The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure

Charlie Edwards, Senior Adviser, Strategy and National Security;
Nate Seidenstein, Research Assistant

August 2025

IISS
The International Institute
for Strategic Studies

Contents

Cover

A DHL package-delivery cargo airplane stands at Leipzig/Halle Airport on October 15, 2024, in Schkeuditz, Germany. (Photo by Jens Schlueter/Getty Images)

Executive Summary

Russia is waging an unconventional war on Europe. Through its campaign of sabotage, vandalism, espionage and covert action, Russia's aim has been to destabilise European governments, undermine public support for Ukraine by imposing social and economic costs on Europe, and weaken the collective ability of NATO and the European Union to respond to Russian aggression. This unconventional war began to escalate in 2022 in parallel to Russia's invasion of Ukraine. While Russia has so far failed to achieve its primary aim, European capitals have struggled to respond to Russian sabotage operations and have found it challenging to agree a unified response, coordinate action, develop effective deterrence measures and impose sufficient costs on the Kremlin.

IISS has created the most comprehensive open-source database of suspected and confirmed Russian sabotage operations targeting Europe. The data reveals Russian sabotage has been aimed at Europe's critical infrastructure, is decentralised and, despite European security and intelligence officials raising the alarm, is largely unaffected by NATO, EU and member state responses to date. Russia has exploited gaps in legal systems through its 'gig economy' approach, enabling it to avoid attribution and responsibility. Since 2022 and the expulsion of hundreds of its intelligence officers from European capitals, Russia has been highly effective in its online recruitment of third-country nationals to circumvent European counter-intelligence measures. While the tactic has proven successful in terms of reach and volume, enabling operations at scale, the key challenge facing the Russian intelligence services has been the quality of the proxies, who are often poorly trained or ill-equipped, making their activities prone to detection, disruption or failure.

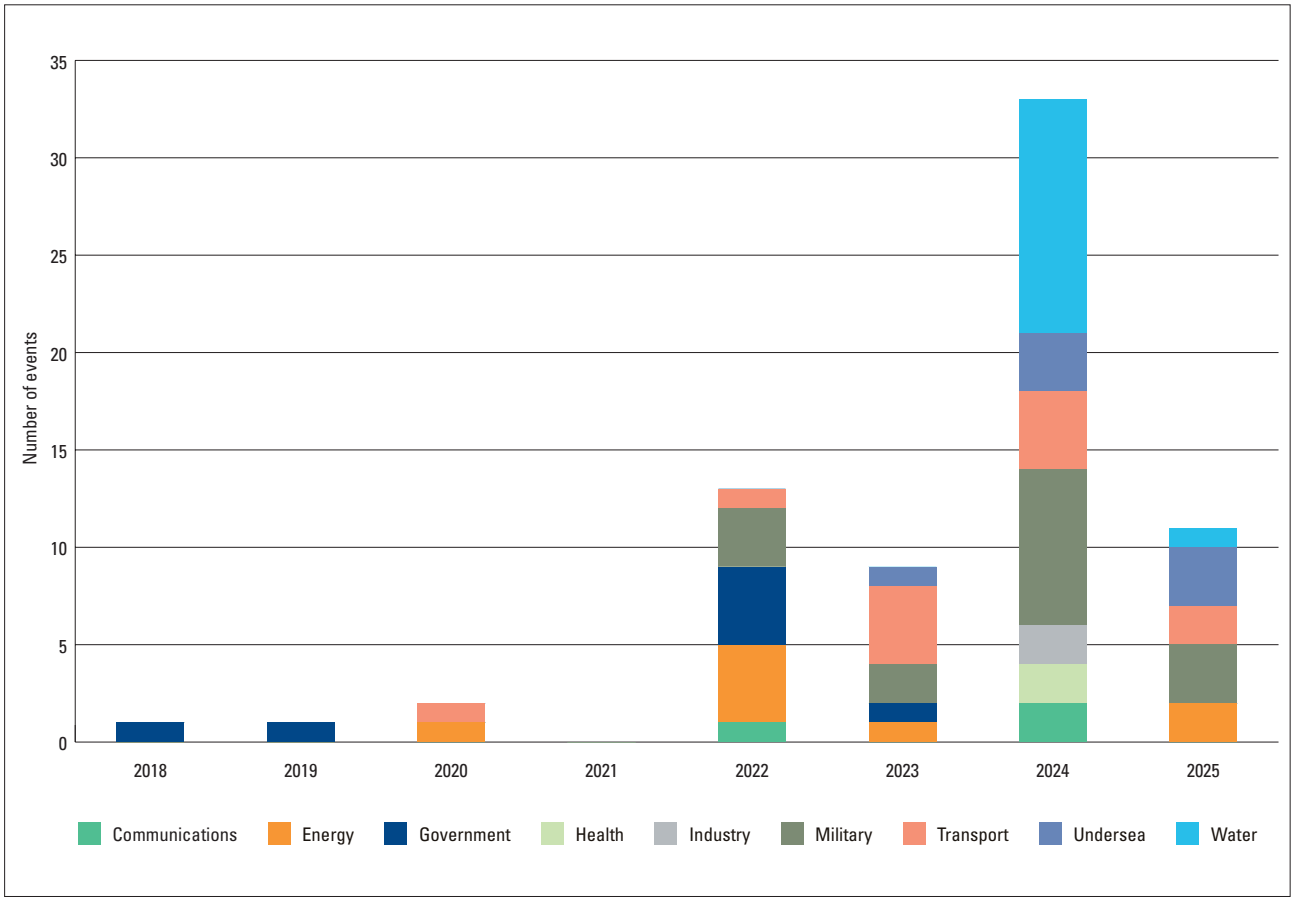
Russia's military doctrine deeply integrates Critical National Infrastructure (CNI) sabotage within *gibridnaya voyna* (hybrid warfare). Europe's critical infrastructure is particularly vulnerable to sabotage because it is in such a poor state following decades of deferred maintenance and a lack of investment from national governments and the private sector. Russia has targeted critical infrastructure to generate direct strategic gain in its war in Ukraine and as part of its broader conflict with the West. While some initiatives, such as the *Baltic Sentry* NATO maritime operation in the Baltic Sea, have been somewhat effective, the lack of budget and resources has kept NATO and the EU from adopting a long-term and sustained response. Furthermore, it is unclear, faced with competing national security priorities, how committed European capitals are to deterring Russia's unconventional war on Europe.

Introduction

As part of Russia's unconventional war on Europe, the Kremlin's sabotage operations and campaign of subversion and disinformation, combined with the full-scale invasion of Ukraine in 2022, are integral to its broader hybrid war aimed at undermining the West. A primary objective of Russia's unconventional war on Europe is to diminish support for Ukraine by increasing costs for governments and industries, harassing populations and exploiting vulnerabilities in European defences.[1] Ukraine has also actively engaged in cyber and drone operations against Russian oil and gas infrastructure and defence-industry installations, exploiting persistent vulnerabilities. These tit-for-tat operations aim to impose costs, disrupt operations and influence public will on both sides, characterising a broader, global contest.

