Managing Hybrid Threats: Building Europe's Response to Russian Sabotage

by Carla Coiffard

King's Policy Journal

KCL Policy Research Centre

Centre for Security & Defence

Word Count: 2061

January 2026

Managing Hybrid Threats: Building Europe's Response to Russian Sabotage by Carla Coiffard

Europe is witnessing the most intense wave of Russian covert activity since the Cold War. Across the continent, recent assessments indicate a total of more than one hundred attempts of Russian sabotage - ranging from attacks on energy infrastructure in the Baltic Sea and unexplained fires in Poland, to defacing Holocaust monuments in Paris and interference in Germany's 2025 elections (Rekawek et al., 2025). This operational tempo sharply accelerated from 2022 onwards as Moscow sought new tools to pressure democracies supporting Ukraine and destabilize European societies. New actors, profit-seeking amateurs, have come into play, broadening Moscow's reach and complicating attribution. Yet, despite the rising frequency of such incidents, hesitant and fragmented European responses have allowed Moscow to continue operating within the grey zone.

This paper seeks to assess the strategic objectives behind Moscow's operations and examine the challenges Europe faces in coordinating a collective, timely and credible deterrent strategy. It argues that Europe ought to develop a consistent response framework by strengthening intelligence-sharing and public attribution, aligning its threshold and response with NATO, and expanding their toolkit with more assertive, targeted measures.

Russia's Sabotage Playbook: Vandalism, Disinformation, and Arson

The 'Gig-Economy' Model

The mass expulsion of Russian intelligence officers across Europe following the Skripal poisoning in 2018 and again after the invasion of Ukraine severely weakened Moscow's traditional human intelligence networks and laid the ground for a shift in operational methods. Deprived of diplomatic cover, the Russian military intelligence GRU 29155 unit turned towards what is describe as a 'gig-economy' model of sabotage: an outsourced, flexible, low-cost system relying on loosely connected individuals, short-term recruits and highly deniable operations (Jones, 2025; Richterova et al., 2024). In practice, Russian handlers post anonymous 'job offers' on Telegram channels, promise payment, and assign tasks broken down into small, compartmentalized steps such as filming a railway junction, painting a symbol, or leaving an object at a designated location (Richterova et al., 2024). The digital era has removed the single greatest vulnerability of espionage, the need for physical meetings, allowing Moscow to sustain operational reach without exposing official personnel (Rekawek et al., 2025).

Amateur recruits often are economically vulnerable, have a criminal background, are Russian sympathizers, and in many cases Russian-speaking nationals from post-Soviet states - echoing the Soviet practice of using Warsaw Pact nationals as operational cover (Rekawek et al., 2025). Some

intermediaries appear unaware of the identity of their handlers or the political significance of their tasks. Payments are made with anonymous wire transfers and Telegram trading bots, often in cryptocurrency, and can be as low as $53 for painting Stars of David on Parisian buildings (Richterova et al., 2024, p. 18). If arrested, these 'agent-saboteurs' are disposable and rapidly replaced. This approach minimizes the recruitment process, costs and risks for Moscow, while maximizing deniability and operational reach.

Cases across Europe

France and Germany, two pivotal countries in the EU's political architecture and in supporting Ukraine's defense, have become key targets of this campaign (Richterova et al., 2024). France has been the stage for some of the most symbolic acts of vandalism, particularly given President Macron's firm stance on Ukraine. Russia-linked operatives have orchestrated a series of highly mediatized antisemitic and Islamophobic incidents, exploiting societal, intercommunal and geopolitical tensions (Blistène & Richterova, 2025). Acts included spraying red handprints on the Wall of the Righteous Holocaust monument in Paris, leaving pigs' heads outside mosques, painting Stars of David across the capital, and depositing coffins at the Eiffel Tower engraved with 'French soldiers in Ukraine'. These acts were designed to deepen pre-existing social divisions and fuel social unrest, particularly amid a context of rising support for far-right parties (Harding, 2025).

