PRIMING, DESTABILIZING, COERCING:
Russian Hybrid Tactics in Europe 2022–2025

The Soufan Center
March 2026

Supported by

Airey Neave Trust

PRIMING, DESTABILIZING, COERCING:
Russian Hybrid Tactics in Europe 2022-2025

The Soufan Center
Co-Authored by: Clara Broekaert, Nikkie Lyubarsky, Colin Clarke, Joseph Shelzi
March 2026

Supported by

Airey Neave Trust

Cover Image: The Soufan Center

TABLE OF CONTENTS

Executive Summary

This report draws on 255 hybrid incidents targeting six European countries (France, Germany, the United Kingdom, Estonia, Moldova, and Georgia) between February 2022 and December 2025. Analysis of Russian hybrid tactics, techniques, and procedures (TTPs) is based on an open-source incident database compiled by the authors, as well as 22 expert interviews conducted across government, intelligence, academia, and civil society.

Two Overarching Objectives for Russia

- Impose costs on Europe cheap enough for Russia to sustain: this strategy drains the financial resources, military capabilities, and political bandwidth of countries supporting Ukraine, or withdrawing from its traditional sphere of influence, while providing a testing ground to refine tactics for potential future conflict with NATO.

- Erode the guardrails that make democracies resistant to interference by exploiting pre-existing societal schisms, undermining trust in institutions and keeping populations polarized and confused.

The Core Logic: Cost Asymmetry

Russia's hybrid strategy throughout the observation period was an exercise in cost asymmetry and probing. Operations were cheap, often deniable, and scalable for Moscow, but the costs were absorbed almost entirely by the targets.

- Russia did not need to succeed at every operation. Moscow simply needed Europe to keep expending thinly stretched resources to defend against all of them.
- The apparent amateurish nature of many operations attested to both a trial-and-error approach and the suboptimal means at the Kremlin's disposal after the mass expulsion of Russian agents from Europe following the start of the full-scale invasion of Ukraine.
- More overt Russian operations under the threshold of declared war indicated deliberate probing and testing of thresholds for retaliation and response.

Context-Dependent Playbooks

Russia appeared adept at calibrating TTPs to what each country represents to the Kremlin.

France

- Russia rarely fabricated divisions and instead exploited fractures that already existed: pig heads at nine Parisian mosques; Stars of David spray-painted across the city; fake coffins draped in French flags placed beneath the Eiffel Tower.
- There was a **240 percent** increase in hybrid incidents in France between 2022 and 2024, timed to coincide with the Paris Olympics, legislative elections, and European Parliament vote.

Germany & the UK

- The dominant tools Russia utilized were drones, shadow fleet vessels, and espionage networks.
- **57** incidents were recorded in Germany — the highest in the dataset — with 'Intelligence preparation' being the single most frequent tool utilized. Russian assets mapped weapons routes, surveilled Ukrainian troops training on German soil, and identified vulnerabilities in critical infrastructure.
- In the UK, Russian vessels loitered near undersea cables and likely planted underwater surveillance devices near submarine routes.

Moldova

- Russian TTPs focused on creating an information environment hostile to Western institutions and European Union (EU) integration.
- Russia utilized its dominant legacy in the country to sustain influence. Years of peddling polarizing narratives, clergy bribery, and vote-buying culminated in an all-out campaign to reverse the country's EU trajectory.

Estonia

- Russia applied near-continuous pressure on Estonia since 2022 with a wide array of TTPs, ranging from disinformation targeting Russian speakers to severing undersea cables that are costly to repair.
- An occurring trend in increasingly brazen and overt incursions into land and air space denoted the importance of the Baltics for Russia as a testing ground for NATO response thresholds.

Georgia

- During the observation period, Russia appeared to have achieved its major strategic objectives without conventional armed conflict.
- **37 percent** of Georgia's logged incidents classified in the "coercing" phase, reflecting two decades of Russian occupation of Georgian territory and hybrid operations.
- Through years of information operations (IOs) exploiting conservative and religious sentiment, Russia helped cultivate conditions in which the ruling Georgian Dream party froze EU accession and adopted Russian-style legislation targeting civil society.

What Changed Between 2022 and 2025

Two structural shifts defined the evolution of Russia's TTPs across the observation period.

- **1. Outsourcing to intermediaries:** 'Russia through intermediary individuals' became the dominant actor category by 2024. These are disposable agents, often with criminal backgrounds, recruited via social media for small sums. Intermediaries provided deniability and importantly, allowed to compensate for the mass expulsion of Russian agents posing as diplomats in response to the full-scale invasion of Ukraine.
- **2. Physical escalation in 2025:** Russia's campaign became more physically assertive, shifting from virtual operations to direct probing in many traditional Western European states in 2025. This may be due to the EU's goal — as well as the stated goal of the UK — to build out a more independent strategic defense architecture.

What Works — and What Doesn't

- Despite near-continuous pressure, Estonia refused to be provoked into overreaction and eschewed playing into Russian narratives of Western warmongering or Russophobia. A population inoculated over decades of Russian hybrid threats has proven remarkably resistant to Kremlin interference.
- A pro-European parliamentary majority in Moldova was secured in 2025 despite the most intensive interference campaign in the country's history. The government publicly quantified interference in real time, raided vote-buying networks, and excluded Russian-backed parties through legal means. Key lesson: telling citizens what is being done to them can blunt Russian TTPs when done right.
- Despite brazen operations in the UK — for example, arson attacks on properties linked to the Prime Minister — British institutions have been systematically reluctant to publicize the threat. The UK faced an "ice-

berg problem": the public sees only roughly 5 percent of what occurred. This reticence prevented public resilience and signaled to Moscow that sub-threshold operations carry no meaningful cost.

What Needs to Change

Countering cost asymmetry requires action on both sides of the equation simultaneously: raising Russia's costs while reducing the domestic surface area of impact.

Raise the Costs

- Systematic, coordinated **public** attribution across European partners.
- 255 incidents — likely only the tip of the iceberg — represent an operational tempo with no adequate collective response architecture.

Reduce the Surface Area

- Societal factors, not Russian operational tempo, appear to be the primary determinant of impact.
- Independent civil society, strong local governance, and judicial accountability make or break a Russian operation.

Exercise Strategic Muteness

- Overreactions and constant messaging on hybrid TTPs play into Russia's narratives of Western hysteria and Russophobia.
- Do not treat every incident as a provocation requiring public response — Russia benefits as much from overreaction as from silence; flooding the zone with low-cost operations is partly designed to force democracies into a choice between looking weak or looking hysterical, and either outcome serves the Kremlin.
- Differentiate between low-level nuisance and impactful operations that may change the Kremlin's perception of European and NATO thresholds of response.

Introduction

On the evening of 3 June 2024, a blast tore through a modest hotel room in Roissy-en-France, shattering the quiet of the unassuming town on Paris' northeastern periphery. Inside, investigators found that the room had been transformed into a makeshift laboratory by a 26-year-old Russian-Ukrainian from Donbas who had spent two years in the Russian army.[1] Before he was taken to the hospital with severe burns, he had been assembling an improvised explosive device intended for a hardware store in the suburbs of Paris — a mundane target selected in an apparent effort to promote social unrest, mirroring other suspected Russian sabotage operations across Europe. Yet the episode barely registered: public outrage was muted, and both domestic and international media coverage of the failed sabotage plot was fleeting.

Since Russia's full-scale invasion of Ukraine in February 2022, a consistent operational tempo of hostile activities on European soil appears to have become normalized, folded into the fabric of daily life. Yet the cumulative record remains striking: the life of the CEO of Rheinmetall, one of Europe's largest defense manufacturers, has been threatened,[2] a supermarket and restaurant in Estonia have been torched,[3] planeloads of cash have been funneled into Moldova to tilt elections in Moscow's favor,[4] clandestine sensors aimed at tracking Royal Navy submarines carrying the UK's nuclear deterrent have been discovered in British waters,[5] and Russian as well as separatist forces in Tskhinvali/South Ossetia and Abkhazia have continued to advance the occupation line, shifting border markers into Georgian territory under the cover of night.[6] **Charting known or suspected Russian hybrid operations, this report traces the intensification and evolution of Russia's hybrid toolkit since 2022. It examines the hybrid TTPs Russia employs in targeted countries, the purposes they serve, the patterns of activity, and assesses what this means for countering these threats.**

So far, there has been no systematic analysis of the Tactics, Techniques, and Procedures (TTPs) Russia has used across different cultural and geopolitical contexts. This paper develops six case studies, France, Germany, the United Kingdom, Estonia, Moldova, and Georgia, through which it examines the TTPs of hybrid operations conducted by Russia across different European contexts since the full-scale invasion of Ukraine. It draws on a database constructed by the authors of publicly disclosed hybrid

1 Jacques Follorou, "Man arrested with explosives near Paris airport was part of vast Russian sabotage campaign," *Le Monde*, June 27, 2024, https://www.lemonde.fr/en/france/article/2024/06/27/man-arrested-with-explosives-near-paris-airport-was-part-of-vast-russian-sabotage-campaign_6675959_7.html.

2 "Armin Papperger: The German Arms Boss Russia Wants Dead," *The Economist*, May 21, 2025, https://www.economist.com/europe/2025/03/21/armin-papperger-the-german-arms-boss-russia-wants-dead.

3 "Arson Attack on Ukrainian Restaurant in Estonia Ordered by Russian Intelligence," News, *ERR*, July 2, 2025, https://news.err.ee/1609735683/arson-attack-on-ukrainian-restaurant-in-estonia-ordered-by-russian-intelligence.

4 Sarah Rainsford, "Moldova Election: Russian Cash-for-Votes Flows into Ukraine's Neighbour as Nation Heads to Polls," *BBC*, October 20, 2024, https://www.bbc.com/news/articles/c23kdjxxx1jo.

5 Olena Goncharova, "Russian Sensors Found Tracking UK Nuclear Submarines, Sunday Times Reports," *The Kyiv Independent*, April 7, 2025, https://kyivindependent.com/russian-sensors-found-tracking-uk-nuclear-submarines-sunday-times-reports/.

6 *Consolidated Report on the Conflict in Georgia (November 2022 – March 2023)* (Council of Europe, 2023), https://rm.coe.int/consolidated-report-on-the-conflict-in-georgia-november-2022-march-2023/1680aacba0.

threat incidents, both suspected and confirmed, as well as extensive consultations with experts across government, private sector, intelligence services, and civil society in the case study countries and beyond.

The report proceeds in three parts. The first outlines the conceptual boundaries and terminology that frame hybrid activity, followed by a detailed explanation of the dataset and coding methodology underpinning the analysis. The second part presents six country chapters that trace the evolution of Russian tactics between 2022 and 2025. The final sections draw these patterns together and consider their implications for European and transatlantic security.

What Are Hybrid Threats?

Historically, the synchronous deployment of all instruments of national power has been a hallmark of statecraft across the continuum of peace and conflict. In Sun Tzu's *The Art of War*, many of the key concepts that undergird hybrid threats were already expounded; the importance of deception and manipulation, as well as the idea of "victory without fighting," were laid out in this work from the 5th century B.C.E.7 Although the concept of hybrid threats may appear intuitive, challenges persist due to contested terminology and its overuse to describe virtually every aspect of conventional and unconventional warfare.

In Western academic and policy contexts, terms such as "hybrid threats," "hybrid warfare," and "grey zone conflict" are frequently used, often interchangeably, and lack universally agreed-upon definitions. The terms "hybrid warfare" and "hybrid threats" gained traction in Western military and academic circles in the early 2000s, as various insurgencies around the world combined irregular tactics with conventional armed forces. In 2005, Lieutenant General James Mattis and Lieutenant Colonel Frank Hoffman of the U.S. Marine Corps introduced the concept of hybrid warfare in an article on the nature of future conflicts.[8] In a 2007 elaboration, Hoffman defines hybrid threats as "competitors who will employ all forms of war and tactics, perhaps simultaneously," later specifying such threats as "any adversary that simultaneously and adaptively employs a fused mix of conventional weapons, irregular tactics, terrorism, and criminal behavior in the battle space to obtain their political objectives."[9] In its early conceptualization, hybridity thus referred to an observed transformation in the nature of kinetic conflict. But like other terminology, its use and meaning evolved over time.

Current discussions of hybrid threats largely draw on the term's usage since the onset of the Russo-Ukrainian war in 2014, particularly the Russian annexation of Crimea and the Kremlin's use of "little green men." In that example, hybridity came to denote the various ways in which states conduct operations below the threshold of conventional armed conflict, often leveraging plausible deniability to

7 Sun Tzu, "The Art of War," 500 BCE, https://classics.mit.edu/Tzu/artwar.html.

8 James N. Mattis and Frank Hoffman, "Future Warfare: The Rise of Hybrid Wars," U.S. Naval Institute, November 1, 2005, https://www.usni.org/magazines/proceedings/2005/november/future-warfare-rise-hybrid-wars.

9 Frank Hoffman, "Armed vs Compound War," Armed Forces Journal, October 1, 2009, https://web.archive.org/web/20260111030304/http://armedforcesjournal.com/hybrid-vs-compound-war/; Frank Hoffman, "Conflict in the 21st Century: The Rise of Hybrid Wars," *Conflict in the 21st Century*, December 2007, https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

pursue their strategic objectives.[10] Hybrid threats have thus largely become viewed as "unacceptable foreign interference in sovereign states' internal affairs and space."[11]

The concept itself has been contested as too broad, resting on the assumption that not all conflicts feature a blend of coercive instruments, as lacking analytical utility, or as unjustly claiming novelty.[12] Some have described it as "old wine in new bottles," a spruced-up version of the old term: Military Operations Other Than War (MOOTW). Hybrid threats have largely been conceptualized as a mode of war, as described by Hoffman, a strategic approach to foreign policy, as observed in Russian activities in the Donbas, or as a conceptual signal that Western policymakers and militaries neglected grand strategy that encompasses domains beyond the military, thus leveraging the concept to correct a prior.[13]

While definitions vary, interwoven within the conceptual debates surrounding hybrid threats, there are several recurring definitional components:

- The asynchronous or synchronous use of diverse methods, primarily non-military, to advance strategic objectives.
- The conduct of such activities below the threshold of conventional areas of conflict or declared war generates ambiguity, at times complicating attribution, and constraining retaliation.
- The characterization of these activities as coercive, distinguishing them from benign forms of exerting influence.

The guiding definition for this paper considers **hybrid threats to be the coercive use of various instruments of national power to advance strategic objectives below the threshold of conventional armed conflict. Often designed to preserve ambiguity of attribution, these threats exist along a continuum and, at their most effective, are used in conjunction with one another, making them multi-modal and often functioning as a force multiplier.** To avoid crossing the threshold of conventional armed conflict through escalatory spiraling, hybrid operations rely on plausible deniability and obfuscation. Plausible deniability is best understood as a variable instrument shaped by context rather than a defining criterion of hybrid operations. In some cases, hybrid activities are obscured to mask intent rather than attribution, while in others, the activity is designed to provide plausible deniability for a specific audience, such as neutral states or the Russian public.

---

10 Keir Giles, "Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power," Chatham House, March 21, 2016, https://www.chathamhouse.org/2016/03/russias-new-tools-confronting-west-continuity-and-innovation-moscows-exercise-power.

11 Georgios Giannopoulos et al., *The Landscape of Hybrid Threats: A Conceptual Model* (European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), 2021), https://doi.org/10.2760/44985.

12 Christopher Paul, "Confessions of a Hybrid Warfare Skeptic: What Might Really Be Interesting but Hidden Within the Various Conceptions of Gray Zone Conflict, Ambiguous Warfare, Political Warfare, and Their Ilk," *Small Wars Journal*, March 3, 2016, https://archive.smallwarsjournal.com/index.php/jrnl/art/confessions-of-a-hybrid-warfare-skeptic; Damien Van Puyvelde, "Hybrid War – Does It Even Exist?," NATO Review, May 7, 2015, https://web.archive.org/web/20241125174159/https://www.nato.int/docu/review/articles/2015/05/07/hybrid-war-does-it-even-exist/; Michael Kofman, "Russian Hybrid Warfare and Other Dark Arts," War on the Rocks, March 11, 2016, https://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/.

13 Joseph Henrotin, "La Guerre Hybride Comme Avertissement Stratégique," *Stratégique* 111, no. 1 (2016): 11–31, https://doi.org/10.3917/strat.111.0011.

Russia's integrated approach to leveraging all instruments of national power below the threshold of conventional armed conflict traces back to the Soviet concept of *aktivnye meropriyatiya,* or "active measures." This term described the myriad covert subversion techniques employed by the Committee for State Security (KGB) and other agencies in pursuit of the Soviet Union's foreign policy objectives, including propaganda, disinformation, political assassinations, and support of foreign political movements and revolutionary groups.[14] Following the collapse of the Soviet Union (USSR), the eastward expansion of NATO, paired with the various Color Revolutions[15] in Russia's near abroad, led the Kremlin to increasingly view "active measures" as a tool used by the West against Russia. As a result, Russia's National Security Strategy (NSS) Reports and Military Doctrines demonstrate a shift toward greater emphasis on information security, the role of non-military means, and the defense of traditional Russian values against foreign interference in this period.

Contemporary Russian strategic literature reveals a Russian approach to foreign influence that is grounded in utilizing decentralized, self-regulating actors who pursue personal interests aligned with Kremlin objectives rather than being coercively and externally imposed, often referred to as "useful idiots." Domestically, and in its historic sphere of influence, researchers at the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) point to prominent Russian academic Vladimir Lepskiy's similar concept of *polisubjekts* — cohesive social units unified by shared values and a sense of "Russianness" — which allows the state to assert indirect control over a population through ideological coherence and patriotic upbringing.[16]

Polisubjekts hacker groups or private military companies, for example — can then be used to help advance Russian foreign policy aims. This strategy is often complemented by the doctrine of *reflexive control*, a Soviet-era theory developed by Russian cybernetics researcher, Vladimir Lefebvre in the 1960s, which focuses on shaping an adversary's psychology, or decision-making, by manipulating information, assumptions, and perceptions rather than through direct coercion.[17]

By the 1980s, Soviet military and political strategists began actively developing reflexive control as a practical tool for influencing adversaries. Over time, and especially in the period after the 2008 war in Georgia, when Russia embarked on major military reforms and capacity-building, Russian military thinkers further refined reflexive control into a coordinated process that could exploit and influence an adversary's decision patterns without necessarily requiring detailed insight into their psychology.[18] Its inconspicuous nature fit a strategic environment in which the boundary between war and peace is blurred, enabling Russia to pursue its objectives while operating below the threshold of overt conven-

14 Mark Galeotti, "Active Measures: Russia's Covert Geopolitical Operations," George C. Marshall European Center For Security Studies, June 2019, https://www.marshallcenter.org/en/publications/security-insights/active-measures-russias-covert-geopolitical-operations-0.

15 "Color revolutions" refers to a wave of mass protest movements that toppled or pressured governments, notably in Georgia (Rose Revolution, 2003), Ukraine (Orange Revolution, 2004), and Kyrgyzstan (Tulip Revolution, 2005), with later cases sometimes discussed in the broader family of similar mobilizations such as in Armenia (Velvet Revolution, 2018). To Moscow, these revolutions are frequently not interpreted as an organic movement but as an externally supported plot by the U.S.

16 Giannopoulos et al., *The Landscape of Hybrid Threats: A Conceptual Model*.

17 Giannopoulos et al., *The Landscape of Hybrid Threats: A Conceptual Model*.

18 After the Five-Day War (2008), Russian and external assessments highlighted problems with command-and-control, communications, intelligence, interoperability, and outdated equipment. Among the rank-and-file, long-running issues such as dedovshchina (hazing) and weak non-commissioned officers culture contributed to chronic professionalism problems.

tional conflict.

The Kremlin views its approach to hybrid warfare as inherently defensive, shaped by the belief that the West — particularly the United States — has waged a continuous hybrid war against Russia since the end of the Cold War. This perception is deeply embedded in official doctrine. Russia's 2021 NSS places "information security" at its core, identifying significant threats from foreign interference through the spread of "false information" and attempts at undermining "traditional Russian values" through the "falsification of history."[19] The 2023 Concept of the Foreign Policy of the Russian Federation states that "the United States of America (USA) and its satellites used the measures taken by the Russian Federation as regards Ukraine to protect its vital interests as a pretext to aggravate the longstanding anti-Russian policy and unleashed a new type of hybrid war. It is aimed at weakening Russia in every possible way, including … limiting its sovereignty in foreign and domestic policy, violating its territorial integrity."[20]

Russian analysts perceive and/or frame developments ranging from NATO expansion to support for democratic movements like the Arab Spring and Ukraine's EuroMaidan as Western-led coordinated efforts to destabilize regimes and reshape the global order in favor of Western interests. This analysis is rooted in Russia's own worldview. This perspective not only drives the continuous adaptation of Russia's military and foreign policy doctrines, but also serves to justify the use of similar tactics within its own sphere of influence and beyond — historically in Afghanistan and Syria, and more recently in Libya and across the Sahel — where Moscow has relied on "polisubjekts" such as the Wagner Group and, later, Africa Corps to entrench influence in pursuit its objectives. Nevertheless, this perspective, that purported Western aggression has become a key driver of Russian strategic behavior, blurs the line between Russian military planning and its own propaganda.[21]

19 "Указ Президента Российской Федерации От 02.07.2021 № 400 'О Стратегии Национальной Безопасности Российской Федерации,'" Официальное опубликование правовых актов, July 2, 2021, http://publication.pravo.gov.ru/Document/View/0001202107030001.

20 "The Concept of the Foreign Policy of the Russian Federation," Министерство иностранных дел Российской Федерации, March 31, 2023, https://www.mid.ru/ru/detail-material-page/1860586/?lang=en.

21 Mason Clark, *Russian Hybrid Warfare*, Military Learning and the Future of War Series (Institute for the Study of War, 2020), https://understandingwar.org/research/russia-ukraine/russian-hybrid-warfare-2/.

Methodology and Framework

This study adopts a multimethod research design that combines structured open-source data collection and expert interviews to analyze Russian hybrid activity across six European states between February 2022 and December 2025. The core of this methodology is a custom incident database developed by the authors that records hybrid operations attributable to Russian state actors, Russian-linked groups, or intermediaries acting on Russia's behalf, with varying levels of confidence.

The database structure is based on the conceptual model of hybrid threats published in February 2021 by the Hybrid CoE and the Joint Research Centre of the European Commission (JRC).[22] This conceptual model describes the hybrid threat landscape and establishes a common language for analyzing it. Further refinements to this framework, specifically the addition of 'Unit of Analysis', 'Actor', and 'Certainty Attribution' categories, were introduced by the research team to enhance the granularity of the framework and the completeness of our hybrid threat incident database. The database is publicly available and includes further methodological notes, available on The Soufan Center website.

The resulting dataset comprises entries describing individual hybrid threat incidents and includes the following variables:

- **Incident**: A factual description of the incident.
- **Unit of Analysis:** Classifies the incident as a campaign or a discrete event.
- **Event Start & End Dates**: Recorded with associated date certainty levels (approximate or exact).
- **Status:** Indicates whether the activity is ongoing or concluded.
- **Tools Used**: Specific mechanisms employed for operation, categorized according to the Hybrid CoE Conceptual Model for Hybrid Threats.[23]
- **Domains Affected**: National instruments of power targeted by the incident, derived from the Hybrid CoE's list.
- **Phase**: The stage of progression within the hybrid threat escalatory ladder – priming, destabilizing, coercing (see below for more).
- **Actor**: The responsible entity, categorized as Russian authorities/officials/services, groups linked to Russia, or third-party individuals recruited by Russia (see below for more).
- **Certainty Attribution**: A confidence level assigned to each incident to indicate the strength of attribution to Russia (see below for more)

Case Country Selection

The six countries in this study (France, Germany, the United Kingdom, Estonia, Moldova, and Georgia) were selected to capture variation in geopolitical alignment, membership in collective security organizations, historical relationships with Russia, and levels of exposure to Russian influence. These cases include NATO and non-NATO members, EU and non-EU members, frontline and non-frontline states, and countries where Russian activity both predates and postdates the 2022 invasion. The inclusion of

22 Giannopoulos et al., *The Landscape of Hybrid Threats: A Conceptual Model*.

23 See dataset on The Soufan Center website for full list of tools. Tools include but are not limited to physical operations against infrastructure, cyber espionage, airspace violation, territorial water violation, armed forces conventional/sub-conventional operations, electronic operations (GNSS jamming and spoofing), targeted assassinations (attempted and successful), and creating and exploiting infrastructure dependency (including civil-military dependency).

frontline states like Estonia, Moldova, and Georgia, therefore, reflects continuity that intensified during the 2022–2025 period, rather than a claim that Russian activity in these settings began only after the full-scale invasion. The case-country selection is designed to capture variation in Russian hybrid activity, not to represent Europe in its entirety; therefore, the findings show patterns within this sample rather than offering continent-wide generalizations.

Inclusion and Exclusion Criteria

Hybrid threats in this study refer to the coercive use of various instruments of national power to advance strategic objectives below the threshold of conventional armed conflict. Often designed to preserve ambiguity of attribution,[24] these threats exist along a continuum and, at their most effective, are used in conjunction with one another, making them multi-modal and often functioning as a force multiplier. Russian hybrid incidents in Europe in the 2022–2025 period include coercive, sub-threshold actions that are openly attributable yet still designed to avoid triggering conventional military responses. Some scholarship refers to such activities as "sub-threshold activities."[25] These are distinguished from conventional military activity intended for combat, which remains outside the scope of this report on hybrid threats.

Inclusion criteria:

- occurred between February 2022 and December 2025 in one of the six case study countries;
- met the definitional criteria outlined above;
- could be linked to Russia at one of the defined attribution tiers;
- had sufficient open-source evidence to support classification.

Exclusion criteria:

- purely speculative allegations without evidence;
- domestic political activities without demonstrable Russian involvement.

Units of Analysis

To avoid redundancy and double-counting and improve comparability, incidents are classified into two analytical units.

- **Campaign:** Multi-episode, sustained effort conducted by a single orchestrator or network (e.g., Matryoshka, complex espionage operations, Storm-1516, Killnet, R-FBI). These are logged once as continuous entries. Such campaigns may include thousands of narratives and millions of pieces of content.
- **Event:** Discrete, attributable act such as vandalism, cyber intrusions, arson, staged protests, or reconnaissance activities.

This means that subcampaigns and individual narratives within a broader disinformation campaign were not logged separately in the database. Likewise, not every cyberattack was recorded. Instead, the

24 To avoid crossing the threshold of armed conflict through escalatory spiraling, hybrid operations rely on plausible deniability and obscuration. Deniability is best understood as a variable instrument shaped by context rather than a defining criterion of hybrid operations. In some cases, hybrid activities are obscured to mask intent rather than attribution, while in others the activity is designed for plausible deniability for a specific audience, such as neutral states, or the Russian public.

25 Matus Halas, "NATO's Sub-Conventional Deterrence: The Case of Russian Violations of the Estonian Airspace," Contemporary Security Policy 43, no. 2 (2022): 350–81, https://doi.org/10.1080/13523260.2022.2028464.

authors applied the following rules:

- State-linked or strategically consequential cyber incidents were logged.
- Disinformation campaigns were coded as single continuous entries, i.e., "campaign."
- Individual narratives within disinformation campaigns were not separately logged to avoid inflating incident counts.
- Physical disinformation operations were recorded as individual events.[26]

Data Collection and Sources

Incidents were identified through systematic open-source research, drawing on publicly available government reports, news media, academic publications, social media content, open data portals, and legal documents. Keywords were searched in multiple search engines to surface operations, and English as well as the case-study country languages were used to conduct comprehensive searches of local sources.

Attribution Framework

To assess the likelihood of Russian responsibility, the study uses a four-tier classification:

- **Certain:** Official attribution and/or convergent independent investigations with (digital) forensic corroboration.
- **Probable:** Multiple independent sources with strong pattern consistency but lacking (digital) forensic proof.
- **Likely:** One strong or several moderate sources, or partial pattern match, or indirect indicators.
- **Suspected:** Preliminary indicators only — used for early signals that remain uncorroborated.

Hybrid Spectrum and Phases

The Conceptual Model for Hybrid Threats charts hybrid threats across an escalation spectrum. Specifically, it proposes three phases, understood as sequential but nonlinear stages of hybrid threat activity used by a hostile actor to achieve strategic objectives. Every incident in our dataset was classified as pertaining to one of these phases.

- **Priming:** The initial, often long-term, low-visibility phase of the hybrid threat ladder. Typically, this phase seeks to compel the target to voluntarily choose actions that benefit the hostile actor or seeks to operate below detection thresholds using psychological influence, infiltration, or economic tools.
- **Destabilizing:** The phase of the hybrid threat ladder defined by more visible and intense activity. Operations in this tier typically move beyond reflexive control and seek to directly influence the behaviors and actions of the targeted population.
- **Coercing:** Activity in this phase typically extends beyond the usual "below the threshold" hybrid activity and appears in its most overt form. The coercion phase is the most detectable and attributable of the three phases, aiming to compel action from a target through more forceful efforts, often targeting the military domain.

26 Physical disinformation operations are orchestrated realworld acts that plant false or misleading cues intended to be shared and amplified to shape perceptions or political interpretations.

Actors

Since the fullscale invasion of Ukraine, Russia has increasingly relied on intermediate actors to carry out its operations in Europe after the mass expulsion of diplomats, many of whom were also GRU undercover agents at embassies.[27] These include not only disposable agents recruited for one-off tasks, but also operatives reused across multiple operations. To capture trends around the exact actors behind Russian hybrid threat activities in Europe systematically, each hybrid operation in the dataset is coded according to the type of actor involved:

- **Russian state directly:** Operations conducted by Russian state organs such as intelligence services, border forces, or cyber units.
- **Russia through intermediary non-state group:** Operations conducted by intermediary groups and organizations including activist networks, extremist organizations, and charitable or civic entities**.**
- **Russia though intermediary individuals:** Operations conducted by intermediary individuals including disposable agents as well as reused operatives acting on Russia's behalf.

Coding Process

All authors coded an initial sample of incidents, followed by an adjudication process to harmonize interpretations and to make the dataset more useful. Disputes over classification (e.g., attribution tier, hybrid inclusion criteria, phase categorization) were resolved in team discussions.

Interviews

In addition to qualitative and quantitative analyses of hybrid incidents using the incident database, the research team conducted extensive semi-structured interviews in 2025 with stakeholders involved in studying, investigating, or countering hybrid threats to surface different perspectives on Russian TTPs and their ultimate objective. Interviewees were drawn from the public, private, and civil society sectors to ensure a breadth of perspectives. Individuals interviewed had expertise in disinformation, grand strategy, cybersecurity, counterintelligence, strategic communications, and related domains. Additional participants were identified through a snowballing process, with initial interviewees recommending additional relevant experts.

In total, 22 interviews were conducted using a semi-structured format.[28] Each interview was guided by a standardized set of questions developed by the authors, covering themes including threat perception in the case study country, incident attribution practices, institutional responses, and the perceived objectives of the hybrid campaign. The semi-structured approach allowed interviewers to expand the question set in response to the flow of each conversation.

27 "Диверсии с Безопасного Расстояния," Dossier Center, July 24, 2024, https://dossier.center/diversion/.

28 Margaret C. Harrell and Melissa A. Bradley, *Data Collection Methods: Semi-Structured Interviews and Focus Groups* (2009), https://www.rand.org/pubs/technical_reports/TR718.html.

Limitations

The authors recognize the limitations posed by the exclusive use of open sources, the politicized and strategic nature of state disclosures and incident attribution, and the inherent uncertainty associated with confidence levels in attribution in open-source investigative reporting. It is additionally important to note that attribution may evolve as investigations progress. There are multiple entries in our dataset of incidents that are likely or probably attributable to Russia that are under active investigation or still being adjudicated in court. Not all court decisions and investigation outcomes are made public, depending on sensitivities and jurisdictions.

The most challenging aspect of compiling a database of hybrid operations — ambiguous and often plausibly deniable by design — is striking the balance between attributing hostile acts to Russia and avoiding overstatement of its capabilities or reach. Russia benefits from both. If one drone sighting is in fact a Moscow directed reconnaissance effort while another is simply an overeager teenager flying too close to an airport, and both are publicly treated as Russian operations, the Kremlin can dismiss them both as civilian anomalies and evidence of Western Russophobia. This ambiguity is precisely what allows Russia to reap the advantages of hybrid operations.

Case Studies

i. France

Introduction

In May of 2025, French President Emmanuel Macron announced that France would begin to systematically attribute Russian hostile acts on its soil, breaking with its long tradition of not publicly identifying the foreign governments behind these activities. This new paradigm has been incrementally established since 2021, as it applies to Russia, reflecting deteriorating relations with Moscow and Macron's desire to raise awareness of the Russian threat within France.[29]

This latest juncture in Russia-France relations, at a time of unprecedented hybrid threats, may appear in contrast to France's posture in the weeks leading up to the full-scale Russian invasion of Ukraine in February 2022. At the time, Macron traveled to Moscow and Kyiv and reassured officials that Russian President Vladimir Putin had made known that the Ukraine crisis would not escalate in return for security guarantees.[30] Months into the invasion, President Macron insisted that Russia should not be humiliated so that diplomatic solutions to the conflict remained viable.[31] Rapidly weaned off the belief that diplomatic engagement and the provision of off-ramps would be embraced by Putin, Macron's position on Russia has grown markedly tougher since the early months of the invasion, declaring that the possibility of Western troops being deployed in Ukraine cannot be ruled out.[32] Increasingly, the Russia-Ukraine War has served as a vehicle for establishing greater European strategic autonomy, a key objective of Macron's platform since being elected in 2017.[33] It has now led to a more assertive policy of attributing hostile activities to Russia.

The recent surge in hybrid activities on French soil and their impact should not solely be viewed through the lens of the full-scale invasion of Ukraine, but also through the historical relations between Paris and Moscow. France carries layered, historical memories of Russia and its Soviet progenitor and has historically viewed the USSR as an important element in preserving a broader balance of power within the international system, especially during the Cold War.[34]

Notably, former President Charles de Gaulle's security strategy emphasized autonomy at a time of deepening commitment to collective security pacts in the Global North and maintained skepticism toward supranational military structures that, in his view, diluted national sovereignty. This in part led

---

29 Quentin Jalabert et al., "Calling Out Russia: France's Shift on Public Attribution," War on the Rocks, July 3, 2025, https://warontherocks.com/2025/07/calling-out-russia-frances-shift-on-public-attribution/.

30 "Macron Says Putin Gave Him Assurances over Russia-Ukraine Crisis," *Al Jazeera*, February 8, 2022, https://www.aljazeera.com/news/2022/2/8/macron-says-putin-told-him-russia-wont-escalate-ukraine-crisis.

31 "Russia Must Not Be Humiliated despite Putin's 'historic' Mistake, Macron Says," *Reuters*, June 4, 2022, https://www.reuters.com/world/europe/russia-must-not-be-humiliated-despite-putins-historic-mistake-macron-2022-06-04/.

32 Joshua Berlinger et al., "Macron Says 'Nothing Ruled out,' Including Using Western Troops, to Stop Russia Winning Ukraine War," *CNN*, February 27, 2024, https://www.cnn.com/2024/02/27/europe/france-macron-troops-ukraine-intl.

33 Ian Bremmer, "From Dove to Hawk: Explaining Macron's Russia-Ukraine Journey," GZERO Media, March 27, 2024, https://www.gzeromedia.com/by-ian-bremmer/from-dove-to-hawk-explaining-macrons-russia-ukraine-journey.

34 Teona Giuashvili, "France's Eastern Zeitenwende?," Elcano Royal Institute, May 8, 2024, https://www.realinstitutoelcano.org/en/analyses/frances-eastern-zeitenwende/.

to France's 1966 withdrawal from NATO's integrated military command, a decision that was only reversed by President Nicolas Sarkozy in 2009. In addition to reaffirming France's military independence, de Gaulle's call for "détente, entente, and cooperation" with the USSR created a distinctively French approach to managing East–West tensions.[35] While de Gaulle was also suspicious of the USSR, debates remain on whether active measures shaped his decision to withdraw from NATO, at a time when such measures sought to damage Franco-American relations.[36] Today, Russian information operations routinely attempt to tap into that enduring legacy, exploiting concerns about autonomy in order to undermine confidence in institutions like NATO.[37] A majority of Frenchmen continue to view NATO favorably, indicating these operations have not yet made a significant dent.[38]

After the collapse of the USSR, various French presidents sought to bring Russia into the European fold. A key moment in France–Russia relations came during the 2008 Russia–Georgia War, when President Nicolas Sarkozy positioned himself as the main diplomatic broker between Tbilisi and Moscow.[39] While some touted Sarkozy's intervention as a diplomatic success at the time, critics noted that the agreements he reached with Russian President Dmitry Medvedev were short-sighted and vague, offering no firm guarantees for Georgia's territorial integrity and setting no clear deadlines for the withdrawal of Russian forces.[40] Incredulously, Sarkozy approved the sale of two Mistral-class amphibious-assault helicopter-carrier ships to Russia in 2011, just three years after the Russian invasion of Georgia. The sale was only annulled under significant pressure from a number of European NATO members and the United States at the onset of the Donbas War in 2014.[41] The idea that Moscow could become integrated into the European fold seems to have also been present in the early days of the full-scale invasion of Ukraine, when Macron believed that "through trust, and intellectual discussion, a path with Putin" could be established.[42]

Since then, France's former Chief of Defense Staff Thierry Burkhard shared publicly that Russia has designated France as a primary adversary in Europe and has used its hybrid arsenal to target the country extensively.[43] As the EU's second-largest economy and its only independent nuclear deterrent since Brexit, France remains a central pillar of Europe's security architecture and thus of significant strategic

35 Anton W. DePorte, "De Gaulle's Europe: Playing the Russian Card," *French Politics and Society* 8, no. 4 (1990): 25–40.

36 Nicolas Quénel, *Allô, Paris ? Ici Moscou. Plongée Au Cœur de La Guerre de l'information* (Denoël, 2023).

37 "Disinfo: France Is Not a Sovereign Country," EUvsDisinfo, May 18, 2021, https://euvsdisinfo.eu/report/france-is-not-a-sovereign-country/.

38 Moira Fagan et al., "Views of NATO," Pew Research Center, June 23, 2025, https://www.pewresearch.org/global/2025/06/23/views-of-nato-2025/.

39 Mark Tran, "Enter Sarkozy the Peacemaker," *The Guardian*, August 12, 2008, https://www.theguardian.com/world/2008/aug/12/georgia.russia4.

40 Hélène Février, "Guerre de 2008 En Géorgie : Le "cadeau" de La France à La Russie," *TV5 Monde*, August 7, 2013, https://information.tv5monde.com/international/guerre-de-2008-en-georgie-le-cadeau-de-la-france-la-russie-20009.

41 John Daly, "France to Refund Russia $1.2 Billion for Non-Delivery of Mistral Helicopter Carriers," 04 2015, https://jamestown.org/france-to-refund-russia-1-2-billion-for-non-delivery-of-mistral-helicopter-carriers/.

42 François Vignal, "Ukraine : Comment Expliquer l'évolution d'Emmanuel Macron Face à La Russie ?," Public Sénat, March 2024, https://www.publicsenat.fr/actualites/international/ukraine-comment-expliquer-levolution-demmanuel-macron-face-a-la-russie.

43 "La Russie a Désigné La France Comme « son Principal Adversaire En Europe », Selon Le Chef d'état-Major Français," *Le Monde*, July 11, 2025, https://www.lemonde.fr/international/article/2025/07/11/la-russie-a-designe-la-france-comme-son-principal-adversaire-en-europe-selon-le-chef-d-etat-major-francais_6620666_3210.html.

relevance to Moscow. Early in the Russia-Ukraine war, Paris raised the idea of a shared European nuclear umbrella, though questions about the role of the *Force de dissuasion*, the credibility of extended deterrence, and the practicalities of joint nuclear decision-making among EU partners remain unresolved.[44]

France has had a significant impact on Europe's defense policy in recent years. Since 2017, President Macron has accelerated interest at the EU-level in greater European strategic autonomy, now openly stated as a goal in various EU policies, with France as a central driver behind new defense-industrial instruments and joint procurement schemes designed to strengthen Europe's ability to produce and purchase its own military capabilities. Beyond defense, Macron's framing of autonomy as a broader sovereignty agenda has shaped various EU economic policies, including the European Chips Act.[45]

France's relevance in Russia's hybrid strategy also stems from its global cultural reach, reflected in the 321 million French speakers worldwide and the cultural institutions that support them. As a former colonial power, France exerts political, cultural, and military influence in regions of significant interest to Russia, notably in Africa and the Middle East, where Russia increasingly vies for influence and access to natural resources. In the Sahel, Russia, including through its proxies Wagner and Africa Corps, has successfully leveraged political instability and the expansion of Salafi Jihadist armed groups to establish its presence. It has traded counterterrorism aid to under-resourced military juntas for access and influence and has used all-encompassing disinformation campaigns to shape public opinion against France and the West more broadly.

While the tempo of hybrid threat incidents in France — and the media attention surrounding them — has increased markedly since Russia's full-scale invasion of Ukraine, the country had already been the target of earlier Russian interference efforts. Before 2022, the Kremlin's overarching ethos in its interference strategy focused on keeping French audiences polarized over domestic issues, giving it free rein on the international stage, including in francophone Africa.[46] Many of the issues targeted by interference related to the information sphere, "also fueled the popularity of far-right parties that were favorable to and aligned with Russia at the time, killing two birds with one stone."[47] In France, both far-right and far-left politicians have maintained close relations with the Kremlin or have justified Russian interventionism, including the annexation of Crimea.[48] Since 2022, Moscow has become more careful to distance itself from far-right parties in the EU that, for example, have visited the Kremlin on various occasions, as this would undermine the official Russian state narrative that movements opposing mili-

---

44 Alexander Sorg, "Force de l'Europe: How Realistic Is a French Nuclear Umbrella?," War on the Rocks, March 24, 2025, https://warontherocks.com/2025/03/force-de-leurope-how-realistic-is-a-french-nuclear-umbrella/.

45 "France to Invest Nearly €3 Billion in Semiconductor Factory to Boost Local Production," *France 24*, June 5, 2023, https://www.france24.com/en/europe/20230605-france-to-invest-nearly-%E2%82%AC3-billion-in-semiconductor-factory-to-boost-local-production.

46 Samuel Ramani, "Why Russia Is a Geopolitical Winner in Mali's Coup," Foreign Policy Research Institute, September 16, 2020, https://www.fpri.org/article/2020/09/why-russia-is-a-geopolitical-winner-in-malis-coup/; Luke Coffey, "Russia Exploits 'Yellow Vest' Turmoil In France," The Heritage Foundation, February 8, 2019, https://www.heritage.org/europe/commentary/russia-exploits-yellow-vest-turmoil-france.