Some NATO member states have assessed Russia's unconventional war to be part of its long-term preparations for a potential military confrontation with NATO.[2] They assess that the focus is on attacking physical and virtual targets using espionage, subversion, ransomware and the abuse of global IT supply chains; and informational operations using widespread disinformation campaigns, propaganda and the dissemination of deepfakes and conspiracy theories.[3] These attack vectors intersect in methods and effects, integrating capabilities across various sectors of the Russian military, intelligence services and non-state actors (including the Wagner Group and criminals).

Figure 0.1: **Frequency of Russian hybrid-warfare activity across Europe, January 2018–June 2025**



Notes: All hybrid attacks in 2022 occurred after the beginning of Russia's full-scale invasion of Ukraine. Energy and communications categories exclude Russian efforts to sabotage undersea cables and pipelines; these actions are counted in the undersea category.
Sources: IISS analysis; Armed Conflict Location & Event Data Project (ACLED), www.acleddata.com; Bart Schuurman, 'Russian Operations Against Europe Dataset', https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/TQ0FMQ

While much attention has been given to Russian cyber operations and disinformation campaigns, far less has been written about the Kremlin's systematic targeting of European Critical Infrastructure (ECI). The targeting of ECI stems from long-standing Russian military doctrine[4] and draws from Soviet-era plans which focused on energy supply systems, such as electric power plants, fuel supply systems, pipelines and refineries.[5] Over the past decade, the Kremlin has targeted energy, transport, banking, financial market infrastructure, health, water, digital infrastructure, and government facilities (including military installations).[6]

More recently, Russian sabotage operations in Europe have increased their range of targets and severity of attacks. The number of attacks almost quadrupled from 2023 to 2024 (see Figure 1). IISS data shows that the most frequent ECI targets are facilities linked to the war in Ukraine and government facilities.[7] Russia targets bases, production facilities and those facilities involved in transporting military aid to Ukraine.

This report draws on a uniquely detailed dataset assembled by the IISS, built on the foundational work of Terrorism and Political Violence Professor Bart Schuurman at Leiden University in the Netherlands and significantly augmented through integration with the Armed Conflict Location & Event Data Project and IISS's own incident monitoring. The result is the most comprehensive open-source database currently available on Russian sabotage operations across Europe and its periphery. It captures the full spectrum of activity with physical effects: from sabotage on undersea cables to GPS blocking across multiple domains and geographies.

The dataset has enabled us to identify patterns in Russia's campaign. However, recognising the inherent uncertainty in attributing covert activity, each incident is assessed using a tiered confidence system, aligned with best practice.[8] Where attribution is ambiguous, the aim has been to distinguish between what is known, what is judged probable, and where there is significant uncertainty. This has been particularly challenging when there is a significant time lag between the underlying events, the completion of long and complex investigations, and court proceedings. Evidence and intelligence often emerge incrementally, which has required careful assessment and corroboration from multiple independent sources.

Decisions about attribution are rarely made in a political vacuum. European governments will likely have weighed up the benefits and disadvantages of 'going public' and may decide the risk is not worth it. Reasons include the fear of escalation, the need to maintain diplomatic space for future negotiations, the protection of sources and methods and to avoid public panic. It may also be, following the expulsion of hundreds of Russian Intelligence Services (RIS) members in 2022, due to a lack of options. As a result, any official attribution of a hostile state act may lag behind sensitive intelligence assessments, while statements made in public reflect broader strategic calculations as much as their confidence in the evidence.

Russia's unconventional war on Europe presents significant policy challenges to Western governments. Russian doctrine intentionally blurs the lines between war and peace, making it challenging for European governments to detect and respond to such aggression. The response by NATO and EU has been to define Russia's unconventional war as operations in the 'grey zone', below the threshold of conventional war. However, the concept of the grey zone, while descriptive of hostile activity below the threshold of direct state-on-state conflict, has outlived its utility: it now too often serves as a bureaucratic shield allowing governments to avoid decisive action and responsibility.

Rather than clarifying the threat, the notion of the grey zone has sown confusion over mandates and accountability, further blurring the boundaries between national security, diplomacy and law enforcement. This disaggregation of responsibility has hindered the emergence of a unified and strategic response; instead, governments frequently default to defensive, reactive measures, doubling down on protection rather than taking the proactive, assertive steps needed to deter and disrupt Russian activity. The tendency to treat each incident in isolation, rather than as part of a wider Kremlin campaign, has compounded the problem and contributed to a lack of coherent, whole-of-government action.

While Russian sabotage operations are estimated to have caused hundreds of millions of euros in physical damage (to submarine cables, pipelines, transport infrastructure, etc.), and to some extent psychological harm

Map 0.1: **Methods of Russian hybrid-warfare activity across Europe, January 2018–June 2025**

Note: Energy and communications categories exclude Russian efforts to sabotage undersea cables and pipelines; these actions are counted in the undersea category.
Sources: IISS analysis; Armed Conflict Location & Event Data Project (ACLED), www.acleddata.com; Bart Schuurman, 'Russian Operations Against Europe Dataset', https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/TQ0FMQ

– by fostering societal anxiety, weakening public trust and exacerbating political divisions – they have yet to be catastrophic. No confirmed civilian deaths have been directly linked to Russian sabotage operations in Europe since the 2022 invasion.

It would, however, be wrong to discount the severity of the threat based on the number of civilian deaths, even if that is a key driver for governments in determining action. The evolving pattern of activity points to a deliberate effort by the Kremlin and the RIS to escalate pressure and uncertainty. The absence of mass casualties does not imply an absence of intent or capability. Rather, it reflects a strategy designed to intimidate, disrupt and probe the resolve of European governments in a manner carefully calibrated to avoid crossing the threshold that would trigger a forceful retaliatory response. Yet

the margin for escalation is narrow: a single security lapse could result in casualties. A small number of outlier incidents, most notably the attempted assassination of Rheinmetall CEO Armin Papperger, point to a more aggressive edge. The targeting of Papperger, and potentially other figures in the defence industry, signals Russia's intent to strike at individuals linked to Western military support for Ukraine, aiming to destabilise the defence-industrial base supporting Kyiv.

The cumulative impact of Russian attacks on physical targets, on virtual targets and via informational operations has been to undermine Western resilience and divide European societies. The effect has also been to lower the threshold for future escalation and increase the risk of strategic miscalculation on both sides.

The report is divided into three sections. Section 1 identifies the systemic vulnerabilities and dependencies that expose European critical infrastructure to Russian sabotage operations, particularly highlighting ageing infrastructure, private-sector ownership risks and the fragility of interconnected and interdependent systems. Section 2 explores Russia's integration of infrastructure sabotage into its broader hybrid-warfare strategy, detailing the evolving methods employed by Russian secret services, including the use of remote operatives and low-tech sabotage tactics designed to evade deterrence. Section 3 addresses the strategic challenge European governments face in responding effectively to Moscow's campaign in Europe. While NATO and EU members have made advances in recognising and mitigating these threats, responses remain predominantly reactive, fragmented and hampered by clear thresholds for responding to Russian aggression. The report concludes with strategic implications of Russia's sabotage campaign, stressing the urgent requirement for a more assertive and proactive stance to counter Russian aggression and safeguard European security.