Meanwhile, Germany has been subject to large-scale Foreign Information Interference and Manipulation (FIMI) operations. Since at least 2021, Moscow has attempted to influence the German electoral dynamics through aggressive FIMI campaigns designed to weaken centrist parties such as the Greens, the Christian Democrats (CDU), and the Social Democrats' Party. Fabricated allegations, including videos posted on X about psychological instability involving CDU leader Friedrich Merz, who advocated supplying German Taurus missiles to Ukraine, circulated widely on social media, as part of a broader attempt to erode support for Ukraine (Wesolowski & Klug, 2025). By amplifying narratives that portray the German government as prioritizing Ukraine at the expense of its own population, particularly amid a difficult economic climate, Moscow seeks to further undermine public confidence and deepen domestic discontent (Von Loringhoven, 2024). However, The German Ministry of the Interior (n.d.) reports that sanctions on Russian state media have paradoxically led to increased pro-Russian propaganda from private or pseudonymous accounts.

Across Europe, similar incidents have multiplied as Moscow intensifies its 'shadow war' as a response to Western political and military support to Ukraine (Jones, 2025). Arson attacks on infrastructure with links to Ukraine's defense supply chain have been recorded in Lithuania, Britain, and Poland. Severed undersea telecommunications and energy cables in the Baltic Sea have disrupted key nodes supporting both civilian and military networks. According to CSIS reporting, more than

fifty incidents in 2024 alone were assessed as having links to Russian sabotage (Walker, 2025). In addition, as noted by Richterova (2024), kinetic operations are almost always paired with FIMI. These operations serve multiple objectives: disrupting policies, inflicting economic or military damages, undermining unity within states, weakening political leaders and state institutions, and generating an atmosphere of chaos.

Challenges to Europe's Response

Despite the growing evidence linking Russia to sabotage incidents across the continent, Europe continues to struggle with timely attribution and collective response frameworks, which often fall short of deterring further attacks. This difficulty stems from a combination of operational ambiguity engineered by Moscow, fragmented intelligence sharing, and political fears of escalation.

Structural Constraints

A first major challenge lies in the operational design of Russia's actions. Sabotage campaigns exploit legal loopholes and grey zones: many operations are carried out by non-state actors precisely because this complicates the process of establishing state responsibility (Rekawek et al., 2025). As the GLOBSEC (2025) report notes, national doctrines are often poorly equipped to account for hybrid threats executed by criminals, coerced individuals, or profit-motivated proxies even when these actors are directed by Russian intelligence. This intentional diffusion of responsibility delays and complicates attribution. It forces European authorities to build lengthy chains of evidence linking a low-level act of vandalism or arson to the GRU, a task made harder by encrypted communications, informal recruitment channels, and the absence of formal command structures. Public statements, too, face diminishing returns. The Kremin is largely indifferent to reputational costs and dismisses Western accusations as 'Russophobia,' while lengthy judicial procedures can't keep pace with the tempo of incidents (Praks, 2025).

Moreover, attribution in Europe is slowed by institutional fragmentation. Intelligence remains a national-level responsibility, and while mechanisms such as Europol and the EU Intelligence and Situation Centre facilitate information sharing, they do not amount to a unified European intelligence capability (Jones, 2025). Member states vary widely in their willingness to share sensitive findings, domestic intelligence failures, and their political thresholds for public attribution. Some states treat Russian sabotage as a central security threat; others downplay incidents to avoid domestic alarm or diplomatic complications (Richterova et al., 2025). This creates a collective action problem: a coherent European response is difficult when individual governments disagree on the severity, intent, and strategic meaning of the attacks.

Political Caution and Escalation Risks

These challenges are further shaped by political caution with fears that confrontation with Moscow could risk escalation toward wider military conflict (Soldatov & Borogan, 2024). Since Europe is not formally at war with Russia, any escalatory responses carry political costs and strategic risks. These may include retaliation in the energy, cyber or information domains - areas where European vulnerabilities remain significant - and/or Russia intensifying efforts in Ukraine.