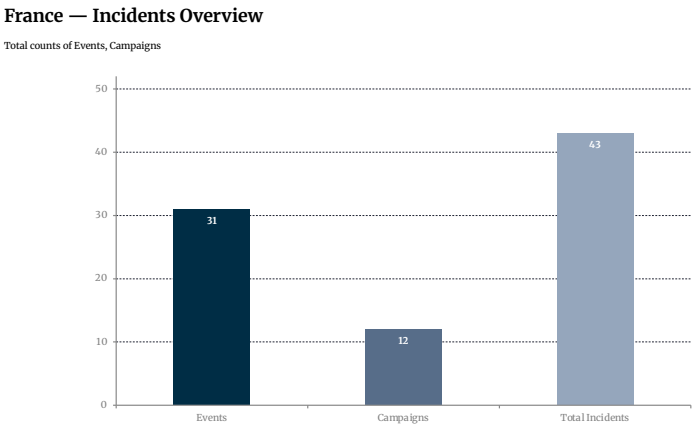
47 Nicolas Quenel, "Interview," 2025.

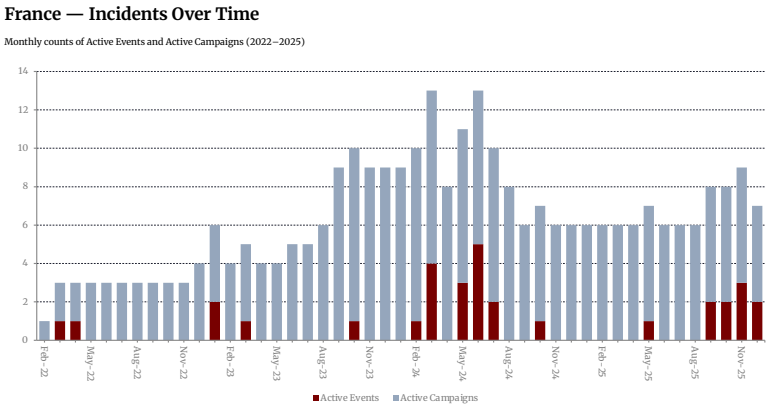
48 "In the Kremlin's Pocket: Who Backs Putin, and Why," *The Economist*, February 12, 2015, https://www.economist.com/briefing/2015/02/12/in-the-kremlins-pocket; Romain Geoffroy and Maxime Vaudano, "Quels Sont Les Liens de Marine Le Pen Avec La Russie de Vladimir Poutine ?," *Le Monde*, April 20, 2022, https://www.lemonde.fr/les-decodeurs/article/2022/04/20/quels-sont-les-liens-de-marine-le-pen-avec-la-russie-de-vladimir-poutine_6122903_4355770.html.

tary support for Ukraine or the rearmament of Europe are entirely organic.[49]

Results

The research team identified 43 hybrid incidents targeting France between February 2022 and December 2025 in open sources. 12 of the incidents were sustained campaigns and 31 incidents were discrete events. Analysis indicates that 39.5 percent of hybrid operations identified were certainly attributable to Russia, 34.9 percent probably, and 9.3 percent likely, while 16.3 percent of incidents were suspected to be Russian-orchestrated. The peak in active incidents occurred in March and June 2024, with 13 incidents logged in those months.



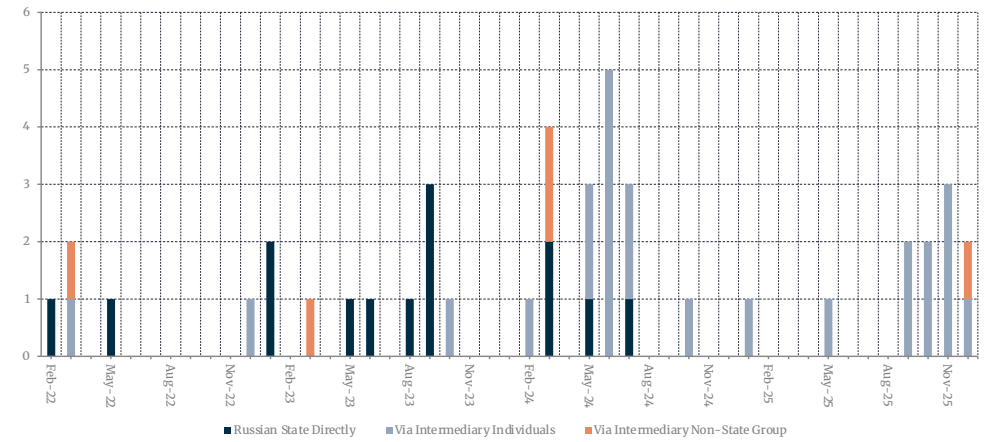


The most common actor behind the hybrid operations identified was 'Russia through intermediary individuals' (24 incidents), the 'Russian state directly' (14 incidents), and 'Russia through an intermediary non-state group' (five incidents). Since June 2024, hybrid threat operations in France have been almost exclusively conducted by 'Russia through intermediary individuals.' Incidents attributed to this actor jumped from 26 percent pre-June to 90 percent post-June 2024.

49 Quenel, "Interview."

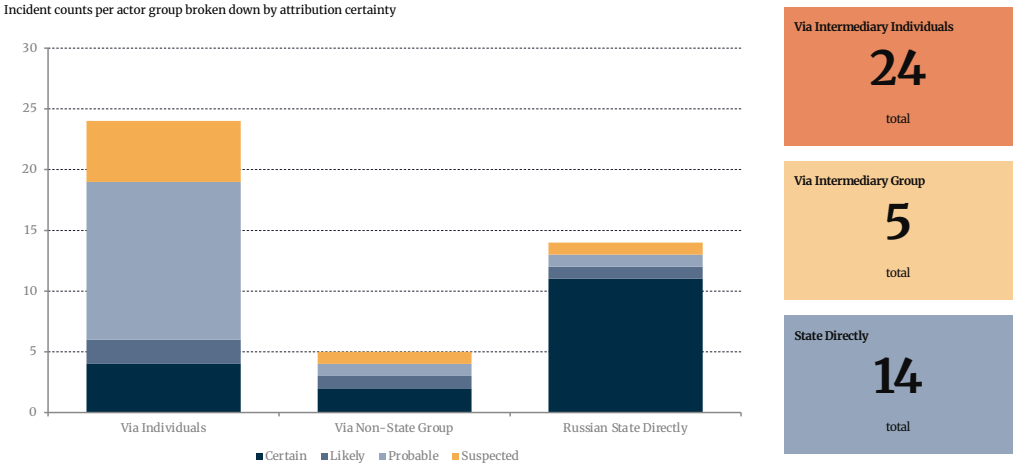
France — Actor Type by Month

Monthly incident counts by actor type — by start date



France — Actor Type & Certainty Levels

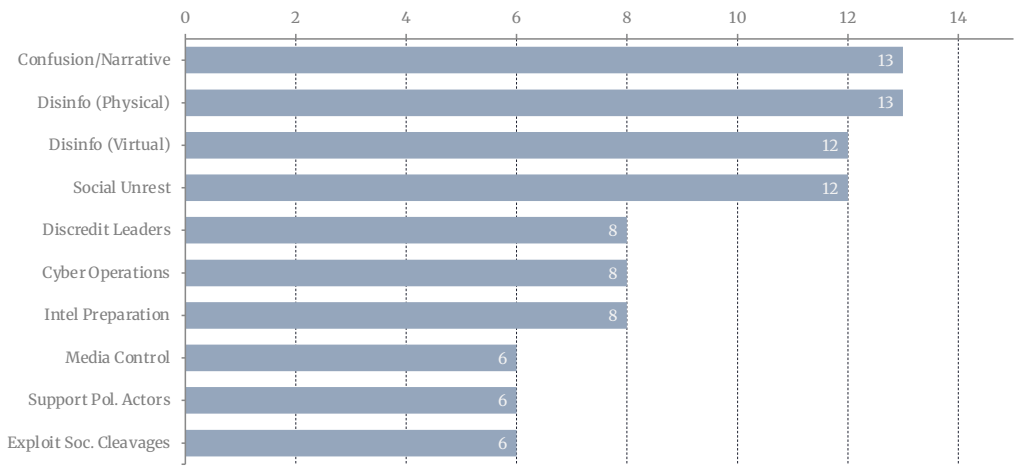
Incident counts per actor group broken down by attribution certainty



The most common tools employed by Russia in hybrid operations targeting France were ‘Creating confusion or a contradictory narrative’ (13 instances), ‘Disinformation campaigns and propaganda (physical)’ (13 instances), ‘Disinformation campaigns and propaganda (virtual)’ (12 instances), ‘Promoting social unrest’ (12 instances), and ‘Cyber operations’ (8 instances). In almost all 43 identified incidents, Russia leveraged multiple tools.

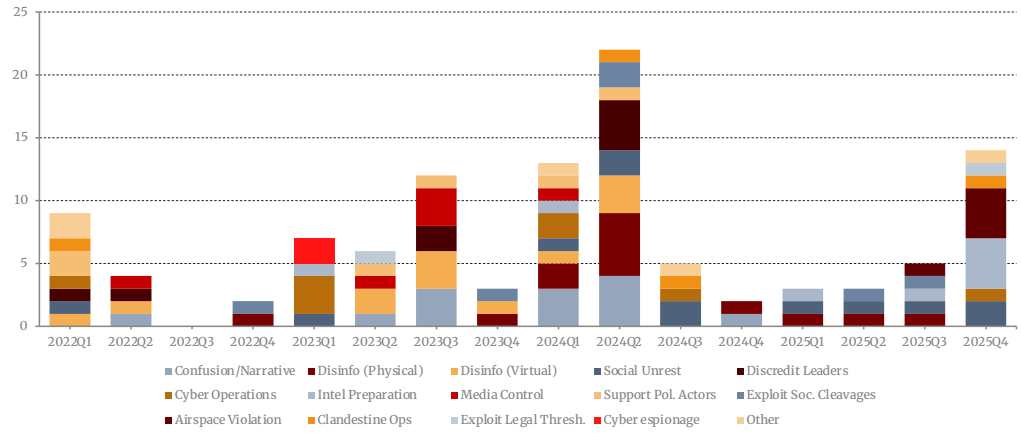
France — Top 10 Tools

Most frequently used tools — total count across all incidents



France — Tools by Quarter

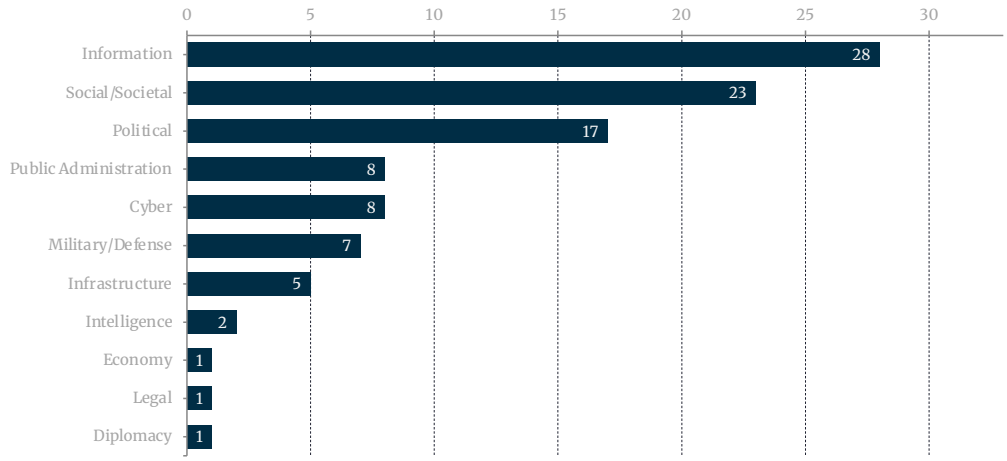
Quarterly counts of tools used at incident start date



The most targeted domain by Russia in France is the ‘Information’ environment (28 instances), ‘Societal/Social’ environment (23 instances), and the ‘Political’ environment (17 instances).

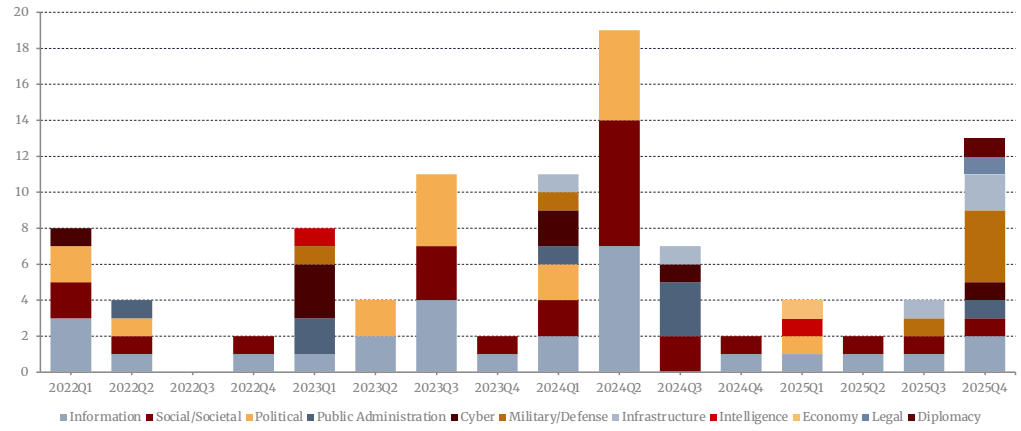
France — Total Domains

Incident counts aggregated by impacted domain



France — Domains by Quarter

Quarterly counts of impacted domains



Findings

Objectives and Effect

While a previous section has laid out the definition of hybrid threats, the objectives Russia pursues by conducting such operations are context dependent. TTP analysis and expert interviews show that these actions serve both domestic and external foreign policy objectives. Professor of Terrorism and Political Violence Bart Schuurman succinctly summarizes the goal of hybrid operations in Europe as an attempt to gain battlefield advantage by throttling aid to Ukraine and undermining political will for such support.[50] Nicolas Quenel, author of an in-depth study on the history of Russian information operations in France and its contemporary forms, highlights that these operations seek to undermine support for Ukraine but argues that their ultimate goal is "to implode the system of alliances that has dominated since the end of World War II, from the European Union to NATO."[51] Quenel also argues that, when it comes to information operations targeting France, the Kremlin's primary target is its domestic audience, bolstering the legitimacy of the Russian regime within its own borders. He cites, for example, the numerous narratives surrounding the Paris Olympics, which were specifically designed to demonstrate to domestic Russian audiences that France, and the West more broadly, is decadent, unsafe, and in decline.[52]

Russia expert and open-source intelligence (OSINT) investigator Milan Czerny from France identified a dissonance between the concept of hybrid threats and the logic of Russian military thinking: specifically, the idea that these hybrid operations are distinct from the spectrum of war. Czerny identified Russian operations in Europe since the full-scale invasion of Ukraine as an integral part of Russia's strategy to gain territory in Ukraine.[53] An intelligence analyst focused on Russia (name withheld) similarly highlighted that hybrid operations seek to deter support for Ukraine, and interdict and damage aid from flowing freely.[54] In his view, these hybrid operations additionally impose a political, economic, and psychological cost on Europe by bringing the war home, such as by staging fake coffins of deceased French soldiers supposedly killed fighting in Ukraine at the Eiffel Tower.[55] As further evidence, he points to Russia's expanding presence in francophone Africa, which continues to be seen as a crucial geopolitical interest for France, while exhausting vast resources in Ukraine. According to him, Russia's ballooning presence in the Sahel was not solely driven by economic interests but also served as an act of defiance against France for its support for Ukraine. Historian and analyst Mark Galeotti has similarly called these hybrid operations a form of "weaponizing inconvenience," showing European powers that they too will feel the impact of that 'distant' war.[56] The intelligence analyst interviewed highlighted that hybrid operations in Europe also serve to test TTPs for future potential conflicts. He particularly referred to the

50 Bart Schuurman, "Interview," 2025.

51 Quenel, "Interview."

52 This includes but is not limited to the amplification of narratives that the balconies in France would collapse during the Olympics opening ceremony, and a fake, staged Hamas video threatening to attack the global sports event.

53 Milàn Czerny, "Interview," 2025.

54 Intelligence Analyst (name withheld), "Interview," 2025.

55 Hugh Schofield, "Russia Link Suspected in Eiffel Tower Coffin Mystery," *BBC*, June 3, 2024, https://www.bbc.com/news/articles/cldd-7n97dvro.

56 Mark Galeotti, "Interview," 2025.

hiring of third-country nationals to execute operations and to find ways to smuggle necessary technology and goods into Russia for its war effort, a point echoed by Mark Galeotti.

Despite the surge in incidents in France, the effect of these incidents — and whether they in fact weaken support for Ukraine, fracture internal cohesion, and undermine Western alliances while reinforcing Kremlin legitimacy and testing tactics for future conflicts — remains difficult to measure. Analysis of the narratives promoted in Russian information operations in the French context indicates that they tend to ride existing currents and schisms rather than create them. Nonetheless, some hybrid operations, such as sabotage operations and intelligence collection efforts, may move the needle in Russia's strategic objectives. These more brazen and impactful operations, such as flying drones over sensitive military infrastructure, were not a significant part of its toolbox in France before the war and show both escalation as well as potential target scouting and intelligence collection efforts. Czerny similarly assesses the impact of the online information operation campaigns as minimal. Quenel likewise states that there is no tangible proof that these operations have significantly impacted French politics or society.

Interviewees emphasized that the seemingly amateurish nature of many operations in France was not merely a byproduct of the 2023 expulsion of Russian diplomats and intelligence officers from Europe. They viewed it instead as indicative of a deliberate trial and error approach and a reliance on whatever operational resources Russia could mobilize. To some, these primitive, sometimes brute operations also highlight the fragmentation of the Russian agencies behind these operations. Czerny pointed out that these operations serve to build a track record for Russian intelligence and security services, allowing them to negotiate access to resources within the Russian security apparatus. As Galeotti noted, this is driven by the 'do something' doctrine that dominates Russia's intelligence and security apparatus, in which different agencies, primarily the GRU and FSB, in France, seek to demonstrate their operational capabilities and build a track record of activity. These operations, thus, may be deemed successful even if their impact on French public opinion is minimal, provided they serve their internal turf wars well. Even if these operations appear amateurish or low effort from a Western perspective, they provide valuable 'lessons learned' for the Russians, according to the intelligence analyst (name withheld) interviewed. It is thus prescient not to underestimate their operations, as farcical as some of them seem.

Trends

While a host of different hybrid TTPs are observed in the 2022 to 2025 study period, Russia's tactics in France stand out for its focus on the information environment. Analysis of our dataset shows that France is one of the primary European targets of Russian information operations, further corroborated by the 152 Foreign Information Manipulation and Interference (FIMI) cases detected by the European External Action Service targeting France, making it one of the most beleaguered European nations by Russia when it comes to IOs.[57] Across hybrid incidents targeting the information environment, Russian operations relied on three instruments: creating narrative confusion, promoting social unrest, and manipulating the information environment through both physical and virtual means. While the bulk of activity was digital — notably Operation Matryoshka, Portal Kombat, and RRN-Doppelgänger — a significant share of disinformation operations employed direct physical provocations on French soil,

57 *3rd EEAS Report on Foreign Information Manipulation and Interference Threats: Exposing the Architecture of FIMI Operations* (European Union External Action Service, 2025), https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf.

including the placement of severed pigs' heads at mosques across Paris,[58] the defacement of Jewish sites,[59] and the tagging of anti-war graffiti on the walls of prestigious French newspapers.[60]

A defining feature of the French case is thus the online-offline architecture of hybrid threats; Russia digitally amplifies physical provocations to reinforce its impact psychologically and politically. On October 26, 2023, Stars of David were spray-painted on buildings in Paris and its suburbs by a Moldovan couple paid by a handler, an operation linked to the Russian Federal Security Service (FSB).[61] The RRN-Doppelgänger disinformation network then amplified images of this graffiti to further bolster the narrative that an antisemitic act had taken place in Paris.[62] Notably, some of these campaigns appeared to pursue dual domestic and international objectives. RRN-Doppelgänger, for example, the campaign that impersonates major French media outlets and governmental institutions to spread Kremlin narratives, does not only seek to undermine the support for Ukraine in France, it also is used to promote the idea in Russia that its foreign policy is widely supported among European citizens but is purportedly ignored by their governments. For example, the anti-Kyiv narratives in the fake French newspapers of RRN-Doppelgänger can be used in Russia to persuade domestic audiences that reputable European media entities align with the Kremlin — something also highlighted in the interview conducted by the authors with Nicolas Quenel.[63]

The France data set shows a clear election- and event-centric escalation pattern used by Russia. Hybrid incident frequency more than tripled across the dataset period, rising from 5 in 2022 to 10 in 2023 and peaking at 17 in 2024 — a 240 percent increase over three years. 2025 registered 11 incidents. The 2024 surge coincides directly with three convergent high-stakes moments: the French legislative elections (June 30 and July 7), the European Parliament elections (June 6–9), and the Paris Olympics and Paralympics (July–September). Quarterly tool-frequency analysis likewise surfaces operational clusters tied to these events.

The year 2022 is dominated by cyber operations and virtual disinformation tools. These incidents paint a picture of a Russia that, at the outset of the war, leaned heavily on digital tools to shape narratives about its invasion for external audiences in Europe. The notable exception to this period focused on cyber/digital operations is when Russian intelligence services orchestrated a series of staged pseudo-protests in Paris and other European capitals to discredit Ukraine. Concretely, they hired individuals to go to a Paris protest unrelated to the war in Ukraine, with banners that were supposed to show organic

58 Jacques Follorou, "Têtes de Cochon Devant Des Mosquées : L'enquête Privilégie La Piste Du Renseignement Militaire Russe," *Le Monde*, September 27, 2025, https://www.lemonde.fr/societe/article/2025/09/27/tetes-de-cochon-devant-des-mosquees-l-enquete-privilegie-la-piste-du-renseignement-militaire-russe_6643121_3224.html.

59 Christophe Cornevin, "Jets de Peinture Verte Sur Des Lieux Juifs : Les Suspects Interpellés Sont Des Ressortissants Serbes," *Le Figaro*, June 2, 2025, https://www.lefigaro.fr/actualite-france/jets-de-peinture-verte-sur-des-lieux-juifs-les-suspects-interpelles-sont-des-ressortissants-serbes-20250602.

60 "Tags de cercueils liés au conflit ukrainien : plusieurs Moldaves seront jugés en février," Le Figaro, October 9, 2025, https://www.lefigaro.fr/international/tags-de-cercueils-lies-au-conflit-ukrainien-plusieurs-moldaves-seront-juges-en-fevrier-20251009.

61 "France Blames Russia's FSB for Anti-Semitic Star of David Graffiti Campaign," France 24, February 23, 2024, https://www.france24.com/en/france/20240223-france-blames-russia-s-fsb-for-anti-semitic-star-of-david-graffiti-across-paris.

62 Maxime Tellier, "Derrière Les Tags d'étoiles de David à Paris, Un Vaste Réseau de Désinformation Russe," *Radio France*, January 26, 2024, https://www.franceinfo.fr/enquetes-franceinfo/enquete-franceinfo-derriere-les-tags-d-etoiles-de-david-a-paris-un-vaste-reseau-de-desinformation-russe_6325623.html.

63 Quenel, "Interview."

opposition to Ukraine, of which images were subsequently disseminated online to give the impression of widespread anti-Ukraine sentiment.[64] By late 2023, however, Moscow's approach had expanded to include physical provocations aimed at inflaming France's intercommunal tensions. The largescale Stars of David graffiti operation of October 2023 exemplifies this turn, but many similar incidents followed.[65]

With 17 incidents, 2024 was Russia's most active year in France, and Q2 alone accounted for 9 of them. As three major events converged (the Paris Olympics, French legislative elections, and European Parliament elections), operations shifted sharply toward *physical* disinformation operations, now focused on bringing the Ukraine war closer to French domestic audiences. For example, Moldovan nationals hired for small sums painted stenciled coffins on the façades of Parisian media outlets, including Le Figaro, accompanied by slogans such as "Stop Death Now."[66] Another team of third-country nationals (German, Ukrainian, and Bulgarian) placed coffins draped in French flags emblazoned with the words "French soldiers in Ukraine" under the Eiffel Tower.[67] The concentration of such activity coincides with Russia's anti-Olympics messaging push, in which AI-generated videos portrayed France as unprepared, unsafe, and on the brink of chaos ahead of the 2024 Paris Games.

While France has not faced the scale of kinetic sabotage of infrastructure seen in some Eastern European states, with the exception of the June 2024 bombing plot of a hardware store in the suburbs of Paris,[68] the TTP dataset shows a measurable shift in 2025: airspace violations, absent from the database before 2025, account for five incidents, indicating an escalation towards reconnaissance and probing. In November and December 2025, drones were observed over the Île Longue submarine base,[69] an intelligence training center of the French military,[70] a Leclerc tank convoy in Mulhouse,[71] and the Eurenco gunpowder plant in Bergerac.[72] Each incident contributed to the surge in 'Airspace violation' and 'Intelligence preparation' tools logged in Q4 2025. Additionally, in early October, French authori-

64 Thomas Eydoux and Margaux Farran, "Pour discréditer l'Ukraine, la Russie organise de faux rassemblements en Europe," *Le Monde*, May 8, 2023, https://www.lemonde.fr/international/article/2023/05/07/pour-discrediter-l-ukraine-la-russie-organise-de-faux-rassemblements-en-europe_6172447_3210.html.

65 Tellier, "Derrière Les Tags d'étoiles de David à Paris, Un Vaste Réseau de Désinformation Russe."

66 "France: Two Moldovans Charged over Coffin Graffiti in Paris," *Le Monde*, June 23, 2024, https://www.lemonde.fr/en/france/article/2024/06/22/france-two-moldovans-charged-over-coffin-graffiti-in-paris_6675480_7.html.

67 Antoine Albertini et al., "Cercueils à La Tour Eiffel : Un Lien Direct Établi Avec l'affaire Des Mains Rouges et Des Soupçons Pointant Vers La Russie," *Le Monde*, October 29, 2025, https://www.lemonde.fr/pixels/article/2024/06/03/cercueils-a-la-tour-eiffel-un-lien-direct-etabli-avec-l-affaire-des-mains-rouges_6237067_4408996.html.

68 Jacques Follorou, "Derrière l'opération avortée d'un Russo-Ukrainien à Roissy-en-France, une vaste campagne de sabotage orchestrée depuis Moscou," *Le Monde*, June 27, 2024, https://www.lemonde.fr/societe/article/2024/06/26/derriere-l-operation-avortee-d-un-russo-ukrainien-a-roissy-en-france-une-vaste-campagne-de-sabotage-orchestree-depuis-moscou_6244099_3224.html.

69 Chloé Hoorman and Elise Vincent, "Drones Au-Dessus de La Base Navale de l'île Longue : Les Autorités Françaises Assument Une Nouvelle Fois La Discrétion," *Le Monde*, December 10, 2025, https://www.lemonde.fr/international/article/2025/12/05/drones-au-dessus-de-la-base-navale-de-l-ile-longue-les-autorites-francaises-assument-une-nouvelle-fois-la-discretion_6656185_3210.html.

70 Louise Rasmussen, "Suspected Drones Seen over French Military Intelligence Base, Armed Forces Say," *Reuters*, December 9, 2025, https://www.reuters.com/world/europe/suspected-drones-seen-over-french-military-intelligence-base-armed-forces-say-2025-12-09/.

71 Jean-Philippe Liabot, "Unidentified Drones Spark Security Alert at French Military Base," Euronews, September 26, 2025, https://www.euronews.com/my-europe/2025/09/26/unidentified-drones-spark-security-alert-at-french-military-base.

72 "Bergerac : Un Drone a Survolé Un Site Produisant Des Tonnes de Poudre Pour l'armée Française, Une Enquête Ouverte," *Le Monde*, November 11, 2025, https://www.lemonde.fr/economie/article/2025/11/11/bergerac-un-drone-a-survole-illegalement-un-site-de-production-de-poudre-de-la-societe-eurenco-une-enquete-ouverte_6653022_3234.html.

ties intercepted the Russia-linked vessel, the Boracay, off Saint-Nazaire, suspected of having been the launchpad for drones that caused disruptions in Denmark weeks earlier.[73] Hybrid incidents in France in 2025 show a clear shift in Russia's modus operandi, from relying on virtual operations toward reconnaissance and physical probing. Nonetheless, airspace violations in France should not just be considered as tools for Russia to probe, gather intelligence, and plan operationally: these operations may also seek to promote social unrest and signal capability and presence to domestic and external audiences.

A notable trend that emerged from TTP analysis in France is Russia's systematic reliance on intermediary individuals for on-the-ground operations, especially physical disinformation campaigns. These individuals are typically nationals from third countries — often Moldovan, Serbian, and Bulgarian in the context of France — and were not always treated as one-off operational assets as was assumed when reports first emerged of Russian use of third-country nationals and petty criminals to conduct operations on its behalf in Europe.[74] For instance, a Serbiabased coordinator appears at the center of two operations aimed at inflaming intercommunal tensions in 2025. In late May, Serbian nationals carried out a coordinated wave of greenpaint vandalism against Jewish sites in Paris.[75] Months later, in September, two men delivered pigs' heads to nine mosques across the capital. French investigators explicitly identified the same Serbian individual as the organizer behind both efforts.[76]

A second similar case that featured the reuse of third-country nationals concerns a Bulgarian operative involved in a sequence of GRUlinked physical disinformation operations in the spring of 2024. In mid-May, Bulgarian nationals carried out the "red hands" vandalism at the Holocaust Memorial and other Jewishassociated areas of Paris.[77] Shortly thereafter, during the June 1st coffininstallation operation near the Eiffel Tower, French authorities identified a direct personnel overlap: one suspect in the coffin action was the same Bulgarian individual previously involved in the May graffiti campaign.[78] The third instance of explicit reuse of operatives centers on a Moldovan handler involved in multiple vandalism operations in Paris during June 2024. When two Moldovan men were arrested for placing coffinthemed graffiti on prominent media outlets, investigators identified their recruiter as a Moldovan activist already implicated in earlier graffiti operations at the French National Assembly in the same month.[79]

Russian hybrid TTPs in France illustrate that while Russia sought to bank on intercommunal tensions and political schisms through targeting the information domain, it has increasingly pivoted to physical

---

73 *Flotte Fantôme Russe : L'Europe Hausse Le Ton Après l'arraisonnement Au Large de Saint-Nazaire*, October 20, 2025, https://www.ouest-france.fr/europe/russie/flotte-fantome-russe-leurope-hausse-le-ton-apres-larraisonnement-au-large-de-saint-nazaire-7e94ab86-adac-11f0-a829-eb0d2e70677d.

74 Shaun Walker, "'These People Are Disposable': How Russia Is Using Online Recruits for a Campaign of Sabotage in Europe," *The Guardian*, May 4, 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.

75 Cornevin, "Jets de Peinture Verte Sur Des Lieux Juifs : Les Suspects Interpellés Sont Des Ressortissants Serbes."

76 Follorou, "Têtes de Cochon Devant Des Mosquées : L'enquête Privilégie La Piste Du Renseignement Militaire Russe."

77 Matthieu Suc, "Opération « Mains Rouges » : Des Agents Provocateurs Néonazis à La Solde Du Kremlin," Mediapart, January 2, 2025, https://www.mediapart.fr/journal/international/020125/operation-mains-rouges-des-agents-provocateurs-neonazis-la-solde-du-kremlin.

78 Albertini et al., "Cercueils à La Tour Eiffel : Un Lien Direct Établi Avec l'affaire Des Mains Rouges et Des Soupçons Pointant Vers La Russie."

79 *Tags de Cercueils En Lien Avec l'Ukraine: Quatre Hommes Nés En Moldavie Jugés à Paris En Février*, October 9, 2025, https://www.laprovence.com/article/france-monde/34850979070970/tags-de-cercueils-en-lien-avec-lukraine-quatre-hommes-nes-en-moldavie-juges-a-paris-en-fevrier.

probing and reconnaissance of sensitive military sites. This may be a response to France's increasingly clear position on rearmament and EU collective security as the war in Ukraine continues.

Response

As noted in the introduction, in May 2025, President Emmanuel Macron announced that France would henceforth systematically attribute hostile acts, backed by a 16-page intelligence report that acknowledged previous restraint had failed to deter Russian operations.[80] In parallel, the French Service for Vigilance and Protection Against Foreign Digital Interference (VIGINUM), has continued to make information public about digital Russian interference campaigns targeting France since the full-scale invasion of Ukraine. The National Cybersecurity Agency of France (ANSSI) likewise has publicly attributed cyber intrusions to Russian military intelligence.[81] France has also increased public awareness around Russian digital interference for domestic and international audiences. In February 2025, France launched "French Response," an official X account dedicated to countering foreign disinformation by directly engaging hostile narratives as they emerge.[82] In July 2025, its National Strategy Review explicitly highlighted the "capability to operate in the hybrid domain" as one of 11 strategic objectives to be achieved by 2030.[83]

In addition to public attribution, France has also made significant military and technological investments to counter hybrid threats. The government increased the 2026 defense budget by €6.7 billion, recognizing that hybrid threats demand sustained investment across traditional military capabilities and emerging domains, including cyber and space.[84] It has also been active in crafting NATO's response to hybrid threats. For example, in September 2025, France participated in NATO's response to Russian airspace incursions by deploying fighter jets to reinforce air cover on NATO's eastern flank alongside Denmark and Germany.[85] In line with its objective of greater European strategic autonomy, France has also shaped the response to hybrid threats at the EU level, advocating for stronger instruments and sanctions.

80 Quentin Jalabert et al., "Calling Out Russia."

81 Daryna Antoniuk, "France Blames Russian Military Intelligence for Years of Cyberattacks on Local Entities," The Record, April 29, 2025, https://therecord.media/france-blames-russian-military-intelligence-for-hacks-against-local-orgs.

82 Anaella Jonah, *From Soft Power to Digital Firepower: France Steps up Fight against Disinformation*, September 8, 2025, https://www.france24.com/en/france/20250908-from-soft-power-to-digital-firepower-france-steps-up-against-online-disinformation-french-response.

83 *Revue Nationale Stratégique 2025* (Secrétariat général de la défense et de la sécurité nationale, 2025), http://www.sgdsn.gouv.fr/publications/revue-nationale-strategique-2025.

84 William Horobin et al., "France's Macron Raises Defense Budget, Says Europe Under Threat," *Bloomberg*, July 13, 2025, https://www.bloomberg.com/news/articles/2025-07-13/france-s-macron-raises-defense-budget-says-europe-under-threat.

85 Louise Souverbie, "Russian Incursions and Hybrid Warfare: Europe Under Aerial Pressure," IRIS, September 26, 2025, https://www.iris-france.org/en/russian-incursions-and-hybrid-warfare-europe-under-aerial-pressure/.

ii. Germany

Introduction

Few European states shape the strategic environment of the Russia–Ukraine war as directly as Germany. Recognizing this, Moscow has intensified its hybrid campaign in Germany since the start of the full-scale invasion, seeking to punish and deter support to the defense of Ukraine. These operations are neither isolated nor improvisational; they reflect long-standing Russian doctrines that seek to achieve political outcomes through non-military means. This case study examines how Russia has applied these methods in Germany, the vulnerabilities exploited, and the impact on national and European security between 2022 and 2025.

Germany has held a central position in Russian strategic thinking for decades. As a divided frontline of the Cold War, Germany was a key arena for competition between the Soviet Union and the West. To solidify its influence over the Warsaw Pact's western flank, Russia developed deep and enduring business, energy, and intelligence ties to East Germany. Across the inner German border, Soviet intelligence services, aided by the Stasi, the intelligence service and secret police of East Germany, achieved deep and systematic penetration of West German institutions, while conducting 'active measure' subversion operations that prefigure today's hybrid methods.[86] Contemporary Russian intelligence services continue to benefit from this legacy, drawing on longstanding organizational experience operating in Germany and, in some cases, exploiting residual access and networks created through Cold War era penetration of German political, economic, and security structures.

Following the dissolution of the Soviet Union, the newly unified German republic built on the economic ties that had existed between Bonn and Moscow, as a means of ensuring stability through cooperative economic engagement. This era of Russlandpolitik or "Ostpolitik 2.0" was defined by a deliberate joining of the two economies through trade deals and infrastructure projects like the Nord Stream 1 pipeline. Former German Chancellor Gerhard Schröder became the primary champion of deeper German-Russian ties, emphasizing energy partnerships through Nord Stream and forming a close personal relationship with the recently elected Russian President Vladimir Putin, who had spent time living in East Germany as a young KGB officer.[87] Schröder's successor, Angela Merkel, who had grown up in East Germany and learned fluent Russian studying in the Soviet Union, continued this policy of economic engagement and energy interdependence, despite growing signs of Putin's authoritarian instinct and territorial ambitions.

The 2014 annexation of Crimea and the outbreak of conflict in the Donbas marked the beginning of a turning point in the relationship between Berlin and Moscow. Chancellor Merkel's reluctant but unambiguous condemnation of Russian aggression in Ukraine triggered a salvo of retaliation from Moscow that foreshadowed the intensified post-2022 hybrid campaign discussed in this report. Moscow's retaliation included a 2015 cyberattack on the Bundestag and the fabricated 2016 "Lisa case," which exploited immigration debates to erode public trust in German law enforcement while bolstering the

86 Laura Daniels, "Russian Active Measures in Germany and the United States: Analog Lessons From the Cold War," War on the Rocks, September 27, 2017, https://warontherocks.com/2017/09/russian-active-measures-in-germany-and-the-united-states-analog-lessons-from-the-cold-war/.

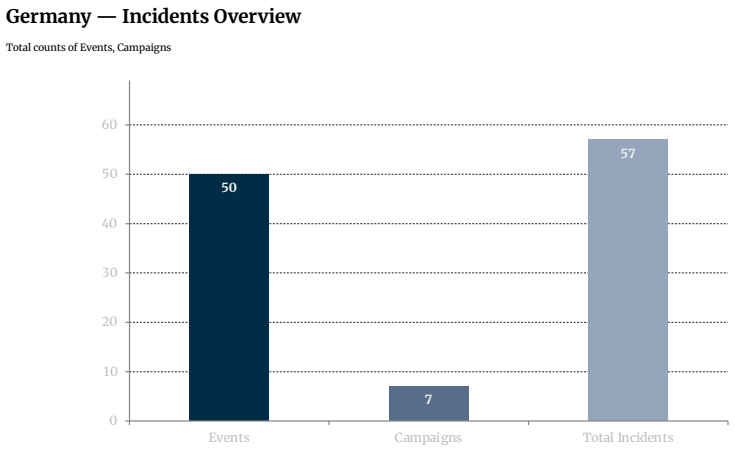
87 Angela Stent, *Putin's World: Russia Against the West and with the Rest* (Twelve, 2019).

far-right Alternative für Deutschland (AfD).[88] The 2019 assassination of a Chechen dissident in Berlin's Kleiner Tiergarten further demonstrated Russia's willingness to conduct lethal operations on German soil. Russia's full-scale invasion of Ukraine in 2022 did not initiate this hybrid campaign but dramatically escalated it, prompting Chancellor Olaf Scholz's *Zeitenwende*, or watershed moment, speech, which crystallized the necessity of energy and economic disentanglement and the reassertion of German hard power as a pillar of European defense.

Moscow's sustained focus on Germany reflects the country's strategic importance as a key leader of the European Union and NATO, institutions which are anathema to Putin's authoritarian and imperial world view. Germany anchors NATO's eastern defense, hosting substantial allied garrisons and serving as the critical logistics hub through which forces deploy to the alliance's eastern flank.[89] Despite its early reluctance to provide lethal aid — Berlin was ridiculed early in the war for sending helmets rather than weapons — Germany has become Ukraine's second-largest military supplier after the United States.[90] As the EU's largest economy, Germany wields significant influence within the 27-member bloc, playing a central role in shaping both sanctions regimes targeting Russia and the coordination of European military aid to Ukraine. Russian strategy therefore seeks to neutralize Berlin's leadership in sustaining these pressure campaigns against Moscow.

Results

A total of 57 hybrid operations targeting Germany between February 2022 and December 2025 were identified in the dataset. As with the broader study methodology, persistent multi-month 'Campaigns,' such as prolonged intelligence-gathering efforts or sustained pressure activities, were counted as single incidents even when they comprised multiple sub-actions. The availability of approximate or exact start dates for each incident enables a temporal analysis of operational tempo and escalation patterns.



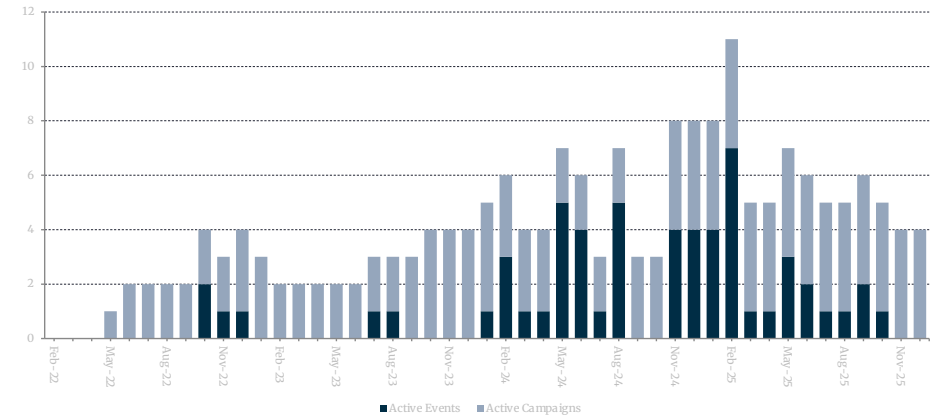
88 András Rácz, *Germany's Shifting Policy towards Russia: The Sudden End of Ostpolitik* (Finnish Institute of International Affairs, 2022), https://fiia.fi/en/publication/germanys-shifting-policy-towards-russia.

89 "Operational Plan for Germany," Bundeswehr, last updated spring 2025, https://www.bundeswehr.de/en/organization/bundeswehr-joint-force-command/missions/operational-plan-for-germany.

90 "Ukraine Support Tracker - A Database of Military, Financial and Humanitarian Aid to Ukraine," Kiel Institute, December 10, 2025, https://www.kielinstitut.de/topics/war-against-ukraine/ukraine-support-tracker/.