1. The Vulnerability of Europe's Critical Infrastructure

ECI is vulnerable to sabotage due to a combination of inherent systemic weaknesses and an increasingly complex threat landscape. Modern economies and societies, driven by efficiency and the ever-increasing pace of globalisation, have created increasingly interdependent systems where individual disruptions can have widespread effects. For example, the European blackout of November 2006 occurred when a high-voltage transmission line was purposefully shut down in northern Germany, causing the wider system to overload and switch off. Within seconds the failure had cascaded across multiple borders, reaching as far as Tunisia.[9]

NATO and EU policymakers have highlighted significant ongoing concerns with the resilience of European critical infrastructure. Firstly, there has been a significant lack of investment in ECI in recent decades. The average electricity-grid asset age is around 40 years, meaning about 60% of the total EU grid investment will need to go into basic distribution-grid upgrades.[10] Transportation networks are some of Europe's oldest critical infrastructure. European railways are particularly vulnerable and are prominent targets for sabotage given their critical role in NATO's military logistics. The nature of railroads means a single failure in one system can halt traffic across thousands of miles. The Alliance recognises that credible deterrence and defence relies on adequate logistics capability – not least on its Eastern flank.[11] In some cases, RIS used local criminals to spy on NATO logistics. In Poland, Belarusians, Poles and Ukrainians were tasked with monitoring the flow of military aid to Ukraine, using methods such as placing cameras along railway lines.[12]

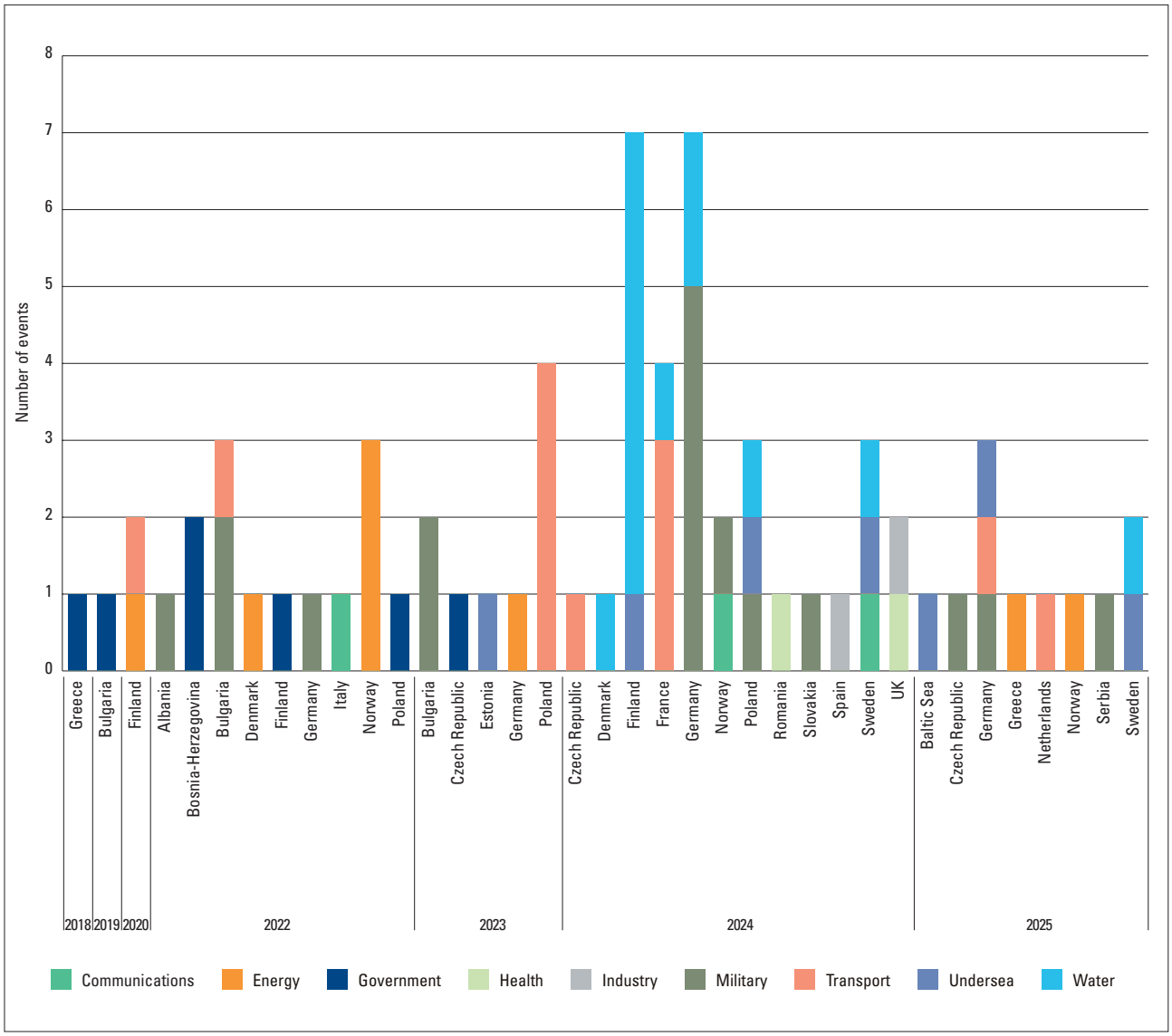
Legacy systems also present their own challenges: Lithuania continues to use Russia's KLUB-U railway locomotive control system, which poses serious cybersecurity risks and potentially enables remote sabotage, surveillance or disruptions.[13] The project to replace the system is expected to take until the end of 2027.

A second concern is the continued use of old computer systems and out-of-date software in ECI. In June 2024, the Netherlands Advisory Council on International Affairs (AIV) found the Netherlands' hydraulic water management seriously outdated, relying on old computer systems connected to digital networks for remote operation but lacking the requisite security. A sabotaged dyke would cause significant damage in a country mostly below sea level. In Haarlemmermeer, North Holland, for example, flooding could reach a metre deep, very quickly overwhelming the entire infrastructure of Schiphol Airport, including highways and rail links.[14]

A third concern is that a significant portion of critical infrastructure is privately owned or operated. While security and resilience are increasingly motivations for investment, as insurers and shareholders push for business security, profit-driven models prioritise efficiency over redundancy, creating inherent weaknesses. About 90% of NATO's military transportation uses civilian assets; more than half of the satellite communications for defence purposes are provided by the commercial sector; and 75% of the support NATO operations receive from host nations comes from local commercial sources.[15] The lack of a single, harmonised regulatory framework and differing national standards for critical infrastructure protection across EU and NATO members complicate efforts to ensure consistent security levels. Regulatory limitations often focus on discrete assets rather than a holistic, system-wide approach to resilience, making it challenging to address transboundary issues and the complex interplay of risks.