This is amplified by the inherent nature of hybrid conflict. Russia deliberately operates below the threshold of armed attack as defined by NATO's Article 5, exploiting ambiguity to make proportional responses politically fraught (Jones, 2025). This dynamic produces a strategic asymmetry of risk: Russia is willing to absorb the arrest of its low-cost intermediaries, the exposure of its sabotage networks, or even the occasional diplomatic expulsion as costs of doing business. Europe, by contrast, operates in a stricter political, legal, and normative environment, where misattribution carries reputational risks and overreaction could trigger unintended consequences (Soldatov & Borogan, 2024). As a result, with the EU's primary coercive tools already deployed or normalized - sanctions, diplomatic expulsions, and political attribution - this asymmetry limits the deterrent effect of further punitive measures.

Policy Recommendations

- Building Situational Awareness and an Attribution System:

The current fragmentation of intelligence practices and the reluctance of several governments to share sensitive information, impedes Europe's ability to detect, interpret and respond to Russian operations. A strengthened EU Intelligence and Situation Centre (INTCEN), mandated specifically to coordinate and analyze intelligence on hybrid and kinetic threats, should serve as the central hub for fusing national inputs. Regularized intelligence exchanges would facilitate early detection of sabotage networks and help identify cross-border patterns. Crucially, Europe must adopt a common EU definition of hybrid threats within national security strategies to ensure consistent thresholds for detection and response. It must as well fully operationalize the EU Hybrid Toolbox and the FIMI Toolbox as part of a unified EU-wide mechanism capable of delivering rapid, politically credible assessments of Russian responsibility (Council of the EU, 2024). It also requires expanded monitoring to include platforms that facilitate the gig-economy recruitment model such as neobanks, encrypted apps, and international money transfers (Rekawek et al., 2025). This would accelerate attribution and reduce the deniability that Russia relies on. Additionally, consistently attributing attacks publicly would set a legal basis in international law and could facilitate alliance rallying (Praks, 2025).

- Establishing a EU-NATO Joint Task Force :

The EU and NATO should establish a joint operational mechanism to bridge the divide between internal resilience and collective defense. The existing EU–NATO Task Force on Critical Infrastructure is a useful starting point but remains too narrowly focused on energy, transport, and digital networks (Jones, 2025). Its remit does not cover sabotage, proxy actors, covert kinetic operations, or escalation management. A NATO–EU Joint Task Force on Hybrid Threats could enhance real-time information sharing, coordinated attribution, joint planning for response options. Escalation-scenario simulations would also reinforce alliance signaling by aligning EU and NATO deterrence messaging and response thresholds.

However, enduring differences in mandate, membership, and decision-making procedures would constrain the depth of integration achievable. The effectiveness of such a task force would therefore depend on clearly defined competences, political buy-in from member states, and safeguards against duplication. While it would not eliminate all vulnerabilities, enhanced EU–NATO coordination would nonetheless complicate Russia's ability to exploit gaps between civilian and military domains in the hybrid space.

- Expanding Deterrent Measures Below the Threshold of Armed Conflict:

Although Europe's toolkit has shrunk after multiple sanction packages, additional calibrated measures can be mobilized to raise the costs on Russia. These include targeting sanctions against individuals involved in covert operations - such as GRU Unit 29155 operatives, intermediaries, and financial facilitators - information campaigns targeting Russian population and allies, and targeted cyber operations against economic or military targets (Jones, 2025). Diplomatic options include coordinated expulsions of undeclared intelligence officers and more rigorous visa screening for Russian and Belarusian nationals with high-risk profiles, which would further constrain Russia's human networks in Europe (Praks, 2025). Additionally, member states should deploy strategic communication campaigns to raise awareness about Russia's recruitment methods, manipulation tactics, and the legal penalties for individuals involved - explicitly warning that individuals with demonstrable links to Russian operations will face terrorism-related charges and sentences (Rekawek et al., 2025).