Germany — Incidents Over Time

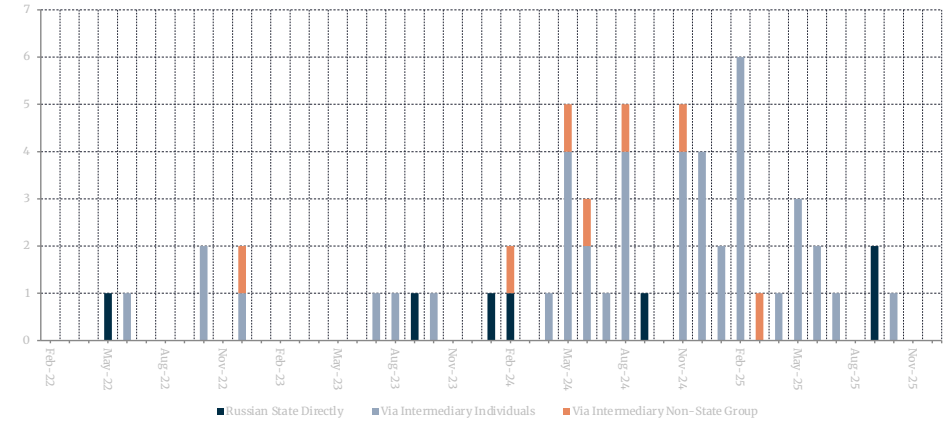
Monthly counts of Active Events and Active Campaigns (2022–2025)



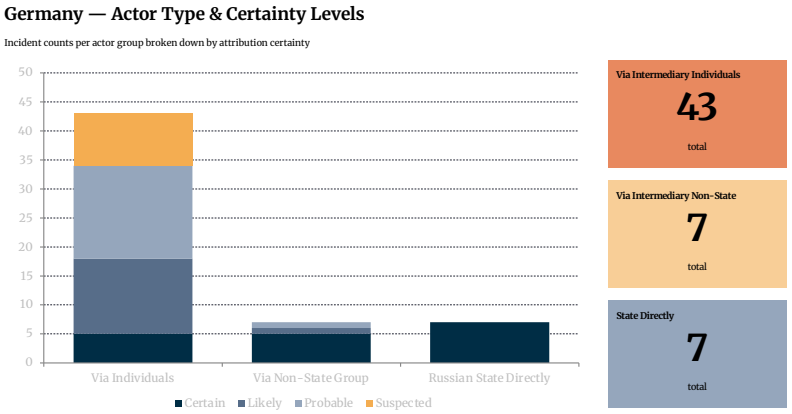
Russian hybrid activity in Germany over time remained relatively limited in 2022 and 2023, with six incidents starting in 2022 and four in 2023, before intensifying beginning in 2024. The most pronounced jump in activity occurred in February 2025, which recorded six incident starts, the highest of any month in the dataset. The number of active operations running concurrently also climbed with 11 simultaneously active incidents in February 2025.

Germany — Actor Type by Month

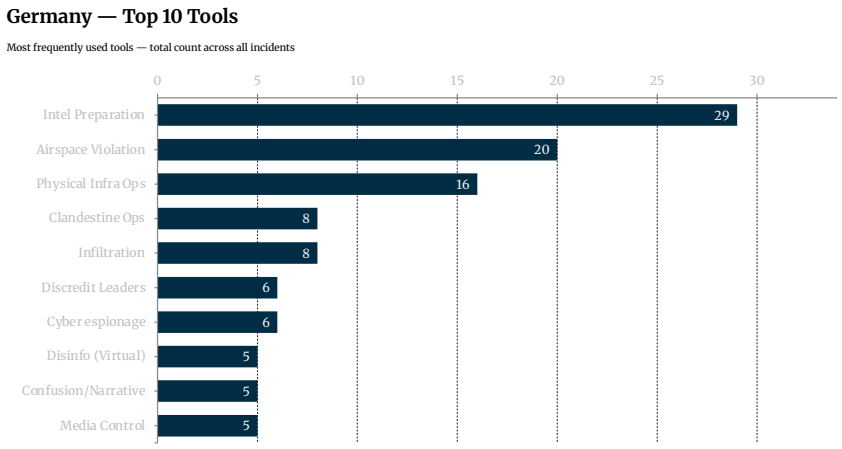
Monthly incident counts by actor type — by start date

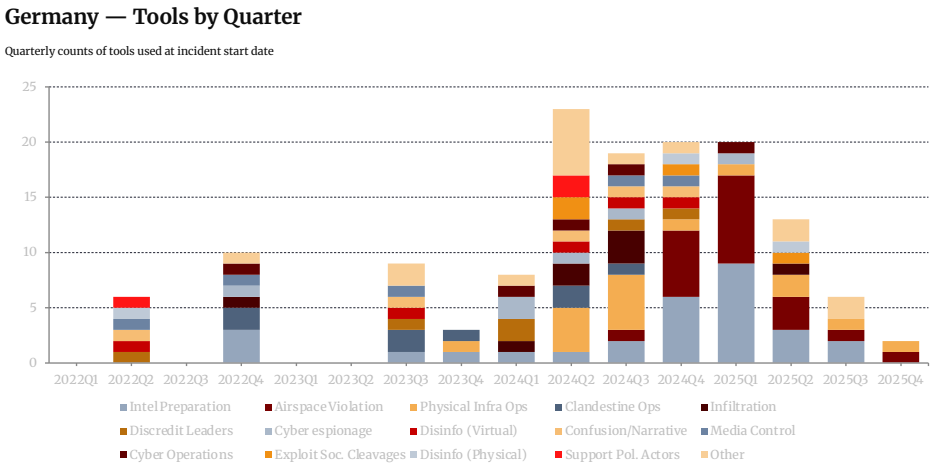


In Germany, a clear trend was the use of intermediary actors to execute Russia-linked operations. The most frequent actor category was ‘Russia through intermediary individuals’ (43 incidents), followed by ‘Russian state directly’ (7 incidents) and ‘Russia through an intermediary non-state group’ (7 incidents).

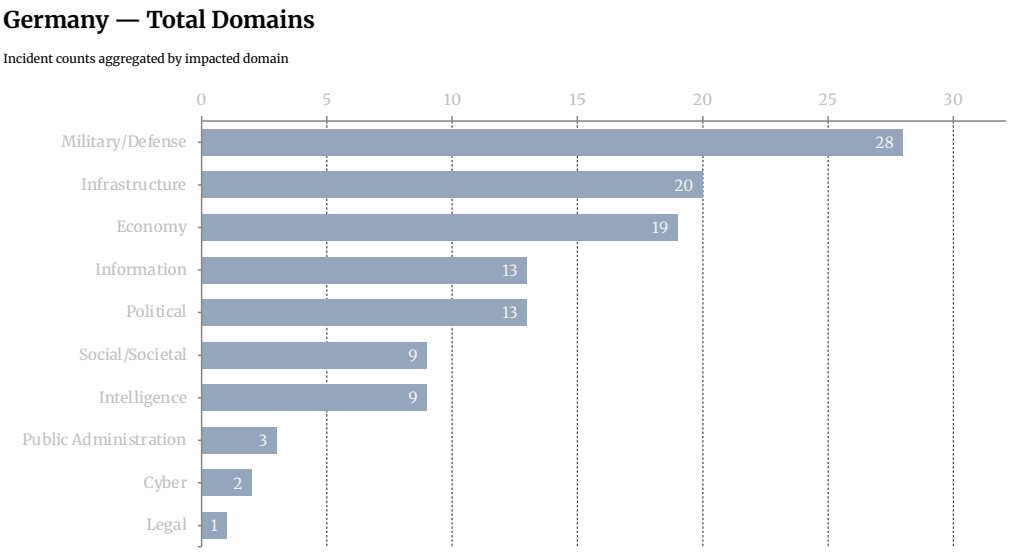


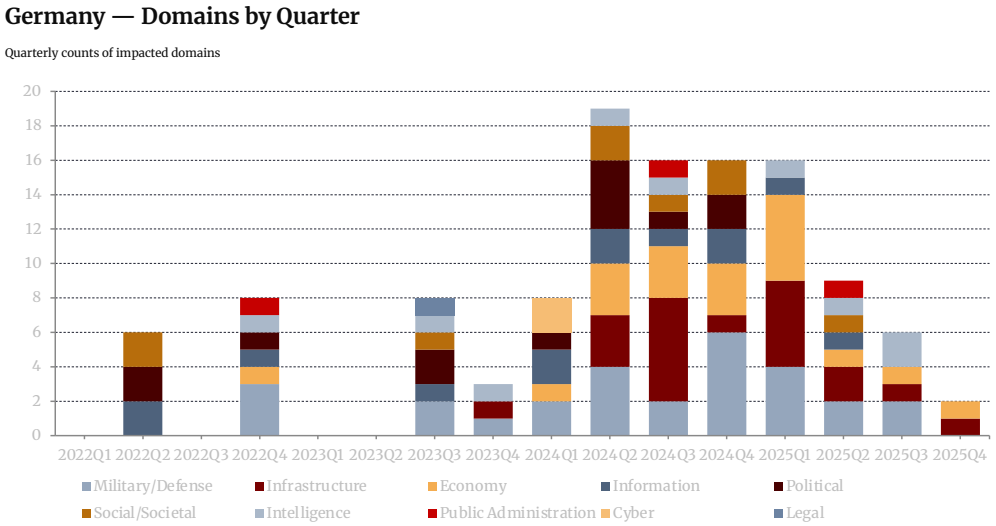
The TTPs employed by Russia in Germany focused on pre-operational groundwork and coercive signaling. Across all incidents, the most frequently observed tool was ‘Intelligence preparation’ (29 instances), indicating a sustained Russian effort of reconnaissance and intelligence gathering efforts. This was followed by the ‘Airspace violation’ TTP (20 instances), almost all involving drone overflights linked to intelligence collection, and by ‘Physical operations against infrastructure’ (16 instances). Additional tools such as ‘Infiltration’ (8), ‘Clandestine operations’ (8), and several categories of information manipulation and sociocultural exploitation appeared at lower frequencies.





The ‘Military/Defense’ sector was most frequently affected (28 instances), reflecting Germany’s strategic role within NATO and its support to Ukraine. ‘Infrastructure’ (20 instances) and the ‘Economy’ (19 instances) were also prominent targets of Russian hybrid activity. The ‘Information’ and ‘Political’ environments were each affected in 13 instances, while ‘Intelligence’ and ‘Social/Societal’ domains appeared less frequently but remained notable. Taken together, the results suggest a Russian hybrid campaign against Germany that prioritizes security, infrastructure, and economic resilience while intermittently shaping political and informational conditions.





Findings

Objectives and Effect

The hybrid incidents detailed above have absorbed institutional attention, strained security and counterintelligence capacities, and complicated political consensus-building in Germany, even in the absence of open military confrontation. The patterns observed in the data suggest that Russian hybrid activities in Germany are shaped by strategic objectives rather than ad hoc behavior. Building on the empirical overview provided by the database and informed by expert interviews, this section interprets these patterns as components of a broader and internally coherent Russian hybrid strategy directed at Germany since February 2022.

Germany's central role within the EU, NATO, and its increasing commitment to the defense of Ukraine make it a primary target for Russian interference. The immediate objective of Russia's hybrid campaign in Germany is to punish and deter German support for Ukraine. Peter Clement, a former senior U.S. intelligence official who led the CIA's Office of Russian and Eurasian Analysis, explains that Russian leadership perceive Germany as a belligerent for its involvement in the war, therefore making it "a legitimate target."[91] Hybrid operations thus function as a form of coercive messaging: support for Ukraine carries costs, and Germany is not insulated from the conflict simply because it is not a battlefield state.

This messaging is directed not only at decisionmakers in Berlin, but also at the German public. A key objective is the creation of fear and a persistent sense of vulnerability among German society and policymakers. Operations resulting in widespread impact to the civilian population, such as the August 2024 suspected sabotage attempt of water treatment facilities in North Rhine-Westphalia[92] and the closure of the Munich airport in October 2025[93] are intended to elicit a sense of insecurity in the public. High visibility incidents like these normalize the idea that Russia can operate inside Germany with relative ease. This further implies the possibility, real or not, that Russia could increase the severity and frequency of its operations if tensions further escalate. Dr. András Rácz, a security policy analyst and Russia expert whose work focuses on Russia's foreign and security policy and its implications for Germany, describes this as an "information deterrence effect."[94] The aim is not persuasion in the classical sense, but demonstration. Convincing German and European audiences that Russia can strike anywhere, anytime, and across multiple domains demonstrates commitment and the potential for escalation dominance. This reinforces the broader deterrent message behind Russia's actions without crossing clear thresholds of armed conflict.

In addition to these psychological effects, Russian hybrid activity addresses concrete military objectives tied to the war in Ukraine and a potential confrontation with NATO. A central component is reconnaissance and monitoring of German and allied military infrastructure–intelligence preparation. Russian drone activity over key infrastructure, military bases, and training sites such as Grafenwöhr, is the most visible example of this, though other collection activity relies on cyber, signals intelligence, and human intelligence sources. As a major garrison and logistics and training hub for NATO forces, Germany has been a longstanding military intelligence target. Since the full-scale invasion, the presence of Ukrainian forces training in Germany and arms shipments destined for the frontline have reinvigorated Russian collection activities. Russian intelligence has also focused on mapping critical military and civilian infrastructure — pipelines, electricity distribution, rail networks, water treatment — to identify nodes whose disruption would generate disproportionate systemic effects if a war with Germany and NATO were to break out.

Beyond military goals, Russian hybrid operations pursue longer-term political objectives aimed at weakening Germany's internal cohesion and its role within European and transatlantic institutions.

---

91 Peter Clement, "Interview," 2025.

92 "Germany: New Sabotage Warning Issued for Water Supply," *DW*, August 16, 2024, https://www.dw.com/en/germany-new-sabotage-warning-issued-for-water-supply/a-69958621.

93 "Press: Another Drone Sighting at Munich Airport," Munich Airport, October 4, 2025, https://www.munich-airport.com/press-another-drone-sighting-at-munich-airport-35720233.

94 András Rácz, "Interview," 2025.

Torben Schütz, a German security policy expert whose work focuses on German and European defense, explains that a core aim of Russia's hybrid campaign is to undermine EU and NATO unity, enabling the Kremlin to engage with European states bilaterally from a stronger relative position.[95] To achieve this, Russia supports and amplifies Eurosceptic, NATO-skeptic, and pro-Russian political forces — most notably the AfD — in order to sow societal discord, polarize public debate, and erode political consensus around support for Ukraine and alliance commitments.

These tactics were employed against Germany prior to 2022, as evidenced by the 2016 "Lisa case," and the broader use of state-backed outlets such as *RT Deutsch* (now *RT DE*) and *Sputnik* to amplify divisive narratives.[96] Even before the full-scale invasion and the subsequent increase in Russian hybrid operations in Germany, the public was alert to Russian attempts to fragment political consensus. Polling indicates the public is aware of the threat: nearly 90 percent of German voters expressed concern about foreign manipulation, with 45 percent identifying Russia as the principal threat actor.[97] This may indicate that while Russian operations since 2022 have increased and have been sustained as per our dataset, their impact will have been dampened by the German public's awareness to the threat.

Trends

Analysis of Russian hybrid TTPs in Germany from February 2022 through December 2025 highlights a toolkit dominated by intelligence collection, sabotage, airspace violations, and propaganda and disinformation campaigns. Russian-orchestrated assassination attempts and intimidation tactics were less numerous but stand out nonetheless due to their brazen nature.

Many of the incidents logged in the database demonstrate that Russian hybrid TTPs in Germany focused on 'priming' actions, as seen by the repeated intelligence and reconnaissance activities that constituted roughly half of the recorded activities. Intelligence collection on arms shipments to Ukraine[98] and on Ukrainian forces training in Germany[99] indicate that German territory is used for Russian situational and battlefield awareness. It is thus likely the case that Russian military planning may directly derive intelligence from German territory for the war in Ukraine. This subset of activities in Germany indicate that Germany is treated not only as a political actor but also as an operational space whose functions — logistics, training, and transit — have direct impact on the battlefield in Ukraine.

Russian reconnaissance efforts extend beyond Ukraine-linked targets. Intermediary individuals using drones have conducted surveillance of critical infrastructure, including transport, energy, and communications nodes. These incidents, featuring heavily in the German data set, suggest a Kremlin-orches-

95 Torben Schütz, "Interview," 2025.

96 Jim Rutenberg, "RT, Sputnik and Russia's New Theory of War," *The New York Times*, September 13, 2017, https://www.nytimes.com/2017/09/13/magazine/rt-sputnik-and-russias-new-theory-of-war.html.

97 Jon Shelton, "Germany: Nearly 90% of Voters Fear Manipulation," *DW*, February 6, 2025, https://www.dw.com/en/germany-nearly-90-of-voters-fear-foreign-manipulation/a-71528481.

98 Julian E. Barnes and Eric Schmitt, "Russian Drones Are Flying Over U.S. Weapons Routes in Germany, Officials Say," *The New York Times*, August 28, 2025, https://www.nytimes.com/2025/08/28/us/politics/russian-drones-weapons-routes.html.

99 Dan Sabbagh, "Spy Ring Plotted to Obtain Details from Phones of Ukrainians at US Airbase in Germany, UK Court Hears," *The Guardian*, December 3, 2024, https://www.theguardian.com/uk-news/2024/dec/03/spy-ring-plotted-to-obtain-details-from-phones-of-ukrainians-at-us-air-base-in-germany-uk-court-hears.

trated effort to build a detailed understanding of potential vulnerabilities in German infrastructure. This may then be fed into future operations like sabotage, coercion, or disruption in the event of heightened tensions with NATO. The emphasis on reconnaissance rather than immediate exploitation — in most incidents — denotes the long-term, priming nature of this activity. This may indicate Russia's expectation that Germany will be a critical logistical gateway for allied forces transiting to the eastern flank in response to a crisis.

Russian targeting of infrastructure in Germany was not limited to pre-operational planning. Of the 16 recorded instances of 'Physical operations against infrastructure,' 14 involved sabotage or attempted sabotage of infrastructure. Some of these operations involved NATO-specific targets, as in the May 2024 incident in which a cache of explosives was discovered buried near a kerosene pipeline supplying NATO airbases in Western Germany,[100] while others targeted civilian infrastructure. These incidents offer insights into what a Russian sabotage campaign might look like in the event of a confrontation with NATO.

Each of the 16 cases of 'Physical operations against infrastructure' were attributed to intermediary individuals, highlighting the importance of plausible deniability during sensitive or potentially escalatory actions. Indeed, across the 57 recorded incidents, three out of four relied on intermediary individuals. This reliance on intermediaries also blurs the line between state-directed activity and criminal or activist behavior, complicating attribution and increasing the burden on German authorities to distinguish between ordinary criminality and hostile state action.

The July 2024 parcel-device incident illustrates how such deniable methods can be applied to acts of physical sabotage. An incendiary device concealed in a parcel ignited at a DHL logistics facility at Leipzig Airport in Germany after being sent through commercial courier networks with a timed ignition mechanism.[101] The device began burning shortly before it was scheduled to be loaded onto a cargo aircraft, raising concerns about the potentially grave consequences had it ignited in flight.

Investigators later concluded that the incident formed part of a coordinated sabotage effort across Europe attributed to operatives linked to Russia's GRU. European officials assessed the operation as a likely test of whether such devices could be surreptitiously placed on transatlantic flights. Lithuanian authorities ultimately charged fifteen individuals connected to the network. This brazen operation, which more closely resembled a terrorist plot than the activity of a state, highlights the risks inherent in Russia's expanding hybrid campaign. Had such a device ignited aboard a cargo aircraft — or worse, a passenger flight — the resulting loss of life could have triggered a severe international crisis.

Some operations employed additional measures to obfuscate Russian involvement and complicate attribution. For example, following the disruption of a Russian-orchestrated assassination plot against Rheinmetall CEO Armin Papperger, arsonists later targeted a property linked to him, accompanied by a purported confession letter posted on the far-left Indymedia platform. The letter, attributed to a radical left-wing group and denouncing Rheinmetall for profiting from the war in Ukraine, was quickly called into question by German authorities, who pointed to prior Russia-linked threats against Papperger and the use of ideological framing consistent with Soviet-era active measures designed to mask state

100 "NATO to Confront Russian 'sabotage' Attempts — Stoltenberg," *DW*, June 13, 2024, https://www.dw.com/en/nato-to-confront-russian-sabotage-attempts-stoltenberg/a-69350359.

101 Pjotr Sauer and Shaun Walker, "Explosive Sex Toys and Cosmetics: The Story behind the DHL Parcels Plot," *The Guardian*, May 5, 2025, https://www.theguardian.com/world/2025/may/05/explosive-sex-toys-and-cosmetics-the-story-behind-the-dhl-parcels-plot.

involvement behind ostensibly domestic actors.[102]

Although the data show few standalone disinformation operations, as compared to instances of intelligence activities, several of the recorded incidents represent protracted, months-long campaigns involving myriad coordinated false narratives. A notable component of Russia's hybrid operations in Germany has been the use of sustained disinformation campaigns designed to undermine support for Ukraine, erode trust in democratic institutions, and reinforce skepticism toward Germany's security and foreign policy choices. Long-running operations such as Doppelgänger have relied on fake news sites and imitations of established German media outlets to disseminate misleading stories framed as legitimate journalism, often focusing on economic hardship, political hypocrisy, or the alleged futility of supporting Ukraine.[103] These narratives frequently resonate with pre-existing concerns in German public discourse, including sensitivities rooted in the country's post-war historical legacy, unease with military escalation, and fears that confrontation with Russia carries disproportionate risks for Germany's security and prosperity. Other campaigns, including those attributed to Matryoshka-associated networks, sought to overwhelm international factcheckers and media outlets with non-German language content impersonating German media outlets like *DW* and *Bild*, to undermine international confidence in German elections and denounce support to Ukraine.[104] These incidents illustrate that Russian disinformation targeting Germany is structured as a persistent, high-volume effort to shape both domestic discourse and international perceptions.

Russian disinformation operations in Germany also demonstrated a high degree of reactivity, with narratives rapidly intensifying around developments of particular strategic sensitivity to the Kremlin. During periods of fighting around Ukraine's Zaporizhzhia Nuclear Power Plant, disinformation narratives in the German media environment quickly elevated claims about nuclear escalation, alleged Ukrainian plans to build a "dirty bomb," and accusations of bias against the International Atomic Energy Agency (IAEA) after inspections contradicted Russian claims.[105] As Berlin debated transferring Leopard main battle tanks to the Ukrainian military, these narratives were further adapted to portray German military assistance as an escalatory step, amplifying warnings of nuclear catastrophe and framing Western support as pushing the conflict toward a broader, potentially nuclear confrontation.

Temporal analysis of Russian disinformation operations targeting Germany underscores their event-driven nature, with coordinated surges in activity ahead of, and in response to, key events such as the February 2025 federal election. Q4 2024 saw the introduction of two mutually supporting online disinformation campaigns to Germany's information environment. Storm 1516, previously deployed against French and U.S. elections, began spreading pro-Russian narratives and false claims to discredit

---

102 Bojan Pancevski et al., "U.S., Germany Foil Russian Plot to Kill Defense Executive," *Wall Street Journal*, July 12, 2024, https://www.wsj.com/world/europe/u-s-germany-foil-russian-plot-to-kill-defense-executive-9cc497f3.

103 *Germany Targeted by the Pro-Russian Disinformation Campaign "Doppelgänger"* (Federal Foreign Office, 2024), https://www.auswaertiges-amt.de/resource/blob/2682484/2da31936d1cbeb9faec49df74d8bbe2e/technischer-bericht-desinformationskampagne-doppelgaenger-1--data.pdf.

104 *Country Report: Assessment of Foreign Information Manipulation and Interference (FIMI) in the 2025 German Federal Election* (Institute for Strategic Dialogue, 2025), 32, https://www.isdglobal.org/isd-publications/country-report-assessment-of-foreign-information-manipulation-and-interference-fimi-in-the-2025-german-federal-election/.

105 *Russian Invasion of Ukraine Narrative Report: Germany* (Global Disinformation Index, 2023), 8, https://www.disinformationindex.org/.

candidates via counterfeit websites sometime in late 2024.[106] Around the same time, the "Foundation to Battle Injustice" (R-FBI), an entity purporting to be a Russian human rights NGO, disseminated similar narratives through many of the same German social media accounts that had amplified Storm 1516 content, indicating a coordinating link between the two campaigns.[107] Both campaigns sought to smear Christian Democratic Union (CDU) and Green Party candidates through fabricated claims of corruption and allegations of sexual violence against minors,[108] potentially benefitting pro-Russian and Eurosceptic party candidates like the AfD's Alice Weidel.

Disinformation activity in the run-up to the election was not solely confined to the online information space. Between December 2024 and January 2025, over 270 vehicles across Germany were sabotaged and tagged with stickers of Green Party co-leader Robert Habeck to falsely implicate environmental activists before the February election.[109] The incident represents a rare German example of the physical disinformation operations more frequently observed in France during the reporting period. It is difficult to assess the effect these campaigns had on voters, but the widespread awareness of Russian influence attempts among the German public suggests the impact may have been less than what it otherwise might have been.

Response

Germany has formally acknowledged the severity of Russian hybrid threats targeting its democracy and critical infrastructure. In December 2025, Germany summoned Russia's ambassador over what it described as "a massive increase in threatening hybrid activity by Russia, ranging from disinformation campaigns to espionage and cyberattacks to attempts at sabotage,"[110] with Foreign Ministry spokesperson Martin Giese stating that "we are monitoring Russia's actions very closely and will take action against them."[111]

This recognition has driven coordinated government action across multiple domains. At the intelligence level, the Federal Office for the Protection of the Constitution (BfV) has positioned itself as a central actor in identifying and countering Russian interference. The BfV created a dedicated task force for the February 2025 elections to monitor foreign interference, warning that disinformation campaigns, cyberattacks, espionage and sabotage should be expected, while working with international partners to

106 "Germany Warns of Russian Disinformation Targeting Election," *Reuters*, February 21, 2025, https://www.reuters.com/world/europe/germany-warns-russian-disinformation-targeting-election-2025-02-21/.

107 Julia Smirnova et al., "Storm-1516 and R-FBI: Russian Attempts to Interfere in the German Election," Alliance4Europe, February 13, 2025, https://alliance4europe.eu/storm-1516-german-elections.

108 Julia Smirnova et al., "Storm-1516 and R-FBI."

109 Roman Lehberger et al., "Deutschlandweite Sabotageserie offenbar von Russland gesteuert," *Der Spiegel*, February 5, 2025, https://www.spiegel.de/panorama/justiz/hunderte-autos-beschaedigt-deutschlandweite-sabotageserie-offenbar-aus-russland-gesteuert-a-7625e908-2f28-4ef8-bb69-35e5bacd6125.

110 Christopher F. Schuetze, "Germany Accuses Russia of Sabotage, Cyberattacks and Disinformation," World, *The New York Times*, December 12, 2025, https://www.nytimes.com/2025/12/12/world/europe/germany-russia-cyberattacks-sabotage-hybrid-war.html.

111 "Russia-Ukraine War: List of Key Events, Day 1,388," *Al Jazeera*, December 13, 2025, https://www.aljazeera.com/news/2025/12/13/russia-ukraine-war-list-of-key-events-day-1388.

release joint cybersecurity advisories highlighting Russian state-sponsored cyber campaigns targeting Western logistics entities and technology companies involved in assistance to Ukraine.[112] The German Federal Criminal Police (BKA) also launched a public information campaign warning of the risks of becoming a disposable agent on behalf of Russia.[113] To address drone incursions, the BKA established a new counter-drone unit in December 2025, which will employ jamming systems and interceptor drones to protect critical civilian and military infrastructure. On the legislative front, the Federal Cabinet adopted the KRITIS Umbrella Act in September 2025, requiring operators of critical infrastructure across 11 sectors (e.g., energy, health, water) to conduct risk analyses and meet minimum security standards, though many proposed physical protection measures are not expected to become mandatory until 2030.[114] Germany has also taken measures to restrict Russian information operations, with the EU and Germany banning *Russia Today* and *Sputnik* in February 2022,[115] while the Network Enforcement Act obliges social media platforms with over two million users to remove "clearly illegal" content within 24 hours and all illegal content within seven days, or face a maximum fine of €50 million.

112 "Protecting the 2025 Bundestag Elections from Hybrid Threats and Disinformation," Federal Ministry of the Interior, https://www.bmi.bund.de/SharedDocs/schwerpunkte/EN/disinformation-election/disinformation-election-artikel.html.

113 "Wegwerf-Agenten: Kurzer Einsatz, Hohes Risiko," Das Bundeskriminalamt (BKA), https://www.bka.de/DE/Landingpages/LLA/lla_node.html.

114 Kamil Frymark and Michał Kędzierski, "Germany: New Law on the Protection of Critical Infrastructure," Centre for Eastern Studies (OSW), February 4, 2026, https://www.osw.waw.pl/en/publikacje/analyses/2026-02-04/germany-new-law-protection-critical-infrastructure.

115 Gjeraqina Tuhina, "Two Years Into EU Ban, Russia's RT And Sputnik Are Still Accessible Across The EU," *Radio Free Europe/Radio Liberty*, February 3, 2024, https://www.rferl.org/a/russia-rt-sputnik-eu-access-bans-propaganda-ukraine-war/32803929.html.

iii. United Kingdom

Introduction

In mid-December 2025, the new head of MI6, Blaise Metreweli, stated that "the export of chaos is a feature not a bug in the Russian approach to international engagement…we should be ready for this to continue until Putin is forced to change his calculus."[116] These remarks echo a similar sentiment expressed a year earlier by Ken McCallum, the Director General of MI5, who said that the agency had been forced to "pare back" its counter-terrorism focus due to the growing threat from Russia, as well as other hostile states.[117] Director McCallum was suggesting that, as resources get stretched thin, the British intelligence service has fewer tools available to deal with other threats to national security. This is perhaps something that has gotten lost in much of the media reporting on hybrid threats in the UK: the second and third order effects that are not apparent but have a potentially disastrous impact on the country's security and defense posture.

The history of Russian covert operations in the United Kingdom is sordid and long. Russia is an established military adversary of the UK, but beyond that, Moscow has also posed a persistent intelligence and counterintelligence threat, often operating with skill and sophistication. With the end of the Cold War, the threat persisted but morphed into alternate forms. An influx of Russian cash into London in the post-Cold War era led to accusations that the British government had gotten soft on oligarchs, and the emergence of 'Londongrad' brought with it plenty of opportunities for corruption and illicit financial ties.[118] The fact that the Russian kleptocracy has historically used London as a clearinghouse for billions of dollars has led to entrenched interests in perhaps not rooting out Moscow's use of both licit and illicit finance.

In the ongoing war between Russian and Ukraine, and Russia's increasingly brazen hybrid operations against Europe, the UK's geography is both a blessing and a curse. While not as accessible, it is vulnerable, especially in the North Sea and the English Channel, and as this chapter lays out in detail, myriad Russia-linked vessels have been found hovering near undersea cables and other critical infrastructure the UK depends upon.

From targeted assassinations to cyber-attacks and from sabotage operations to disinformation campaigns, Russian hybrid threats directed at the UK should make it clear that London remains squarely in the crosshairs of Russian President Vladimir Putin. While the operational tempo has clearly picked up since the UK's support for Ukraine after the full-scale invasion in February 2022, some of Russia's most brazen pre-2022 hybrid operations in Europe took place on UK soil. In 2006, the poisoning of former Russian intelligence officer who defected to the UK is one such case. According to a UK public inquiry, it was probable that Putin had approved the crime together with Nikolai Patrushev, then head of the FSB intelligence service and one of Putin's longtime confidants, and part of his inner circle.[119] Litvinenko

116 Charles Clover, "Russia Is 'Exporting Chaos', New Head of Britain's Spy Agency MI6 Warns," *Financial Times*, December 15, 2025, https://www.ft.com/content/5cbedc56-b29a-4284-901b-aef5f6853135.

117 "MI5 Forced to 'Pare Back' Counter-Terrorism Work Due to Rogue States, Says Chief," *The Guardian*, December 6, 2024, https://www.theguardian.com/uk-news/2024/dec/06/mi5-forced-to-pare-back-on-counter-terrorism-work-due-to-hostile-states-says-agency-chief.

118 Patrick Radden Keefe, "How Putin's Oligarchs Bought London," *The New Yorker*, March 17, 2022, https://www.newyorker.com/magazine/2022/03/28/how-putins-oligarchs-bought-london.

119 Jane Croft et al., "Litvinenko Inquiry: Report Points Finger at Vladimir Putin," Financial Times, January 21, 2016, https://www.ft.com/content/53ecb19c-c01f-11e5-9fdb-87b8d15baec2.

was poisoned with polonium-210 after sipping green tea during a November 1, 2006, meeting with two individuals at Mayfair's Millennium Hotel.

Two incidents in 2014 further highlighted Russia's role as a hybrid threat actor. The first was Russia's invasion and annexation of Crimea, which caught the West by surprise and signaled a new era in Russian-NATO relations. The move was condemned by the then-foreign secretary of the UK, labeled as a "land grab," an "annexation of part of the sovereign territory of an independent European state through military force," and the "use of force to change borders."[120] The U.S. and the UK, along with other Western countries, responded with economic sanctions, but as Moscow's February 2022 re-invasion of Ukraine would later prove, the Western response to Russia's 2014 annexation of Crimea were perceived as soft by the Kremlin and did nothing to deter Putin from a full on invasion of Ukraine eight years after his initial land grab of Ukrainian territory.

Later that same year, in September, there was a referendum on Scottish independence. Nearly 400,000 Twitter messages about Scottish independence were posted by fake accounts, most believed to be Russian, and the accounts' activity coincided or overlapped with major Scottish events.[121] The aim was to discredit the Scottish independence vote by spreading false rumors that the election was rigged to ensure a pro-UK outcome. The suspected Russian accounts engaged in behavior consistent with other pro-Kremlin accounts, including those operated by the infamous "troll factory" in St. Petersburg that meddled extensively in the 2016 U.S. Presidential election.[122] Though the exact extent and nature of Russian meddling in the 'Brexit' referendum is unclear, the UK Parliament Intelligence and Security Committee's assessment of Russia's malign interference in UK politics concluded that the intelligence and security services "underestimated the response required to the Russian threat and are still playing catch up." The report went on to say that "Russian influence in the UK is the new normal […] the UK is clearly a target for Russian disinformation."[123]

In 2018, another major inflection point occurred in the Russian hybrid threats arrayed against the UK. The attempted murder of Sergei Skripal and his daughter Yulia using Novichok, a military-grade nerve agent, was a plot directed by the Russian state at those that the Kremlin considers traitors, and followed a similar pattern to the Litvinenko poisoning in 2006.[124] Several of the interviewees identified the British response to this incident as the correct response and believe it should serve as a model for reactions to other Russian hybrid threats. The UK expelled 23 Russian diplomats, identified as undeclared intelligence officers, the largest expulsion in decades.[125]

---

120 "Ukraine: UK Condemns Russian 'land Grab' of Crimea," *BBC*, March 18, 2014, https://www.bbc.com/news/uk-politics-26632857.

121 Severin Carrell, "Russian Cyber-Activists 'Tried to Discredit Scottish Independence Vote,'" *The Guardian*, December 13, 2017, https://www.theguardian.com/politics/2017/dec/13/russian-cyber-activists-tried-to-discredit-scottish-independence-vote-says-analyst.

122 "#ElectionWatch: Scottish Vote, Pro-Kremlin Trolls," DFRLab, January 22, 2018, https://medium.com/dfrlab/electionwatch-scottish-vote-pro-kremlin-trolls-f3cca45045bb.

123 Donatienne Ruy, "Did Russia Influence Brexit?," Center for Strategic & International Studies, July 21, 2020, https://www.csis.org/blogs/brexit-bits-bobs-and-blogs/did-russia-influence-brexit.

124 David Omand, "Hybrid CoE Working Paper 2: From Nudge to Novichok: The Response to the Skripal Nerve Agent Attack Holds Lessons for Countering Hybrid Threats," The European Centre of Excellence for Countering Hybrid Threats, April 2018, https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-2-from-nudge-to-novichok-the-response-to-the-skripal-nerve-agent-attack-holds-lessons-for-countering-hybrid-threats/.

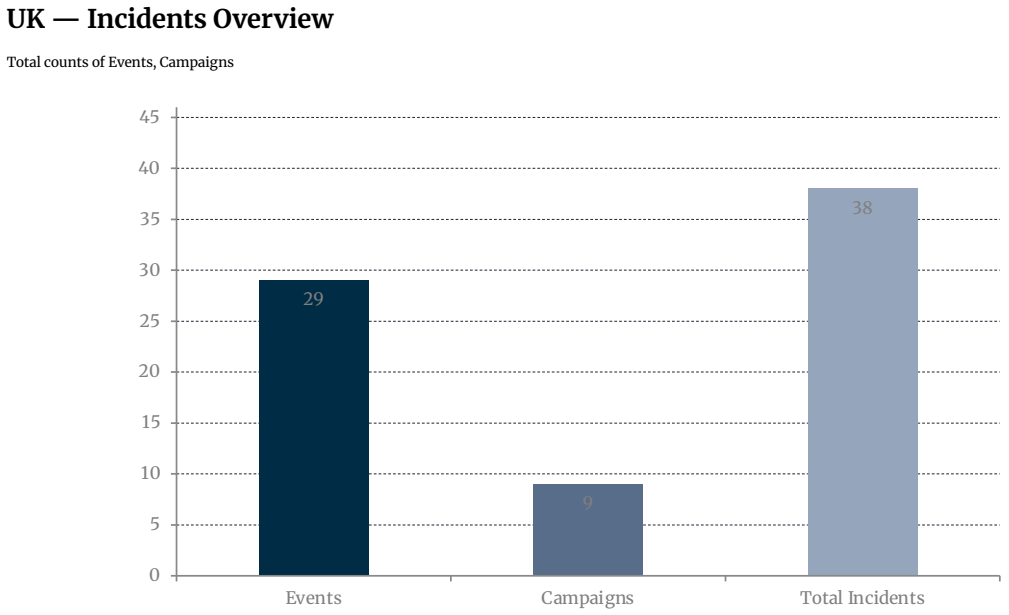
125 Jill Lawless and Danica Kirka, "Britain Boots 23 Russian Diplomats over Spy Poisoning," AP News, March 14, 2018, https://apnews.com/article/db50f6e2d32b4f7482d32beee9a31c76.

After Russia's invasion of Ukraine in February 2022, the UK became one of Kyiv's most ardent and vocal supporters. Then-British Prime Minister Boris Johnson was the first Western leader to visit Ukrainian President Volodymyr Zelenskyy, and his April 2022 trip to Kyiv became one of the defining images of early Western solidarity with Ukraine. Johnson developed close rapport with Zelenskyy, and the UK moved quickly to supply Ukraine with significant military aid, including anti-tank weapons, air defense systems, and, most notably, Storm Shadow cruise missiles. Johnson's successor Rishi Sunak maintained the same line on Ukraine, as did Keir Starmer after his election victory, making Ukraine one of the rare areas of cross-party consensus in British politics.

Russian hybrid TTPs waged against the UK span the entire spectrum from non-kinetic to kinetic, encompassing everything in between.[126] This includes information warfare and basic tactics of political warfare, sabotage, assassinations, and a range of cyber operations, from basic to sophisticated. Russian operatives engage in reconnaissance and casing of land and sea infrastructure, including undersea internet cables and energy and gas connector cables.

Results

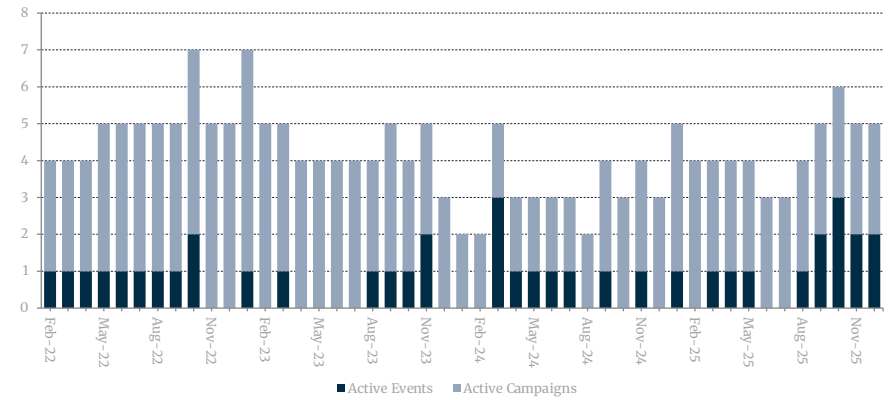
38 hybrid incidents targeting the United Kingdom between February 2022 and December 2025 were identified by the research team, of which 29 were discrete events and 9 were sustained campaigns. Analysis indicates that roughly 66 percent of hybrid operations targeting the UK were certainly attributable to Russia, 13 percent probably, 16 percent likely, and 5 percent suspected. October 2022, and January 2023, were the peak months in terms of active incident volume.



126 Michael McCarthy et al., "Deterring Russia in the Gray Zone," *Books, Monographs & Collaborative Studies*, March 20, 2019, https://press.armywarcollege.edu/monographs/379.

UK — Incidents Over Time

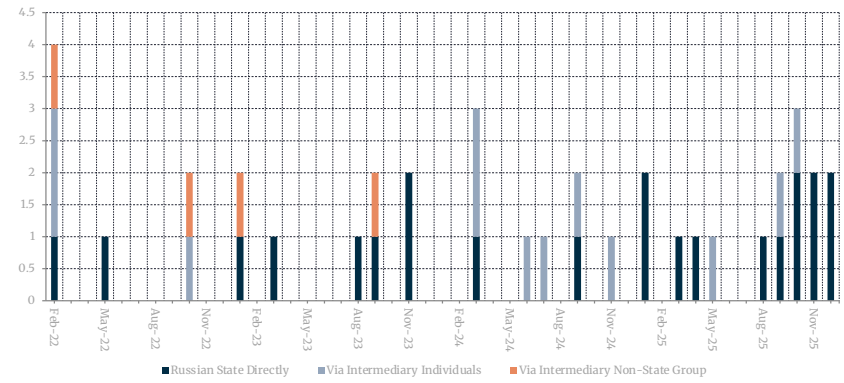
Monthly counts of Active Events and Active Campaigns (2022–2025)



The most common actors behind the hybrid operations were identified as ‘Russian state directly’ (22 incidents), ‘Russia through intermediary individuals’ (12 times), and ‘Russia through intermediary non-state group’ (4 incidents). The incidents in which the Russian state intervenes directly primarily involve airspace incursions and territorial water violations.