Lastly, policymakers have been increasingly concerned by the vulnerability of submarine cables given how reliant the European economy is on them. Cables transmit around 95% of global data flows and underpin an estimated USD$10 trillion in financial transactions every day, and yet they are vulnerable due to physical exposure, strategic importance, large attack surface and limited redundancy.[16] Submarine cables are particularly vulnerable, with more than 70% of yearly incidents caused by unintended cable damage from commercial marine activity.[17]

Figure 1.1: **Russian hybrid-warfare activity by country and year, January 2018–June 2025**



Notes: All hybrid attacks in 2022 occurred after the beginning of Russia's full-scale invasion of Ukraine. Energy and communications categories exclude Russian efforts to sabotage undersea cables and pipelines; these actions are counted in the undersea category.
Sources: IISS analysis; Armed Conflict Location & Event Data Project (ACLED), www.acleddata.com; Bart Schuurman, 'Russian Operations Against Europe Dataset', https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/TQ0FMQ

While the ECI landscape is broad and complex, IISS data suggests that Russian sabotage and covert operations include both random acts of vandalism (designed to sow fear and discord in the local population) and targeted attacks on specific single points of failure within systems. The latter suggests a pattern over the past few years which has included the sabotage of high-speed rail lines hours before the 2024 Paris Olympics opening ceremony;[18] the arrest in Poland of a spy ring placing cameras along railway lines where a single line blockage could halt military logistics to Ukraine;[19] the sabotage of submarine cables[20] where failure cascades regionally; and sabotage of water-treatment plants, such as in August 2024 when German authorities temporarily sealed off a German military base near Cologne airport to investigate suspected sabotage of its water supply. The Cologne incident came shortly after another suspected water-supply sabotage at a NATO base in Geilenkirchen, the headquarters of NATO Airborne Warning and Control System aircraft and an important transport hub for Ukrainian soldiers trained in Germany.[21]

2. Russia's Unconventional War on Europe

Gibridnaya voyna describes aggressive and coercive actions with an emphasis on using all tools of the state and associated non-state actors to achieve political power. In reality, hybrid warfare is an amorphous term with wide theoretical variance in definitions across academic and policy contexts that first emerged around 2005 to describe insurgent conflicts in the Middle East but has since been adapted to a wide array of engagements.[22]

For the Kremlin, *gibridnaya voyna* is used to describe what they perceive as informational warfare waged by the West against Russia and aimed at amplifying internal social, political and ideological divisions to weaken the country from within.[23] General Valery Gerasimov, chief of the general staff of the Russian armed forces, wrote in 2016 that *gibridnaya voyna* aims to 'achieve political goals with a minimal military influence on the enemy … by undermining its military and economic potential by information and psychological pressure, the active support of the internal opposition, and partisan and subversive methods.'[24] An example of this approach is the destruction of Warsaw's largest shopping centre, Marywilska 44, by a fire in May 2024, which Polish officials publicly linked to Russia, illustrating the targeting of civilian commercial facilities with arson.[25] Other incidents of vandalism suggest a broader pattern of low-level, deniable hostile activity.[26]

When describing Russia's comprehensive approach to conflict, which integrates military and non-military means, Russian analysts typically prefer terms like 'new generation warfare' or 'information confrontation' rather than *gibridnaya voyna*. A defining characteristic of this strategy is its whole-of-government approach, where all activities, including conventional military operations, are subordinate to an overarching information campaign with the objective of shaping a target state's governance and geostrategic orientation.[27]

Gerasimov suggests a 4:1 ratio of non-military to military means that broadly employ political, economic, informational, humanitarian and other non-military measures,[28] but that is ultimately rooted in the credible use of military force.[29] Unlike Western approaches, which often separate cyber and information operations, Russian doctrine treats 'information technical' and 'information psychological' activities as inherently integrated.[30]

However, it is worth noting that while that Russian doctrine outlines an integrated, all-encompassing approach to conflict, European security and intelligence agencies perceive a gap between this theoretical framework and its practical, often fragmented, opportunistic and at times counterproductive implementation.[31]

As IISS data shows, confirmed Russian sabotage of ECI increased 246% from 2023 to 2024. This sharp escalation aligns closely with Western removal of restrictions on Ukraine's use of advanced Western-supplied weapons, particularly long-range systems used to strike inside Russia.[32] In the first five months of 2025, publicly available information suggests there have 25 incidents of sabotage, espionage and vandalism against NATO military infrastructure. In May, Germany foiled a Russian-linked parcel-bomb plot targeting logistics networks. Over the past four months, Sweden has investigated suspected sabotage targeting over 30 telecommunications towers along the E22 highway. Because Sweden's civilian and military communications are integrated, damage to fibre networks along major routes like the E22 is highly likely to disrupt secure defence communications and surveillance infrastructure.

Russian sabotage efforts, particularly against critical infrastructure, are not a recent development. The Kremlin has historically targeted submarine cables. In October 2015, United States authorities monitored Russian submarine patrols and the Russian surface ship *Yantar* in a corridor of the North Atlantic that hosts a cluster of undersea cables. The Project 22010-class intelligence ship operated by the Russian Navy carried deep-sea submersibles and cable-cutting gear.[33]

More recently, some of the most disruptive attacks have involved anchor-dragging by Russia's 'shadow fleet'. The shadow fleet travels to and from the ports of Primorsk and Ust-Luga over a large number of submarine cables and undersea infrastructure in a narrow corridor between Finland and Estonia and outside any country's territorial

jurisdiction.[34] In international waters, the flag state has an obligation to punish ships for damaging cables, but there is no authority for the aggrieved states to do so.[35]

Recent Russian sabotage incidents in the Baltic Sea include those involving the Cook Islands-flagged *Eagle S*, which dragged its anchor and cut the Estlink-2 undersea cable in the Gulf of Finland, and the Chinese-flagged *Yi Peng 3*, which is suspected of having deliberately dragged its anchor to cut the C-Lion1 cable connecting Finland and Germany and the Arelion cable linking Sweden and Lithuania.[36] Repairing just one severed cable or pipeline costs tens of millions of euros, not including the economic damage inflicted by the loss of capacity or the additional costs of policing, investigating and defending the maritime domain.[37]

In February 2022, NATO member states began to expel hundreds of Russian officials in retaliation for Russia's full-scale invasion of Ukraine. Of the 600 expelled from Europe in 2022, around 400 were from the RIS.[38] This round of expulsions followed a similar process in the aftermath of Russia's attempt to assassinate Sergei Skripal in 2018 in the United Kingdom when '150 Russian intelligence officers [were] expelled by mainly Western countries'.[39]

The widespread expulsions significantly reduced the number of experienced Russian intelligence officers on the ground and reduced the physical operational capabilities of Russian special services in European countries. It also disrupted the support apparatus through which Russia traditionally conducts many of its operations. In response, the Kremlin adopted a new 'gig economy' approach to sabotage in its operations in terms of recruitment, direction, cost and scale.[40] This allowed the RIS to recruit widely and flexibly while offering limited operational direction and managing their assets remotely. While the tactic has enabled operations at scale, the key challenge facing the RIS has been the quality of the people they recruit, who are often poorly trained or ill-equipped, making their activities prone to detection, disruption or failure.

