Shield" scheduled for implementation between 2024 and 2028, aiming to enhance Poland's resilience to attacks and hybrid warfare from the Russian and Belarusian borders.[136] The project includes fortifications, defensive structures, natural obstacles, intelligence and threat detection systems, forward bases, logistics hubs, warehouses, and counter-drone systems. Additionally, by February 2026, Poland and the Baltic states officially withdrew from the Ottawa Convention on anti-personnel mines[137] to strengthen border protection.

While the Eastern Flank of NATO and EU has been most affected Russia has also employed migration as an instrument against other European countries. At the end of 2023, Finland temporarily closed border crossing points with Russia after Moscow organized an influx of asylum seekers to exert political pressure.[138] Since August 2023, more than 1,300 third-country nationals had arrived in Finland from Russia without visas[139], and Finnish authorities reported thousands more waiting near the border.[140]

4. MILITARY SIGNALING AND THRESHOLD TESTING

AIRSPACE VIOLATIONS, MILITARY AND OTHER PROVOCATIONS

Russian military provocations show a gradual increase in frequency, boldness, and operational complexity. While individual incidents often remain below escalation thresholds, their cumulative effect is to test response mechanisms and normalise risk. The introduction of new tools — such as drones and unconventional aerial objects — further blurs the boundary between civilian disruption and military signalling.

Since the Russian full scale invasion of Ukraine, Russian military provocations and airspace violations have steadily increased. While Russian initial intention was to deliberately stay below NATO's article 5 threshold, its provocations have become increasingly blatant. In the absence of a clear response from NATO, Moscow appears to be gradually eroding the Western red lines.

Typical Russian provocations have long included approaching NATO aircraft, drones, or ships closely, flying with transponders off and without filing flight plans, flying near NATO airspace, and even briefly entering it. While this is a dangerous practice, NATO usually classifies such provocations as "unsafe or unprofessional behavior" rather than as a direct threat; it intercepts and escorts the aircraft out. Russia uses these actions to test Western air defence readiness, conduct surveillance, and signal its military posture.

Numerous incidents illustrate this pattern. In 2025, two Russian military aircraft were detected in the air defense identification zone of Alaska,[141] Russian military jet overflew the German navy frigate in the Baltic Sea[142] and the Polish petrol platform Petrobaltic.[143] Russian surveillance aircraft violated Polish airspace over the Baltic Sea[144], and so did a Russian military helicopter.[145] In March 2025, a Russian Su-35 fighter jet engaged in a dangerous provocation against a French Reaper drone over the Mediterranean Sea, approaching it consecutively for three times.[146]

While such provocations are often classified as non-threatening, they still pose risks. For example, in March 2023, two Russian Su-27 aircraft conducted a dangerous interception of a U.S. Air Force MQ-9 surveillance and reconnaissance drone in international airspace over the Black Sea, as a result of which the drone was damaged and lost.[147]

Estonia further illustrates Russia's gradual escalation. Since Russian occupation of Crimea in 2014 – and as of September 2025 – Russian military aircraft have violated Estonian airspace more than 40 times.[148] In 2025 there were four severe incidents, including Russian Su-35 fighter for less than a minute,[149] Russian Mi-8 helicopter for about four minutes,[150] and three Russian MiG-31 fighter jets for a total of 12 minutes. In all cases, NATO intercepted the aircraft, but responses have so far not deterred Russia from intensifying violations.

141 https://www.airandspaceforces.com/norad-russian-warplanes-alaska-nato/
142 https://euromaidanpress.com/2025/09/25/russia-overflew-a-german-navy-frigate-germany-says-it-was-no-accident/
143 https://x.com/Straz_Graniczna/status/1969080427445907624
144 https://x.com/DowOperSZ/status/1933540824085680261
145 https://x.com/DowOperSZ/status/1916040992966267264
146 https://x.com/SebLecornu/status/1896929663118680335
147 https://www.reuters.com/world/europe/us-says-reaper-drone-crashes-into-black-sea-after-russian-intercept-2023-03-14/

A similar pattern can be observed with the Russian drones flying into the air space of the NATO/EU countries. By now, there were multiple such instances, but the countries concerned would classify them as not purposefully threatening. However, on the night of September 10, about 20 Russian drones flew into Polish airspace, with some of them flying nearly 300 km deep from the eastern border, highlighting deliberate intent. Also for the first time the drones were flying directly from Belarus into Poland, as Prime Minister Tusk noted.[151] Moreover, Ukrainian President Zelenskyy later noted that more than 90 drones were flying into the direction of the Polish border but were intercepted by Ukrainian air defence. Polish air defence shot down only a few, with authorities assessing the rest as not posing any threat. Since then the remnants of drones were found in different parts of the country – most recent one in March 2026.[152]