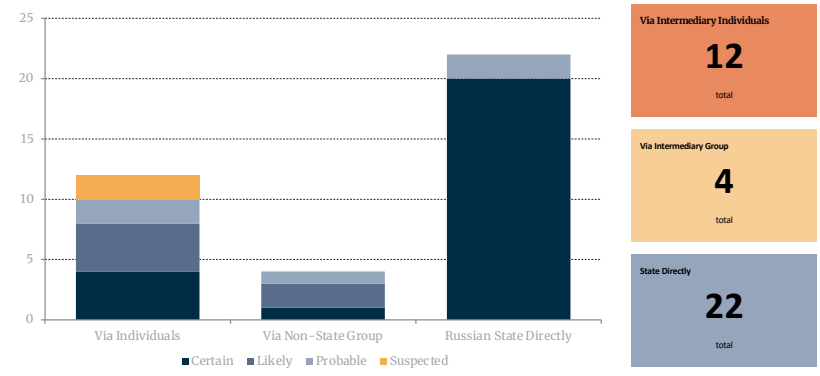
UK — Actor Type by Month

Monthly incident counts by actor type — by start date

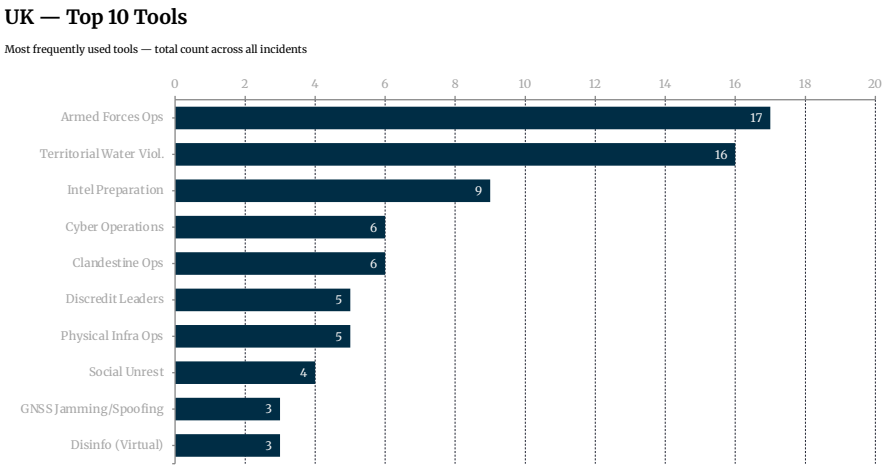


UK — Actor Type & Certainty Levels

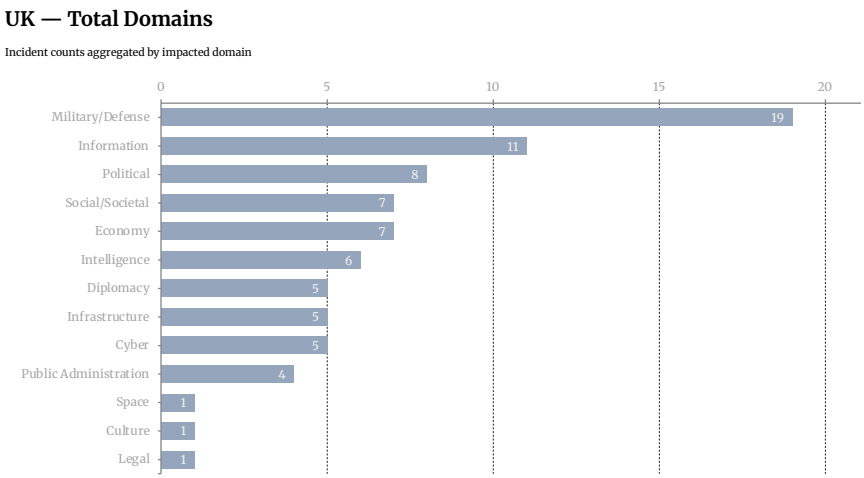
Incident counts per actor group broken down by attribution certainty



The most common tools employed by Russia in hybrid operations targeting the UK were 'Armed forces conventional/sub-conventional operations,' (17 instances), 'Territorial water violation' (16 instances), 'Intelligence preparation' (9 instances), 'Cyber operations' (7 instances), and 'Clandestine operations' (6 instances). In all 38 hybrid threat incidents, the Russians relied on multiple tools. This should not be altogether surprising. As Seely has observed, "while most of the individual tools — with the exception of cyber — are not new, the success in combining so many forms of power is novel."[127]



The most targeted domains by Russia in the UK are 'Military/Defense' (19 instances), 'Information' (11 instances), and 'Political' (8 instances).



127 Robert Seely, "Defining Contemporary Russian Warfare: Beyond the Hybrid Headline," *RUSI Journal* 162, no. 1 (2017): 50–59, https://doi.org/10.1080/03071847.2017.1301634.

Findings

Objectives and Effect

Russia's approach to hybrid threats in the UK lays out something of a blueprint for autocrats seeking to stymie the West and its ability to respond vigorously. The UK occupies a particular position in the Kremlin's threat calculus: viewed historically as "the most devious adversary," in the words of security analyst Mark Galeotti, Britain continues to loom large in Russia's geopolitical imagination, only intensified by the UK's "outsized role for a European country in supporting Ukraine."[128]

Although already used to Russian hybrid operations since before the full-scale invasion of Ukraine, the UK continues to struggle to contain the threat. Dr. Robert Seely, MBE, expert on Russian hybrid warfare and author of the book *The New Total War*, lamented, there is no NATO or allied strategy to address the threat, since "we're still fighting over definitions."[129] Keir Giles, Russia commentator and author of *Who Will Defend Europe?,* has noted that in some states, potentially including the UK, the response has been impeded by institutional reticence: the decision not to publicize Russian interference is made at the political level, driven by a reluctance to be seen to demand action. As Giles put it, "If we point out that something is happening, we need to do something about it."[130] The result, he argues, is an iceberg problem in which the public and even analysts are examining the same approximately five percent of incidents that have become known, while the vast majority remains hidden — an important asterisk to any analysis of hybrid threats based on open sources (including this report).

This reluctance exacerbates the hybrid threat issue. The slightest hint of acquiescence will only draw further aggression, as Putin views capitulation as a sign of weakness, not compromise. Russia, meanwhile, is more comfortable operating on a geopolitical chessboard that is ambiguous and murky in nature.[131] In fact, Moscow prefers an operating environment in which red lines have been erased, and its operatives can push for first-mover advantage. As Seely stated in an interview, "Everything is a weapon for the Russians," noting that the Kremlin has integrated conventional and political warfare, including the use of active measures, which the West still struggles to identify and counter.[132] This is particularly clear in the UK. Galeotti describes Russia's strategic aim in Britain as paralysis, exacerbating existing societal fissures, and bringing the war 'home' to the UK public. According to Galeotti, Brexit shows the same modus operandi: Russia almost certainly did not change many minds on the decision to leave the UK, but it was adept at amplifying divisions and ideas that were already present.[133]

In an interview, Dr. Ofer Fridman, Senior Lecturer at the Department of War Studies at King's College London, similarly stated that Russia's overarching objective through hybrid threats is not any single effect but rather the systemic weakening of an adversary's will and capacity to act and resist.[134] The end

128 Galeotti, "Interview."

129 Robert Seely, "Interview," 2025.

130 Keir Giles, "Interview," 2025.

131 Kathleen H. Hicks, "Russia in the Gray Zone," *Center for Strategic & International Studies*, July 25, 2019, https://www.csis.org/analysis/russia-gray-zone.

132 Seely, "Interview."

133 Galeotti, "Interview."

134 Ofer Fridman, "Interview," 2025.

goal of this strategy is not victory in a conventional sense, but the erosion of cohesion within all institutions that matter: governments, relations between allies, and societies.

In the UK context, hybrid threats and their effects seem to some extent be tied back to the concept of reflexive control. Indeed, according to Galeotti, the strategic corruption dimension of Russia's hybrid campaign in the UK is the most underexplored angle in mainstream analysis but an important one. According to him, corruption in the UK operates diffusely, and Russia's interests are protected by those that have received no orders from Moscow. For example, financial institutions that profited from Russian capital in London may receive no direct instruction from Moscow but have financial incentives to keep Russian interests protected. This facilitation of Russian interests, in combination with the institutional reticence identified by Giles, make for a particularly dangerous combination.

Trends

Across the full 2022–2025 study observation period, the dataset records 38 incidents in the UK. What distinguishes the UK from the peer countries in this study is the predominance of military and naval tools used, with 'Armed forces conventional/sub-conventional operations' (17 incidents) and 'Territorial water violations' (16 incidents) the most often logged. Hybrid operations in the UK mostly focused on using elements of the Russian state directly through territorial water violations and general probing. This could be thought of as the 'death by a thousand cuts' strategy. Each time, the Russians seek to go a bit further, stay a bit longer, attempting to gauge the response time and the force of reaction before repeating these violations, perhaps in an effort to make the defenders numb and lead them to interpret these probes as benign or innocuous. These incidents should be viewed cumulatively when assessing their impact. In an interview with *The Times,* an unnamed UK Defence official referred to these continued incidents as the Russians "pissing in our backyard."[135]

The dataset records three sub-types within the broad category of 'Armed sub-conventional operations' and 'Territorial water violations.' The first and most frequent involves Russian naval vessels transiting UK waters while being shadowed by Royal Navy ships. The dataset records at least 12 such incidents, involving frigates, destroyers, corvettes, and submarines passing through the English Channel and the North Sea. While these passages may be benign, the ambiguity and potential for sabotage, drone launches, and espionage render these incidents extremely resource-draining: every vessel has become a potential liability that needs to be shadowed requiring significant resources, which itself is part of the hybrid rationale of Russia. The second sub-type involves intelligence collection and infrastructure reconnaissance by vessels. The Russian research vessel Yantar, widely assessed as engaged in undersea infrastructure mapping, was tracked loitering near UK critical undersea cables in both January and November 2025.[136] During the November incident, it directed lasers at a Royal Air Force aircraft and conducted GPS jamming before being pushed back by a Royal Navy submarine surfacing alongside the vessel.[137] Most worryingly, in April 2025, the UK military recovered multiple underwater devices from

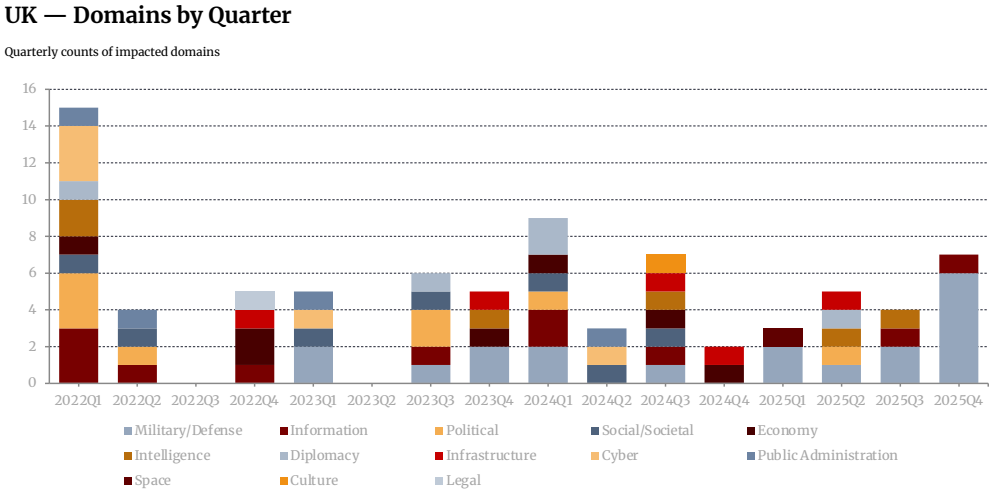
135 Harry Yorke, "Revealed: Russia's Secret War in UK Waters," *The Times*, April 5, 2025, https://www.thetimes.com/uk/defence/article/russia-secret-war-uk-waters-submarines-dpbzphfx5.

136 Becky Morton et al., "UK Warns Putin after Russian Spy Ship Seen near British Waters," *BBC*, January 23, 2025, https://www.bbc.com/news/articles/cqjv7qgpw28o.

137 "Royal Navy Activated Twice in Two Weeks to Intercept Russian Ships in UK Waters," Royal Navy, November 24, 2025, https://www.royalnavy.mod.uk/news/2025/november/24/20251124-royal-navy-tracks-russian-ships-including-research-ship-yantar.

seas around Britain, likely deployed by Russia to monitor the UK's nuclear-armed submarines.[138] The third sub-type is drone incursions over military airbases. In November 2023 and again in November 2024, unidentified drones swarmed airbases in England hosting U.S. forces. In a 2023 incident, an investigation identified suspected GRU officers near the incident base posing as farm workers.[139]

The UK experienced a notable increase in logged incidents in 2025. Many of these were territorial water violations, including sightings of the Russian spy ship Yantar, as noted previously. This may in part be attributable to Prime Minister Keir Starmer's June 2025 announcement that the UK was moving toward "warfighting readiness" in light of its Strategic Defense Review, which outlined a significant upgrade in the UK's defensive and offensive capabilities in response to the growing Russian threat.[140] This would have not only raised the UK's target profile in the Kremlin's view, but also may have changed the UK military's reporting standards, resulting in more water and air encounters being publicized and thus recorded into the incident database.

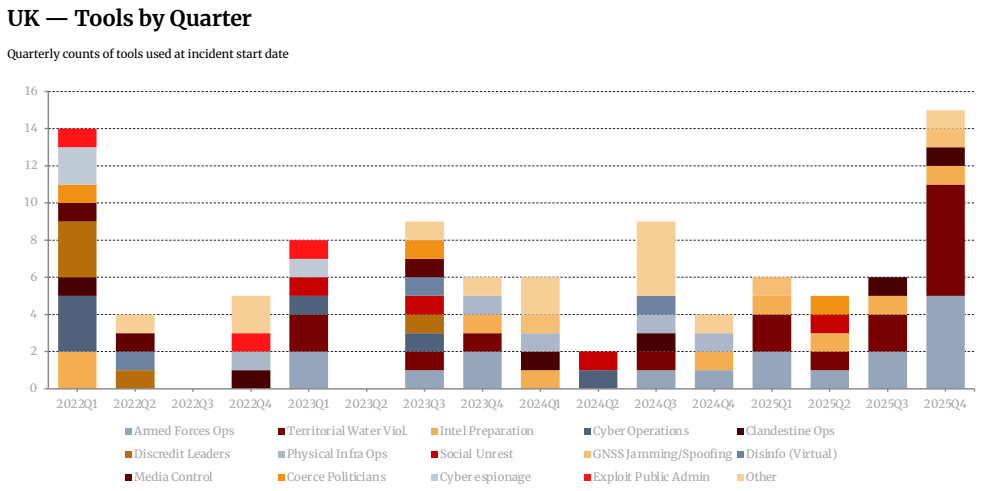


Additionally, out of the 9 campaigns logged across the UK databse, 5 were recorded as beginning in 2022. The most frequent tool utilized in these campaigns was 'Discrediting leadership and/or candidates,' however, 'Media control', 'Intelligence preparation', 'Cyber operations' and 'Clandestine operations' were all leveraged tools as well. The 'Information' and 'Political' domains were the most targetted.

138 Yorke, "Revealed: Russia's Secret War in UK Waters."

139 Jon Lake, "Drone Activity over US Air Bases Blamed on Russian Agents," Aerospace Global News, February 27, 2025, https://aerospaceglobalnews.com/news/drone-activity-over-us-air-bases-blamed-on-russian-agents/.

140 Alex Nichol, "What UK's Strategic Defense Review Means for Ukraine," *The Kyiv Independent*, June 9, 2025, https://kyivindependent.com/what-uk-strategic-defense-review-means-for-ukraine/.



It is important to note that although most incidents logged for the UK fall under the broad category of 'Armed sub-conventional operations' and 'Territorial water violations,' the campaigns concentrated in 2022 were more narrative-driven and focused on information and political influence. These incidents included the hacking of former UK Prime Minister and Foreign Secretary Liz Truss's phone; an RRN-Doppelgänger disinformation campaign aimed at spreading false narratives about the war in Ukraine; and the activities of a group dubbed "the Minions," a reference to the yellow sidekicks from *Despicable Me*. According to British authorities, the group targeted investigative journalists Christo Grozev and Roman Dobrokhotov on behalf of the GRU and also conducted espionage targeting Ukrainian soldiers training at Patch Barracks in Germany in 2022. The ring was directed by Jan Marsalek, an Austrian-born businessman turned Russian agent, and was responsible for planning and running covert operations across Spain, Germany, Austria, Hungary, and Montenegro, using the UK as a hub.[141]

Many of these incidents, however, were active sometime before 2022, but coded as such to fit within the study's observation period. This nevertheless demonstrates that Russia's involvement in the UK has long transcended simply sub-conventional operations. The invasion of Ukraine also likely serves as an immediate trigger. The RRN-doppelgänger campaign was reported to have begun in spring of that year. Additionally, political crises surrounding former Prime Minister Boris Johnson's resignation, Liz Truss's brief premiership and Rishi Sunak's subsequent ascension into the PM office, could have produced public disillusionment that was ripe for Russian exploitation.

Russia also worked through intermediary individuals in some operations. However, this was the case only in roughly one-third (28 percent) of the time. In May 2025, Bulgarian nationals and members of the "Minions," Katrin Ivanova, Vanya Gaberova, and Tihomir Ivanchev, all based in London, were convicted of spying for Russia.

Perhaps the hybrid operation that was most brazen in nature was the March 2024 arson attack. A

141 Madeline Field, "Putin's Spies for Hire: What the U.K.'s Biggest Espionage Trial Revealed about Kremlin Tactics in Wartime Europe," War on the Rocks, April 8, 2025, https://warontherocks.com/2025/04/putins-spies-for-hire-what-the-u-k-s-biggest-espionage-trial-revealed-about-kremlin-tactics-in-wartime-europe/.

warehouse on the Cromwell Industrial Estate in Leyton, east London, used by a Ukrainianowned business to store supplies destined for Ukraine, was deliberately set alight, causing around £1 million in damage. Following a Counter Terrorism Policing investigation, several men were charged with aggravated arson and offences under the UK's National Security Act 2023, after prosecutors said the attack had been orchestrated on behalf of the Wagner Group, a Russian statelinked private military organization.[142] Dylan Earl admitted orchestrating the attack and other planned acts of sabotage after establishing contact with Wagner, while Jake Reeves pleaded guilty to aggravated arson and to agreeing to accept a material benefit from a foreign intelligence service.[143]

A year later, in May 2025, a series of arson attacks targeted properties associated with UK Prime Minister Keir Starmer, including his current and former residences and a vehicle. Five individuals were arrested; three — two Ukrainians and one Romanian — pleaded not guilty at the Old Bailey in November 2025, with trial set for April 2026.[144] British security officials, including MI5, are investigating potential Russian involvement. In January 2026, a fifth arrest was made with regard to the arson attack incidents.[145]

Another brazen attack, which rises to the level of state-sponsored terrorism, occurred in July 2024 when a fire at a DHL warehouse in Minworth, near Birmingham, was caused by an incendiary device concealed in a parcel. The package was part of a broader sabotage campaign orchestrated by the GRU, which also targeted courier facilities in Germany and Poland. The devices were hidden inside shipments of sex toys, massage pillows, and fake cosmetics, and were sent through commercial courier networks, including DHL and DPD, with timed fuses designed to ignite during transit.[146] Western officials assessed the incidents as a GRU "test run" to determine whether such devices could be placed aboard cargo aircraft bound for North America.[147] The parcels originated in Lithuania, and analysis of the Birmingham fire indicated the device could have caused catastrophic damage if it had detonated mid-air. Had this been a group like the Islamic State or far-right extremists, it would no doubt have been labeled terrorism. In other words, calling this state-sponsored terrorism would appear accurate. The incidents triggered a multinational investigation, which led the Lithuanian authorities to charge 15 people in connection with the plot, all maintaining ties to the GRU.[148]

The Russian hybrid approach thus appears largely agnostic to the *means* of attack; it simply requires the best tool to get the job done.

---

142 "Men Who Organised Russia-Backed Arson at London Warehouse Jailed," *Counter Terrorism Policing*, October 24, 2025, https://www.counterterrorism.police.uk/men-who-organised-russia-backed-arson-at-london-warehouse-jailed/.

143 Adina Campbell and Kathryn Armstrong, *Three Men Found Guilty of Wagner Group-Linked Arson Attack in London*, July 8, 2025, https://www.bbc.com/news/articles/cx2k37x91vlo.

144 Sofia Ferreira Santos, "Third Man Charged over Fires at Homes Linked to Keir Starmer," *BBC*, May 21, 2025, https://www.bbc.com/news/articles/c8xgg7rr1q8o.

145 "Police Make Fifth Arrest over Arson Attacks on Properties Linked to Keir Starmer," *BBC*, January 29, 2026, https://www.bbc.com/news/articles/c20dyzp4r42o.

146 Sauer and Walker, "Explosive Sex Toys and Cosmetics: The Story behind the DHL Parcels Plot."

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

148 "Lithuania Charges 15 With Terrorism Over 'Russia Bomb Plot,'" *Barron's*, September 17, 2025, https://www.barrons.com/news/lithuania-charges-15-with-terrorism-over-russia-bomb-plot-d03d3f1b.

Response

As stated above, there is a real lack of visibility into what is happening in the UK because British authorities are largely unwilling to publicize the problem — what Keir Giles has described as the 'iceberg problem'.[149] The decision *not* to be more transparent appears to be a political one according to our interviewees, marked by extreme hesitancy to discuss the Russian problem openly. Giles contends that because we don't see nearly everything that is happening, we can't possibly have a firm grasp of how tactics are evolving, at least in a UK context.

There is a general attempt to build societal resilience in the UK, and, according to one interviewee, this has improved over the past decade.[150] Still, it can be difficult to accurately assess societal resilience as a metric, and progress can be reversed. A concrete policy recommendation that has come up in multiple interviews is for the UK to focus on establishing institutions and developing procedures to better protect the information space. Dr. Andrew Mumford believes that one of the most effective approaches is to rely on cross-government relationships since the threats span the entire government and societal spectrum.[151]

Regarding whether, how, and how forcefully the UK should respond to Russia's hybrid threat campaign, opinions among respondents in this study varied widely. While some lamented a lack of response, others believe that *no response* is the correct response. As one interviewee suggested, the decision to do nothing is actually the correct one in many cases. Hybrid activities are similar to terrorism or propaganda by the deed, and when they are reported, they attract more attention, which is what the perpetrators aim to provoke to lead to an eventual shift in policy. Decisions to eschew a forceful response can help avoid playing into the attackers' hands.

From a policy perspective, Mumford believes that London should be more aggressive in pushing back, naming and shaming Russian operatives and expelling spies and diplomats from the UK. In any conflict, stated or unstated, there comes to be something equivalent to an 'acceptable level of violence,' to tolerate from one's adversary. The same applies to counterterrorism campaigns. But there seems to be no agreement on what that acceptable level of hybrid threats might be, no agreed-upon threshold, with some fine with the status quo, and others seeking a far more aggressive strategy to push back. This quandary extends to the challenge of finding the proper balance between deterrence and resilience. Many would argue that the UK is well-heeled in this regard, having an above-average level of resilience that has become culturally ingrained in the country, reflected in the slogan 'Keep Calm and Carry On,' even in the face of all-out war.

In a long-ranging profile in *Foreign Policy,* MI6 chief Blaise Metreweli made it clear countering Russia's campaign to export chaos throughout arson, sabotage, cyberattacks on critical infrastructure, and provocations throughout sea, land, and air will be a top priority for her agency. "We will sharpen our edge and impact with audacity, tapping into —if you like — our historical SOE instincts," referring to the Special Operations Executive, a secret British organization formed by Winston Churchill and Hugh

149 Giles, "Interview."

150 Fridman, "Interview."

151 Andrew Mumford, "Interview," 2025.

Dalton, designed to conduct espionage, sabotage, and reconnaissance during WWII.[152]

iv. Estonia

Introduction

On the sidelines of the 2024 NATO Summit in Washington, D.C., Estonia's Defense Minister Hanno Pevkur spoke with clarity about the recent surge in Russian hybrid incidents in his country; it was Moscow's aim to distract European nations with internal disruptions while it presses on with its war in Ukraine.[153] Pevkur also cautioned against disproportionate responses to such provocations and has since warned against playing into Russian President Vladimir Putin's narrative of a 'warmongering NATO alliance,' repeated ad infinitum through the Kremlin's sprawling disinformation networks.[154]

In October 2025, when armed Russian special forces were spotted at the Saatse Boot, a bootshaped protrusion of Russian territory that carves into Estonia and through which a short Estonian road crosses, Estonian Interior Minister Igor Taro reassured the public that the security situation remained unchanged.[155] The road on which the special forces were spotted was permanently closed, and an alternative route around the boot is being completed.[156] This approach has come to typify Estonia's response to Russian operations in the country; immediate, calm, and firm. The country has seen some of Russia's most brazen hybrid operations in Europe since the full-scale invasion of Ukraine, including repeated violations of its airspace to signal capability, arson attacks, and sabotage operations. Yet, Tallinn has extensive experience countering such sub-threshold Russian tactics since regaining independence from the Soviet Union in 1991, and has built robust systems across the information, cyber, and defense domains to mitigate their impact and, at the same time, avoid overreactions.

In international fora, Estonian officials have expressed greater alarm about Russia's threat to the Baltic states. In Washington D.C., in November 2025, Margus Tsahkna, Estonia's Minister of Foreign Affairs, warned that Russia will "return to our Baltic borders with even more troops and military equipment than they had before the full-scale invasion" within "two to three years, or less."[157] This underscores a central dilemma for Estonia: avoiding the exaggeration of the Russian threat while simultaneously creating international incentives to keep the NATO alliance strong and engaged.

Following the full-scale invasion of Ukraine, Tallinn has become one of Europe's most vocal advocates for robust military support to Kyiv and has provided over €500 million in military aid.[158] Since the inva-

152 Edward Lucas, "Britain's New Spy Chief Has a New Mission," Foreign Policy, March 5, 2026, https://foreignpolicy.com/2026/01/23/mi6-sis-blaise-metreweli-intelligence-espionage-britain-russia/.

153 Lee Ferran, "Estonia Won't 'Fall into' Russia's 'Trap' by Overreacting to Hybrid Attacks: Defense Minister," Breaking Defense, July 9, 2024, https://breakingdefense.com/2024/07/estonia-wont-fall-into-russias-trap-by-overreacting-to-hybrid-attacks-defense-minister/.

154 Tim Zadorozhnyy, *Estonian Defense Minister on NATO's Response to Russian Threats*, Kyiv Independent, 2025, https://www.youtube.com/watch?v=KKRN1cQUmLw.

155 Andres Einmann, "Igor Taro: Meie Andmetel on Vene Relvastatud Üksus Saatse Saapa Juurest Lahkunud," *Postimees*, October 11, 2025, https://www.postimees.ee/8340944/igor-taro-meie-andmetel-on-vene-relvastatud-uksus-saatse-saapa-juurest-lahkunud.

156 "Saatse Boot Transit Route Closed," Police and Border Guard Board, October 16, 2025, https://www.politsei.ee/en/the-vaerska-saatse-road.

157 Alex Raufoglu, "Baltic Countdown: Estonia Warns Russia Will Return With More Troops, Equipment in 'Two Years or Less,'" Kyiv Post, November 18, 2025, https://www.kyivpost.com/post/64408.

158 "Estonia's Military Aid to Ukraine," Kaitseministeerium, April 9, 2024, https://kaitseministeerium.ee/et/abi-ukrainale.

sion, Estonia has had to contend with a stream of think tank and journalistic discourse about whether "Narva may be next" — a reference to a potential Russian invasion of Estonia, likely through its northeast. Most assessments of such an invasion (see, for example, RAND Corporation's 2016 report[159] on wargaming NATO's defense of the Baltic states) ended in Russian success. However, some of these probabilistic forecasts on whether Putin can and will invade have been modified after the losses Russia has sustained in Ukraine, wiping out capabilities needed for a conventional military invasion or a hybrid attack using special forces in the coming years.[160] Estonian security experts have highlighted the robust defense posture of Estonia as a NATO member and the implausibility of a successful operation involving 'little green men', as seen in Crimea in 2014.[161] Nonetheless, since the full-scale invasion of Ukraine, multiple brazen Russian incursions into Estonian territory have taken place.[162] In 2024, Estonia, Latvia, and Lithuania launched the Baltic Defence Line, a border fortification project which foresees anti-mobility defensive installations on the border of all three countries.[163] By the end of 2027, Estonia will have completed 600 concrete bunkers along its border with Russia.[164]

The relationship between Estonia and Russia, shaped by decades of Soviet repression, has remained tense and deeply fraught since Estonia regained its full independence in 1991. Since then, relations with Moscow remained strained by the memory of Soviet-era crimes as well as border disputes.[165] Estonia's accession to NATO and the EU in 2004 further crystallized its move away from Russia's sphere of influence. Historical memory, including the removal of Soviet war monuments and Russian narratives about discrimination against Russian-speakers, continue to be important themes in Russian hybrid activities in the country.[166]

Estonia has decades of experience confronting modern Russian hybrid operations and has been an early testing ground for Russian hybrid TTPs, including the use of cyber-attacks, infiltration, and the strategic use of diasporas to exploit domestic schisms at particularly tense political moments. Most notably in Russia's subthreshold repertoire was the Bronze Soldier crisis in 2007. Estonia became the first target of a major statesponsored cyber-attack, an event that impacted government functions and

159 David A. Shlapak and Michael Johnson, *Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defense of the Baltics* (RAND Corporation, 2016), https://www.rand.org/pubs/research_reports/RR1253.html.

160 Jennifer Kavanagh and Jeremy Shapiro, "The Bear in the Baltics: Reassessing the Russian Threat in Estonia – European Council on Foreign Relations," European Council on Foreign Relations, December 18, 2025, https://ecfr.eu/publication/the-bear-in-the-baltics-reassessing-the-russian-threat-in-estonia/.

161 Marek Kohv, "Estonia's Robust Security Posture: Dispelling the 'Is Narva Next?' Narrative," International Centre for Defense and Security, July 21, 2025, https://icds.ee/en/estonias-robust-security-posture-dispelling-the-is-narva-next-narrative/.

162 Franziska Müller and Gavin Blackburn, "Russian Border Guards Briefly Cross into Estonian Territory, Foreign Ministry Says," *Euronews*, December 18, 2025, http://www.euronews.com/2025/12/18/russian-border-guards-briefly-cross-into-estonian-territory-foreign-ministry-says.

163 "Baltic Defence Line," Riigi Kaitseinvesteeringute Keskus, January 2024, https://www.kaitseinvesteeringud.ee/en/baltic-defence-line/.

164 Chris Gattringer, "Estonia Starts Building up to 600 Bunkers along Border with Russia," Brussels Signal, December 18, 2025, https://brusselssignal.eu/2025/12/estonia-starts-building-up-to-600-bunkers-along-border-with-russia/.

165 Claire Bigg, "Russia: Moscow Withdrawing From Treaty With Estonia Over References To 'Occupation,'" *Radio Free Europe/Radio Liberty*, June 28, 2005, https://www.rferl.org/a/1059557.html.

166 Raphael Cohen and Andrew Radin, *Russia's Hostile Measures in Europe: Understanding the Threat* (RAND Corporation, 2019), https://doi.org/10.7249/RR1793.

public services and ultimately catalyzed the development of Estonia's cyber defense capabilities.[167] The cyber-attack illustrates the scale of Russian operations against Estonia well before the fullscale invasion of Ukraine in 2022, but also its multi-pronged approach to exploiting domestic tensions that extend beyond cultural and informational manipulation.

The cyber-attack came after Tallinn's decision to relocate the Bronze Soldier; a monument originally named the "Monument to the Liberators of Tallinn" in honor of the Soviet Red Army's liberation of Tallinn from Nazi occupation. While some consider the monument a memorial for lives lost at the hands of Nazis during World War II, Estonians primarily viewed the monument in the middle of the capital as a Soviet relic. The monument was relocated to the military cemetery on the outskirts of Tallinn, causing large-scale riots in both Estonia and Russia. In Moscow, a large crowd besieged the Estonian embassy for several days.[168] In Estonia, a Kremlin-sponsored group guarded the statue in shifts, and two nights of riots shook Tallinn as preparations to relocate the statue were underway. The 2007 cyber offensive disrupted banking services and defaced government websites.[169] After the 2007 attacks, Estonia formalized an already close-knit cyber community into a volunteer Cyber Defence Unit within the Estonian Defence League and strengthened publicprivate cooperation on this difficult issue set.[170]

Results

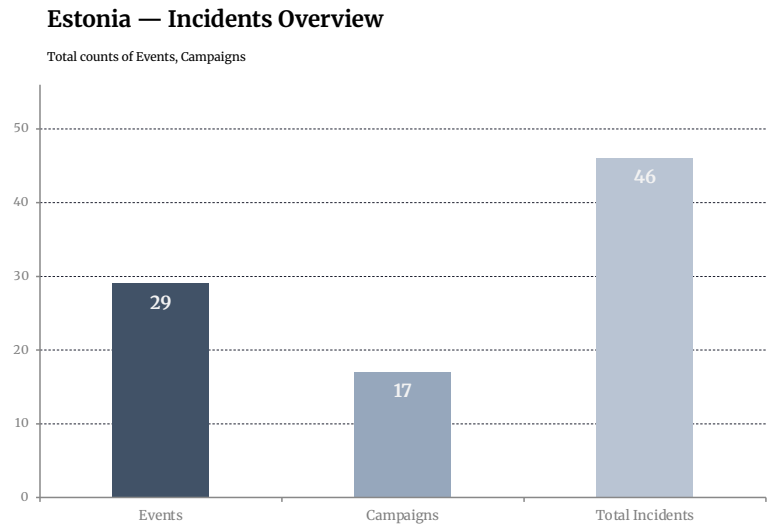
The research team identified 46 hybrid incidents targeting Estonia between February 2022 and December 2025, of which 29 were discrete events and 17 were sustained campaigns. In Estonia, 65 percent of incidents were assessed as certainly attributable to Russia or its proxies, 15 percent as probably attributable, 9 percent as likely attributable, and 11 percent as suspected. There were no clear trends over time in terms of hybrid incidents by start date, but charting monthly active hybrid operations revealed that 2022 and 2023 were the most intense in Estonia.

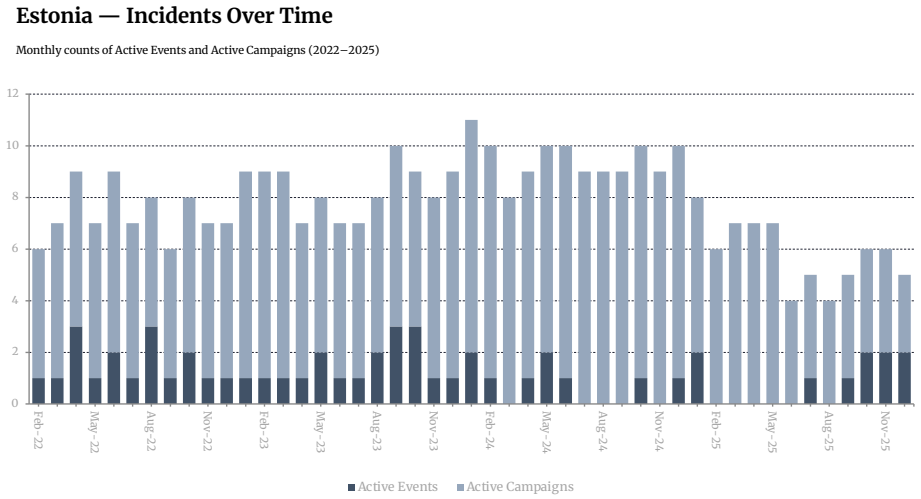
167 Ivo Juurvee and Anna-Mariita Mattiisen, *The Bronze Soldier Crisis of 2007: Revisiting an Early Case of Hybrid Conflict* (International Centre for Defence and Security, 2020), https://icds.ee/en/the-bronze-soldier-crisis-of-2007/.

168 Christian Lowe, "Russian Protesters 'Lay Siege' to Estonian Embassy," *Reuters*, August 9, 2007, https://www.reuters.com/article/world/russian-protesters-lay-siege-to-estonian-embassy-idUSL03545498/.

169 Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security* 4, no. 2 (2011): 49–60, https://doi.org/http://dx.doi.org/10.5038/1944-0472.4.2.3.

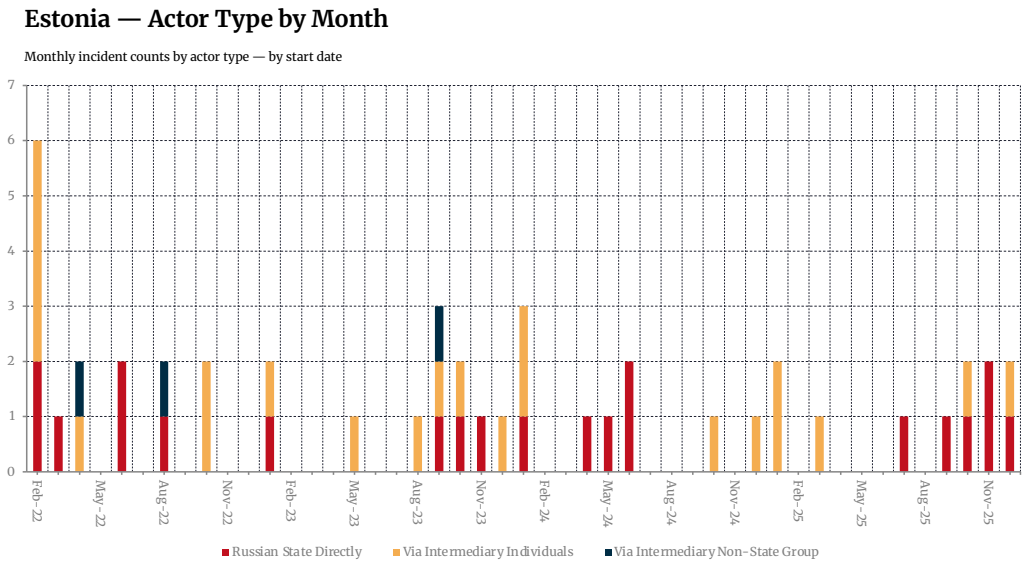
170 FP Analytics, "Lessons from Estonia's Whole-of-Society Approach to Cyber Defense: A Q&A with Hanno Pevkur," Digital Front Lines, August 31, 2023, https://digitalfrontlines.io/2023/08/31/lessons-from-estonias-whole-of-society-approach-to-cyber-defense/.

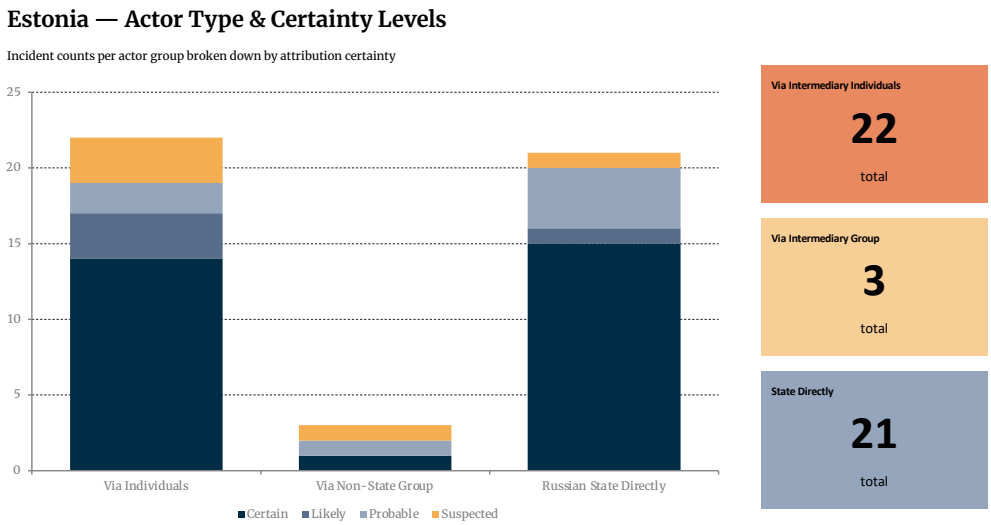




The most common actor behind identified hybrid operations are intermediary individuals used by Russia (22 incidents), followed by the 'Russian state directly' (21) and 'Russia through intermediary nonstate groups' (3).[171] No clear temporary evolution in actor attribution was observable in the Hybrid TTP dataset for Estonia.

171 For several cyber and disinformation incidents attributed to Russia, Estonian state agencies did not specify whether the operations were carried out by a particular Russian state-linked entity or by a Kremlin-aligned proxy. Concretely, this may have translated into an over-attribution to the Russian state directly rather than intermediary groups.

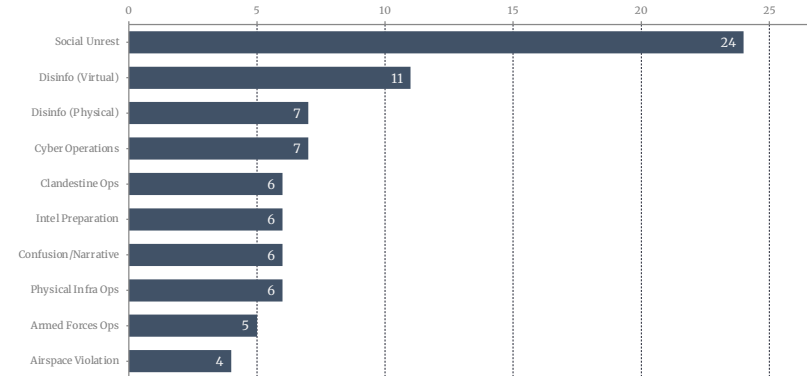




The most common tools employed by Russia in hybrid operations targeting Estonia were ‘Promoting social unrest’ (24 instances), ‘Disinformation campaigns and propaganda (virtual)’ (11 instances), ‘Disinformation campaigns and propaganda (physical)’ (7 instances), ‘Cyber operations’ (7 instances), and ‘Clandestine operations’ (6 instances).