Operational work is led by Russia's military intelligence, GRU Unit 29155.[41] What began as a campaign to destabilise Ukraine has evolved into a broader, escalating 'shadow war' against the West.[42] Russian handlers post ads in employment forums, especially on the Dubai-based social networking app Telegram, targeting Eastern European immigrant communities. Russian intelligence officers then assign tasks ranging from posting pro-Russian propaganda posters or petty vandalism to ECI sabotage.[43] The GRU have also been rebuilding capacity by targeting, among others, foreign students and elements within the Russian exile community.

This gig economy approach to sabotage has been successful because vulnerabilities associated with ECI require relatively unsophisticated sabotage efforts. While intelligence obtained through traditional means, such as information gathered by intelligence officers through informants, likely provides direction to foreign nationals, the majority of attacks involve minimal technical sophistication, such as arson. This has allowed Russia to operate undeterred and partially undetected. The substantial increase in vandalism is an indicator of the prevalence of the gig economy approach in action. IISS data shows Russian vandalism has increased every year since 2021, with eight substantial incidents reported in 2024.[44] Criminal sanctions, where they exist, have not limited Russia's operational capacity, as its agents can be replaced. If legal mechanisms cannot hold Russia directly accountable and create a deterrent against malign action, then states must pursue other forms of deterrence and prevention.

Legislation such as the UK's National Security Act 2023, which imposes penalties for working with a foreign intelligence service comparable to those for terrorism offences, may deter some individuals from accepting Russian sabotage offers, but it is far from a complete solution and is unlikely to deter sabotage at large. Even in the highest-profile cases of Russian spying, intelligence officers remain untouchable.[45]

Russian sabotage operations in Europe have accelerated, increasing in both the frequency and boldness of physical attacks. It is highly likely that, in July 2024, the GRU attempted to target cargo planes by implanting a magnesium-based flammable substance in electric massagers. These devices exploded at DHL logistics hubs in Germany, Poland and the UK and were test runs for potential future attacks against cargo aircraft.[46] About 40 arson plots have been linked to Russia in Germany and Poland, including the destruction of the Warsaw shopping centre. In May 2024, a major fire broke out in Berlin at a Diehl Group factory, which produces IRIS-T surface-to-air missiles used in Ukraine. Russia has also been linked to an explosion at a warehouse in Spain storing communications equipment for Ukraine.[47]

3. Europe's Response to Russian Sabotage Operations

Russian sabotage operations in Europe have continued into 2025, although IISS data suggests a lull in such activity during the first half of the year. While reported attacks appeared to dip between January and July, several factors may explain this. Firstly, some incidents from early 2025 are likely still unconfirmed by local authorities and law-enforcement and intelligence agencies often take time to gather evidence, creating a lag in the data. Secondly, it is possible that the start of US President Donald Trump's second term may have prompted the Kremlin to pause operations temporarily to avoid alienating a more conciliatory US administration. Finally, the US-led response to the DHL incident in 2024 may have made the Kremlin pause and led RIS to rein in their operations.[48]

European governments have launched a number of initiatives this year. In March 2025, Estonia, Latvia, Lithuania and Poland withdrew from the Ottawa Convention forbidding anti-personnel mines, citing a 'fundamentally deteriorated security situation' in the Baltic region.[49] On 1 April, Finland followed suit. Such a change likely signals enhanced military readiness to the Kremlin, which aims to avoid direct military confrontation with NATO. In the maritime domain, *NorthSeal*, a joint security effort in the North Sea, was stood up in 2025 along with *Baltic Sentry*.

But there are also reasons to be cautious in interpreting the lack of sabotage activity as an apparent lull. It is possible that following a spate of arrests and disruptions by European law enforcement in 2024 and 2025, the RIS are regrouping networks, recalibrating tactics or avoiding detection. Covert recruitment by RIS via Telegram has continued[50] and is targeting third-country nationals, specifically in Eastern European migrant communities. Under-reporting bias remains significant given that sabotage may be initially misidentified as a technical failure or accident. Media speculation can also create public anxiety by hinting at malign Russian involvement, as seen following the March 2025 electricity-substation fire that shut Heathrow Airport in the UK.[51] Events like this also risk absorbing the police and security services' time, taking them away from other real and potential incidents. In this case, UK officials struck a cautious note by suggesting that, while there was no indication of foul play, they retained an open mind.

But maintaining high-tempo security operations in a contested environment is resource-intensive and difficult to sustain, prompting a search for more cost-effective and enduring solutions. Less than six months after *Baltic Sentry* began, Jean Charles Ellermann-Kingombe, NATO's assistant secretary general for innovation, hybrid and cyber, said the operation, though crucial, had become prohibitively costly.[52] He suggested uninhabited systems – such as the Saildrone *Voyager*, an uninhabited surface vehicle currently on NATO sea trials in the Baltic Sea – offer a more sustainable alternative for long-term security in the region. However, the absence of crewed ships will likely change Russian deterrence calculations. When NATO Secretary General Mark Rutte announced *Baltic Sentry*, he said the goal was 'to strengthen the protection of critical infrastructure … and enhance NATO's military presence in the Baltic Sea.'[53] Rutte went on to stress the importance of robust enforcement, highlighting how Finland had demonstrated that firm action within the law was possible with the boarding of the *Eagle S* in late 2024.

The shift from *Baltic Sentry*'s robust military presence to a pared-back, semi-autonomous approach suggests Europe's preferred approach of prioritising deterrence through denial rather than deterrence through punishment. This reflects a trend in NATO and EU policy of prioritising resilience and capacity building, largely in response to infrastructure failures and for economic reasons.[54]

NATO's belated recognition of the importance of protecting critical infrastructure in 2016 followed the Russian invasion of Ukraine in 2014. The Alliance set out seven baseline requirements for civil preparedness and agreed to pursue them while accepting that civil preparedness was primarily a national

responsibility.[55] NATO further developed its approach with its Strategic Concept at a Madrid summit in June 2022, which recognised resilience as a key enabler for deterrence and defence; the Joint Declaration on EU-NATO Cooperation in January 2023; and the Alliance Resilience Objectives at the Vilnius Summit in July 2023, which aimed to prepare the Alliance for 'strategic shocks and disruptions'.[56]

The EU-NATO Task Force on Resilience of Critical Infrastructure, launched in January 2023, was intended to bridge gaps between military, intelligence and law-enforcement communities, sharing best practices and enhancing situational awareness. The Strategic Concept declared that NATO could consider 'a single or cumulative set of malicious cyber activities' or other hybrid attacks as triggering Article 5. But such a policy is not credible absent a coherent framework to identify incremental actions or, more importantly, the political will to go to war without a clear and obvious provocation.[57] Russia likely assesses that Article 5 would not be invoked in response to most of its opportunistic sabotage, leaving it undeterred.