Conclusion

Russia's renewed campaign of covert sabotage has exposed structural weaknesses in Europe's ability to attribute and respond to hostile state activity below the threshold of war. As long as Moscow continues to exploit ambiguity, intermediaries, and political hesitation, these operations will remain a low-cost, high-impact tool of pressure. Even though prudence remains essential to avoid unintended escalation, Europe must simultaneously deepen intelligence cooperation, strengthen attribution

mechanisms, and deploy calibrated measures against Russian targets. Together, these measures would raise the cost of Russian hybrid activities**,** help ensure a coordinated European posture, and close the space in which covert operations thrive, without allowing caution to become paralysis.

References

Blistène, P., & Richterova, D. (2025). Strategic Vandalism: Decoding the French “Red Hands” Trial. Retrieved from King’s Centre for the Study of Intelligence website: https://kcsi.uk/kcsi-insights/strategic-vandalism-decoding-the-french-red-hands-trial

Council of the European Union. (2024). Council Conclusions on Democratic Resilience. Available at : https://data.consilium.europa.eu/doc/document/ST-10119-2024-INIT/en/pdf

Disinformation related to the Russian war of aggression against Ukraine. (n.d.). Retrieved from Federal Ministry of the Interior website: https://www.bmi.bund.de/SharedDocs/schwerpunkte/EN/disinformation/disinformation-related-to-the-russian-war-of-aggression-against-ukraine.html

European Commission. (2023). EU-NATO Task Force On The Resilience Of Critical Infrastructure . Available at : https://commission.europa.eu/system/files/2023-06/EU-NATO_Final%20Assessment%20Report%20Digital.pdf

Harding, A. (2025). Hand of Moscow? The men jailed for vandalism in French hybrid warfare case. BBC News. Available at : https://www.bbc.co.uk/news/articles/c891d43l8pyo

Jones, S. G. (2025). Russia’s Shadow War Against the West. Center for Strategic and International Studies (CSIS). JSTOR. https://doi.org/10.2307/resrep68536

Jordán, J. (2024). How to interpret the Russian sabotage campaign in Europe. Retrieved from Global Strategy website: https://global-strategy.org/russian-sabotage-campaign-europe/

Praks, H. (2025). Russia’s Hybrid Attacks in Europe: From Deterrence to Attribution to Response. International Centre for Defence and Security (ICDS). JSTOR. https://doi.org/10.2307/resrep69138

Rekawek, K., Lanchès, J., & Zotova, M. (2025). Russia’s Crime-Terror Nexus : Criminality as a Tool of Hybrid Warfare in Europe. In D. Hajdu (Ed.), GLOBSEC. Available at : https://icct.nl/sites/default/files/2025-09/Russia%20Crime%20Terror%20Nexus_Criminality%20as%20a%20Tool.pdf

Richterova, D., Grossfeld, E., Long, M., & Bury, P. (2024). Russian Sabotage in the Gig-Economy Era. The RUSI Journal, 169(5), 10–21. https://doi.org/10.1080/03071847.2024.2401232

Soldatov, A., & Borogan, I. (2024). Putin’s New Agents of Chaos. Retrieved November 15, 2025, from Foreign Affairs website:

https://www.foreignaffairs.com/ukraine/paris-olympics-putin-agents-chaos-andrei-soldatov-irina-borogan

Von Loringhoven, A. F. (2024). Germany in the Crosshairs of Russia's Information War. Retrieved from CEPA website: https://cepa.org/article/germany-in-the-crosshairs-of-russias-information-war/

Walker, S. (2025, May 4). "These people are disposable": how Russia is using online recruits for a campaign of sabotage in Europe. The Guardian. Available at : 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

Wesolowski, K., & Klug, T. (2025, February 18). Fact check: Russia's influence on Germany's 2025 election. Available at : https://www.dw.com/en/russian-disinformation-aims-to-manipulate-german-2025-election/a-71664788