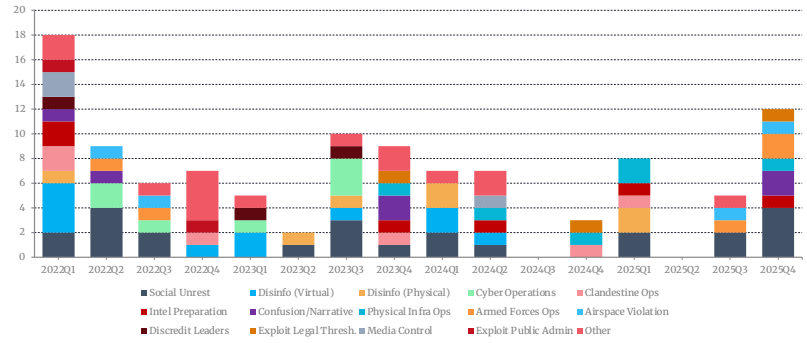
Estonia — Top 10 Tools

Most frequently used tools — total count across all incidents



Estonia — Tools by Quarter

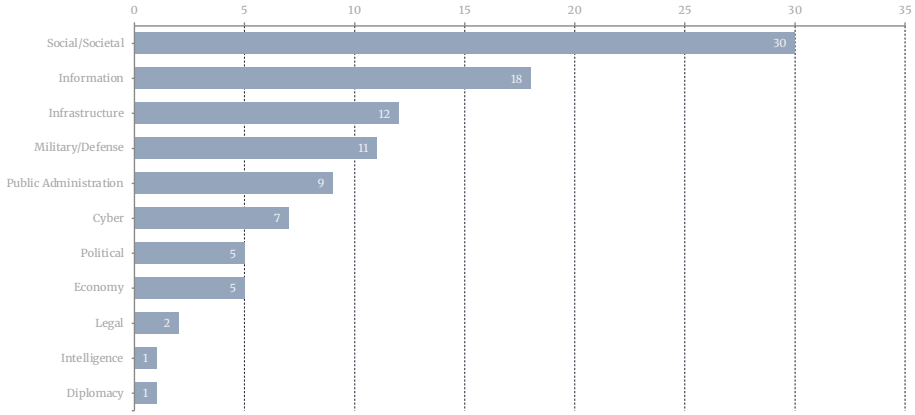
Quarterly counts of tools used at incident start date

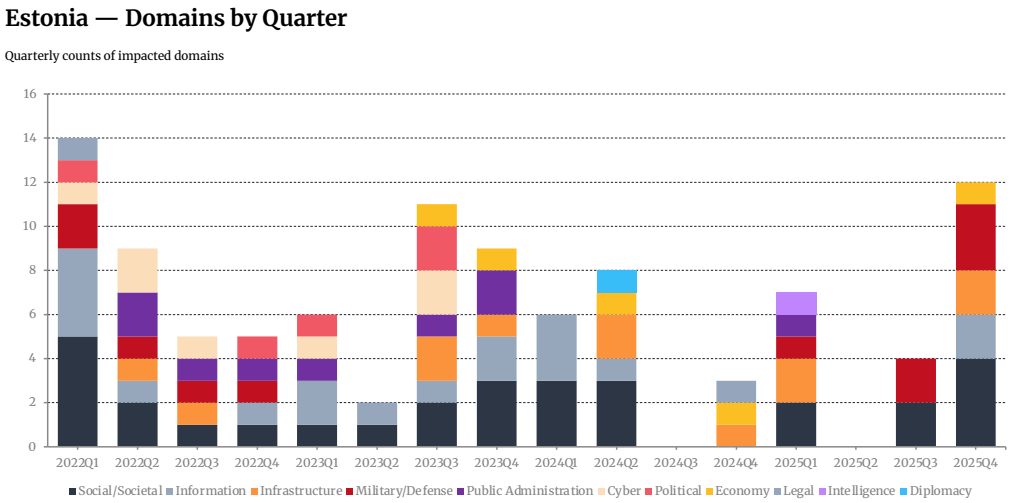


The most targeted domains by Russia in Estonia were the ‘Social/Societal’ environment (30 instances), the ‘Information’ environment (18 instances), and the ‘Infrastructure’ domain (12 instances).

Estonia — Total Domains

Incident counts aggregated by impacted domain





Findings

Objectives and Effect

Estonia's history with Soviet occupation and large Russophone minority has led to some assessments that hybrid operations seek to create the conditions for a future military invasion. Assessments vary, with many experts, including ones interviewed for this report, expressing skepticism that Russia is currently capable of sustained kinetic confrontation with a NATO member state.[172]

Marek Kohv, the Head of the Security & Resilience Programme at the International Centre for Defence and Security (ICDS) in Estonia observed that Tallinn has confronted these forms of Russian interference continuously since regaining independence in 1991, well before the emergence of the concept of "hybrid threats" or the full-scale invasion of Ukraine.[173] Kohv highlighted that while hybrid warfare can be a useful umbrella term to understand Russian operations in Estonia, it may obscure Russia's criminal acts and sabotage into something that sounds abstract or ambiguous. However, while he has highlighted the robust defense posture of Estonia, he has also emphasized that Estonian policymakers and security services view these activities through the lens of potential kinetic escalation, as illustrated in Ukraine where hybrid operations preceded and accompanied conventional invasion. Nonetheless, he assessed the impact of these operations in Estonia as minimal. He attributed this to Baltic societies having effectively been "inoculated" against Kremlin interference in the information domain due to their long exposure to these operations. In general, he assessed that Moscow is less successful at creating new problems than at exploiting existing fractures within societies it has studied closely for decades, reflected in the narratives it chooses to amplify. For example, it has pushed the idea that Estonia "voluntarily" joined the USSR and benefited from Soviet rule, sometimes describing it as a "privileged" republic.[174] In the case of Estonia, the Russian-speaking minority, and especially older generations,

172 Kohv, "Estonia's Robust Security Posture: Dispelling the 'Is Narva Next?' Narrative."

173 Interview, Marek Kohv, 2025

174 "Being Occupied as a Privilege," EUvsDisinfo, June 24, 2020, https://euvsdisinfo.eu/being-occupied-as-a-privilege_baltic_states/.

have, on average, poorer media literacy, and are more often targeted with bespoke narratives by the Kremlin. This was echoed by Russia expert and OSINT investigator Milàn Czerny, who distinguished between the success of information operations by Russia in France and that in countries with significant Russian-speaking populations such as Estonia, Georgia, and Israel.[175]

According to an intelligence analyst who spoke on the condition of anonymity, Russian hybrid operations in the Baltics have been markedly more brazen following the full-scale invasion of Ukraine. In his assessment, these activities are not solely aimed at interdicting aid to Kyiv or polarizing public opinion but also serve to refine TTPs for potential future conflict scenarios.[176] Retired CIA Operations Officer Edward Bogan, who has worked extensively in Ukraine, offers a parallel assessment, characterizing hybrid threats in the post-Soviet space as practically unchanged in aims and intent, but amplified through the new technologies at its disposal.[177] According to Bogan, the more we insist on labeling these interference activities as something other than war, the more we normalize and ultimately enable them. Bogan also stated that the impact of Russian disinformation campaigns should not be understated, and points to mitigating activities in this sphere as a critical tool, especially in post-Soviet states — aligned with our own dataset.

An interview conducted by *New Lines Magazine* with Estonia's Director General of the Estonian Foreign Intelligence Service, Kaupo Rosin, highlighted, similarly to our interviewees, that hybrid threats in Estonia should be understood in the framework of a future potential military conflict with NATO.[178] From Rosin's perspective, Moscow fully regards NATO as an adversary and is deliberately working to shape conditions for a future military confrontation in the Baltic region. Rosin argues that Russia's strategy is not about a sudden invasion but about escalatory conditioning to test NATO's resolve and raise the perceived cost of defending Estonia for other NATO members. In his assessment, the ultimate objective is to weaken alliance cohesion and the cost of defending Estonia, so that NATO scales back activity in the Baltic Sea region, creating an opening for Russian domination or annexation. Rosin rejects the idea that hybrid activity is categorically different from war. Nonetheless, in a different interview, given in December 2025, Rosin stated that "Russia currently has no intention of attacking any of the Baltic states or NATO more broadly."[179] He also claims that Russia is increasingly signaling to Europe that it will not seek to attack it in a bid to slow down European rearmament.

175 Czerny, "Interview."

176 Intelligence Analyst (name withheld), "Interview."

177 Edward Bogan, "Interview," 2025.

178 Floriana Bulfon, "How Estonia Became the Front Line in the New Cold War," New Lines Magazine, January 12, 2026, https://newlinesmag.com/reportage/how-estonia-became-the-front-line-in-the-new-cold-war/.

179 Epp Ehand, "Estonia's Spy Chief: Russia Not Planning to Attack a Baltic Country at This Time," *ERR*, December 29, 2025, https://news.err.ee/1609896976/estonia-s-spy-chief-russia-not-planning-to-attack-a-baltic-country-at-this-time.

Trends

Across the period from February 2022 to December 2025, 46 hybrid incidents were recorded in Estonia, of which 80 percent were classified as destabilizing phase operations and 20 percent as priming operations. Since 2022, Russia's hybrid TTPs in Estonia has evolved from cyber and disinformationfocused pressure to increasingly physical and infrastructuretargeting operations.

From the outset of the full-scale invasion of Ukraine, Russia has maintained near continuous hybrid pressure against Estonia, rather than episodic surges tied solely to elections or singular political moments as was seen in the France case study, for example. Nonetheless, it is clear that it uses hybrid operations to signal its discontent with certain policies. In April 2022, during a NATO cyber defense exercise, Locked Shields, Estonia experienced coordinated distributed denial-of-service (DDoS) attacks with the websites of the President, the Ministry of Foreign Affairs, and the Police and Border Guard Board targeted.[180] Simultaneously, the NATO Cyber Defence Centre of Excellence in Tallinn was defaced by two Latvian nationals recruited by the GRU with graffiti reading "Killnet hacked you."[181] Months later, in August 2022, the most extensive cyberattack in Estonia since the 2007 Bronze Soldier crisis was conducted shortly after officials removed the Soviet T-34 tank monument in Narva and transported it to a museum.[182] The attack was claimed by the pro-Russia hacker group Killnet.[183] This echoes the same logic of Russian cyberattacks in 2007, when it coordinated these activities at a time of domestic tensions over Soviet-era monuments.

While Estonia saw significant hybrid activity by the Russian state conducted directly, there were numerous incidents attributable to intermediaries acting on behalf of the Russian intelligence services. Of the 46 recorded incidents, 22 were attributed to Russia through intermediary individuals, 21 directly to the Russian state, and 3 to intermediary non-state groups, a near even split between direct and proxy-mediated action. A large number of these individuals have a criminal background, a well-documented phenomenon throughout Europe since 2022.[184] Rather than disposable agents, some of the individuals involved in operations in Estonia were involved in multiple sabotage and vandalism operations.[185] In August 2023, the cars of Estonian Interior Minister Lauri Läänemets and a journalist in Tallinn were vandalized in a coordinated act traced back to the GRU through a network of pro-Russian activists and unknowing proxies.[186] The leader of the network, Allan Hantsom, had been given a list by the GRU of individuals to target for vandalism. According to Margo Palloson, Director General of the Estonian Security Police, most individuals that were arrested had a criminal background, and while some were recruited in Russia, others were approached on social media and were completely unaware of any links

---

180 "DDoS Cyberattacks Temporarily Disrupt Estonian Government Websites," *ERR*, April 22, 2022, https://news.err.ee/1608573376/ddos-cyberattacks-temporarily-disrupt-estonian-government-websites.

181 Inga Spriņģe et al., "Exclusive: Inside Russia's Latvian Sabotage Squad," The Insider, https://theins.ru/en/politics/272989.

182 Andrius Sytas, "Estonia Says It Repelled Major Cyber Attack after Removing Soviet Monuments," *Reuters*, August 18, 2022, https://www.reuters.com/world/europe/estonia-says-it-repelled-major-cyber-attack-after-removing-soviet-monuments-2022-08-18/.

183 "Killnet: Inside the World's Most Prominent Pro-Kremlin Hacktivist Collective," Flashpoint, https://flashpoint.io/intelligence-101/killnet/.

184 Kacper Rekawek et al., "Russia's Crime-Terror Nexus: Criminality as a Tool of Hybrid Warfare," International Centre for Counter-Terrorism, September 30, 2025, https://icct.nl/publication/russias-crime-terror-nexus-criminality-tool-hybrid-warfare.

185 Spriņģe et al., "Exclusive: Inside Russia's Latvian Sabotage Squad."

186 ""Pro-Russian Activist Handed 6.5 Year Prison Sentence for Vandalizing Minister's Car," ERR, December 5, 2024, https://news.err.ee/1609542394/pro-russian-activist-handed-6-5-year-prison-sentence-for-vandalizing-minister-s-car.

to the Kremlin.[187]

In addition to these covert operations, six clandestine operations which all involved Estonians, dual Russian Estonian citizens, and third country nationals were logged in the 2022 to 2025 period. These clandestine operations included secret intelligence collection on life in Estonia,[188] smuggling and sanctions evasions,[189] and cash transfers for sanctioned cultural organizations.[190] The details that have been made publicly available about these clandestine operations indicate that Russian intelligence agencies focused on recruiting border agents, members of Estonia's volunteer Defense League, and dual citizens with social ties across the border. While some of these intelligence collection activities can serve to plot future sabotage and vandalism operations, they can also serve to prepare for a potential future invasion.

All incidents in Estonia were part of the priming or destabilizing phases of Russia's hybrid strategy, yet certain incidents indicate the ambition of Russia to coerce Estonia through its sub-threshold activities in the longer term. Aivo Peterson, the leader of the pro-Russian political party KOOS, and his conspirators were convicted in 2024 after it was discovered that they aimed to set up a political association to support Russian propaganda narratives in Estonia, backed by a paramilitary organization. This "civil defense unit" was to be formed under KOOS to serve as an army in case of a power vacuum, and its establishment was planned with the aid of the GRU.[191] Peterson campaigned for the 2024 European Parliament elections from prison, receiving 11,500 votes nationwide, which shows some but limited support for these brazen Kremlin-linked acts among the Estonian electorate. This is a key aspect that needs to be stressed; while the Russophone community of Estonia is not a homogenous political group, it has been especially targeted by hybrid operations, similar to operations targeting Russophone citizens in East Ukraine by Russia in 2014.

Indeed, a consistent throughline in Russian hybrid operations in Estonia is the exploitation of societal cleavages, particularly linguistic and historical divides, through disinformation operations that are both physical and virtual in format. During the 2023 parliamentary elections, Russian-linked accounts spread divisive narratives about the ruling Reform Party and amplified tensions between Estonian- and Russian-speaking communities. False narratives about the e-voting system also started circulating, claiming the system was able to discard votes from the Russian minority.[192] Estonian reporting highlights the differentiated impact of these disinformation operations: for example, false bomb threats that are likely Russia-orchestrated produced higher absenteeism in Russianlanguage schools in Estonia, indicating segregated information ecosystems and unequal trust in state counter messaging when these informa-

187 "ISS: Russian Special Services behind Attack on Estonian Minister's Car," *ERR*, February 20, 2024, https://news.err.ee/1609258853/iss-russian-special-services-behind-attack-on-estonian-minister-s-car.

188 "Estonian Defense League Member Jailed for Collaborating with Russian Intelligence," *ERR*, October 7, 2025, https://news.err.ee/1609822980/estonian-defense-league-member-jailed-for-collaborating-with-russian-intelligence.

189 *Annual Review, 2022-2023* (Estonian Internal Security Service, 2023), https://kapo.ee/sites/default/files/content_page_attachments/Annual%20Review%202022-23_0.pdf.

190 "Estonian Court Sentences Woman to 16 Months in Prison for Violating Sanctions," *ERR*, April 15, 2025, https://news.err.ee/1609665356/estonian-court-sentences-woman-to-16-months-in-prison-for-violating-sanctions.

191 "Prosecutor: Pro-Kremlin Agitator Tried to Set up Armed Anti-State Militia in Estonia," News, *ERR*, May 27, 2025, https://news.err.ee/1609705992/prosecutor-pro-kremlin-agitator-tried-to-set-up-armed-anti-state-militia-in-estonia.

192 Iryna Matsiuk, "The Kremlin's Shadow: Strategy and Tactics of Russian Interference in the Baltic States Elections," Blue Europe, September 3, 2025, https://www.blue-europe.eu/analysis-en/full-reports/the-kremlins-shadow-strategy-and-tactics-of-russian-interference-in-the-baltic-states-elections/.

tion operation occur.[193] The 'Social/Societal' domain was the most frequently affected across the entire dataset, targeted by 65 percent of incidents, while 'Promoting social unrest' was the single most used tool, appearing un 52 percent incidents.

Since 2025, Russian TTPs in Estonia seem to have pivoted toward more overt probing, testing Estonian airspace, maritime boundaries, and land borders. Recurrent helicopter incursions, fighter jet incursions, maritime boundary violations, and patrol movements into Estonian territory serve to signal military capability and to provoke and test whether Tallinn and NATO at large may invoke Article 4 or Article 5. These actions differ from drone overflights as seen in Western Europe (see France and Germany case studies, for example). In Estonia, attribution is usually immediate, and Russian responsibility is explicit. Rather than plausible deniability, these operations emphasize ambiguity of their intent, whether it is assessing NATO's thresholds or reinforcing the perception of permanent risk to Estonians. On December 17, 2025, in one of the most brazen incursions yet, three Russian border guards crossed into Estonia for more than 20 minutes and landed a hovercraft before they retreated and returned to Russia.[194] A couple of months earlier, in September 2025, three Russian MiG-31 fighter jets violated Estonian airspace. In response, Estonia invoked NATO's Article 4. The aircraft were armed with R-33 air-to-air missiles during the incursion into Estonian airspace.[195]

In addition to overt probing of territorial defense, there was a notable expansion of plausibly deniable physical operations against infrastructure. Across the dataset, the 'Infrastructure' domain was affected in 12 of 46 incidents (26 percent), with 'Physical operations against infrastructure' recorded 6 times, concentrated in 2023–2025. In January 2025, two arson attacks were perpetrated by Moldovan intermediaries working on behalf of the GRU — one against a Ukrainian restaurant in Tallinn and one against a supermarket in Osula.[196]

While these operations have significant psychological and media potency, the operations targeting public infrastructure have proven particularly disruptive and resource-draining: they have led to outages, disruptions in telecommunications, and cost significant money to repair. Undersea infrastructure in the Baltic Sea has been frequently targeted in plausibly deniable but almost certainly Russia-linked operations. In total, three Estonialinked undersea infrastructure incidents were tallied during the studied period; the Baltic connector pipeline and telecom cables in October 2023,[197] the Estlink 2 power interconnector in December 2024,[198] and the Helsinki–Tallinn telecom cable in December 2025.[199] All

193 "Why Did the Bomb Threat Cause Panic among Tallinn's Russian Community but Not among Estonians?," Propastop (Estonian Defence League), November 20, 2025, https://www.propastop.org/en/2025/11/20/why-did-the-bomb-threat-cause-panic-among-tallinns-russian-community-but-not-among-estonians/.

194 Müller and Blackburn, "Russian Border Guards Briefly Cross into Estonian Territory, Foreign Ministry Says."

195 "Estonia Says Russia Flew Three Fighter Jets over Its Airspace," *Le Monde*, September 20, 2025, https://www.lemonde.fr/en/russia/article/2025/09/19/estonia-says-russia-flew-three-fighter-jets-over-its-airspace_6745560_140.html.

196 Malek Fouda, "Russia Instructed Arson Attack on Ukrainian Restaurant, Estonia Says," *Euronews*, n.d., http://www.euronews.com/my-europe/2025/07/03/estonia-says-arson-attack-on-ukrainian-restaurant-was-order-by-russias-intelligence-servic.

197 "Captain of Ship That Destroyed Balticconnector Pipeline Appears in Hong Kong Court," *ERR*, July 5, 2025, https://news.err.ee/1609738404/captain-of-ship-that-destroyed-balticconnector-pipeline-appears-in-hong-kong-court.

198 David Mchugh, "Finland Stops Russia-Linked Vessel over Damaged Undersea Power Cable in Baltic Sea," *AP News*, December 26, 2024, https://apnews.com/article/eu-finland-estonia-baltic-sea-power-cable-6741ef1ce9130602abac6214d7297717.

199 "Finnish Customs: Sanctioned Russian Steel Found on Fitburg," *Helsinki Times*, January 1, 2026, https://www.helsinkitimes.fi/finland/finland-news/domestic/28371-customs-sanctioned-steel-cargo-found-on-fitburg-ship.html.

three incidents fit a wider pattern of a vast uptick in cable incidents in the Baltic Sea, which Nordic and Baltic officials have repeatedly linked to Russian hybrid warfare. In this type of operation, Russia uses shadowfleet tankers and other civilian vessels as deniable proxies that engage in anchor dragging to damage critical undersea cables. The Estlink 2 electricity cable repair costs are roughly €50 million.[200]

GPS and GNSS jamming since June 2023 has also caused significant disruption in Estonia; four jammers between Narva and St. Petersburg, with one activated in July 2024 very close to the Estonian border, have caused continuous disruption.[201] While the effects of GPS jamming in Estonia are considered a byproduct of Russia repelling Ukrainian drone attacks by some, they also serve as a tool to disrupt civilian life and infrastructure in NATO states bordering Russia. According to Estonia's Ministry of Interior, GPS jamming between May and July 2025 caused damage to the internal security sector of up to half a million euros.[202] Some satellite communication signals and navigation systems used by the police and border security agencies across the Baltic states have effectively been rendered inoperable by these jammers. Civilian and economic impacts have been felt as well; in April 2024, Finnair halted flights to Tartu for a month due to GPS jamming and spoofing, which made approaches unsafe.[203]

Response

Estonia's response to Russian hybrid operations since 2022 is primarily characterized by its deliberate refusal to be provoked into overreaction. This approach is visible in how Estonia has handled repeated "thresholddancing" incidents that fall seek to test NATO's red lines. The September 19, 2025, MiG31 airspace violation, which triggered Article 4 consultations but not an Article 5 response, illustrates this tension. Russia's strategy in Estonia has not yielded its intended payoff. Instead of exposing fractures and undermining cohesion, it has catalyzed increased defense spending, reinforced allied presence in the Baltics, and accelerated hardening of critical infrastructure.[204] According to Foreign Intelligence Service Director General Kaupo Rosin, Russia too knows its strategy has backfired: "Following various incidents — starting with the undersea cables some time ago or the different drone incursions into NATO airspace or aircraft violations — what we've seen is that, in response to reactions from the West or NATO, Russia has taken various measures to prevent such incidents from happening again in the future."[205]

In the Parliament's statement on its decision in January 2026 to establish a crossparty committee to

200 "EstLink 2 Repair Work Starts in the Gulf of Finland," *ERR*, May 22, 2025, https://news.err.ee/1609701564/estlink-2-repair-work-starts-in-the-gulf-of-finland.

201 "Russia's New Jammer Increases GPS Interference on Estonia's Eastern Border," *ERR*, July 24, 2025, https://news.err.ee/1609752713/russia-s-new-jammer-increases-gps-interference-on-estonia-s-eastern-border.

202 "Damage from Russia's GPS Jamming Amounts to over €500,000, Estonia Says," *ERR*, July 31, 2025, https://news.err.ee/1609759581/damage-from-russia-s-gps-jamming-amounts-to-over-500-000-estonia-says.

203 "Finnair Suspends Flights to Tartu for 1 Month to Seek GPS Jamming Solution," *ERR*, April 29, 2024, https://news.err.ee/1609328058/finnair-suspends-flights-to-tartu-for-1-month-to-seek-gps-jamming-solution."container-title":"ERR","title":"Finnair suspends flights to Tartu for 1 month to seek GPS jamming solution","URL":"https://news.err.ee/1609328058/finnair-suspends-flights-to-tartu-for-1-month-to-seek-gps-jamming-solution","issued":{"date-parts":[["2024",4,29]]}}],"schema":"https://github.com/citation-style-language/schema/raw/master/csl-citation.json"}

204 "Estonia to Invest over €10 Billion in Defence in 2026-2029," Kaitseministeerium, July 30, 2025, https://www.kaitseministeerium.ee/en/news/estonia-invest-over-eu10-billion-defence-2026-2029.

205 Ehand, "Estonia's Spy Chief: Russia Not Planning to Attack a Baltic Country at This Time."

investigate Russia's influence activities, Russian operations are explicitly acknowledged as part of a "broader strategy that seeks to weaken the security and resilience of the Estonian state, target Estonia's Russian-speaking population and social cohesion, and spread narratives that are damaging to the Estonian state and its allies." [206]

The committee will map funding for influence activities, NGO and public sector involvement, as well as the impact of propaganda on different population segments, and make proposals for counter and prevention measures which will be released in February 2027.

Operationally, Estonia has doubled down on its total defense model, which far predates the full-scale invasion of Ukraine, extending it into the hybrid domain. On the physical side, Tallinn is creating a reserve unit of 1,000 trained reservists to support police at the eastern border, with an explicit focus on countering migrationbased and hybrid attacks by Russia and Belarus.[207] This gives Estonia full capacity to respond to greyzone incursions without immediate recourse to NATO escalation and thus avoids playing into the Kremlin's hand. Estonia is also expanding its civilian volunteer structures and Defense League capabilities.[208] The underlying rationale is that a small state can offset its limited standing forces by mobilizing trained civilian capacity during crises such as wide ranging cyberattacks, or conventional conflict.

Whether Estonia's response is adequate will have to be time-tested. Nonetheless, Russia's alleged recalibrating to avoid triggering responses it cannot control is perhaps the clearest measure of Estonia's success: the demonstrated ability to raise the costs of hybrid operations.

206 "The Riigikogu Established a Committee of Investigation for Russia's Influence Activities," Riigikogu, January 21, 2026, https://www.riigikogu.ee/en/news-from-committees/constitutional-committee/the-riigikogu-established-a-committee-of-investigation-for-russia-s-influence-activities/.

207 Iida-Mai Einmaa, "Estonia to Establish 1,000-Strong Crisis Unit to Curb Migration Attacks," *ERR*, October 20, 2024, https://news.err.ee/1609497499/estonia-to-establish-1-000-strong-crisis-unit-to-curb-migration-attacks.

208 Natalia Smolentceva, "Estonians Prepare to Defend Themselves against Russia," *DW*, December 10, 2024, https://www.dw.com/en/estonian-volunteers-prepare-for-potential-russian-attack/a-70436904.

v. Moldova

Introduction

On September 22, 2025, just one week before Moldova's consequential parliamentary elections, President Maia Sandu addressed her country. Sandu warned citizens that Moldova's "sovereignty, independence, territorial integrity, and European future are in danger. The Kremlin is pouring hundreds of millions of euros to buy hundreds of thousands of votes on both banks of the Nistru River and abroad. People are intoxicated daily with lies. Hundreds of individuals are paid to provoke disorder, violence, and spread fear." She warned that if Russian meddling in the election was successful, "Europe would stop at Moldova's border." [209] Sandu's party won an outright parliamentary majority in a landslide victory, despite deep domestic and international concern over the "unprecedented" level of Russian hybrid TTPs levied across Moldova in an effort to sway the election.[210] This followed an earlier, albeit less consequential, 2024 presidential vote, which Sandu paired with an EU referendum. The 2024 election only narrowly broke in Sandu's favor, in part because the referendum linkage was unpopular and widely viewed as a cheap political maneuver. Her margin was largely carried by the Moldovan diaspora, many of whom live in Europe — an electorate Russia increasingly targeted in the run-up to the 2025 election.

Russia has long had an outsized influence in Moldova, a landlocked former Soviet republic wedged between Romania (an EU and NATO member) and Ukraine, often considered both a corridor and a buffer between Russia and Europe. On Moldova's eastern bank sits Transnistria, a breakaway region that has operated for decades under a separatist administration — the so-called Pridnestrovian Moldavian Republic (PMR) — and remained tightly enmeshed with Russia politically, militarily, and economically; Russian "peacekeeping" troops have stayed in the territory since the early 1990s, providing Moscow a durable lever inside Moldova's internationally recognized borders.[211]

Transnistria hosts key industrial assets and, critically, the Moldavskaya GRES (MGRES) power plant, which has historically supplied a large share of Moldova's electricity. The plant is controlled by Russian state-linked entities — it is owned by Inter RAO, a Russian state-owned energy company, and operates on Russian gas supplied by Gazprom — giving Moscow substantial indirect leverage over Moldova's power system.[212] In 2024, Transnistria was estimated to have contributed to roughly 15 percent of Moldova's GDP, significant for a country that is still among Europe's poorest states.[213] Former CIA analyst Peter Clement, calls Transnistria a "willing instrument" for Russian influence, arguing that its relationship benefits both parties, with the separatist government receiving financing, and backing from Moscow in return for a persistent Russian military (peacekeeping force) presence in (or near) Moldova.[214]

---

209 "President Maia Sandu's Address in the Context of the Parliamentary Elections of September 28, 2025," Presidency of the Republic of Moldova, September 22, 2025, https://presedinte.md/eng/discursuri/adresarea-presedintei-maia-sandu-in-contextul-alegerilor-parlamentare-din-28-septembrie-2025.

210 "Winning the Battle, Not the War: Moldova's Fight Against the Kremlin's Hybrid Arsenal," The Soufan Center, September 30, 2025, https://thesoufancenter.org/intelbrief-2025-september-30/.

211 James J. Coyle, *Russia's Border Wars and Frozen Conflicts* (Palgrave Macmillan Cham, 2017).

212 *Market Design – Moldova Energy Profile* (International Energy Agency, 2021), https://www.iea.org/reports/moldova-energy-profile/market-design.

213 "BTI 2024 Moldova Country Report," BTI 2024, https://bti-project.org/en/reports/country-report?isocode=MDA&cHash=810883b9fb88ff046a65443aeca5eced.

214 Clement, "Interview."

Moldova's political landscape had long been riddled with Russian money and political puppets, until a 2014 banking fraud scandal saw roughly $1 billion siphoned out of three Moldovan banks through fraudulent lending and shell-company schemes, triggering a financial crisis.[215] In response to public outcry, Moldovan regulators and law enforcement moved against opaque bank ownership and "raider" schemes by blocking shareholder blocs, unwinding contested shareholdings, and pushing major banks toward more transparent, vetted control.[216] In March 2017, parliamentary leaders said Moldovan officials traveling through Russia were being harassed and "abused" in ways they linked to the ongoing probe, and they accused Russian security-linked actors of obstructing the investigation while Moscow provided no formal response.[217]

In July 2021, the pro-European Party of Action and Solidarity (PAS) — aligned with President Maia Sandu — won snap parliamentary elections and secured an absolute majority, a first in two decades.[218] However, indignation over the country's deep corruption problem, sparked by the banking fraud scandal, helped to create a space for populist rhetoric that blended anti-elite narratives with Russia-friendly positioning, culminating in the Shor Party, which was built around businessman and politician Ilan Shor.[219] The Shor Party also entered parliament in the 2021election, before being banned by the Moldovan constitutional court in 2023 after it had determined the party "sought to overthrow the constitutional order through unlawful means," and that it had been financed by Russia.[220] Shor himself had fled Moldova in 2019 and was convicted in absentia in April 2023 for his role in the bank fraud case.[221]

In October and November 2021, a year after Sandu defeated her Moscow-backed opponent in a 2020 presidential election, Moldova's contract with Gazprom expired, and negotiations over renewal coincided with a dramatic price hike and repeated threats of supply disruption, causing an energy crisis. EU officials at the time said Russia was "bullying" Moldova for the election of pro-Western Sandu.[222] In 2022, Moldova condemned Russia's full-scale invasion of Ukraine and accelerated its EU trajectory, gaining candidacy status on June 23, 2022; but its leadership was also governing under the shadow of Russian energy and economic leverage. Even after Moldova stopped importing Russian gas directly in late 2022, the country's power system remained structurally entangled via Transnistria until 2025, amid

---

215 Tim Whewell, "The Great Moldovan Bank Robbery," *BBC*, June 18, 2015, https://www.bbc.com/news/magazine-33166383.

216 *Republic of Moldova: 2021 Article IV Consultation and Requests for an Arrangement under the Extended Fund Facility and an Arrangement under the Extended Credit Facility-Press Release; Staff Report; and Statement by the Executive Director for the Republic of Moldova* (International Monetary Fund, 2022), https://www.imf.org/en/publications/cr/issues/2022/01/04/republic-of-moldova-2021-article-iv-consultation-and-requests-for-an-arrangement-under-the-511622.2022

217"Moldova Declares Russian Deputy PM Rogozin Persona Non Grata," *Reuters*, August 2, 2017, https://www.reuters.com/article/world/moldova-declares-russian-deputy-pm-rogozin-persona-non-grata-idUSKBN1AI1MY/.

218 "Pro-EU Party in Moldova Wins Clear Majority in Snap Election," *Al Jazeera*, July 13, 2021, https://www.aljazeera.com/news/2021/7/13/pro-eu-party-in-moldova-wins-clear-majority-in-snap-election.

219 Joseph Matveyenko, *Assessing the Impact of Disinformation on Minority Communities in Moldova*, No. 19, Media Forward (Freedom House, 2023), https://freedomhouse.org/sites/default/files/2023-12/fh-pb_19-Disinformation-Moldova-Minorities_Eng-v2.pdf.

220 Vladimir Socor, "Moldova Outlaws Shor's Russophile Party, but the Threat Persists (Part One)," Jamestown, June 21, 2023, https://jamestown.org/moldova-outlaws-shors-russophile-party-but-the-threat-persists-part-one/.

221 "Oligarch Sentenced for Role in Stealing $1B from Moldovan Banks," *AP News*, April 14, 2023, https://apnews.com/article/moldova-oligarch-ilan-shor-bank-fraud-chisinau-israel-maia-sandu-e7c9639f354f27c4975030f7b40629be.

222 Robin Emmott, "Russia Using Gas to Bully Moldova, Says EU," *Reuters*, October 28, 2021, https://www.reuters.com/business/energy/gas-being-weaponised-against-moldova-eu-says-2021-10-28/.

another energy crisis.[223] Moldovan political scientist Sergiu Ostaf noted to interviewers that Russia's leverage during this period helped keep Moldova from fully aligning with other European states on sanctions, reinforcing a lesson in restraint."[224]

Before the full-scale invasion of Ukraine, and besides the overt economic, infrastructure, and territorial tools Russia has leveraged over Moldova, Russia maintained a dense influence ecosystem in Moldova built around language, media, and political proxies. Russian-language television and online outlets dominated large parts of the media market, carrying narratives that framed the EU as morally decadent or economically risky while presenting Russia as a guarantor of stability. These messages were reinforced by pro-Russian political forces and business networks, including figures later associated with the Shor Party.[225] During this period, influence was normalized. It was less about election cycles and more about shaping baseline attitudes; these methods began to shift, however, after Russia's 2022 invasion of Ukraine and Moldova's subsequent EU candidate status.

Results

41 hybrid incidents targeting Moldova between February 2022 and December 2025 were identified in open sources. It is important to note that sustained disinformation campaigns, such as Matryoshka, KillNet, or Storm 1516, were logged as one continuous entry, rather than logging every sub-incident or narrative. Additionally, unique to Moldova is the presence of Russian "peacekeeping" troops in Transnistria, which is logged as a sustained campaign. Analysis indicated that 30 percent of logged hybrid incidents were certainly attributed to Russia, 14 percent were likely attributed to Russia, 44 percent were probably executed by Russia, and 12 percent were suspected to have been conducted by Russia.

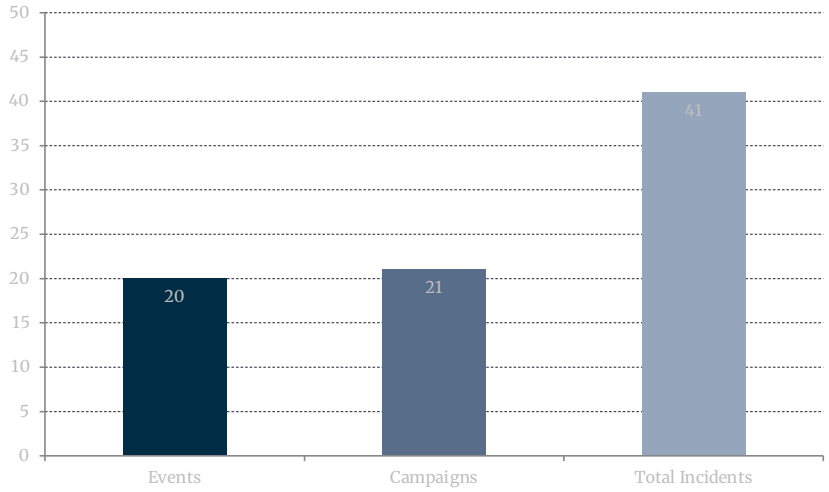
223 "Moldova's Gas Crisis: The Cost of Defying Russia," The Soufan Center, January 17, 2025, https://thesoufancenter.org/intel-brief-2025-january-17/.

224 Sergiu Ostaf, "Interview," 2025.

225 Joseph Matveyenko, Assessing the Impact of Disinformation on Minority Communities in Moldova.

Moldova — Incidents Overview

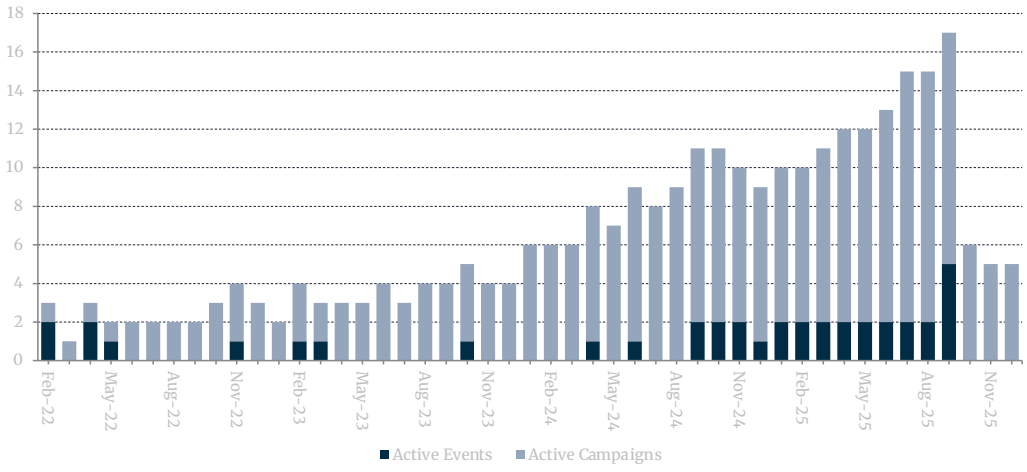
Total counts of Events, Campaigns



These incidents had approximated or exact start dates, allowing an analysis of TTP evolution over time. The peak in incidents occurred in September 2025, the month of Moldova's landmark parliamentary elections.

Moldova — Incidents Over Time

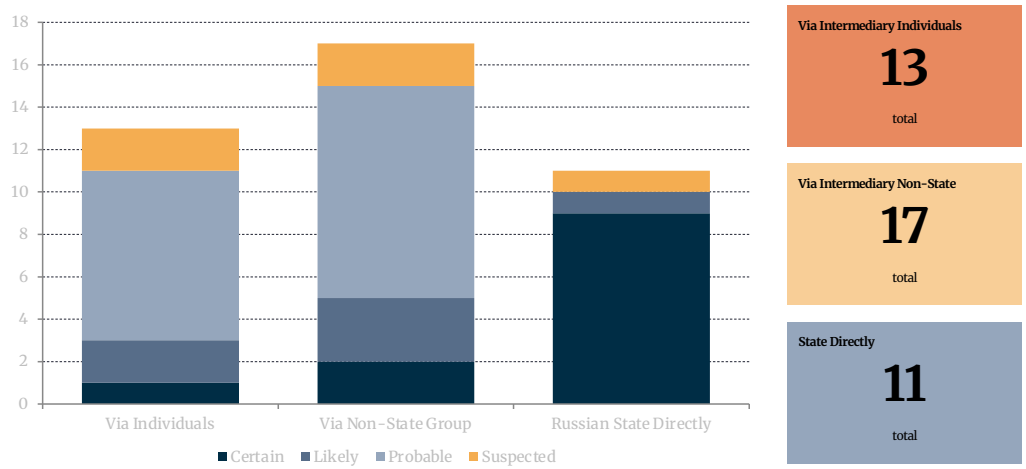
Monthly counts of Active Events and Active Campaigns (2022–2025)



While 'Russia through an intermediary non-state group' was technically identified as the most common actor behind hybrid operations in Moldova (with 17 logged incidents), the other key actors — 'Russia through intermediary individuals' (13 incidents) and 'Russian state directly' (11 incidents) — remained relatively close in frequency, with no single actor clearly standing out. Incidents attributed to 'Russia through intermediary non-state group' rose from 39 percent of incidents logged pre-August 2025 to 60 percent in September 2025 alone.

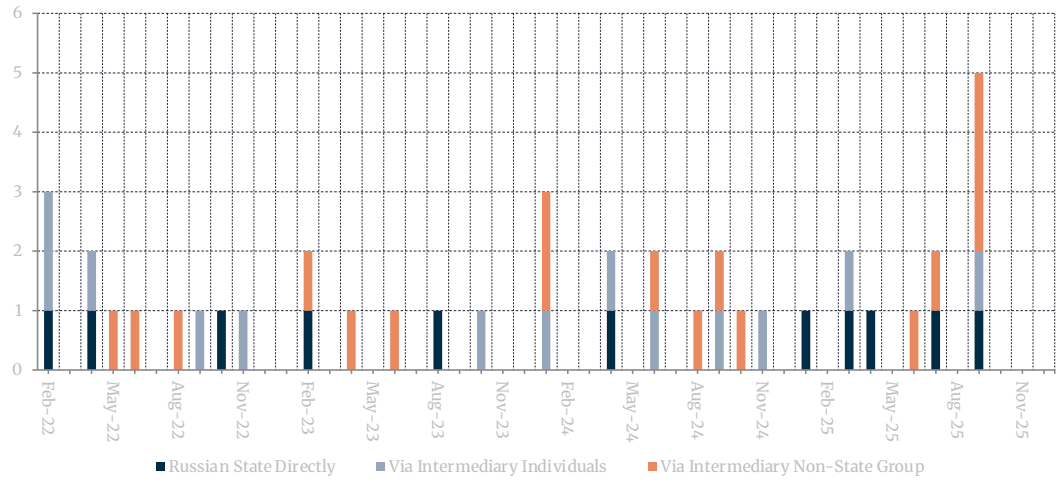
Moldova — Actor Type & Certainty Levels

Incident counts per actor group broken down by attribution certainty



Moldova — Actor Type by Month

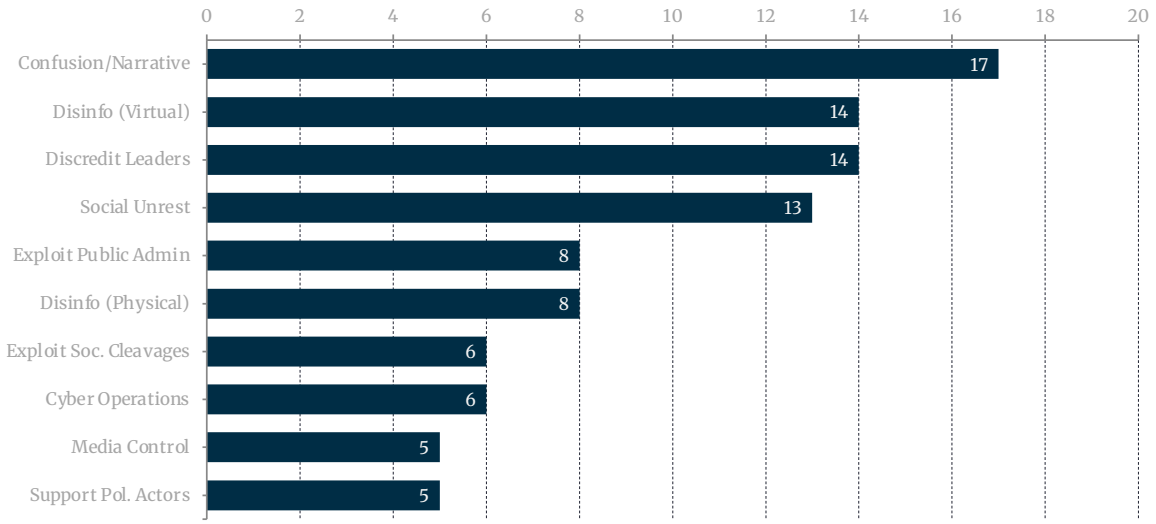
Monthly incident counts by actor type — by start date



The most common tools employed by Russia in hybrid operations targeting Moldova were 'Creating confusion or a contradictory narrative' (17 incidents), ''Disinformation campaigns and propaganda (virtual)' (14 incidents), 'Discrediting leadership and/or candidates' (14 incidents), 'Promoting social unrest' (13 incidents) and 'Exploiting vulnerabilities in public administration (including emergency management)' (8 incidents). In almost all 40 identified incidents, Russia leveraged multiple other tools.