Furthermore, by misreading Russia's strategic calculus in the grey zone, Western states underestimate the necessity of deterrence through force, thereby weakening it. Russia perceives itself to be in a continuous, existential and intractable struggle with the West. Russia blurs the lines between war and peace to achieve its political goals without triggering a conventional conflict, in which it knows that it is underpowered compared with NATO. European governments have largely decided they are not 'at war', that Russia's activities remain in the grey zone and will unlikely meet the Article 5 threshold, without a substantial shift. Europe has been reluctant to impose sufficient costs, often fearing escalation.[58]

One recent example is instructive in this regard. The British government has recently stepped up efforts to challenge Russia's shadow fleet by routinely demanding proof of insurance as these vessels transit British waters.[59] While this is a welcome development, and follows an agreement with Denmark, Estonia, Finland, Poland and Sweden to increase the number of checks on shipping insurance, the practical impact appears limited. Many ship operators respond evasively or ignore requests altogether. Only one ship has been sanctioned.[60] The opacity of vessel ownership continues to hamper enforcement, suggesting it is not deterring shadow fleet operations.

Russia operates below traditional deterrence thresholds due to both its own design and European policy failures. Europe's reactive posture has failed to inflict sufficient penalties.[61] Despite persistent challenges, however, some European countermeasures have imposed costs. This includes the expulsion of Russian diplomats and intelligence operatives, which degraded the Russian intelligence services' networks and infrastructure. Pre-bunking efforts, such as unprecedented public US and UK intelligence disclosures[62] before Russia's 2022 invasion of Ukraine, pre-empted Russian false flag operations and blunted Kremlin narratives, demonstrating the strategic value of proactive information operations.

Efforts at deterrence by denial have strengthened resilience. Undersea surveillance, the creation of NATO's Critical Undersea Infrastructure Coordination Cell, and public-private partnerships to harden cyber and physical infrastructure have raised the cost of sabotage. Yet many NATO countries remain unable to replicate such partnerships independently. Resilience alone has not deterred Russia, not least as sabotage operations remain cheap and effective in the gig economy.

European strategic culture further constrains effective deterrence. Western democratic legal systems and values impose limitations that authoritarian adversaries exploit externally and can ignore at home. Attribution remains challenging. While Western intelligence assessments frequently conclude with high confidence that Russia is responsible for sabotage, political and legal hesitancy often delays public attribution, undermining deterrence by signalling to the Kremlin that they will pay minimal reputational costs. Despite France's allies, including Germany, the Netherlands, the UK and the US, having a policy of attribution, France has largely avoided publicly blaming state sponsors.[63] In May 2025, however, President Emmanuel Macron announced that France would begin to attribute hostile acts in response to the growing Russian threat.[64]

Russia's sabotage of ECI is central to its unconventional war on Europe and designed to weaken Western resilience

and unity. It presents significant policy challenges to European governments. Russian doctrine intentionally blurs the lines between war and peace, making it challenging for European governments to detect and respond to such aggression. The response by NATO and EU has been to define Russia's unconventional war as operations in the grey zone, below the threshold of conventional war. However, the grey zone concept, while descriptive of hostile activity below the threshold of direct state-on-state conflict, has outlived its utility: it now too often serves as a bureaucratic shield, allowing governments to avoid decisive action and responsibility. As military historian Hew Strachan has noted, a critical shortfall in Western security thinking lies in a lack of clarity on what constitutes war, creating dangerous confusion.[65] Allowing the Kremlin to normalise sabotage as a tool of statecraft risks long-term strategic erosion and miscalculation that could drag Europe into deeper conflict.

Notes

1 Andrei Soldatov and Irina Borogan, '*Arsonist, Killer, Saboteur, Spy: While Trump Courts Him, Putin Is Escalating Russia's Hybrid War Against the West*', *Foreign Affairs*, 20 March 2025, https://www.foreignaffairs.com/russia/arsonist-killer-saboteur-spy-vladimir-putin-donald-trump.

2 Constitution Protection Bureau, '2024 Annual Report', Republic of Latvia, February 2025, https://www.sab.gov.lv/files/uploads/2025/02/SAB-gada-parskats_2024_ENG.pdf.

3 Julia Voo and Virpratap Vikram Singh, 'Russia's Information Confrontation Doctrine in Practice (2014©–Present): Intent, Evolution and Implications', International Institute for Strategic Studies, June 2025, pp. 8–10, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/06/russias-information--confrontation-doctrine--in-practice-/09-pub25-077-russia-information-confrontation-v5.pdf.

4 V. Roldugin and Yu. Kolodko, 'Общие положения методики выбора поражаемыхкомбинатций критически важных объектов противника' [General Elements of the Methodology of Selection of Combinations of Adversary Critical Objects for Strikes], '*Strategicheskaya stabil'nost'*, no. 4, 2014; quoted in Michael Kofman, Anya Fink, Dmitry Gorenburg et al., 'Russian Military Strategy: Core Tenets And Operational Concepts', Center for Naval Analyses, October 2021, p. 68, https://www.cna.org/reports/2021/10/Russian-Military%20-Strategy-Core-Tenets-and-Operational-Concepts.pdf.

5 Daniela Richterova, 'The Long Shadow of Soviet Sabotage Doctrine?', War on the Rocks, 19 August 2024, https://warontherocks.com/2024/08/the-long-shadow-of-soviet-sabotage-doctrine.

6 For example, on 27 April 2007, a series of cyber attacks targeted websites of Estonian organisations including financial institutions, government departments, Parliament and the Estonian media following a disagreement with Russia about the relocation of the Bronze Soldier of Tallinn.

7 'Safeguarding the US Defence Industrial Base and Private Industry Against Sabotage', Office of the Director of National Intelligence, 21 November 2024, https://www.dni.gov/files/NCSC/documents/products/FINAL_Safeguarding_DIB_Against_Sabotage.pdf.

8 Government of the United Kingdom, 'Explaining Uncertainty in UK Intelligence Assessment', 24 March 2025, https://www.gov.uk/government/publications/explaining-uncertainty-in-uk-intelligence-assessment/explaining-uncertainty-in-uk-intelligence-assessment.

9 Erik Van der Vleuten, 'Critical Infrastructure: Europe's Vulnerability Geography', Encyclopédie d'histoire numérique de l'Europe [Digital Encyclopedia of Europe's History], https://ehne.fr/en/node/21303.

10 Alberto Toril Castro, 'Europe's Grids Are Not Up to Grade', Breakthrough Energy, 22 May 2024, https://www.breakthroughenergy.org/newsroom/articles/europe-grid-infrastructure/.

11 North Atlantic Treaty Organization, 'Vilnius Summit Communiqué', 11 July 2023, https://www.nato.int/cps/en/natohq/official_texts_217320.htm.

12 Karolina Jeznach, Thomas Grove and Bojan Pancevski, 'The Misfits Russia Is Recruiting to Spy on the West', Wall Street Journal, 15 May 2024, https://

www.wsj.com/world/europe/the-misfits-russia-is-recruiting-to-spy-on-the-west-7417b2b5.

13 Justina Budginaite-Froehly, 'The Missing Link: Railway Infrastructure of the Baltic States and Its Defence-related Implications', GLOBSEC, 12 January 2024, https://www.globsec.org/what-we-do/commentaries/missing-link-railway-infrastructure-baltic-states-and-its-defence-related.

14 Advisory Council on International Affairs, 'Hybrid Threats and Societal Resilience', no. 126, June 2024, p. 14, https://www.advisorycouncilinternationalaffairs.nl/documents/publications/2024/06/04/hybrid-threats-and-societal-resilience.