Missile overflights have also raised concerns, especially for Poland, which has seen a number of such cases. In November 2022, a missile landed in Polish territory during Russia's large-scale attack on Ukraine, killing two civilians. While its origin was debated, authorities attributed responsibility to Russia, as the attack occurred due to Moscow's war operations. Another incident involved the X-55 missile remnants found near Bydgoszcz in April 2022 [153] , reportedly fired from Belarus several months before during the December 2022 Russian strikes. Because of its late discovery, the incident provoked discussion on whether Polish air defence even spotted the missile. Polish authorities confirmed radar tracking of the missile along its 400 km trajectory but admitted that the Minister of Defence had not been informed in real time.[154] Officials later stated the missile "posed no serious threat" and appeared intended to confuse Ukrainian defenses.[155]

In December 2023, a Russian missile (X-22 or X-101) entered Polish airspace for about 40 km before returning to Ukraine.[156] Although fully tracked by radar, no defensive action was taken. Since then, Poland has scrambled F-16 jets during every major Russian strike on Ukraine to monitor incursions more actively. Polish air defense continues to assess that these missiles are not aimed at targets on Polish territory and therefore does not engage them.

148 https://news.err.ee/1609806794/russian-jets-have-breached-estonian-airspace-over-40-times-since-2014
149 https://rus.err.ee/1609694261/rossijskij-istrebitel-narushil-vozdushnoe-prostranstvo-jestonii
150 https://rus.err.ee/1609793487/rossijskij-vertolet-narushil-vozdushnoe-prostranstvo-jestonii
151 https://x.com/PremierRP/status/1965693174283915499
152 https://polskieradio24.pl/artykul/3659393,dron-znaleziony-w-wielkopolsce-na-miejscu-pracuja-sluzby
153 https://www.eurointegration.com.ua/articles/2023/05/15/7161663/
154 https://www.rmf24.pl/raporty/raport-wojna-z-rosja/news-blaszczak-wskazuje-winnego-w-sprawie-rakiety-pod-bydgoszcza,nId,6771225#crp_state=1
155 https://english.nv.ua/nation/poland-says-russian-missile-that-crashed-near-bydgoszcz-in-december-was-no-threat-50326262.html
156 https://www.rmf24.pl/fakty/polska/news-rosyjska-rakieta-wleciala-na-terytorium-polski-ustalenia-po-,nId,7238116#crp_state=1

Another example is the use of the meteorological sondes and smugglers balloons. Since 2022 Russian full-scale invasion, such violations have occurred intermittently, but by 2024-2025 they became a highly disturbing practice. Several incidents with meteorological balloons were reported in Poland in March[157], June[158] 2024 and January 2025,[159] originating from Kaliningrad region of Russia. In October 2025, the scale of the incidents escalated. On 26 October 2025, Lithuanian authorities reported 66 such objects in their airspace[160] . Massive incursion of smugglers balloons from Belarus forced temporary closure of the airspace over the Vilnius airport and its border crossings with Belarus. On 27 October, the authorities decided to fully close the border with Belarus until 30 November.[161] Vilnius airport continued to face disruptions in its work in November, too, with a peak of the smugglers' balloons from Belarus recorded on 24 November.[162] On 9 December 2025, the Lithuanian government declared a state of emergency due to the meteorological sondes from Belarus.[163] With some measures taken, the intensity of incidents decreased, but they still continued.

Since September 2025, Russia has also employed a new dangerous practice to disturb civilian aviation of European countries with the use of "unknown" drones. The airports in Copenhagen (Denmark), Oslo (Norway)[164] , Vilnius (Lithuania), Munich[165], Berlin[166], Bremen[167] (Germany), Brussels and Liege (Belgium)[168] , Gothenburg (Sweden)[169] were disrupted. Drones have also been observed over critical infrastructure, military facilities, and factories in various European countries. In early December 2025, four "unidentified military-style drones" breached the no-fly zone close to the Dublin airport and flew close to the flight trajectory of the Ukrainian president's plane.[170]

157 https://www.eurointegration.com.ua/news/2024/03/5/7181076/
158 https://x.com/DowOperSZ/status/1803814997291864223
159 https://www.rmf24.pl/regiony/olsztyn/news-balon-meteorologiczny-z-rosji-znaleziony-na-mazurach,nId,7886198#crp_state=1
160 https://www.lrt.lt/naujienos/lietuvoje/2/2727011/nkvc-vadovas-sekmadienio-vakara-lietuvos-link-skrido-daugiau-balionu-nei-pries-diena
161 https://edition.cnn.com/2025/10/27/europe/lithuania-closes-border-belarus-drones-latam-intl
162 https://news.liga.net/en/politics/news/lithuania-complains-about-the-strongest-weather-probe-attack-in-november-airport-closed-twice
163 https://www.reuters.com/world/lithuania-declares-state-emergency-over-smuggler-balloons-belarus-2025-12-09/
164 https://www.nrk.no/norge/moglege-droneobservasjonar-ved-oslo-lufthamn-1.17599293
165 https://www.reuters.com/business/aerospace-defense/munich-runways-closed-again-pilot-blames-drone-sightings-2025-10-03/
166 https://www.spiegel.de/politik/deutschland/zwischenfaelle-mit-drohnen-auch-ber-flughafen-betroffen-weitere-forderungen-nach-drohnenabwehrzentrum-a-6315b5ab-7178-4529-9ba9-68142723e101
167 https://www.zeit.de/news/2025-11/26/drohne-in-airport-naehe-mann-sorgt-fuer-luftraumsperrung
168 https://edition.cnn.com/2025/11/04/europe/drones-close-brussels-liege-airports-latam-intl
169 https://tvpworld.com/89891458/sweden-shuts-down-gothenburg-airport-after-drone-sighting
170 https://www.thejournal.ie/drones-dublin-ireland-hybrid-warfare-russia-6893104-Dec2025/?utm_source=thejournal&utm_content=top-stories
171 https://www.nato.int/cps/en/natohq/topics_49187.htm#:~:text=Under%20Article%204%20of%20NATO%E2%80%99s%20founding%20treaty%2C%20members,1949%2C%20Article%204%20has%20been%20invoked%20nine%20times.