Moldova — Top 10 Tools

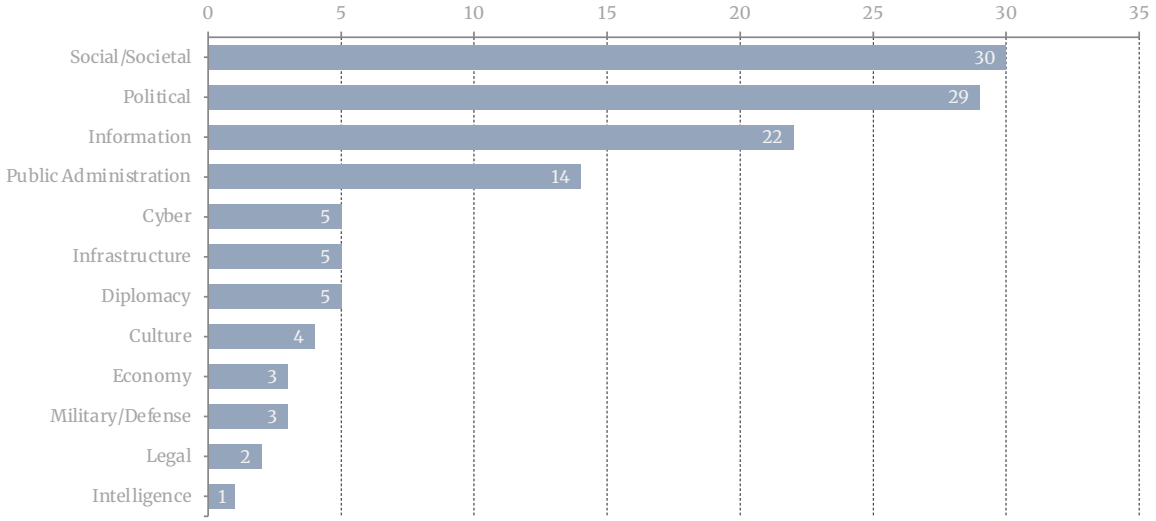
Most frequently used tools — total count across all incidents



The two targeted domain in Moldova was the 'Social/Societal' domain (30 incidents), followed by 'Political' (29 incidents). The 'Information' (22 incidents) and 'Public Administration' (14 incidents) domains were also common.

Moldova — Total Domains

Incident counts aggregated by impacted domain



Findings

Objectives and Effect

In former Soviet Republics, such as Moldova, Russian tactics aim to deter, or in some cases, undermine EU or NATO integration or alignment. Although Moldova borders Romania — a culturally and linguistically similar country already integrated into the EU — Moldovan political scientist Sergiu Ostaf notes that Moldova has remained economically exposed to Russia, even in the years following Russia's invasion of Ukraine. This makes it far more dependent on its eastern neighbor than on its European partners. Apart from the energy sector, in which Russia has historically played a large role, Russians are also well represented in construction and financial services. In fact, Ostaf claims that "the Russian economy is still vibrant and vivid in Moldova."[226]

Many pro-Western Moldovan politicians frame Moscow as an existential security threat; however, this most often refers to Russia's efforts to undermine pro-Western governance, institutional integrity, and public sentiment, rather than to the likelihood of a full-scale kinetic invasion akin to Ukraine, despite the continued presence of Russian "peacekeeping" forces in Transnistria. Ahead of consequential parliamentary elections in September 2025, pro-Western Moldovan Prime Minister Maia Sandu claimed in a speech to European Parliament that "the Kremlin's goal is clear… to capture Moldova through the ballot box, to use us against Ukraine, and to turn us into a launchpad for hybrid attacks on the European Union."[227] Since Moldova is neither a NATO member nor, at present, more than an EU candidate, Russia need not occupy Moldovan territory by force, particularly if it can undermine democratic governance and pro-Western alignment through hybrid tactics. However, full membership in either organization would likely constitute a red line for Moscow and could trigger an escalation toward more overt "coercive" measures, including intensified leverage over Chișinău's economic and infrastructure dependencies — areas where Moldova would have limited recourse — even as it has worked to reduce its dependence on certain Russian sectors, such as energy. Former CIA analyst Peter Clement offered an important assessment into viewing Russian hybrid operations in the East, which he claims, "at their core, are a signaling mechanism to demonstrate Russia's opposition to Western attempts to influence its near abroad."[228]

Russia's objectives in Moldova can be seen quite clearly in the domains it targets, with the 'Political', 'Social/Societal', 'Information', and 'Public Administration' being the most targeted domains in the database by far. The most common tools utilized by Russia — 'Creating confusion or a contradictory narrative', 'Disinformation campaigns and propaganda (virtual)', 'Promoting social unrest' and 'Discrediting leadership and/or candidates' — are also extremely telling of Russia's objectives to reduce public confidence and political cohesion around a pro-EU trajectory. Russia not only seeks to influence and consolidate a pro-Russian base — which in Moldova largely consists of older, more conservative, and predominantly Russian-speaking segments of the population — but also aims to sow discord and erode trust in institutions, particularly democratic ones. As retired CIA Operations Officer Edward Bogan

226Ostaf, "Interview."

227"President Maia Sandu Says Russia Wants to Turn Moldova against Europe," European Parliament, September 9, 2025, https://www.europarl.europa.eu/news/en/press-room/20250905IPR30176/president-maia-sandu-says-russia-wants-to-turn-moldova-against-europe.

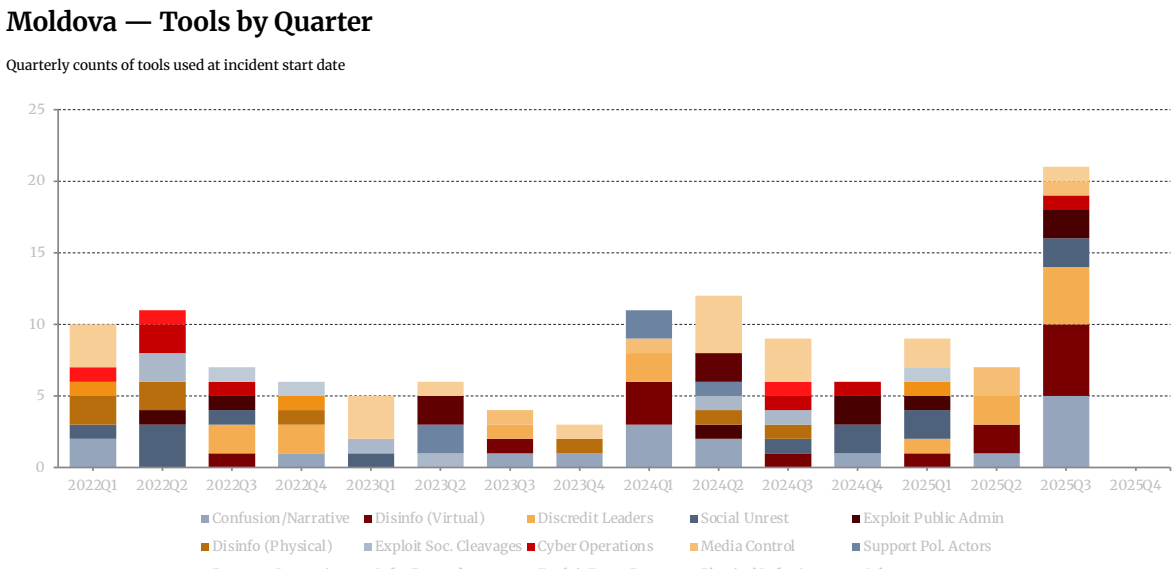
228Clement, "Interview."

notes, “steering chaos is the goal in itself.”[229]

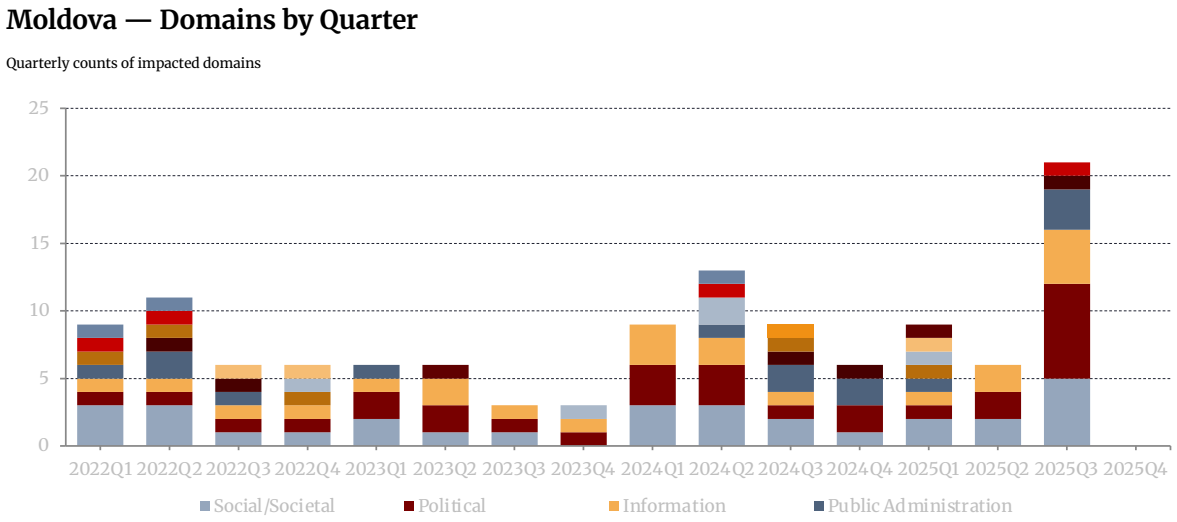
Trends

Trend analysis reveals a clear evolution in the nature of Russian hybrid activity in Moldova, marked by a transition from sporadic, event-driven interference to sustained, campaign-style operations. Early activity in 2022 and 2023 was characterized by short bursts with limited continuity, whereas later periods (2024-2025) showed increasingly prolonged “active” campaigns rather than shorter events. This implies that Russia was maintaining an infrastructure of influence, with particular surges in 2024 and 2025.

This trend is further illustrated by breaking down the most frequently used tools on a quarterly basis. As shown in the data there are clear spikes in Q2 of 2024 (April–June) and Q3 of 2025 (July–September), as well as a large number of incidents during Q1 of 2024 (January–March). During all three periods, the predominant tools centered on disinformation, narrative confusion, and the undermining of pro-Western political leaders (or the support of pro-Russian politicians). The domains targeted during these same quarters reflect a similar pattern. In both Q1 and Q2 of 2024 and Q3 of 2025, the ‘Political’ domain was the most frequently targeted, with the ‘Information,’ ‘Social/Societal’ and ‘Public Administration’ domains also consistently affected across both periods.



229 Bogan, “Interview.”



The surges in active campaigns in 2024–2025, and the corresponding spikes in quarterly activity, coincided with two major national elections in Moldova. The presidential election occurred on October 20, 2024, and was paired with a referendum on future EU membership. The more consequential contest took place on September 28, 2025, when parliamentary elections took place, determining the control of the legislature and the direction of government policy. Crucially, in both cases, but especially in 2024, analysis showed a significant "runway" into the election period, rather than spikes coinciding with actual election months or weeks. This is consistent with Russia's attempts to shape and confuse election narratives ahead of the actual vote. It should also be noted that in June 2024, Moldova and the EU officially began accession negotiations.[230] While overall actor attribution is relatively balanced between direct state action and 'Russia through intermediary actors', incidents attributed to 'Russia through intermediary non-state groups' rise sharply during the most politically consequential moments, particularly around the September 2025 parliamentary elections.

A handful of recurring Russian-aligned campaigns accounted for much of the sustained runway into both votes, combining "narrative manufacturing" with episodic surges around key milestones. Operation MiddleFloor emerged in August 2024 and relied on spoofed emails and forged or impersonated institutional communications to seed controversy — well ahead of the October 2024 referendum/presidential election window.[231] In 2025, Matryoshka (often described as part of the broader "Overload"-style ecosystem) ran rapid, high-volume disinformation bursts aimed at President Sandu and EU-Moldova engagement moments. Before Matryoshka's foray into Moldova, it had been active for some time in other case study countries like France and Germany.[232] Over the same period, analysts described Storm-1516, a similar network, active in Moldova since at least August 2023, as a durable

230 "EU and Moldova Forge Deeper Ties at Historic First Summit in Chișinău," Directorate-General for Enlargement and Eastern Neighbourhood, July 4, 2025, https://enlargement.ec.europa.eu/news/eu-and-moldova-forge-deeper-ties-historic-first-summit-chisinau-2025-07-04_en.

231"Operation MiddleFloor: Unmasking the Disinformation Campaign Targeting Moldova's National Elections," Check Point Blog, October 9, 2024, https://blog.checkpoint.com/research/operation-middlefloor-unmasking-the-disinformation-campaign-targeting-moldovas-national-elections/.

232 Eva Maitland et al., "Russia's Matryoshka Propaganda Machine Picks New Target, Pushing 39 False Claims Against Moldova Over Past Three Months," *NewsGuard*, July 15, 2025, https://www.newsguardtech.com/special-reports/russia-matryoshka-propaganda-moldova.

"information manipulation set" using fabricated personas, counterfeit "evidence" and coordinated amplification that was repeatedly repurposed for election-focused objectives.[233] The R-FBI campaign also emerged as an enabling influence operation (masquerading as an NGO) that helped drive and amplify anti-Sandu/PAS content during mid-2025 (June–September), overlapping operationally with Storm-1516.[234] Alongside influence operations, pro-Russian hacktivist pressure — most prominently through the group Killnet — periodically threatened or conducted politically framed DDoS-style disruption against Moldovan targets, adding a cyber-nuisance layer to the broader interference environment.[235]

Across these campaigns, as well as smaller scale ones reported in the TTP database, elections were consistently framed as pre-determined or rigged, externally controlled by the EU, NATO or "the West," and institutionally compromised. Russia also tailored its narrative to the highly religious, and often conservative culture in Moldova. Campaigns frequently amplified anti-LGBTQ+ narratives and falsely overstated links between the EU and the LGBTQ+ community. One campaign, for example, spread disinformation claiming Moldovan ministries would be required to display the LGBTQ+ flag outside state buildings. As for religious institutions, not only did several campaigns, such as Matryoshka and Storm 1516, accuse President Sandu and her Party of Action and Solidarity (PAS) of persecuting the Orthodox church, the Orthodox church itself was utilized to disseminate pro-Kremlin propaganda. In one campaign, ahead of the EU referendum and presidential election, Moldovan Orthodox clergy were allegedly bribed by Russian officials to disseminate anti-Sandu and PAS messaging to churchgoers.[236]

These campaigns also crucially worked to discredit and undermine pro-Western politicians, framing them as puppets of the West, unable to govern, corrupt, and known to rig elections. The sheer volume of these TTPs is intended to flood Moldova's information sphere, exhausting the recipient. Overall, the goal is to not only influence voters in their favor, but more importantly, to prime voters to contest unfavorable (pro-Western) election results, or to distrust the election process enough that they will not bother showing up to cast their vote on election day. Moldovans are not entirely inoculated to this messaging. Ostaf notes that the 2024 EU referendum would have failed if not for the votes from Moldovans living abroad.[237]

In addition to these long-running campaigns, which were at their most active in the later period of observational study (2024 and 2025), Russia also used short but coordinated cyber and physical attacks surrounding important dates. For example, on September 28, 2025, during the parliamentary election, a large-scale cyber campaign involving tens of millions of automated requests again targeted election-related government systems, coinciding with a surge in coordinated disinformation questioning

233 Eva Maitland et al., "New Kremlin-Linked Influence Campaign Targeting Moldovan Elections Draws 17 Million Views on X and Infects AI Models," *NewsGuard*, September 26, 2025, https://www.newsguardtech.com/special-reports/kremlin-linked-influence-campaign-targets-moldovan-elections-infects-ai-models.

234 Saman Nazari et al., "Still Marching on(Line): How R-FBI Targets Moldova's Elections," Alliance4Europe, September 26, 2025, https://alliance4europe.eu/still-marching-online-how-r-fbi-targets-moldovas-elections.

235 Daryna Antoniuk, "Russia's Cyberattacks Aimed at 'Destabilizing' Moldova, PM Says," The Record, February 9, 2023, https://therecord.media/russias-cyberattacks-aimed-at-destabilizing-moldova-pm-says.

236 Christian Lowe et al., "Holy War: How Russia Recruited Orthodox Priests to Sway Moldova's Voters," Reuters, September 26, 2025, https://www.reuters.com/investigations/holy-war-how-russia-recruited-orthodox-priests-sway-moldovas-voters-2025-09-26/.

237 Ostaf, "Interview."

the vote's legitimacy.[238] Cyber-security expert Justin Novak, noted that "in the lead-up to the EU referendum, the level of cyber-attacks [in Moldova] was unprecedented"[239] Similarly, in October 2024, acts of vandalism against state buildings were linked to Russian-connected clandestine networks.[240]

Contrary to the influx of sustained campaigns surrounding elections that characterized 2024 and 2025, the earlier period of the observational study (2022 and 2023), which took place in the immediate aftermath of Russia's invasion of Ukraine in February, appeared in the analysis to be more episodic: operations tended to surface in short, coordinated bursts designed to stress institutions and shape perceptions at politically sensitive or critical moments. This early phase was defined by Moldova's acceleration toward Europe. In June 2022, when EU candidacy was announced as a response to Russia's invasion of Ukraine, Moldova experienced a wave of coordinated bomb threats targeting public institutions.[241] In parallel, actors such as Killnet used cyber campaigns (most notably repeated DDoS waves and "leaks"-style information exploitation) throughout 2022 and 2023 to generate disruptions that reinforced Kremlin-amplified narratives of incompetence.[242]

In October 2022, Russian state-owned Gazprom sharply reduced gas deliveries to Moldova creating a major energy emergency. In parallel, the pro-Russian Shor Party organized anti-government protests explicitly tied to inflation and energy prices.[243] Together, these cases illustrate the early period "burst logic," which followed a very clear logic: use energy/economic disruption to create a grievance, then encourage mobilization against pro-European leadership, right when the EU trajectory becomes more concrete. It should be noted that although incidents logged as exploiting economic or infrastructure dependency, such as the Gazprom incident, represent a smaller share of the dataset, economic and energy TTPs functioned as the bedrock of much of Russian hybrid activity in Moldova.

In December 2023, the European Council officially declared it would start accession negotiations with Moldova. An intensification of Russian hybrid TTPs occurred two months later in February 2023, when two incidents were logged in the 'coercion' phase — the only instances of that phase in the Moldova case study. Moldovan authorities reported that the Ukrainian intelligence services had intercepted a Kremlin-orchestrated plan to overthrow the pro-European government, allegedly involving militarily saboteurs tasked with attacking state buildings and exploiting unrest to destabilize the state.[244] Also in February, senior Russian officials escalated their pressure on Moldova's pro-European government; Foreign Minister Sergey Lavrov warned on February 2 that Moldova could face the "same fate

238 Kate Tsurkan, "Moldova Casts Blame on Russia for Attempts to Disrupt Pivotal Parliamentary Elections," The Kyiv Independent, September 28, 2025, https://kyivindependent.com/moldovas-election-infrastructure-targeted-in-mass-cyber-attacks-during-consequential-parliamentary-elections/.

239 Justin Novak, "Interview," 2025.

240 "Moldova Accuses Moscow In Wave Of Vandalism In Capital Ahead Of Vote," *Radio Free Europe/Radio Liberty*, September 28, 2024, https://www.rferl.org/a/moldova-vandalism-russia-trained/33138585.html.

241 Madalin Necsutu, "Moldovans Face Bomb Threats and Cyberattacks," Institute for War and Peace Reporting, September 5, 2022, https://iwpr.net/global-voices/moldovans-face-bomb-threats-and-cyberattacks.

242 Daryna Antoniuk, "Russia's Cyberattacks Aimed at 'Destabilizing' Moldova, PM Says."

243 Alexander Tanas, "Thousands in New Moldova Anti-Government Protest," *Reuters*, October 23, 2022, https://www.reuters.com/world/europe/thousands-new-moldova-anti-government-protest-2022-10-23/.

244 "Moldovan Police Say They Foiled Russian-Backed Unrest Plot," *Radio Free Europe/Radio Liberty*, March 12, 2023, https://www.rferl.org/a/moldova-police-foil-russian-plot-unrest/32314304.html.

as Ukraine" if President Maia Sandu pursued closer ties with the West.[245] Later that month, Kremlin spokesman Dmitry Peskov accused Moldovan leaders of stoking "anti-Russian hysteria," while Russian lawmaker Sergey Mironov threatened retaliation if Moldova moved against Transnistria, framing reintegration efforts as a nationalist conspiracy.[246] On February 21, President Vladimir Putin revoked a 2012 decree that had referenced Moldova's sovereignty and a peaceful resolution for Transnistria, a symbolic step that further called Moldova's territorial integrity into question.[247]

Response

In 2024, Moldova's response to Russian influence campaigns was defined by early, public attribution and political signaling: as the presidential election and EU-referendum vote approached, President Sandu and other officials repeatedly warned that the ballots were facing an "unprecedented" campaign of outside interference — explicitly framing this as a Russian effort to derail Moldova's EU path and preparing the public for manipulation tactics (vote-buying, disinformation, and disruption).[248] The European Parliament later described the 2024 vote as occurring amid "manipulative interference," illicit financing, disinformation, and cyber-attacks — reinforcing Chișinău's claims and validating the government's decision to treat interference as its primary national-security issue.[249] In 2025, Moldova paired its transparency with aggressive attempts to disrupt the machinery behind Russian interference. Police and prosecutors carried out large-scale raids and detentions against alleged Russian-backed vote-buying networks and plans to foment mass unrest.[250] Moldova's election authorities also took preemptive legal steps, such as excluding multiple pro-Russian parties from the ballot over suspected illegal financing. Though controversial, it was central to the state's "deny the platform" approach to foreign-backed political capture.[251] Moldovan officials continuously publicly quantified the scale of interference, providing as many actors, costs, and statistics as possible. This included publicly claiming that Russian agents spent about €200 million to influence the 2024 election/referendum via vote-buying.[252]

By late 2025 and into 2026, external assessments also emphasized Moldova's growing capacity for strategic communication and interagency coordination, including the expanding role of the govern-

245 Iulian Ernst, "Russian Lawmakers Warn Moldova's Nato Aspirations May Lead to Its Destruction," IntelliNews, January 25, 2023, https://www.intellinews.com/russian-lawmakers-warn-moldova-s-nato-aspirations-may-lead-to-its-destruction-267920/.

246 "Kremlin Accuses Moldova Of 'Anti-Russian Hysteria,'" *Barron's*, February 20, 2023, https://www.barrons.com/news/kremlin-accuses-moldova-of-anti-russian-hysteria-aaf36f1b.

247 Tom Balmforth and Alexander Tanas, "Moldova's Sandu Decries 'unprecedented' Meddling as EU Referendum Goes to Wire," *Reuters*, October 20, 2024, https://www.reuters.com/world/europe/moldova-votes-election-eu-referendum-shadow-alleged-russian-meddling-2024-10-20/.

248 Tom Balmforth and Alexander Tanas, "Moldova's Sandu Decries 'unprecedented' Meddling as EU Referendum Goes to Wire."

249 European Parliament, "2023 and 2024 Reports on Moldova," June 18, 2025, https://www.europarl.europa.eu/doceo/document/TA-10-2025-0131_EN.html.

250 Dan Peleschuk, "Moldovan Police Launch Sweeping Raids over Alleged Russian Meddling," *Reuters*, September 22, 2025, https://www.reuters.com/world/moldovan-police-raid-over-100-targets-russian-meddling-investigation-2025-09-22/.

251 Reuters, *Moldova Bans Another Pro-Russian Party from Sunday's Vote*, September 27, 2025, https://www.reuters.com/world/moldova-bans-another-pro-russian-party-sundays-vote-2025-09-27.

252 "Moldova Says Russian Agents Spent 200 Mln Euro to Rig Votes Last Year," *Reuters*, April 2, 2024, https://www.reuters.com/world/europe/moldova-says-russian-agents-spent-200-mln-euro-rig-votes-last-year-2025-04-02/.

ment's Strategic Communication/Counter-Disinformation structures and tighter coordination between law enforcement and anti-corruption bodies to counter illicit financing networks.[253] Moldova's ability to publicize the bulk of Russian interference attempts, paired with its attempts to formalize institutions dedicated to countering Russian hybrid TTPs, was integral to its ability to claim victory in 2025, securing a path ahead for a European future.

253 Matthew Schaaf and Andrew Rogan, "A Lesson in Resilience: Moldova's Resistance to Election Interference," International Foundation for Electoral Systems, December 17, 2025, https://www.ifes.org/publications/lesson-resilience-moldovas-resistance-election-interference.

vi. Georgia

Introduction

When EU candidate status was granted to Georgia in December 2023, in response to Russia's invasion of Ukraine, tens of thousands of Georgians poured into the streets of Tbilisi and celebrations stretched across days — an emphatic public signal that the country's "European choice" had deep social legitimacy.[254] A 2023 poll found that 89 percent of Georgians either "fully support" or "somewhat support" joining the EU.[255] By June 2024, however, that pro-European momentum collided with the ruling party's, Georgian Dream's, increasingly illiberal trajectory: after months of domestic unrest over "Russian-style" legislation — most notably, the "foreign agents" law (formally the Law on Transparency of Foreign Influence), which requires civil society organizations and media outlets that receive more than 20 percent of their annual funding from abroad to register as "pursuing the interests of a foreign power" — EU institutions concluded that Georgia's accession process was de facto halted. The rupture widened after the October 2024 parliamentary elections, when Georgian Dream further consolidated power amid widespread allegations of irregularities and "rigging."[256] Soon after, the Georgian government announced it would pause efforts to start accession negotiations, effectively freezing the EU track through 2028, facilitating a political crisis with wide-scale protests, which are still ongoing as of January 26, 2026, marking 425 days of non-stop demonstrations.[257] Multiple international observers, such as Human Rights Watch, have reported on the use of "brutal violence" against, largely, peaceful protestors.[258] Georgia's political trajectory, however, cannot be discussed without the context of Russo-Georgian relations, particularly Russia's sustained use of hybrid TTPs against Georgia.

In April 2008, NATO stated that Georgia and Ukraine would become members of the alliance, even as it deferred a concrete Membership Action Plan. Within weeks, Russia moved to consolidate control over Georgian breakaway territories Abkhazia and Tskhinvali/South Ossetia. In August 2008, the Georgian military attempted to reclaim Tskhinvali/South Ossetia, leading to a swift and overwhelming Russian military response. The conflict then expanded beyond the breakaway regions, with Russian forces advancing into Georgian territory, leading to a full-out military conflict. The five-day war left Georgia with contested borders and diminished prospects for NATO membership, while Russia solidified its presence and influence in Abkhazia and Tskhinvali/South Ossetia, which constitute 20 percent of internationally recognized Georgian territory. The ensuing years saw continued Russian military and economic entrenchment in these regions, with agreements that effectively integrated them into Russia's sphere of influence, despite nominal recognition of their independence.

---

254 "Georgians celebrate EU candidate status," *Le Monde*, December 15, 2023, https://www.lemonde.fr/en/international/article/2023/12/15/georgians-celebrate-eu-candidate-status_6347639_4.html.

255 "IRI Georgia Poll Finds Support for EU Accession High, Weariness of Russian Presence, Lack of Faith in Political Parties," International Republican Institute, April 25, 2023, https://www.iri.org/news/iri-georgia-poll-finds-support-for-eu-accession-high-weariness-of-russian-presence-lack-of-faith-in-political-parties/.

256 "Georgian Dream or Democratic Nightmare? The Struggle for Democracy Amid Voter Fraud and Russian Interference," The Soufan Center, October 30, 2024, https://thesoufancenter.org/intelbrief-2024-october-30/.

257 Felix Light, "Protesters Clash with Georgian Police over Government's EU Application Delay," *Reuters*, November 29, 2024, https://www.reuters.com/world/europe/georgia-says-it-will-not-enter-eu-membership-talks-until-2028-snub-brussels-2024-11-28/.;

258 "Georgia: Brutal Police Violence Against Protesters," Human Rights Watch, December 23, 2024, https://www.hrw.org/news/2024/12/23/georgia-brutal-police-violence-against-protesters.

For at least a decade, bilateral relations between Russia and Georgia remained strained, and public perception of Russia has remained quite negative by and large. In October 2012, the party that had governed during and after the 2008 war — widely criticized for its illiberalism and human rights abuses — lost parliamentary elections to the Georgian Dream (GD) coalition led by billionaire Bidzina Ivanishvili, who campaigned on easing tensions with Moscow, and whose party positioned itself as a "liberal social-democratic party."[259] Ivanishvili amassed substantial wealth in Moscow during the 1990s and held a significant stake in Russia's state-owned Gazprom. Even after stepping down as Prime Minister, he continues to wield outsized influence over GD, earning a reputation as Georgia's "shadow ruler."[260]

After securing a second term in 2016, GD increasingly prioritized power retention, saw liberal and pro-Western party figures peel away, and adopted rhetoric that grew more distant — and sometimes more confrontational — toward Western partners, while turning to conservative messaging. This began to be reflected in concrete policies, with GD's push to constitutionally define marriage as a union between a woman and a man in 2017, acting as an early marker of the "traditional values" politics GD would wield.[261] Mariam Tokhadze, independent Georgian security expert, also points out that far-right violence against participants and journalists at the 2021 Tbilisi Pride march — alongside the government's failure to protect them and its hesitance to pursue accountability — further marked GD's shift towards conservativism.[262]

Even before Russia's full-scale invasion of Ukraine, Georgia's domestic political shift played out alongside Russian coercive and information pressure. In June 2019, mass protests erupted over perceived Russian interference — sparked in part when a Russian lawmaker addressed Georgia's parliament from the speaker's seat. After widespread protests broke out in Tbilisi following the incident, Russian President Vladimir Putin ordered a suspension of passenger flights from Russia to Georgia, framing it as a protective measure while effectively leveraging Georgia's economic tourism dependence.[263] A few months later, in October 2019, Georgia was hit by a large-scale disruptive cyber-attack that defaced or knocked offline thousands of websites across government, courts, media, NGOs, and businesses; the UK and U.S. publicly attributed the operation to Russia's GRU, stating it was intended to undermine Georgia's sovereignty, sow discord, and disrupt everyday life. Analysts at the Digital Forensic Research Lab (DFRLab) documented how the incident was followed by a broader Russian-linked propaganda and online disinformation effort aimed at shaping public interpretation and deflecting blame.[264]

Russian influence operations were, at that point, already entrenched into the Georgian information-sphere and worked to make "traditional values" politics and anti-West framing more resonant and politically usable. Russian disinformation targeted Georgia repeatedly and exploited local conservative and religious sentiment — often by stoking hostility toward LGBTQ communities and human rights

259 Nino Samkharadze, "Georgian Dream's Populist Conservatism: Fight to Legitimise and Hold On to Power," *GIP*, no. 68 (March 2017), https://gip.ge/publication-post/georgian-dreams-populist-conservatism-fight-to-legitimise-and-hold-on-to-power/.

260Coyle, *Russia's Border Wars and Frozen Conflicts*.

261Coyle, *Russia's Border Wars and Frozen Conflicts*.

262 Mariam Tokhadze, "Interview," 2025.

263 Margarita Antidze and Andrew Osborn, "Georgia and Russia Trade Blame over Unrest as Crisis Brews," *Reuters*, June 21, 2019, https://www.reuters.com/article/world/georgia-and-russia-trade-blame-over-unrest-as-crisis-brews-idUSKCN1TM0O0/.

264 "Russia's 2019 Cyber Attack against Georgia Followed by Full-Spectrum Propaganda Effort," DFRLab, April 23, 2020, https://dfrlab.org/2020/04/23/russias-2019-cyber-attack-against-georgia-followed-by-full-spectrum-propaganda-effort/.

defenders and casting Western alignment as culturally corrosive.[265] In 2018, for example, Putin publicly amplified claims that a U.S. supported public health facility was a cover for U.S. biological weapons work.[266] In early 2019, Facebook/Meta announced it had removed a Russia-originated network that operated through fake or misleading pages and accounts and was linked to staff of Russian state outlet *Sputnik*, and pushed anti-NATO and anti-West narratives.[267] GD was able to capitalize on these narratives to gradually consolidate power, creating space to cautiously ease relations with Moscow despite Russia's deeply negative reputation among many Georgians.

After Russia's full-scale invasion of Ukraine, Russian and GD messaging increasingly evolved — often in tandem — to frame closer alignment with the West as an unnecessary provocation of Russia, even if this storyline had long featured in Russia's playbook. Georgia, in many ways, was an early testing ground for Russian hybrid TTPs, even earlier than many other post-Soviet spaces. As a result, Georgia's domestic political trajectory can serve as a cautionary tale for other interested actors.

Results

30 hybrid incidents targeting Georgia were identified in open sources between February 2022 and December 2025. Sustained influence campaigns were logged as one continuous entry, meaning 18 events and 12 campaigns were logged. Additionally, unique to Georgia is the occupation of Tskhinvali/South Ossetia and Abkhazia. Illegal detentions of Georgian citizens in these breakaway regions, as well as *borderization* [268] incidents, were logged as one continuous entry, with a year-by-year breakdown in the incident summary. This approach reflected uneven incident-level reporting in open sources and underscored the sustained, campaign-like nature of these activities as part of Russia's ongoing occupation of internationally recognized Georgian territory.

The peak in incident start dates is in the first month of the observation period, with the highest number of "new" entries (five) occurring in February 2022; however, the number of active incidents reached and held a high of 11 starting in October 2023 and peaked December 2023. These incident entries had approximate or exact end dates (or were ongoing), allowing the authors to also map incidents targeting Georgia each month that the incidents were still active in the studied period. Additionally, the five "new" entries occurring in February 2022 all reflect campaigns that were active before this study's observational period (February 2022 – December 2025) but are logged as a February 2022 start date for coding consistency.

265 Isabella Wilkinson and Tamar Dekanosidze, "Georgia Must Bolster Resilience to Information Warfare," Chatham House, March 8, 2023, https://www.chathamhouse.org/2022/03/georgia-must-bolster-resilience-information-warfare.

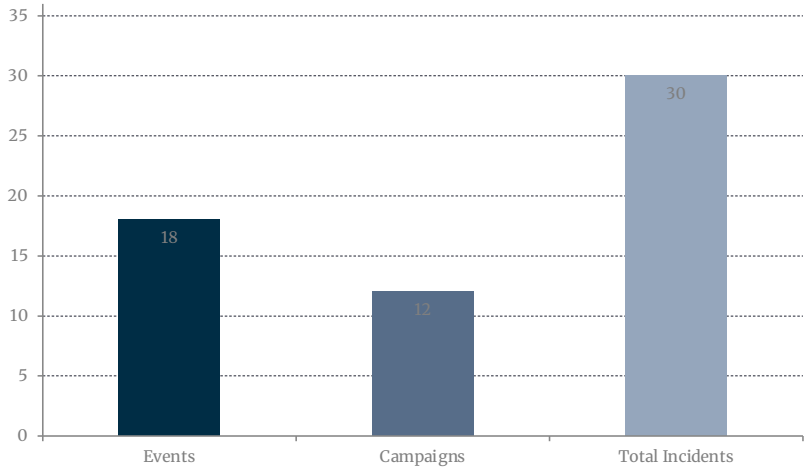
266 "Vladimir Putin Speaks Saakashvili, 'Lugar Lab,'" Civil Georgia, October 19, 2018, https://civil.ge/archives/259804.

267 Nathaniel Gleicher, "Removing Coordinated Inauthentic Behavior from Russia," Meta, January 17, 2019, https://about.fb.com/news/2019/01/removing-cib-from-russia/.

268 The gradual, often state-driven process of transforming an administrative line or ceasefire boundary into a de facto international border through the installation of physical barriers and control measures — such as fences, barbed wire, boundary markers/signage, patrols, checkpoints, and restrictions on movement — typically in and around contested territories, like Abkhazia and Tskhinvali/South Ossetia.

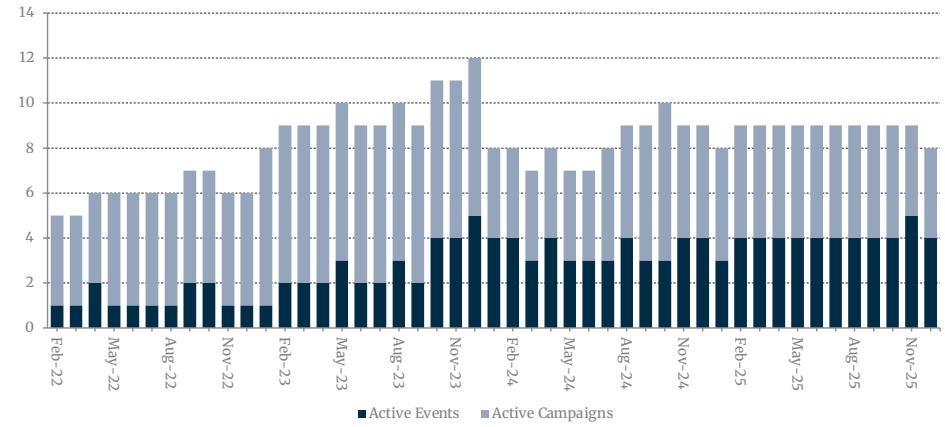
Georgia — Incidents Overview

Total counts of Events, Campaigns



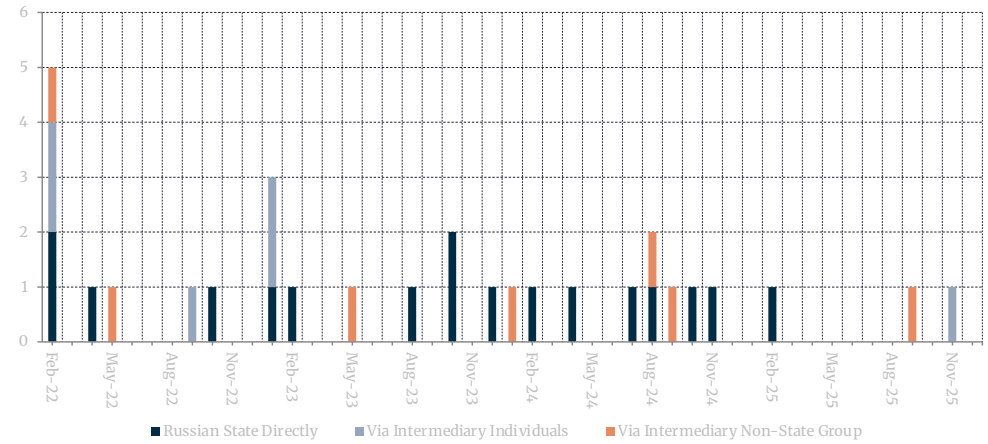
Georgia — Incidents Over Time

Monthly counts of Active Events and Active Campaigns (2022–2025)

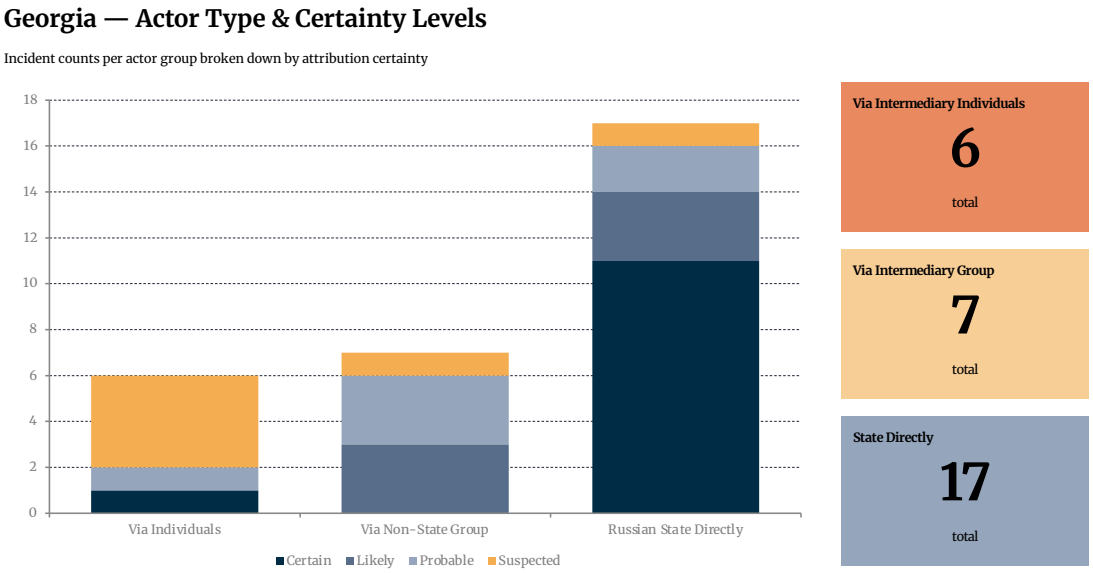


Georgia — Actor Type by Month

Monthly incident counts by actor type — by start date



The ‘Russian state directly’ was identified as the most common actor behind hybrid operations in Georgia (with 17 incidents, approximately 57 percent of all incidents). The other key actors ‘Russia through intermediary non-state group’ (seven incidents) and ‘Russia through intermediary individuals’ were noticeably less common in the data set. 40 percent of logged hybrid incidents were certainly attributed to Russia, while all other incidents were equally distributed among likely, probable, and suspected attribution, with 20 percent respectively. Analysis indicated that certainty is heavily concentrated in direct state attributions, which account for approximately 92 percent of all ‘certain’ cases.