15 'Resilience, Civil Preparendess, and Article 3', North Atlantic Treaty Organization, last updated 13 November 2024, https://www.nato.int/cps/en/natohq/topics_132722.htm.

16 Sophia Besch and Erik Brown, 'Securing Europe's Subsea Data Cables', Carnegie Endowment for International Peace, 16 December 2024, p. 3, https://carnegieendowment.org/research/2024/12/securing-europes-subsea-data-cables.

17 NIS Cooperation Group, 'EU Cybersecurity Risk Evaluation and Scenarios for the Telecommunications and Electricity Sectors', European Union, 23 May 2023, p. 15, https://digital-strategy.ec.europa.eu/en/news/risk-assessment-report-cyber-resilience-eus-telecommunications-and-electricity-sectors.

18 Gabriel Stargardter, 'France Seeks FBI Help in Probe of High-speed Train Sabotage Hours before Olympics', Reuters, 7 Aug 2024, https://www.reuters.com/world/europe/france-seeks-fbi-help-probe-high-speed-train-sabotage-hours-before-olympics-2024-08-07/.

19 Shaun Walker, 'Poland Arrests Nine Over Alleged Plot to Sabotage Ukraine Arms Supplies', *Guardian*, 16 March 2023, https://www.theguardian.com/world/2023/mar/16/poland-arrests-nine-over-alleged-plot-to-sabotage-ukraine-arms-supplies.

20 Nette Nöstlinger, 'Germany on Mysterious Broken Cables in Baltic Sea: "It Is Sabotage"', *Politico*, 19 November 2024, https://www.politico.eu/article/baltic-sea-cable-damage-germany-sabotage/.

21 Nöstlinger and Stuart Lau, 'German Authorities Suspect Water Supply Sabotage on Military Base', Politico, 14 August 2024, https://www.politico.eu/article/water-supply-sabotage-military-bases-germany-nato-cologne-geilenkirchen/.

22 See James N. Mattis and Frank G. Hoffman, 'Future Warfare: The Rise of Hybrid Wars', *Proceedings*, vol. 131, no. 11, November 2005; and Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, December 2007). For the modern application, see Sean S. Costigan and Michael A. Hennessy, 'Hybrid Threats and Hybrid Warfare Reference Curriculum', North Atlantic Treaty Organization, June 2024, https://www.nato.int/cps/en/natohq/topics_227643.htm.

23 See Ofer Fridman, 'Hybrid Warfare or *Gibridnaya Voyna*?: Similar, But Different', *RUSI Journal*, vol. 162, no. 1, 3 April 2017, pp. 42-49, https://doi.org/10.1080/03071847.2016.1253370.

24 Valery Gerasimov, '*Po opytu Sirii: Gibridnaya voyna trebuyet vysokotekhnologichnogo oruzhiya i nauchnogo obosnovaniya*' [According to the Experience in Syria: Hybrid War Requires High-tech Weaponry and Scientific Foundations], *Military-Industrial Kurier*, no. 9, 2016, quoted in Fridman, 'Russian "Hybrid Warfare": Resurgence and Politicization' (London: Oxford University Press, 2018), p. 98, https://doi.org/10.1093/oso/9780190877378.001.0001. See also Gerasimov, 'The Value of Science Is in the Foresight', *Military Review*, January-February 2016, originally published in *Military-Industrial Kurier*, 27 February 2013, pp. 23-29, an earlier and more infamous, but less direct, statement of the same ideas, https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf.

25 'Poland Says Russian Secret Service Behind 2024 Fire in Warsaw Shopping Centre', Reuters, 11 May 2025 https://www.reuters.com/world/europe/poland-says-russian-secret-service-behind-2024-fire-warsaw-shopping-centre-2025-05-11/.

26 For example, Angelique Chrisafis, 'France "Investigating Whether Russia Behind" Graffiti on Holocaust Memorial', *Guardian*, 22 May 2024, https://www.theguardian.com/world/article/2024/may/22/france-russia-paris-holocaust-memorial-graffiti-red-hand.

27 Mason Clark, 'The Russian View of Future War: Unconventional, Diverse, and Rapid', *Russian Hybrid*

Warfare (Washington DC: The Institute for the Study of War, 1 September, 2020), pp. 15-24, https://www.jstor.org/stable/resrep26547.

28 Gerasimov, 'The Value of Science Is in the Foresight', p. 28.

29 Oleksander V. Danylyuk, 'Interagency and International Cooperation in Detecting and Countering Hybrid Warfare', Centre for Defence Reforms, 2020, p. 14.

30 Keir Giles, 'Russian Cyber and Information Warfare in Practice: Lessons Observed from the War on Ukraine', Chatham House, December 2023, p. 4, https://www.chathamhouse.org/2023/12/russian-cyber-and-information-warfare-practice.

31 Ken McCallum, 'Director General Ken McCallum Gives Latest Threat Update', https://www.mi5.gov.uk/director-general-ken-mccallum-gives-latest-threat-update, 8 October 2024.

32 Lara Seligman, '"One Hand Tied Around The Back": Europe Presses US To Lift Ukraine Weapons Limits', Politico, 14 June 2024, https://www.politico.com/news/2024/06/14/europe-presses-us-to-lift-ukraine-weapons-limits-00163443.

33 Tim Johnson McClatchy, 'Undersea Cables: Too Valuable to Leave Vulnerable?', Government Technology, 12 December 2017, https://www.govtech.com/network/undersea-cables-too-valuable-to-leave-vulnerable.html.

34 Baltic Marine Environment Protection Commission, 'Territorial Waters Dataset' and 'HELCOM HOLAS 3 Dataset (2023)', https://maps.helcom.fi/website/mapservice/?datasetID=cae61cf8-0b3a-449a-aeaf-1df752dd3d80

35 UN Convention on the Law of the Sea, 1833 U.N.T.S. 397 (1994), article 113, https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

36 Christy Cooney, 'Sweden Asks China to Co-Operate Over Severed Cables', BBC News, 29 November 2024, https://www.bbc.co.uk/news/articles/c748210k82wo.

37 Carri Ginter and Marcus Niin, 'We Are Advising Finnish and Estonian Energy Companies on Obtaining Insurance Compensation as a Result of the Damage to the Balticconector Gas Pipeline', Sorainen, 25 July 2024, https://www.sorainen.com/deals/we-are-advising-finnish-and-estonian-energy-companies-on-obtaining-insurance-compensation-as-a-result-of-the-damage-to-the-balticconnector-gas-pipeline.

38 Nick Paton Walsh, 'Russian Spying in Europe Dealt "Significant Blow" Since Ukraine War, MI5 Chief Says', CNN, 16 November 2022, https://edition.cnn.com/2022/11/16/uk/mi5-chief-russia-spying-iran-china-threats-intl/index.html.

39 'Spy Poisoning: Russia Expels More UK Diplomats', BBC News, 31 March 2018, https://www.bbc.co.uk/news/world-europe-43604053.

40 Daniela Richterova, Elena Grossfeld, Magda Long et al., 'Russian Sabotage in the Gig-Economy Era', *RUSI Journal*, vol. 169, no. 5, 17 September 2024, pp. 10–21, https://doi.org/10.1080/03071847.2024.2401232.