The increase of the threat from Russia to NATO can also be demonstrated through the formal Article 4 consultations, which provides NATO members with an option to bring an issue to the attention of the principal NATO's decision-making body – North Atlantic Council – in case their territorial integrity, political independence or security is threatened. In the history of the Alliance since 1949, the consultations happened so far nine times, three of them directly related to Russia since 2022, including two initiated in September by Poland and Estonia.

CONCLUSIONS

Russia's ongoing "phase zero war" against Europe demonstrates that hybrid activities are central instruments of strategic coercion, coordinated across multiple domains and actors. Europe's responses to date have often underestimated the scale, sophistication, and cumulative effect of these operations, creating space for Moscow to stretch the limits of what is politically and legally tolerable.

NATO and EU states are trying to avoid a potential confrontation with Russia, even when Russian behavior becomes more aggressive and dangerous to their own security. So far Russia seems to interpret this behavior as an encouragement to further raise the stakes.

Several patterns emerge from the analysis:

1. **Integration across domains** – Cyberattacks, espionage, sabotage, and influence operations increasingly reinforce one another, making isolated defensive measures insufficient.
2. **Use of thresholds** – Operations are deliberately calibrated to stay below formal acts of war while maximizing disruption and political leverage.
3. **Exploitation of vulnerabilities** – Hybrid campaigns often target decision-making bottlenecks, societal divisions, and internal vulnerabilities.
4. **Adaptive operational design** – Russian tactics evolve quickly, combining old methods with new digital tools, intermediaries, and legal or economic levers.

POLICY IMPLICATIONS AND RECOMMENDATIONS

- **Holistic deterrence and resilience:** Europe should develop integrated intelligence, technical, legal, economic, and societal capabilities, reflecting the multi-domain nature of Russian operations.

[172] https://ukrainianvictory.org/publications/stronger-europe-united-front-europe-s-security-is-being-decided-in-ukraine/

- **Strategic acceleration:** The European decision-making mindset must adapt from deliberative peacetime processes to rapid, flexible, and responsive mechanisms, akin to the sense of urgency Ukraine has lived under since 2014.

- **Operational learning from Ukraine:** Ukraine is no longer merely a recipient of support; it is a security provider for Europe. Integrating lessons from its air defense, UAV management, and rapid operational adaptation can help Europe anticipate, absorb, and respond to high-intensity hybrid operations. More on this topic is in the recent paper "Stronger Europe, United Front – Europe's Security Is Being Decided in Ukraine".[172]

- **Mitigation of strategic dependencies:** Europe must reduce reliance on authoritarian-controlled technology and critical components, integrating Ukraine and trusted partners into resilient supply chains.

- **Information and societal resilience:** Counter-disinformation, strengthen media literacy, build trust in institutions, and foster societal cohesion to reduce the impact of cognitive operations.

- **Total defence approach:** Civilian infrastructure protection, horizontal civil society networks, and whole-of-society preparedness are central to credible deterrence.

- **Sanctions enforcement and financial security:** Effective monitoring and enforcement are crucial to prevent circumvention of restrictions. Hungary's blockage of the 90 billion euro loan for Ukraine, as well as of the adoption of the next sanction package significantly undermines Ukraine's financial and strategic security and European cohesion.

Ultimately, Europe's ability to withstand and deter "phase zero" operations depends on recognizing the integrated, multi-domain nature of the threat and responding with rapid and institutionally agile policies. Failure to act decisively risks normalizing coercion, further eroding the threshold of tolerable aggression, and leaving Europe unprepared for the next escalation.

Finally, Russia is not acting alone. As demonstrated by the Russian aggression against Ukraine and recent Iranian attacks against Gulf States, authoritarian[173] regimes continuously co-operate and share technological innovations. Europe equally faces hybrid threats not just from Russia, but from multiple authoritarian regimes. This is why, integrating Ukraine into Europe's security architecture will strengthen democratic consolidation against authoritarian coalitions, as Ukraine's know-how becomes a key pillar of continental security.

This project, «Russia's Undeclared "Phase Zero War" Against Europe», was funded by the European Union. The content of this publication/video/material is the sole responsibility of the "ANTS" NGO and does not necessarily reflect the views of the European Union.

[173] https://www.reuters.com/world/uk/uks-mi5-warns-politicians-they-are-targets-russia-chinese-spying-2025-10-13/