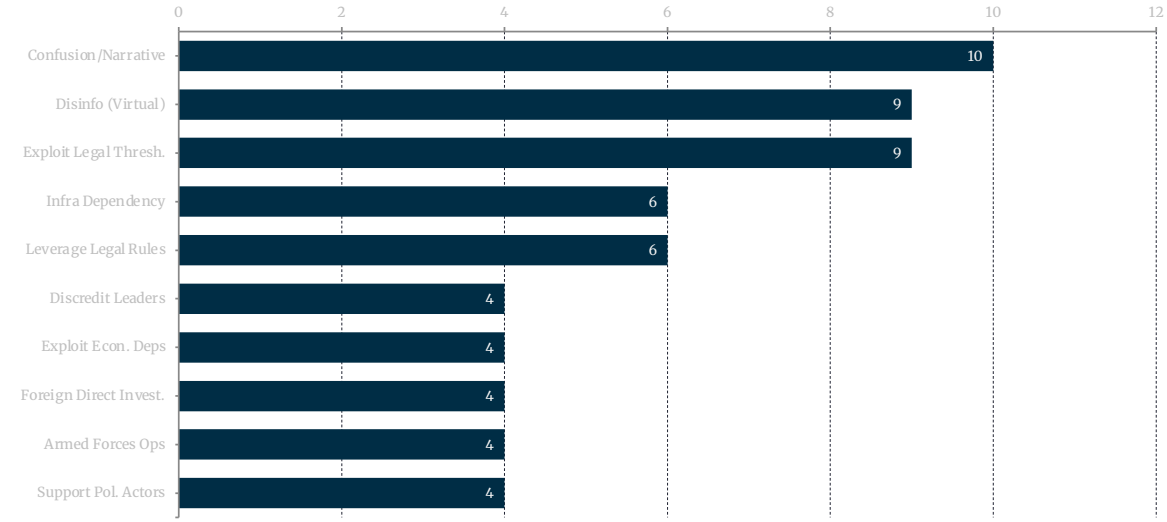


The most common tools employed by Russia in hybrid operations targeting Georgia were ‘Creating confusion or a contradictory narrative’ (10 incidents), ‘Disinformation campaigns and propaganda (virtual)’ (9 incidents), ‘Exploiting thresholds, non-attribution, gaps and uncertainty in the law’ (9 incidents), ‘Creating and exploiting infrastructure dependency (including civil-military dependency)’ (6 incidents), and ‘Leveraging legal rules, processes, institutions and arguments’ (6 incidents). In almost all 30 identified incidents, Russia leveraged multiple other tools.

The most targeted domains in Georgia were ‘Political’ (15 incidents), ‘Social/Societal’ (14 incidents), ‘Information’ (12 incidents), and ‘Legal’ (12 incidents). However, Russia targeted all but one domain (‘Space’) in Georgia.

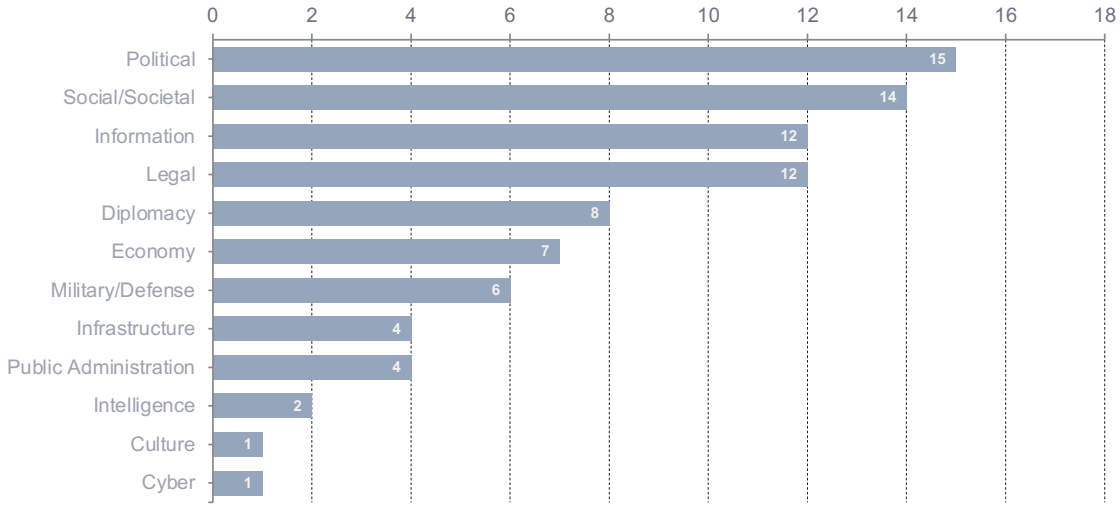
Georgia — Top 10 Tools

Most frequently used tools — total count across all incidents



Georgia — Total Domains

Incident counts aggregated by impacted domain



Findings

Objectives and Effect

In former Soviet republics such as Georgia, Russian hybrid tactics aim to deter — or at a minimum slow — EU and NATO integration or alignment by shaping the political incentives and perceived risks associated with a pro-Western trajectory. In Georgia, this objective operates in a context already defined by Russia's occupation of Abkhazia and Tskhinvali/South Ossetia and the enduring memory of the 2008 war. Some in Georgia, including Georgian cybersecurity expert, Tamar Kapanadze, argue that despite complacency from GD, Russia could still seek more overt control over Georgia, even if it relies heavily on indirect tools in the interim, there is no one consensus.[269] Some, however, believe that Russia can often achieve its core aims just by sustaining a favorable status quo in Tbilisi that delays Western integration and preserves Russian leverage. Mariam Tokhadze, an independent Georgian security expert, contends that Moscow's preference in Georgia is "a comfortable entity in their close proximity that allows things like access to the Black Sea," or other economic benefits. She notes that unlike in Ukraine, Russia can achieve its objectives from a friendly government like GD, arguing that Russia does not need to use force to bring Georgia "back into its empire."[270]

GD's friendliness towards Russia, in part, comes from Georgia's economic dependence on its neighbor. A Georgian security expert (name withheld) noted that Russia has often used economic tools — such as travel restrictions and trade pressure — as mechanisms that can be activated to impose costs or signal red lines.[271] Likewise, Tokhadze noted, "Russians have an [economic] foothold here, and I don't know how we can work around that."[272] The aforementioned anonymous Georgian security expert argues that Russia, at present, does not need to apply economic leverage overtly because Georgians remembered how quickly Moscow could impose costs, like Vladimir Putin's June 2019 order suspending passenger flights from Russia to Georgia, and the earlier seven-year embargo (2006–2013) on Georgian wine and mineral water, which had devastating effects on Georgia's economy.[273] The expert argued that Georgia's economic exposure also grew through more indirect channels after 2022, including the influx of Russians and the expansion of Russian business activity; Russian citizens registered roughly 13,000 legal entities in Georgia in 2023, widely reported as a record.[274]

Russia's occupation of Georgian territory also serves as a coercive tool. Illegal detentions, border incidents, and Russian infrastructure projects are closely observed in Georgia. Tokhadze explains that outside observers often "don't realize how close [the occupied territories] are to the very center of

269 Tamar Kapanadze, "Interview," 2025.

270 Kapanadze, "Interview."

271 Georgian Security Expert (name withheld), "Interview," 2025.

272 Tokhadze, "Interview."

273 "Putin Orders Suspension of Passenger Flights from Russia to Georgia," Reuters, June 21, 2019, https://www.reuters.com/article/world/putin-orders-suspension-of-passenger-flights-from-russia-to-georgia-idUSKCN1TM2IE/.; "Russia Set to Resume Imports of Georgian Wine and Water," Reuters, February 4, 2013, https://www.reuters.com/article/business/russia-set-to-resume-imports-of-georgian-wine-and-water-idUSL5N0B4737/.

274"Forbes: Georgia Leads among Countries Where Russians Opened Businesses in 2023," *Civil Georgia*, January 18, 2024, https://civil.ge/archives/577917; Georgian Security Expert (name withheld), "Interview."

Georgia… we are a very small country."[275] Therefore, in Georgia's political context, whether Georgian Dream — despite some of its figures' links to Russia — was pushed externally to act in ways that align with Russian interests is largely immaterial. GD can frame its approach as prioritizing Georgian security first, with the implicit tradeoff being "non irritation" towards Russia. The Georgian security expert (name withheld) argues that Russia has built an infrastructure of "useful idiots" in Georgia who can circulate Kremlin-aligned narratives on its behalf. Because there is a deep, post-2008 mistrust of Russia among Georgians, she noted that these messages are often carried by Georgian voices and packaged as patriotism rather than pro-Russianness.[276]

Russia's objective is then to reinforce and legitimize these narratives that raised the political and societal costs of Western alignment — particularly by linking NATO and the West to war and escalation. The expert contends that the economic and visa benefits of EU integration are hard to argue against directly, so GD, along with Russia, often frames EU integration as a loss of sovereignty and, increasingly, to religious and socially conservative values.[277] In that sense, since the invasion of Ukraine, Russia's goal in Georgia is not simply persuasion for its own sake, but deterrence-by-perception: to cultivate the belief that deeper Western integration would pull Georgia into conflict or make it a target, and to bolster the domestic messaging ecosystem, especially where GD has incentives to amplify similar claims.

Trends

Trend analysis suggests that Georgia entered this study's observation period already far along in the hybrid process. Importantly, multiple incidents or campaigns coded as 'starting on February 24, 2022' reflected left censoring, meaning they were already ongoing before the observation window opened, rather than newly triggered by the war in Ukraine. *In other words, the dataset captured not the ignition of Russian hybrid pressure in Georgia, but its maintenance and upkeep.* Russia had sustained an influence environment it had spent years shaping, while Georgia's domestic trajectory increasingly reduced the marginal effort required for Russia to keep the country from drifting towards the West. From 2022-2025, Russian activity in Georgia combined a consistent and active coercive baseline, often tied to Abkhazia and Tskhinvali/South Ossetia, while also using episodic political and informational surges timed at particular moments, such as, but not limited to, the Georgian 2024 parliamentary election.

Importantly, the dataset shows a geographic separation of functions across phases. Coercion-coded incidents (11 total) cluster around the occupied territories. These incidents often used legal-administrative integration, security cooperation, and economic and infrastructure levers to consolidate Russia's ability to impose costs and signal escalation dominance. By contrast, priming and destabilization entries more frequently operate in the political-information sphere: candidate discreditation, strategic narrative confusion, and intermediary-driven amplification.

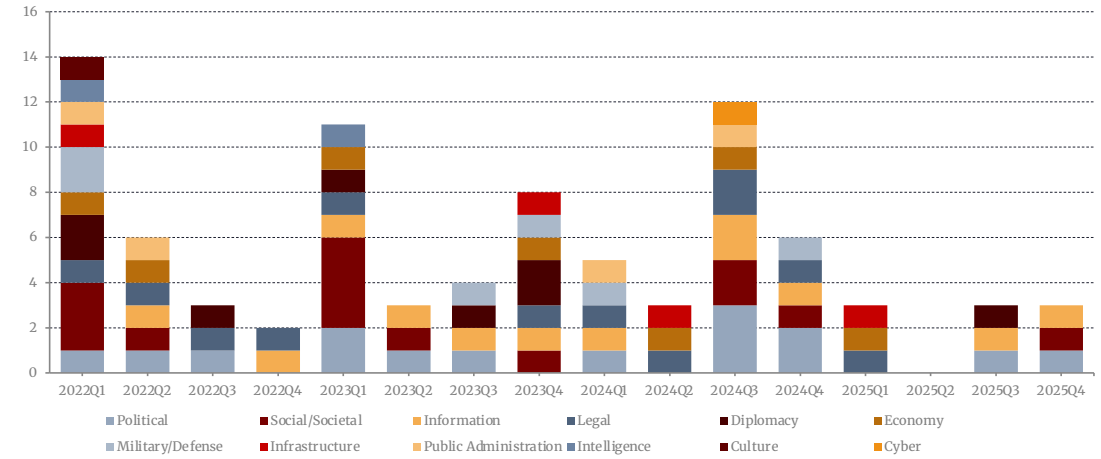
275 Tokhadze, "Interview."

276 Georgian Security Expert (name withheld), "Interview."

277Georgian Security Expert (name withheld), "Interview."

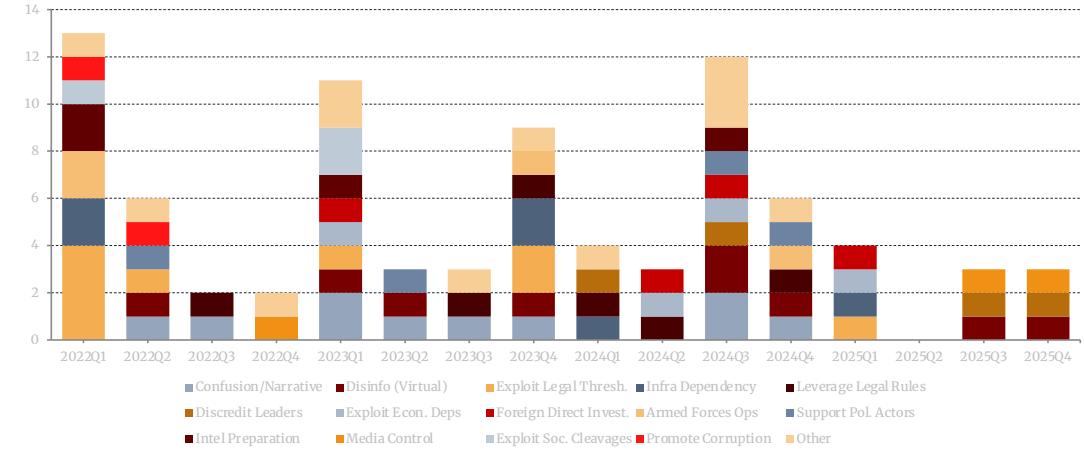
Georgia — Domains by Quarter

Quarterly counts of impacted domains



Georgia — Tools by Quarter

Quarterly counts of tools used at incident start date



When incident timing is examined quarterly, the most meaningful clusters occur after accounting for left censoring. Early post-baseline activity becomes concentrated in Q1 2023 (January–March) and Q4 2023 (October–December), followed by a pronounced surge in Q3 2024 (July–September) and a smaller but consequential cluster in Q4 2024 (October–December). These clusters align with major domestic and geopolitical milestones such as the foreign agents law, national elections, and the status of Georgia's EU candidacy. While the dataset does not encode every domestic law as a Russian hybrid incident, the timing, tools, and narratives logged in the TTP database are strongly consistent with opportunistic exploitation of these political shocks.

Across both 2023 clusters (Q1 and Q4), one lane of Russian TTPs functions as a structural leverage engine in Russian occupied territories. These actions do not need to align to a single discrete trigger; they operate as continuous maintenance of leverage within the occupied territories. The second lane conditions the domestic narrative environment, which can be rapidly amplified by the friendly Georgia

Dream party, or vice versa, utilizing narratives that "the West is instigating unrest," "pushing Georgia into war," and that opposition or protest activity is externally engineered. During the second cluster in December 2023 (Q4), the European Council granted candidate status to Georgia conditional on certain reforms and on countering disinformation and democratic backsliding. During this time, the database logs narratives in which state security framing increasingly shifts away from straightforward condemnation of Russian malign activity and toward allegations that Western-linked actors are fomenting domestic unrest — an early marker of the rhetorical inversion that becomes central in 2024–2025 and central in pushing Georgia away from Euro-Atlantic integration. This period, as well as Q1 2023, also coincides with Georgia's initial introduction of the controversial, and now enshrined, "foreign agents" law.

During the 2023 clusters, most incidents centered on Russia's consolidation efforts in Georgia's occupied territories. In Q1, Abkhazia's de facto cabinet published a draft "apartment law" on February 3, 2023, that would have lifted restrictions on property sales to Russians — an initiative Georgian security services and local reporting linked to sustained Russian pressure and potential demographic engineering; the draft was ultimately withdrawn in July 2024.[278] That same year, Georgia's State Security Service reported Russian promotion of the "Eastern Ossetia" concept to advance claims over the Truso Gorge and portray Georgia as having "seized" land associated with the occupied Tskhinvali region.[279] In Q4, incidents included plans to convert a port in Abkhazia's Ochamchire district into a Russian naval facility (with later open-source analysis confirming construction had begun), alongside Abkhazia's de facto parliament ratifying a 49-year lease transferring the Bichvinta state residence and surrounding territory to Russia — formalizing an arrangement revived through a January 2022 agreement and criticized as enabling expanded Russian land holdings.[280]

However, both Q1 and Q4 also captured moments from Russia's longer-running "maintenance campaigns," which unfolded among Georgia's receipt of EU candidate status on December 14, 2023, and raised the payoff for Russia (and aligned narratives) to cast Western engagement as destabilizing or war-provoking. Prior to that moment, in October 2023 (Q4), Georgia's State Security Service accused the now-defunct U.S. Agency for International Development of funding organizations allegedly seeking to foment civil unrest — a claim that was quickly amplified by pro-Kremlin media. Russian state and fringe outlets used the allegation to advance narratives that the United States was orchestrating a revolution in Georgia and pushing the country toward conflict with Russia, with *Sputnik* publishing multiple articles promoting a sensationalized "U.S.-backed revolution" storyline on the day the accusations were announced. Separately, the SSSG's 2023 security report described "information activities" by foreign special services aimed at stoking anti-Western sentiment and reported efforts by a foreign service — logged in the database as 'suspected' to be Russia — to cultivate ties with Georgian academia to promote its political agenda and shape social life. Both entries were coded as beginning in January 2023 because they derive from the SSSG's annual report rather than discrete incident dates.

The other two notable "clusters" of incidents logged occurred in in Q3 2024 (July–September) as well as slightly in Q4 2024 (October–December). This period had the most diverse use of tools in the entire

278"Demographic Concerns and Controversy Surrounding Abkhazia's 'Apartment Law,'" *Civil Georgia*, July 19, 2023, https://civil.ge/archives/552713.

279 "State Security Service 2023 Report," Civil Georgia, April 21, 2024, https://civil.ge/archives/600294.

280 Natia Seskuria, "Georgia Elections 2024: Can Georgia Repair Its Relations With the EU and United States?," Foreign Policy, October 25, 2024, https://foreignpolicy.com/2024/10/25/georgia-elections-us-china-russia-eu-integration-diplomacy/; "Occupied Abkhazia Transfers Bichvinta Dacha to Russia," *Civil Georgia*, December 27, 2023, https://civil.ge/archives/575811.

Georgia database, using 10 distinct tools including: the use of virtual disinformation campaigns and the promotion of contradictory narratives (both of which were elevated in Q3), coercion of politicians/government, discrediting leadership/candidates, support of political actors, and 'Cyber espionage' and 'Cyber operations,' both of which were used exclusively during this period. During this period, Russia's two-track approach was visible: as Georgia moved toward parliamentary elections in October 2024, Moscow both sustained — and at times escalated — pressure in the occupied territories.

In August 2024, Russia reduced financial assistance to occupied Abkhazia, with de facto leader Aslan Bzhania later stating that the cuts were tied to Abkhazia's failure to fully implement obligations under the 2014 "alliance and strategic partnership" treaty.[281] On October 30, Abkhaz and Russian officials signed an agreement granting tax exemptions to Russian companies investing in Abkhazia, triggering public backlash inside the territory, renewed concerns in Tbilisi about creeping russification, and ultimately Bzhania's resignation in late November; the de facto authorities later voted down ratification of the agreement in December 2024.[282] In November 2024, Russian President Vladimir Putin ratified a military-technical cooperation agreement with Tskhinvali/South Ossetia — originally signed on August 23, 2023 — which Russian authorities framed as deepening cooperation in training, weapons production, acquisition, and military support, and which critics viewed as further entrenching Russia's military and political integration of the territory.[283]

On the other side of the coin, Russia intensified influence and information operations. In August 2024, ahead of parliamentary elections, Meta removed a Russia-originated network targeting Georgia for "coordinated inauthentic behavior" tied to protests against the "foreign agents" law. Meta assessed that the operation used fictitious Georgian-focused news sites and linked social media accounts to criticize protesters while promoting narratives supportive of GD.[284] During the same period, a Russian-linked cyber-espionage actor dubbed "Curly COMrades" conducted sustained intrusions against Georgian judicial and government bodies from late 2024 into early 2025.[285] While this is the only 'Cyber' incident logged in the database, Kapanadze notes that Russia has targeted Georgian government agencies, websites, and citizens (primarily their data) since the invasion of Ukraine, although it is not always publicly reported on.[286]

Russia also increased overt signaling and narrative support aligned with GD. In July 2024, Russia's Foreign Intelligence Service (SVR) issued repeated public statements alleging that the United States sought to engineer GD's removal and provoke mass unrest through a "Tbilisi Maidan," framing its disclosures

281 "Bzhania: Abkhazia Should Implement Its Obligations to Russia," *Civil Georgia*, September 20, 2024, https://civil.ge/archives/625470.

282 "Russian Information Operations in the 2024 Election Cycle," ISFED, April 4, 2025, https://www.isfed.ge/eng/blogi/rusuli-sainformatsio-operatsia-2024-tslis-saparlamento-archevnebtan-dakavshirebit.

283 "Russia Ratifies Agreement on Development of Military-Technical Cooperation with Occupied Tskhinvali," *Civil Georgia*, November 25, 2024, https://civil.ge/archives/637970.

284 "Meta Removes Russian-Origin Accounts, Pages Targeting Protesters of Foreign Agents Law," *Civil Georgia*, August 16, 2024, https://civil.ge/archives/620753.

285 Jonathan Greig, "New 'Curly' Threat Actor Found Targeting Sensitive Organizations in Georgia, Moldova," The Record, August 13, 2025, https://therecord.media/curly-threat-actor-targeting-moldova.

286 Kapanadze, "Interview."

as an effort to preempt a supposed "color revolution."[287] Immediately after the 2024 parliamentary elections and the ensuing protests, Russian officials, state-aligned media, and Russia-linked online networks amplified narratives legitimizing GD's victory — widely alleged to have been rigged — while senior figures, including Sergey Lavrov and Vladimir Putin, echoed claims that Western actors sought to foment instability, impose liberal social agendas, or draw Georgia into war with Russia. In parallel, Russia-linked outlets and pages promoted these narratives.[288]

Response

Georgia's most consistent state-level response to Russian hybrid pressure has been diplomatic and legal-political pushback on its activities in Abkhazia and Tskhinvali/South Ossetia. Tbilisi continues to condemn Russia-backed "so-called elections" and other steps taken by both de facto authorities and Russia in Abkhazia and Tskhinvali/South Ossetia as violations of Georgia's sovereignty. The Georgian government regularly calls on other states to uphold non-recognition and press Moscow on its obligations under post-2008 arrangements.[289] In practice, this is the clearest area where the Georgian state still publicly and repeatedly challenges Russia's coercive posture in the occupied territories.

The State Security Service's annual reporting and parliamentary briefings consistently frame hybrid warfare — including disinformation, influence operations, and cyber threats — as a priority concern and describe efforts to monitor and counter hostile activity linked to foreign services. However, while state attribution has always been vague in reports released during the observation period, recent reports, such as Georgia's 2024 State Security Service report, increasingly mention Western countries and institutions as responsible for disinformation and other hybrid tactics in Georgia, and have failed to explicitly name Russia as behind influence operations.[290] Externally, EU institutions in 2025 described Georgia's current approach as self-defeating for resilience: the European Commission's 2025 Georgia report said high-level officials and ruling-party-aligned channels were driving hostile anti-EU rhetoric and "manipulative narratives," and that "under the pretext" of countering foreign interference, new legal/regulatory measures have instead targeted civil society and independent media — weakening Georgia's ability to counter genuine foreign disinformation threats (including by abolishing the Information Centre on NATO and the EU).[291]

287 Eto Buziashvili, "Russia Is Directly and Indirectly Meddling in Georgia's Upcoming Election," Atlantic Council, October 23, 2024, https://www.atlanticcouncil.org/blogs/new-atlanticist/russia-is-directly-and-indirectly-meddling-in-georgias-upcoming-election/.

288 ISFED, "Russian Information Operations in the 2024 Election Cycle."

289 "The Statement of the Ministry of Foreign Affairs of Georgia Concerning the Illegal So-Called Presidential Elections Held in the Occupied Abkhazia Region," February 15, 2025, https://mfa.gov.ge/en/statements-by-mfa/894797-saqartvelos-sagareo-saqmeta-saministros-gantskhadeba-okupirebul-aphkhazetis-regionshi-chatarebuli-uk.

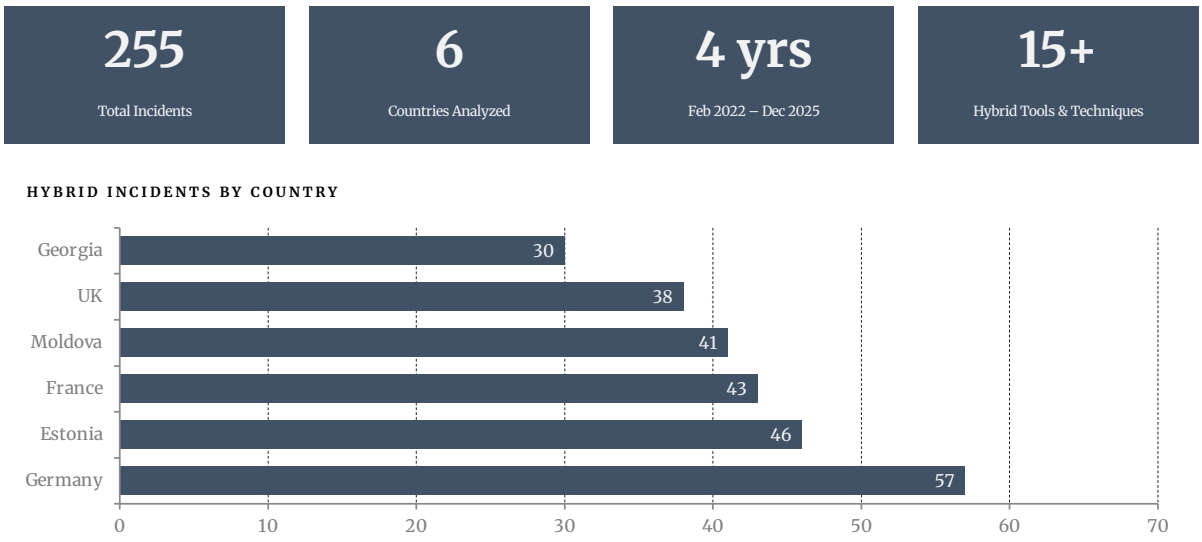
290"SSSG 2024 Report Takes Aim at Western 'Disinformation,' 'Discreditation', Broaches Planned 'Liquidation' of GD Leadership," *Civil Georgia*, April 30, 2025, https://civil.ge/archives/678621.

291 *2025 Communication on EU Enlargement Policy (Extract about Georgia)* (European Commission, 2025), https://enlargement.ec.europa.eu/document/download/b3089ad4-26be-4c6a-84cc-b9d680fe0a48_en?filename=georgia-report-2025.pdf.

Comparative Trend Analysis

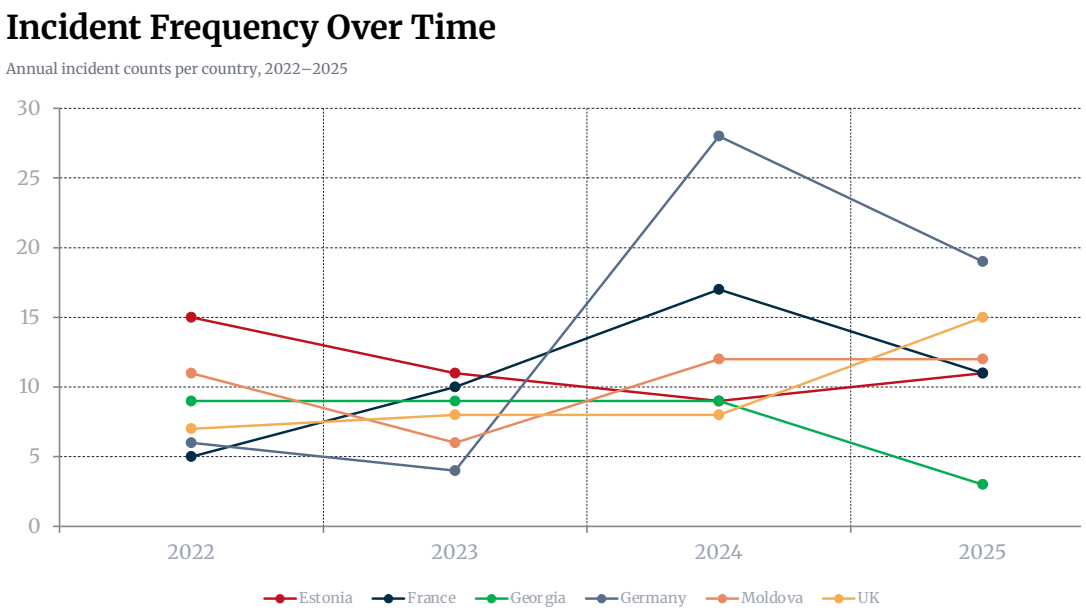
Across the full observation period, 255 incidents were recorded across the six case study countries, employing over 35 distinct tools. Germany recorded the highest incident count, about 22 percent of all incidents, followed by Estonia, France, Moldova, the UK, and Georgia. The disparity in incident counts is due to the types of events or campaigns recorded. For example, much of the hybrid activity in Georgia was sustained before the observation period and was characterized by larger, more campaign-like incidents, whereas in Germany, the incident profile differs significantly.

Dataset Overview



Over the four-year period, France, Germany, and Moldova all appeared to exhibit event-driven escalation, with peaks in 2024 and 2025. France saw a 240 percent increase from 2022 to 2024, the year of its legislative and parliamentary elections and the Paris Olympics. Germany likewise saw a 600 percent increase from 2023 to 2024, before declining to a middle ground in 2025, the year of the German federal election. The peak in 2024 was likely due to pre-election disinformation and influence campaigns such as Storm-1516 and R-FBI. These campaigns were also present in Moldova, which experienced a 100 percent increase in incident counts ahead of the October 2024 and September 2025 elections.

In contrast, Estonia showed the flattest temporal trajectory in the dataset, with a peak of 15 recorded incidents in 2022, declining to 11 and then to 9 across 2023-2024, and then increasing back to 11 in 2025. Similarly, Georgia's trajectory was flat from 2022-2024 and declined in 2025, likely due to the ruling party's increasing political alignment with Russia, which reduced the utility of launching new TTPs. These findings are consistent with the near-continuous pressure that Russia applies to its post-Soviet states to sustain influence outside elections. Moldova likely appears differently because of its pro-European trajectory, which presents a clear threat to Russian interests and could have been undermined during critical junctures like the 2024 and 2025 elections.



The UK also appears differently from its fellow Western European states. This is likely because a majority of its logged incidents — such as naval and airspace incursions or acts of vandalism — remain relatively stable, as there is less publicly available data surrounding political or informational influence operations that can be more concretely linked to Russia. As this study points out, the UK remains one of the most reluctant states to publicize the effects of Russian TTPs, limiting the reliability of the trends our data observes. Nevertheless, the UK did experience a notable increase in incidents — specifically territorial water violations — in 2025, possibly due to Prime Minister Keir Starmer's announcement toward the end of that year that the UK was moving towards "warfighting readiness," which could have raised its target profile.

In taking all six case study countries together, two target profiles emerged. Countries within these profiles are roughly aligned along a geographic and geopolitical axis. France, Estonia, and Moldova all share a profile in which the 'Social/Societal' and 'Information' domains account for the largest share of incidents. In Estonia, roughly 65 percent of incidents targeted the 'Social/Societal' domain, and 39 percent targeted the 'Information' domain. In Moldova, 73 percent of incidents targeted 'Social/Societal' and 54 percent targeted 'Information.' In France, 65 percent of incidents targeted 'Information' and 53 percent targeted 'Social/Societal.' In all three countries, the top tools involve narrative confusion, virtual and physical disinformation, and the promotion of social unrest.

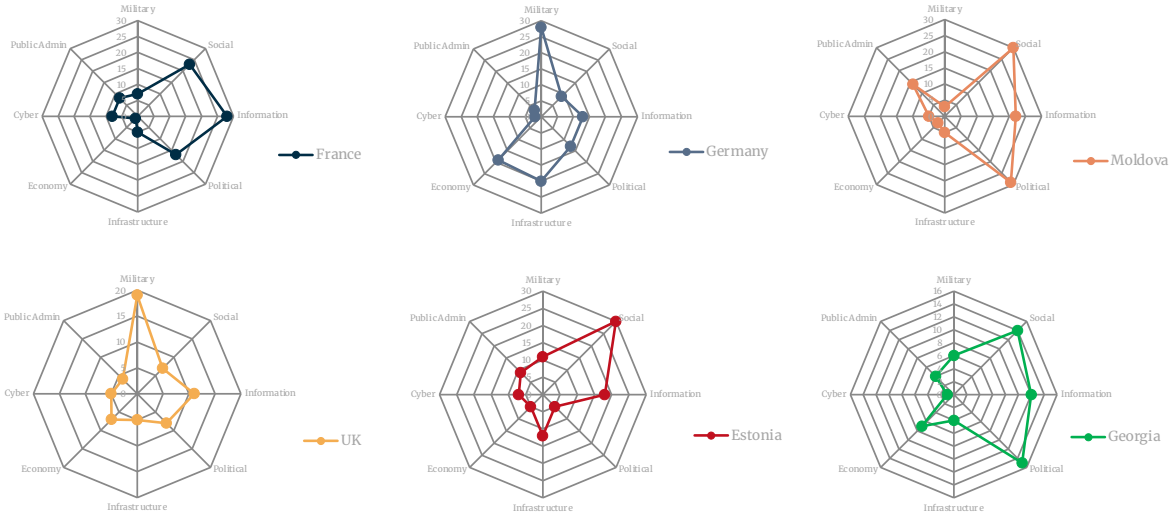
The targeted domains in Germany and the UK, on the other hand, tend to align more closely with military and infrastructure domains. In Germany, the 'Military' domain was implicated in 49 percent of incidents and 'Infrastructure' in 35 percent, and the single most used tool was 'Intelligence Preparation.' In the UK, the 'Military' domain featured in 50 percent of incidents and 'Territorial water violations' in 42 percent, with 'Armed forces operations' and 'Territorial water violations' ranking as the top two tools. This profile reflects Russia's treatment of these states as primarily military and logistical actors,

specifically in NATO.

It should be noted that France also has one of Europe's largest militaries and provides a substantial amount of aid to Ukraine; yet Russia focused primarily on social and informational TTPs. This domain disparity may reflect the exceptional amount mediatized and important political events in France during the observation period, such as elections and the Paris Olympics. The domain gap also indicates that Russia is keenly aware of France being home of the largest Muslim and Jewish population in Western Europe — rendering it ripe for operations meant to stoke societal divides. This is not to say that Russia does not target British or German political or social cohesion — Russia's relationship with the far-right Alternative für Deutschland (AfD) is well documented, even if direct monetary ties are harder to prove, and it has long been believed that Russia may have had an influence over Brexit — but these three counties have different reporting systems in place. This report's database only documents what is publicly reported and what can be publicly tied to Russian tools and tactics.

Domains Targeted

Frequency of domain targeting by country



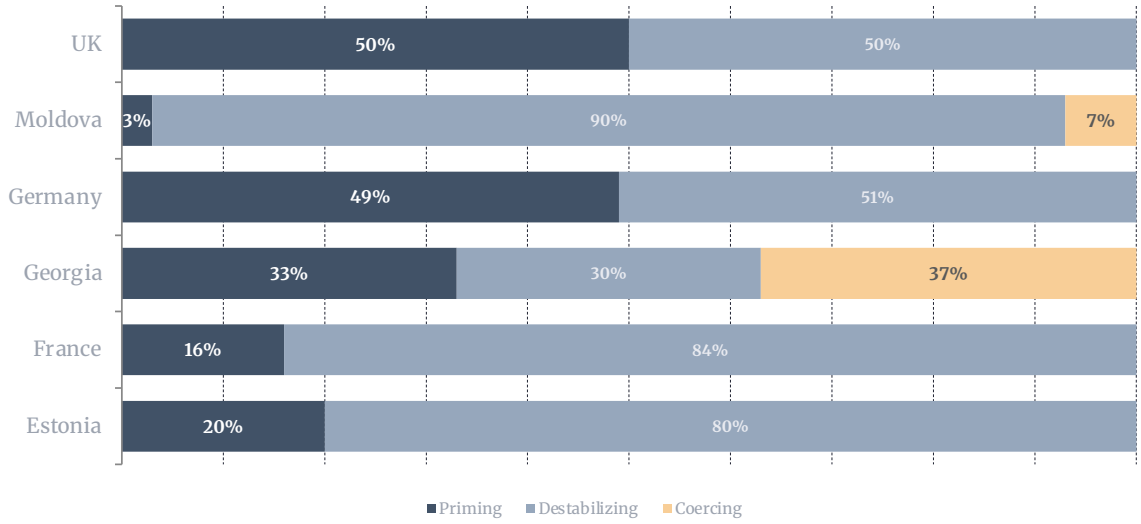
Georgia also does not fit neatly among these profiles. Its most targeted domains are the 'Political' domain, which constitutes 50 percent of incidents, and the 'Social/Societal' domain (47 percent of incidents). Its top two tools, 'Creating confusion or a contradictory narrative' and 'Disinformation (virtual)' resemble the profile of Estonia, France, and Moldova. However, when looking at its phases, Georgia is the only country in the dataset with a substantial 'Coercing' phase (37 percent), which by definition is Russia's most overt phase, often associated with the military domain. Moldova is the only other case study country that logged the 'Coercion' phase, but it represents a much smaller share of the data at just 7 percent. The coercive dimension sets Georgia, and to some extent, Moldova, apart. Both countries, as frontline Eastern states, have the presence of Russian troops on its internationally recognized territory and have been subject to some of the most overt threats as compared to the other case study countries.

Similarly, several tools appear consistently across France, Georgia, and Moldova. 'Creating confusion

or a contradictory narrative' is the top tool in France, Georgia, and Moldova, and features across the broader dataset. 'Disinformation (virtual)' appears in the top five for Estonia, France, Georgia, and Moldova. 'Clandestine operations' appear in the top five for Estonia, Germany, and the UK. 'Discrediting leaders' appears in the top five for France, Moldova, and implicitly in Georgia's information operations against the opposition.

Hybrid Phase Distribution

Priming, Destabilizing, and Coercing operations by country as a percent



Top 5 Tools Used Per Country

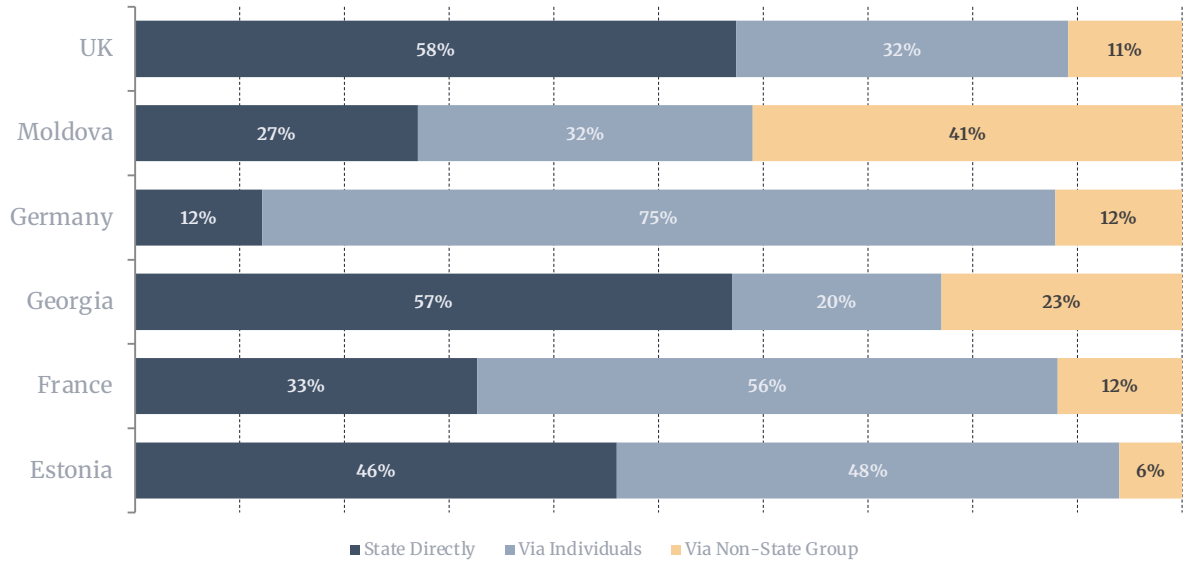
	Estonia	France	Georgia	Germany	Moldova	UK
#1	Social Unrest *24 incidents*	Confusion / Narrative *13 incidents*	Confusion / Narrative *10 incidents*	Intel Preparation *29 incidents*	Confusion / Narrative *17 incidents*	Armed Forces Ops *17 incidents*
#2	Disinfo (Virtual) *11 incidents*	Disinfo (Physical) *13 incidents*	Disinfo (Virtual) *9 incidents*	Airspace Violation *20 incidents*	Disinfo (Virtual) *14 incidents*	Territorial Water Viol. *16 incidents*
#3	Disinfo (Physical) *7 incidents*	Disinfo (Virtual) *12 incidents*	Exploit Legal Thresholds *9 incidents*	Physical Infra Ops *16 incidents*	Discredit Leaders *14 incidents*	Intel Preparation *9 incidents*
#4	Cyber Operations *7 incidents*	Social Unrest *12 incidents*	Infra Dependency *6 incidents*	Clandestine Ops *8 incidents*	Social Unrest *13 incidents*	Cyber Operations *6 incidents*
#5	Clandestine Ops *6 incidents*	Discredit Leaders *8 incidents*	Leverage Legal Rules *6 incidents*	Infiltration *8 incidents*	Exploit Public Admin *8 incidents*	Clandestine Ops *6 incidents*

'Intelligence preparation' is the dominant tool in Germany with 29 incidents logged and appears in the UK's top five (9 incidents), but is comparatively absent from the post-Soviet space, likely because Russia treats Germany and the UK as high-value military or logistical targets.

Furthermore, the UK and Georgia have the highest rates of direct Russian state action, which aligns with the nature of their logged incidents. Naval transits, airspace incursions, and territorial violations in the UK are inherently attributable to the Russian state itself and would largely be unable to be conducted by a proxy group or individual. Similarly, many of the coercive administrative actions in the Georgian-occupied territories involve the Russian state itself. Germany sits at the opposite extreme, with 75 percent of incidents carried out by intermediaries. This is consistent with the German case study's emphasis on plausible deniability in sensitive sabotage operations, where direct attribution would carry significant escalatory risk.