41 Unit 29155 are responsible for an array of infamous operations, including the Salisbury poisonings and the attempted assassination of Alexei Navalny.

42 Christo Grozev, Roman Dobrokhotov and Michael Weiss, 'Hidden Bear: the GRU Hackers of Russia's Most Notorious Kill Squad', The Insider, 31 May 2025 https://theins.ru/en/inv/281731.

43 Constitution Protection Bureau, '2024 Annual Report'.

44 Counting a wave of incidents where animal entrails were mailed to Ukrainian consulates across Europe in 2022 as a single incident.

45 Martha Muir and Helen Warrell, 'Three Bulgarians Linked to Wirecard's Jan Marsalek Found Guilty of Spying for Russia', *Financial Times*, 7 March 2025, https://www.ft.com/content/a3be7f26-f452-4585-9389-c6dc5c4b4978.

46 See for example Paul Kirby and Frank Gardner, 'Mystery Fires Were Russian "Test Runs" to Target Cargo Flights to US', BBC News, 5 November 2024, https://www.bbc.co.uk/news/articles/co7912lxx330.

47 David Ignatius, 'Russia Is Punching Back at NATO in the Shadows', *Washington Post*, 21 June 2024, https://www.washingtonpost.com/opinions/2024/06/21/russia-nato-ukraine-sabotage-attacks.

48 Bojan Pancevski, Thomas Grove, Max Colchester et al., 'Russia Suspected Of Plotting To Send Incendiary Devices On U.S.-Bound Planes', *Wall Street Journal*, 4 November 2024, https://www.wsj.com/world/russia-plot-us-planes-incendiary-devices-de3b8c0a.

49 'Statement by the Estonian, Latvian, Lithuanian, and Polish Ministers of Defence on the Withdrawal From the Ottawa Convention', Estonian Ministry of Defence, 18 March 2025, https://kaitseministeerium.ee/sites/default/files/4_ministers_statement_on_ottawa_convention.pdf.

50 Shaun Walker, '"These People Are Disposable": How Russia Is Using Online Recruits for a Campaign of Sabotage in Europe', *Guardian*, 4 May 2025, https://www.theguardian.com/world/ng-interactive/2025/may/04/these-people-are-disposable-how-russia-is-using-online-recruits-for-a-campaign-of-sabotage-in-europe.

51 'Counter-terror Police Leading Inquiry Into "Unprecedented" Heathrow Fire', *Guardian*, 21 March 2025, https://www.theguardian.com/uk-news/2025/mar/21/counter-terror-police-investigating-unprecedented-fire-shut-heathrow.

52 Mikael Eriksson, 'Nato Ships in Baltic Sea Could Be Replaced by Drones', Radio Sweden, 3 June 2025, https://www.sverigesradio.se/artikel/nato-ships-in-baltic-sea-could-be-replaced-by-drones.

53 North Atlantic Treaty Organization, 'NATO Launches "Baltic Sentry" to Increase Critical Infrastructure Security', 14 January 2025, https://www.nato.int/cps/en/natohq/news_232122.htm.

54 European Commission, 'Critical Infrastructure Protection', 20 October 2004, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:l33259.

55 The seven baseline requirements for civil preparedness include: assured continuity of government and critical government services; resilient energy supplies; ability to deal effectively with uncontrolled movement of people; resilient food and water resources; ability to deal with mass casualties; resilient civil communications systems; and resilient civil transportation systems, see North Atlantic Treaty Organization, 'Commitment to Enhance Resilience', 8 July 2016, https://www.nato.int/cps/en/natohq/official_texts_133180.htm.

56 North Atlantic Treaty Organization, 'Vilnius Summit Communiqué', 11 July 2023, https://www.nato.int/cps/en/natohq/official_texts_217320.htm.

57 North Atlantic Treaty Organization, 'NATO 2022 Strategic Concept', 3 March 2023, p. 7, https://www.nato.int/cps/en/natohq/topics_210907.htm.

58 Laura Kayali, Dirk Banse, Wolfgang Büscher et al., 'Europe Is Under Attack from Russia. Why Isn't It Fighting Back?', Politico, 25 November 2024, https://www.politico.eu/article/europe-russia-hybrid-war-vladimir-putin-germany-cyberattacks-election-interference/.

59 Robert Wright and Chris Cook, 'UK Challenges More Than 40 'Shadow Fleet' Ships a Month in English Channel', https://www.ft.com/content/f3fbc0ec-a1b8-4cc4-9f84-d4d4a80043e3, 8 July 2025.

60 Ewa Krukowska et al., 'Baltic Sea Countries to Start Checking Insurance Status of Tankers Moving Russian Oil', 17 December 2024, https://www.insurancejournal.com/news/international/2024/12/17/805085.htm.

61 Seth G. Jones, 'Russia's Shadow War Against the West', Center for Strategic and International Studies, 18 March 2025, p. 14, https://www.csis.org/analysis/russias-shadow-war-against-west.

62 Shane Harris and Paul Sonne, 'Russia Planning Massive Military Offensive Against Ukraine Involving 175,000 Troops, U.S. Intelligence Warns', *Washington Post*, 3 December 2021, https://www.washingtonpost.com/national-security/russia-ukraine-invasion/2021/12/03/98a3760e-546b-11ec-8769-2f4ecdf7a2ad_story.html.

63 Quentin Jalabert, Damien van Puyvelde and Thomas Maguire, 'Calling Out Russia: France's Shift on Public Attribution', War on the Rocks, 3 July 2025, https://warontherocks.com/2025/07/calling-out-russia-frances-shift-on-public-attribution/.

64 *Ibid*.

65 Frank G. Hoffman, 'The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War', in Dakota L. Wood (ed.), *Index of US Military Strength*, Heritage Foundation, 2016, https://www.heritage.org/military-strength-topical-essays/2016-essays/the-contemporary-spectrum-conflict-protracted-gray.

Acknowledgements

IISS acknowledges the financial support of the Hanns Seidel Foundation for a workshop that helped inform the paper's contents.

The International Institute for Strategic Studies – UK
Arundel House | 6 Temple Place | London | WC2R 2PG | UK
t. +44 (0) 20 7379 7676 **e.** iiss@iiss.org **w.** www.iiss.org

The International Institute for Strategic Studies – Americas
2121 K Street, NW | Suite 600 | Washington DC 20037 | USA
t. +1 202 659 1490 **e.** iiss-americas@iiss.org

The International Institute for Strategic Studies – Asia
9 Raffles Place | #49-01 Republic Plaza | Singapore 048619
t. +65 6499 0055 **e.** iiss-asia@iiss.org

The International Institute for Strategic Studies – Europe
Pariser Platz 6A | 10117 Berlin | Germany
t. +49 30 311 99 300 **e.** iiss-europe@iiss.org

The International Institute for Strategic Studies – Middle East
14th floor, GFH Tower | Bahrain Financial Harbour | Manama | Kingdom of Bahrain
t. +973 1718 1155 **e.** iiss-middleeast@iiss.org