Operation Actor

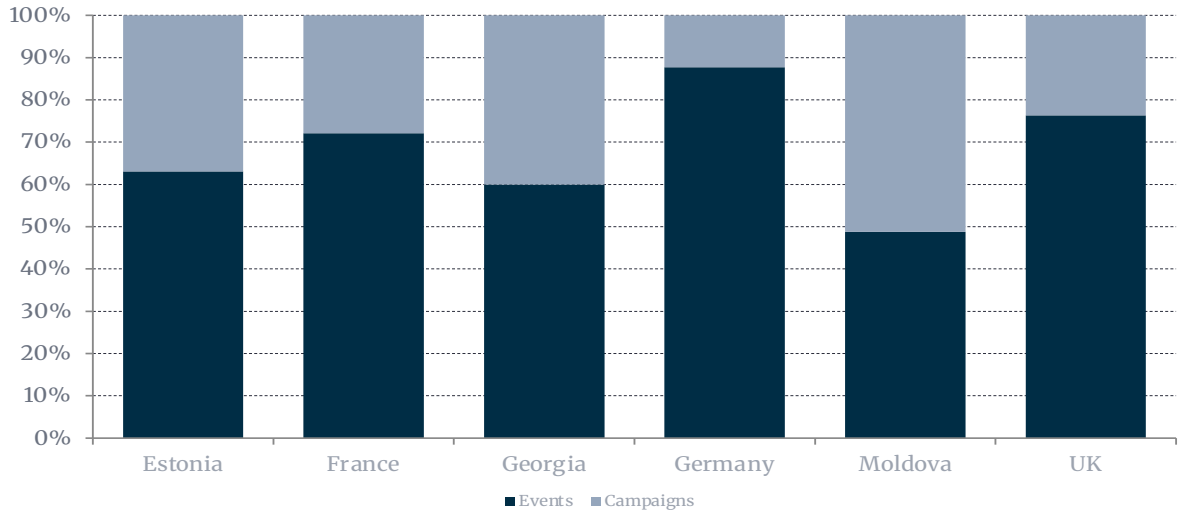
How Russia conducts its operations — directly, through individuals, or non-state groups



Additionally, Moldova is the only country in the dataset where sustained campaigns slightly outnumber discrete events, with 21 campaigns and 20 events logged in the database. Estonia and Georgia also have a large campaign share, with 40 percent of Georgian incidents and 37 percent of Estonian incidents classified as campaigns. This reflects the entrenched nature of Russia's long-running influence infrastructure across the post-Soviet space, whether through influence operations surrounding political figures or disinformation targeting Russian-speaking populations. These countries stand in sharp contrast to Germany, where the dataset is composed primarily of episodic incidents rather than sustained narrative campaigns. Although many incidents in Germany, such as drone incursions occurring around the same time and place, are likely linked, their threat profile differs markedly from the more campaign-like character of many incidents targeting Moldova, Georgia, Estonia, and, at times, France.

Hybrid Incidents: Discrete Events vs. Sustained Campaigns

Operational tempo: targeted sabotage vs. sustained influence operations

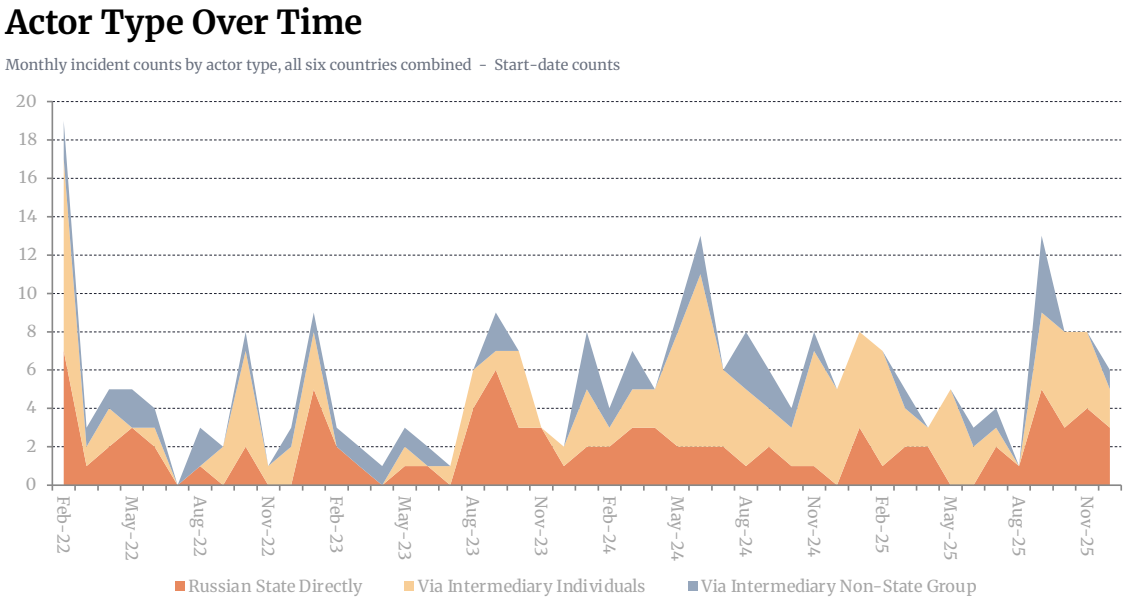


Finally, across the dataset, there was a measurable shift toward more overt physical probing and reconnaissance in 2025, specifically in NATO countries. In France, airspace violations — absent before 2025 — account for five incidents in Q4. In Estonia, 2025 saw Russian MiG-31 incursions into airspace (triggering a NATO Article 4 invocation), a hovercraft border crossing, and continued Baltic Sea undersea infrastructure targeting. In the UK, the Russian research vessel Yantar conducted repeated undersea cable reconnaissance, and underwater devices were recovered from UK waters. Germany's 2025 figures, while down from the 2024 peak, remained well above the 2022 and 2023 counts, and tracked events such as large-scale drone activities surrounding airbases, logistics hubs and other important infrastructure. Moldova even experienced large-scale bombing threats tied to the election.

The dataset also reveals a clear structural shift in how Russia conducts operations over time. In 2022, intermediary individuals were already the plurality actor type at 45 percent of incidents, but 2023 saw a reversal, with the Russian state acting directly surging to 56 percent of incidents — the only year in the dataset where direct state action was the dominant category. From 2024 onward, however, intermediary individuals consolidated as the sustained dominant actor in the database, accounting for 55 percent of incidents in 2024 and 52 percent in 2025. Overall, there was a 254 percent increase from 2023 to 2024 in incidents conducted by intermediary individuals. This mirrors the case study findings. The expansion of physical disinformation operations in France, the infrastructure-sabotage networks in Germany and the UK, and the influence networks in Moldova all rely heavily on recruited individuals rather than on direct state action. Non-state groups spike at specific moments, most visibly in mid-2024 and late 2025, which aligns with election periods in Moldova, France, and Germany. The 'Russian state directly' actor-type is relatively stable throughout the observation period and, as seen in the individual case studies, is often concentrated at times where plausible deniability is either unnecessary or impossible, such as naval transits, airspace incursions, and formal diplomatic pressure.

Taken together, these incidents reveal a Russian hybrid campaign that is simultaneously adaptive and doctrinally coherent. Russia calibrates its toolkit to the specific vulnerabilities, geopolitical functions, and domestic fault lines of each country. Against Eastern frontline states, Russia often deploys sus-

tained influence campaigns designed to undermine erode trust in Western institutions. Against NATO's military and industrial core, Russia often prioritizes intelligence preparation, infrastructure mapping, and plausibly deniable sabotage. Yet in this respect, Estonia and France sit somewhere in the middle. Estonia is a post-Soviet state, but its NATO membership causes it to experience military probing in a way that Moldova or Georgia would not. France, although a traditional Western European power, has intrinsic societal divides that can be easily exploited. France also experienced multiple significant political moments during the observation period, which meant that many of Russia's TTPs mirrored those it commonly utilizes in Eastern Europe. Georgia also occupies a nebulous space in this spectrum. Although it is a traditional post-Soviet state, it appears to be further along in the hybrid process than any other case study, with Russia seemingly achieving its intended outcome through the success of a pro-Russian party in the 2025 parliamentary elections.



Comparatively, the data also suggests that countries with more transparent reporting cultures, such as Estonia and even Germany, will appear more "active" in the dataset than countries like the UK or Georgia, where there are significant constraints surrounding public attribution. Nevertheless, it is clear from the dataset that over the observation period, Russian hybrid activity continued to and even became more physically assertive, further pushing boundaries in 2025.

Conclusion

Russia's hybrid campaign across Europe from February 2022 to December 2025 is characterized by a strategy of cost asymmetry: operations are cheap and often both deniable and scalable for Moscow, while the costs Russia imposes on targets are absorbed almost entirely by the targeted countries. Effectively countering Russia's hybrid toolkit, therefore, requires not just improving social resilience or hardening critical infrastructure but making hybrid activity prohibitively expensive for Russia.

The cost asymmetry of Russia's hybrid strategy is effective in democracies by their very nature. Democracies accommodate and are sustained through dissent and contestation. Foreign actors can thus easily co-opt dissent to embed themselves within civil society, media outlets, or protest movements. This, of course, is almost impossible in an authoritarian context, especially in such a resource-efficient manner. Hybrid campaigns rarely need to fabricate polarization or movements from scratch in democracies; instead, they can be embedded within existing grievances or schisms. Efforts by democracies to mitigate such unacceptable interference by foreign actors risk being profoundly undemocratic or being labeled as such. This makes countermeasures not just potentially antidemocratic but also a perfect propaganda boon for hostile foreign actors.

While the cost asymmetry, which makes hybrid threats the obvious choice for Moscow, explains why this wave of TTPs was observed across the six case studies, it does not explain their impact or lack thereof. The impact of a Russian hybrid operation — incredibly difficult to measure — appears to be shaped in our case study countries by the presence or absence of institutional constraints, attribution mechanisms, and societal cohesion in the targeted country, rather than by the skills, frequency, or intensity of Russian operations.

The impact of hybrid activity, especially in the 'Information' domain, is largely contingent on pre-existing societal factors — which can amplify or blunt operations regardless of Russian operational tempo or skillset. Pre-existing concerns about antisemitism in France rendered the defacement of a Shoah memorial in Paris by Russia-hired disposable agents immediately inflammatory and polarizing. However, efforts to interfere in Estonia's information environment likely do not yield the same result: Estonia's Russian-speaking population has undergone a dramatic shift in media consumption patterns since Russia's full-scale invasion of Ukraine on February 24, 2022. [292] Survey data reveals a decline in both viewership of and trust in Kremlin-controlled media channels. This has made Russia's interference in Estonia's information environment far less effective. In both cases, pre-existing societal factors and attitudes about certain issues, rather than changes in Russian operational tempo or TTPs, shaped outcomes.

In the face of such a complex threat — one that risks being exacerbated by both staying mute and calling it out — public attribution is a necessary but inherently double-edged instrument. Strategic communications on Russian hybrid activity contends with a critical tension: calling out Russian operations to deter further action and warn the public of manipulation and interference, but also not creating panic, triggering further escalation, or giving Moscow a propaganda victory by playing into its hand. Threading this balance requires distinguishing among threat levels of different types of operations, from nuisance-level disinformation to serious military infrastructure probing.

292 Viktoriia Ponomareva, "Changing Channels: How Three Years of Kremlin Propaganda Bans in the EU Have Affected Russian-Speaking Audiences," The Insider, March 18, 2025, https://theins.ru/en/politics/279746.

This tension is particularly acute for the Western European case study countries — France, Germany, and the UK — which face a multi-vector threat landscape. Unlike frontline Eastern states, where Russia looms as the primary security threat, Western European governments must address Russian hybrid threats and manage other competing security priorities. MI5 Director General Ken McCallum has noted that the agency was forced to reallocate counter-terrorism resources to address the growing Russian threat.[293] Whether by design or opportunism, resource exhaustion is forcing European governments to spend more on hybrid threats.

Georgia illustrates another distinct vulnerability of responding to hybrid threats: attribution capacity and institutional will eroding simultaneously. A persistent critique of Western, particularly EU, democracy-building efforts in Georgia holds that these initiatives overemphasized formal parliamentary design at the expense of elite accountability and effective local governance — producing a state that became increasingly "independent of its citizens."[294] The Georgia case indicates that building deterrence and resilience on Europe's eastern flank requires much more than threat awareness. It concretely relies on Western partners to help sustain independent civil society and democratic accountability. This specifically includes stronger local and judicial governance as checks on executive overreach in a context where institutions are still consolidating and corruption risks are persistent.

Russia thus exploits the gap between what is damaging enough to be worth doing and what is attributable enough to provoke a response by Europe; that gap is what makes hybrid operations cheap. Closing it will require action on both sides simultaneously: raising the cost and visibility of Russian operations through attribution and a calibrated response, while reducing the surface area of impact by strengthening institutions, societal cohesion, and democratic accountability that determine whether a given operation lands. Neither line of effort alone is sufficient.

293 *The Guardian*, "MI5 Forced to 'Pare Back' Counter-Terrorism Work Due to Rogue States, Says Chief."

294 Stephen Jones and Natalie Sabanadze, "Perspectives | Elections Are Not Enough: Georgia Needs a New Model of Democracy," Eurasianet, March 10, 2023, https://eurasianet.org/perspectives-elections-are-not-enough-georgia-needs-a-new-model-of-democracy.

Acknowledgments

The generous support of the Airey Neave Trust made this report possible. We wish to express our profound gratitude for the Trust's steadfast commitment to enabling research and for its enduring partnership with The Soufan Center.

We are deeply grateful to the experts who generously shared their expertise and candid assessments through interviews conducted for this report. In particular, we thank Edward Bogan, Peter Clement, Milàn Czerny, Ofer Fridman, Mark Galeotti, Keir Giles, Bob Hamilton, Tamar Kapanadze, Marek Kohv, Justin Novak, Sergiu Ostaf, Nicolas Quenel, András Rácz, Kacper Rekawek, Bart Schuurman, Torben Schütz, Robert Seely, and Mariam Tokhadze for their thoughtful contributions and candid perspectives. We also extend our sincere appreciation to the intelligence and military professionals who spoke with us on condition of anonymity. Their perspectives substantially strengthened the analysis.

The authors are grateful for the thoughtful reviews provided by Dr. Christopher Paul and Dr. Bart Schuurman. Any remaining errors are our own.

Authors

Clara Broekaert*:

Clara Broekaert is a Research Analyst at The Soufan Center. At the Center, she specializes in international security and conflict with a focus on terrorism, violent extremism, and foreign interference. A certified OSINT analyst, Clara has conducted investigations into terrorist groups, analyzing their organizational structures, online ecosystems, and operational tradecraft. She also conducts research on foreign interference and emerging technology in the context of conflict and competition. Clara completed an International Master's degree in Security, Intelligence, and Strategic Studies from the University of Glasgow, Trento University, and Charles University in Prague, where she completed the technology concentration. She earned her Bachelor of Arts degree in Government and International Relations from Smith College.

Nikkie Lyubarsky*:

Nikkie Lyubarsky is a Research Associate at The Soufan Center. Her research focuses on foreign policy, hybrid warfare, and global security issues, specifically surrounding Russia, Eastern Europe, and the Caucasus. She is the author of the report "The War in Sudan: The Role of External Actors and the Prospects for U.S.-Led Conflict Resolution." Before her current role, Nikkie completed a consulting practicum with the U.S. Department of State's Global Engagement Center, focusing on AI-synthetic media, and worked with the United Nations Foundation on the Global Digital Compact, assessing issues related to the global digital divide. Nikkie was awarded a Master of Science in Global Affairs from New York University's Center of Global Affairs, with a concentration in transnational security and a specialization in data analytics. She also holds a Bachelor of Arts in International Relations and History with a minor in Russian and Slavic Studies from New York University's College of Arts and Science.

Colin Clarke:

Colin P. Clarke is the Executive Director at The Soufan Center, where his research focuses on domestic and transnational terrorism, international security, and geopolitics. Prior to joining The Soufan Center, Clarke was a professor at Carnegie Mellon University, and a senior political scientist at the RAND Corporation, where he spent a decade researching terrorism, insurgency, and criminal networks. At RAND, he led studies on ISIS financing, the future of terrorism and transnational crime, and lessons learned from all insurgencies since the end of the World War II. Clarke has testified before Congress on numerous occasions as an expert witness on a range of terrorism-related issues, appears frequently in the media to discuss national security-related matters, and has published several books on terrorism, including his most recent, After the Caliphate: The Islamic State and the Future Terrorist Diaspora. Clarke has a Ph.D. in international security policy from the University of Pittsburgh's Graduate School of Public and International Affairs (GSPIA).

Joseph Shelzi:

Joseph Shelzi is a Research Fellow at The Soufan Center and an Analyst at The Soufan Group. His work focuses on military and operational analysis, conflict resolution, climate security, and the proliferation of terrorist and non-state armed groups. He has published work on the role of cyber power in geopolitics and war, climate security in the Middle East and the Sahel, East Asian security, and cultural geography in Africa. Prior to joining The Soufan Group, he served as a U.S. Army Intelligence Officer. He has worked at the tactical and strategic levels, analyzing both conventional and terrorist threats to U.S. Army operations. While stationed in Japan, he served as a company commander and worked on alliance and security cooperation issues at the U.S. Embassy in Tokyo. He was awarded a Master of International Affairs degree from Columbia University's School of International and Public Affairs (SIPA) and earned a Bachelor of Science degree with honors in Human Geography from the United States Military Academy at West Point.

*** Primary Investigators**

Bibliography

3rd EEAS Report on Foreign Information Manipulation and Interference Threats: Exposing the Architecture of FIMI Operations. European Union External Action Service, 2025. https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf.

2025 Communication on EU Enlargement Policy (Extract about Georgia). European Commission, 2025. https://enlargement.ec.europa.eu/document/download/b3089ad4-26be-4c6a-84cc-b9d-680fe0a48_en?filename=georgia-report-2025.pdf.

Al Jazeera. "Macron Says Putin Gave Him Assurances over Russia-Ukraine Crisis." February 8, 2022. https://www.aljazeera.com/news/2022/2/8/macron-says-putin-told-him-russia-wont-escalate-ukraine-crisis.

Al Jazeera. "Pro-EU Party in Moldova Wins Clear Majority in Snap Election." July 13, 2021. https://www.aljazeera.com/news/2021/7/13/pro-eu-party-in-moldova-wins-clear-majority-in-snap-election.

Al Jazeera. "Russia-Ukraine War: List of Key Events, Day 1,388." December 13, 2025. https://www.aljazeera.com/news/2025/12/13/russia-ukraine-war-list-of-key-events-day-1388.

Albertini, Antoine, Damien Leloup, and Florian Reynaud. "Cercueils à La Tour Eiffel : Un Lien Direct Établi Avec l'affaire Des Mains Rouges et Des Soupçons Pointant Vers La Russie." *Le Monde*, October 29, 2025. https://www.lemonde.fr/pixels/article/2024/06/03/cercueils-a-la-tour-eiffel-un-lien-direct-etabli-avec-l-affaire-des-mains-rouges_6237067_4408996.html.

Alex Nichol. "What UK's Strategic Defense Review Means for Ukraine." *The Kyiv Independent*, June 9, 2025. https://kyivindependent.com/what-uk-strategic-defense-review-means-for-ukraine/.

András Rácz. *Germany's Shifting Policy towards Russia: The Sudden End of Ostpolitik*. Finnish Institute of International Affairs, 2022. https://fiia.fi/en/publication/germanys-shifting-policy-towards-russia.

Annual Review, 2022-2023. Estonian Internal Security Service, 2023. https://kapo.ee/sites/default/files/content_page_attachments/Annual%20Review%202022-23_0.pdf.

Antoniuk, Daryna. "France Blames Russian Military Intelligence for Years of Cyberattacks on Local Entities." The Record, April 29, 2025. https://therecord.media/france-blames-russian-military-intelligence-for-hacks-against-local-orgs.

AP News. "Oligarch Sentenced for Role in Stealing $1B from Moldovan Banks." April 14, 2023. https://apnews.com/article/moldova-oligarch-ilan-shor-bank-fraud-chisinau-israel-maia-sandu-e7c9639f354f27c4975030f7b40629be.

Barnes, Julian E., and Eric Schmitt. "Russian Drones Are Flying Over U.S. Weapons Routes in Germany, Officials Say." *The New York Times*, August 28, 2025. https://www.nytimes.com/2025/08/28/us/politics/russian-drones-weapons-routes.html.

Barron's. "Kremlin Accuses Moldova Of 'Anti-Russian Hysteria.'" February 20, 2023. https://www.barrons.com/news/kremlin-accuses-moldova-of-anti-russian-hysteria-aaf36f1b.

Barron's. "Lithuania Charges 15 With Terrorism Over 'Russia Bomb Plot.'" September 17, 2025. https://www.barrons.com/news/lithuania-charges-15-with-terrorism-over-russia-bomb-plot-d03d3f1b.

BBC. "Police Make Fifth Arrest over Arson Attacks on Properties Linked to Keir Starmer." January 29, 2026. https://www.bbc.com/news/articles/c20dyzp4r42o.

BBC. "Ukraine: UK Condemns Russian 'land Grab' of Crimea." March 18, 2014. https://www.bbc.com/news/uk-politics-26632857.

Berlinger, Joshua, Amy Cassidy, Luke McGee, and Vasco Cotovio. "Macron Says 'Nothing Ruled out,' Including Using Western Troops, to Stop Russia Winning Ukraine War." *CNN*, February 27, 2024. https://www.cnn.com/2024/02/27/europe/france-macron-troops-ukraine-intl.

Bigg, Claire. "Russia: Moscow Withdrawing From Treaty With Estonia Over References To 'Occupation.'" *Radio Free Europe/Radio Liberty*, June 28, 2005. https://www.rferl.org/a/1059557.html.

Bremmer, Ian. "From Dove to Hawk: Explaining Macron's Russia-Ukraine Journey." GZERO Media, March 27, 2024. https://www.gzeromedia.com/by-ian-bremmer/from-dove-to-hawk-explaining-macrons-russia-ukraine-journey.

BTI 2024. "BTI 2024 Moldova Country Report." https://bti-project.org/en/reports/country-report?isocode=MDA&cHash=810883b9fb88ff046a65443aeca5eced.

Bulfon, Floriana. "How Estonia Became the Front Line in the New Cold War." New Lines Magazine, January 12, 2026. https://newlinesmag.com/reportage/how-estonia-became-the-front-line-in-the-new-cold-war/.

Bundeswehr. "Operational Plan for Germany." last updated spring 2025. https://www.bundeswehr.de/en/organization/bundeswehr-joint-force-command/missions/operational-plan-for-germany.

Campbell, Adina, and Kathryn Armstrong. *Three Men Found Guilty of Wagner Group-Linked Arson Attack in London*. July 8, 2025. https://www.bbc.com/news/articles/cx2k37x91vlo.

Carrell, Severin. "Russian Cyber-Activists 'Tried to Discredit Scottish Independence Vote.'" *The Guardian*, December 13, 2017. https://www.theguardian.com/politics/2017/dec/13/russian-cyber-activists-tried-to-discredit-scottish-independence-vote-says-analyst.

Caucasian Knot. "Pro-European Protests in Georgia Have Continued for 425 Days without Interruption." January 26, 2026. https://www.eng.kavkaz-uzel.eu/articles/72301.

Check Point Blog. "Operation MiddleFloor: Unmasking the Disinformation Campaign Targeting Moldova's National Elections." October 9, 2024. https://blog.checkpoint.com/research/operation-middlefloor-unmasking-the-disinformation-campaign-targeting-moldovas-national-elections/.

Christian Lowe, Polina Nikolskaya, and Anton Zverev. "Holy War: How Russia Recruited Orthodox Priests

to Sway Moldova's Voters." *Reuters*, September 26, 2025. https://www.reuters.com/investigations/holy-war-how-russia-recruited-orthodox-priests-sway-moldovas-voters-2025-09-26/.

Civil Georgia. "Bzhania: Abkhazia Should Implement Its Obligations to Russia." September 20, 2024. https://civil.ge/archives/625470.

Civil Georgia. "Demographic Concerns and Controversy Surrounding Abkhazia's 'Apartment Law.'" July 19, 2023. https://civil.ge/archives/552713.

Civil Georgia. "Forbes: Georgia Leads among Countries Where Russians Opened Businesses in 2023." January 18, 2024. https://civil.ge/archives/577917.

Civil Georgia. "Meta Removes Russian-Origin Accounts, Pages Targeting Protesters of Foreign Agents Law." August 16, 2024. https://civil.ge/archives/620753.

Civil Georgia. "Occupied Abkhazia Transfers Bichvinta Dacha to Russia." December 27, 2023. https://civil.ge/archives/575811.

Civil Georgia. "Russia Ratifies Agreement on Development of Military-Technical Cooperation with Occupied Tskhinvali." November 25, 2024. https://civil.ge/archives/637970.

Civil Georgia. "SSSG 2024 Report Takes Aim at Western 'Disinformation,' 'Discreditation', Broaches Planned 'Liquidation' of GD Leadership." April 30, 2025. https://civil.ge/archives/678621.

Civil Georgia. "State Security Service 2023 Report." April 21, 2024. https://civil.ge/archives/600294.

Civil Georgia. "Vladimir Putin Speaks Saakashvili, 'Lugar Lab.'" October 19, 2018. https://civil.ge/archives/259804.

Clark, Mason. *Russian Hybrid Warfare*. Military Learning and the Future of War Series. Institute for the Study of War, 2020. https://understandingwar.org/research/russia-ukraine/russian-hybrid-warfare-2/.

Clover, Charles. "Russia Is 'Exporting Chaos', New Head of Britain's Spy Agency MI6 Warns." *Financial Times*, December 15, 2025. https://www.ft.com/content/5cbedc56-b29a-4284-901b-aef5f6853135.

Coffey, Luke. "Russia Exploits 'Yellow Vest' Turmoil In France." The Heritage Foundation, February 8, 2019. https://www.heritage.org/europe/commentary/russia-exploits-yellow-vest-turmoil-france.

Cohen, Raphael, and Andrew Radin. *Russia's Hostile Measures in Europe: Understanding the Threat*. RAND Corporation, 2019. https://doi.org/10.7249/RR1793.

Consolidated Report on the Conflict in Georgia (November 2022 – March 2023). Council of Europe, 2023. https://rm.coe.int/consolidated-report-on-the-conflict-in-georgia-november-2022-march-2023/1680aacba0.

Cornevin, Christophe. “Jets de Peinture Verte Sur Des Lieux Juifs : Les Suspects Interpellés Sont Des Ressortissants Serbes.” *Le Figaro*, June 2, 2025. https://www.lefigaro.fr/actualite-france/jets-de-peinture-verte-sur-des-lieux-juifs-les-suspects-interpelles-sont-des-ressortissants-serbes-20250602.

Country Report: Assessment of Foreign Information Manipulation and Interference (FIMI) in the 2025 German Federal Election. Institute for Strategic Dialogue, 2025. https://www.isdglobal.org/isd-publications/country-report-assessment-of-foreign-information-manipulation-and-interference-fimi-in-the-2025-german-federal-election/.

Coyle, James J. *Russia’s Border Wars and Frozen Conflicts*. Palgrave Macmillan Cham, 2017.

Croft, Jane, Neil Buckley, and Max Seddon. “Litvinenko Inquiry: Report Points Finger at Vladimir Putin.” Financial Times, January 21, 2016. https://www.ft.com/content/53ecb19c-c01f-11e5-9fdb-87b8d15baec2.

Daly, John. “France to Refund Russia $1.2 Billion for Non-Delivery of Mistral Helicopter Carriers.” 04 2015. https://jamestown.org/france-to-refund-russia-1-2-billion-for-non-delivery-of-mistral-helicopter-carriers/.

Daryna Antoniuk. “Russia’s Cyberattacks Aimed at ‘Destabilizing’ Moldova, PM Says.” The Record, February 9, 2023. https://therecord.media/russias-cyberattacks-aimed-at-destabilizing-moldova-pm-says.

Das Bundeskriminalamt (BKA). “Wegwerf-Agenten: Kurzer Einsatz, Hohes Risiko.” https://www.bka.de/DE/Landingpages/LLA/lla_node.html.

DePorte, Anton W. “De Gaulle’s Europe: Playing the Russian Card.” *French Politics and Society* 8, no. 4 (1990): 25–40.

DFRLab. “#ElectionWatch: Scottish Vote, Pro-Kremlin Trolls.” January 22, 2018. https://medium.com/dfrlab/electionwatch-scottish-vote-pro-kremlin-trolls-f3cca45045bb.

DFRLab. “Russia’s 2019 Cyber Attack against Georgia Followed by Full-Spectrum Propaganda Effort.” April 23, 2020. https://dfrlab.org/2020/04/23/russias-2019-cyber-attack-against-georgia-followed-by-full-spectrum-propaganda-effort/.

Directorate-General for Enlargement and Eastern Neighbourhood. “EU and Moldova Forge Deeper Ties at Historic First Summit in Chișinău.” July 4, 2025. https://enlargement.ec.europa.eu/news/eu-and-moldova-forge-deeper-ties-historic-first-summit-chisinau-2025-07-04_en.

Dossier Center. “Диверсии с Безопасного Расстояния.” July 24, 2024. https://dossier.center/diversion/.

DW. “Germany: New Sabotage Warning Issued for Water Supply.” August 16, 2024. https://www.dw.com/en/germany-new-sabotage-warning-issued-for-water-supply/a-69958621.

DW. “NATO to Confront Russian ‘sabotage’ Attempts — Stoltenberg.” June 13, 2024. https://www.

dw.com/en/nato-to-confront-russian-sabotage-attempts-stoltenberg/a-69350359.

Ehand, Epp. "Estonia's Spy Chief: Russia Not Planning to Attack a Baltic Country at This Time." *ERR*, December 29, 2025. https://news.err.ee/1609896976/estonia-s-spy-chief-russia-not-planning-to-attack-a-baltic-country-at-this-time.

Einmaa, Iida-Mai. "Estonia to Establish 1,000-Strong Crisis Unit to Curb Migration Attacks." *ERR*, October 20, 2024. https://news.err.ee/1609497499/estonia-to-establish-1-000-strong-crisis-unit-to-curb-migration-attacks.

Einmann, Andres. "Igor Taro: Meie Andmetel on Vene Relvastatud Üksus Saatse Saapa Juurest Lahkunud." *Postimees*, October 11, 2025. https://www.postimees.ee/8340944/igor-taro-meie-andmetel-on-vene-relvastatud-uksus-saatse-saapa-juurest-lahkunud.

ERR. "Arson Attack on Ukrainian Restaurant in Estonia Ordered by Russian Intelligence." News. July 2, 2025. https://news.err.ee/1609735683/arson-attack-on-ukrainian-restaurant-in-estonia-ordered-by-russian-intelligence.

ERR. "Captain of Ship That Destroyed Balticconnector Pipeline Appears in Hong Kong Court." July 5, 2025. https://news.err.ee/1609738404/captain-of-ship-that-destroyed-balticconnector-pipeline-appears-in-hong-kong-court.

ERR. "Damage from Russia's GPS Jamming Amounts to over €500,000, Estonia Says." July 31, 2025. https://news.err.ee/1609759581/damage-from-russia-s-gps-jamming-amounts-to-over-500-000-estonia-says.

ERR. "DDoS Cyberattacks Temporarily Disrupt Estonian Government Websites." April 22, 2022. https://news.err.ee/1608573376/ddos-cyberattacks-temporarily-disrupt-estonian-government-websites.

ERR. "EstLink 2 Repair Work Starts in the Gulf of Finland." May 22, 2025. https://news.err.ee/1609701564/estlink-2-repair-work-starts-in-the-gulf-of-finland.

ERR. "Estonian Court Sentences Woman to 16 Months in Prison for Violating Sanctions." April 15, 2025. https://news.err.ee/1609665356/estonian-court-sentences-woman-to-16-months-in-prison-for-violating-sanctions.

ERR. "Estonian Defense League Member Jailed for Collaborating with Russian Intelligence." October 7, 2025. https://news.err.ee/1609822980/estonian-defense-league-member-jailed-for-collaborating-with-russian-intelligence.

ERR. "Finnair Suspends Flights to Tartu for 1 Month to Seek GPS Jamming Solution." April 29, 2024. https://news.err.ee/1609328058/finnair-suspends-flights-to-tartu-for-1-month-to-seek-gps-jamming-solution.

ERR. "ISS: Russian Special Services behind Attack on Estonian Minister's Car." February 20, 2024. https://news.err.ee/1609258853/iss-russian-special-services-behind-attack-on-estonian-minister-s-car.

ERR. "Pro-Russian Activist Handed 6.5 Year Prison Sentence for Vandalizing Minister's Car." December 5, 2024. https://news.err.ee/1609542394/pro-russian-activist-handed-6-5-year-prison-sentence-for-vandalizing-minister-s-car.

ERR. "Prosecutor: Pro-Kremlin Agitator Tried to Set up Armed Anti-State Militia in Estonia." News. May 27, 2025. https://news.err.ee/1609705992/prosecutor-pro-kremlin-agitator-tried-to-set-up-armed-anti-state-militia-in-estonia.

ERR. "Russia's New Jammer Increases GPS Interference on Estonia's Eastern Border." July 24, 2025. https://news.err.ee/1609752713/russia-s-new-jammer-increases-gps-interference-on-estonia-s-eastern-border.

Eto Buziashvili. "Russia Is Directly and Indirectly Meddling in Georgia's Upcoming Election." Atlantic Council, October 23, 2024. https://www.atlanticcouncil.org/blogs/new-atlanticist/russia-is-directly-and-indirectly-meddling-in-georgias-upcoming-election/.

European Parliament. "2023 and 2024 Reports on Moldova." June 18, 2025. https://www.europarl.europa.eu/doceo/document/TA-10-2025-0131_EN.html.

European Parliament. "President Maia Sandu Says Russia Wants to Turn Moldova against Europe." September 9, 2025. https://www.europarl.europa.eu/news/en/press-room/20250905IPR30176/president-maia-sandu-says-russia-wants-to-turn-moldova-against-europe.

EUvsDisinfo. "Being Occupied as a Privilege." June 24, 2020. https://euvsdisinfo.eu/being-occupied-as-a-privilege_baltic_states/.

EUvsDisinfo. "Disinfo: France Is Not a Sovereign Country." May 18, 2021. https://euvsdisinfo.eu/report/france-is-not-a-sovereign-country/.

Eydoux, Thomas, and Margaux Farran. "Pour discréditer l'Ukraine, la Russie organise de faux rassemblements en Europe." *Le Monde*, May 8, 2023. https://www.lemonde.fr/international/article/2023/05/07/pour-discrediter-l-ukraine-la-russie-organise-de-faux-rassemblements-en-europe_6172447_3210.html.

Fagan, Moira, Sneha Gubbala, and Jacob Poushter. "Views of NATO." Pew Research Center, June 23, 2025. https://www.pewresearch.org/global/2025/06/23/views-of-nato-2025/.

Federal Ministry of the Interior. "Protecting the 2025 Bundestag Elections from Hybrid Threats and Disinformation." https://www.bmi.bund.de/SharedDocs/schwerpunkte/EN/disinformation-election/disinformation-election-artikel.html.

Ferran, Lee. "Estonia Won't 'Fall into' Russia's 'Trap' by Overreacting to Hybrid Attacks: Defense Minister." Breaking Defense, July 9, 2024. https://breakingdefense.com/2024/07/estonia-wont-fall-into-russias-trap-by-overreacting-to-hybrid-attacks-defense-minister/.

Field, Madeline. "Putin's Spies for Hire: What the U.K.'s Biggest Espionage Trial Revealed about Kremlin Tactics in Wartime Europe." War on the Rocks, April 8, 2025. https://warontherocks.com/2025/04/putins-spies-for-hire-what-the-u-k-s-biggest-espionage-trial-revealed-about-

kremlin-tactics-in-wartime-europe/.

Flashpoint. “Killnet: Inside the World’s Most Prominent Pro-Kremlin Hacktivist Collective.” https://flashpoint.io/intelligence-101/killnet/.

Flotte Fantôme Russe : L’Europe Hausse Le Ton Après l’arraisonnement Au Large de Saint-Nazaire. October 20, 2025. https://www.ouest-france.fr/europe/russie/flotte-fantome-russe-leurope-hausse-le-ton-apres-larraisonnement-au-large-de-saint-nazaire-7e94ab86-adac-11f0-a829-eb0d2e70677d.

Follorou, Jacques. “Derrière l’opération avortée d’un Russo-Ukrainien à Roissy-en-France, une vaste campagne de sabotage orchestrée depuis Moscou.” *Le Monde*, June 27, 2024. https://www.lemonde.fr/societe/article/2024/06/26/derriere-l-operation-avortee-d-un-russo-ukrainien-a-roissy-en-france-une-vaste-campagne-de-sabotage-orchestree-depuis-moscou_6244099_3224.html.

Follorou, Jacques. “Man arrested with explosives near Paris airport was part of vast Russian sabotage campaign.” *Le Monde*, June 27, 2024. https://www.lemonde.fr/en/france/article/2024/06/27/man-arrested-with-explosives-near-paris-airport-was-part-of-vast-russian-sabotage-campaign_6675959_7.html.

Follorou, Jacques. “Têtes de Cochon Devant Des Mosquées : L’enquête Privilégie La Piste Du Renseignement Militaire Russe.” *Le Monde*, September 27, 2025. https://www.lemonde.fr/societe/article/2025/09/27/tetes-de-cochon-devant-des-mosquees-l-enquete-privilegie-la-piste-du-renseignement-militaire-russe_6643121_3224.html.

Fouda, Malek. “Russia Instructed Arson Attack on Ukrainian Restaurant, Estonia Says.” *Euronews*, n.d. http://www.euronews.com/my-europe/2025/07/03/estonia-says-arson-attack-on-ukrainian-restaurant-was-order-by-russias-intelligence-servic.

FP Analytics. “Lessons from Estonia’s Whole-of-Society Approach to Cyber Defense: A Q&A with Hanno Pevkur.” Digital Front Lines, August 31, 2023. https://digitalfrontlines.io/2023/08/31/lessons-from-estonias-whole-of-society-approach-to-cyber-defense/.

France 24. “France Blames Russia’s FSB for Anti-Semitic Star of David Graffiti Campaign.” February 23, 2024. https://www.france24.com/en/france/20240223-france-blames-russia-s-fsb-for-anti-semitic-star-of-david-graffiti-across-paris.

France 24. “France to Invest Nearly €3 Billion in Semiconductor Factory to Boost Local Production.” June 5, 2023. https://www.france24.com/en/europe/20230605-france-to-invest-nearly-%E2%82%AC3-billion-in-semiconductor-factory-to-boost-local-production.

Galeotti, Mark. “Active Measures: Russia’s Covert Geopolitical Operations.” George C. Marshall European Center For Security Studies, June 2019. https://www.marshallcenter.org/en/publications/security-insights/active-measures-russias-covert-geopolitical-operations-0.

Gattringer, Chris. “Estonia Starts Building up to 600 Bunkers along Border with Russia.” Brussels Signal, December 18, 2025. https://brusselssignal.eu/2025/12/estonia-starts-building-up-to-600-bun-

kers-along-border-with-russia/.

Geoffroy, Romain, and Maxime Vaudano. “Quels Sont Les Liens de Marine Le Pen Avec La Russie de Vladimir Poutine ?” *Le Monde*, April 20, 2022. https://www.lemonde.fr/les-decodeurs/article/2022/04/20/quels-sont-les-liens-de-marine-le-pen-avec-la-russie-de-vladimir-poutine_6122903_4355770.html.

Germany Targeted by the Pro-Russian Disinformation Campaign “Doppelgänger.” Federal Foreign Office, 2024. https://www.auswaertiges-amt.de/resource/blob/2682484/2da31936d1cbeb9faec49df74d8bbe2e/technischer-bericht-desinformationskampagne-doppelgaenger-1--data.pdf.

Giannopoulos, Georgios, Hanna Smith, and Marianthi Theocharidou. *The Landscape of Hybrid Threats: A Conceptual Model*. European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), 2021. https://doi.org/10.2760/44985.

Giles, Keir. “Russia’s ‘New’ Tools for Confronting the West: Continuity and Innovation in Moscow’s Exercise of Power.” Chatham House, March 21, 2016. https://www.chathamhouse.org/2016/03/russias-new-tools-confronting-west-continuity-and-innovation-moscows-exercise-power.

Giuashvili, Teona. “France’s Eastern Zeitenwende?” Elcano Royal Institute, May 8, 2024. https://www.realinstitutoelcano.org/en/analyses/frances-eastern-zeitenwende/.

Gleicher, Nathaniel. “Removing Coordinated Inauthentic Behavior from Russia.” Meta, January 17, 2019. https://about.fb.com/news/2019/01/removing-cib-from-russia/.

Goncharova, Olena. “Russian Sensors Found Tracking UK Nuclear Submarines, Sunday Times Reports.” *The Kyiv Independent*, April 7, 2025. https://kyivindependent.com/russian-sensors-found-tracking-uk-nuclear-submarines-sunday-times-reports/.

Halas, Matus. “NATO’s Sub-Conventional Deterrence: The Case of Russian Violations of the Estonian Airspace.” *Contemporary Security Policy* 43, no. 2 (2022): 350–81. https://doi.org/10.1080/13523260.2022.2028464.

Harrell, Margaret C., and Melissa A. Bradley. *Data Collection Methods: Semi-Structured Interviews and Focus Groups*. 2009. https://www.rand.org/pubs/technical_reports/TR718.html.

Hélène Février. “Guerre de 2008 En Géorgie : Le “cadeau“ de La France à La Russie.” *TV5 Monde*, August 7, 2013. https://information.tv5monde.com/international/guerre-de-2008-en-georgie-le-cadeau-de-la-france-la-russie-20009.

Helsinki Times. “Finnish Customs: Sanctioned Russian Steel Found on Fitburg.” January 1, 2026. https://www.helsinkitimes.fi/finland/finland-news/domestic/28371-customs-sanctioned-steel-cargo-found-on-fitburg-ship.html.

Henrotin, Joseph. “La Guerre Hybride Comme Avertissement Stratégique.” *Stratégique* 111, no. 1 (2016): 11–31. https://doi.org/10.3917/strat.111.0011.

Herzog, Stephen. “Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Re-

sponses." *Journal of Strategic Security* 4, no. 2 (2011): 49–60. https://doi.org/http://dx.doi.org/10.5038/1944-0472.4.2.3.

Hicks, Kathleen H. "Russia in the Gray Zone." *Center for Strategic & International Studies*, July 25, 2019. https://www.csis.org/analysis/russia-gray-zone.

Hoffman, Frank. "Armed vs Compound War." Armed Forces Journal, October 1, 2009. https://web.archive.org/web/20260111030304/http://armedforcesjournal.com/hybrid-vs-compound-war/.

Hoffman, Frank. "Conflict in the 21st Century: The Rise of Hybrid Wars." *Conflict in the 21st Century*, December 2007. https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

Hoorman, Chloé, and Elise Vincent. "Drones Au-Dessus de La Base Navale de l'île Longue : Les Autorités Françaises Assument Une Nouvelle Fois La Discrétion." *Le Monde*, December 10, 2025. https://www.lemonde.fr/international/article/2025/12/05/drones-au-dessus-de-la-base-navale-de-l-ile-longue-les-autorites-francaises-assument-une-nouvelle-fois-la-discretion_6656185_3210.html.

Horobin, William, Samy Adghirni, and Andrea Palasciano. "France's Macron Raises Defense Budget, Says Europe Under Threat." *Bloomberg*, July 13, 2025. https://www.bloomberg.com/news/articles/2025-07-13/france-s-macron-raises-defense-budget-says-europe-under-threat.

Human Rights Watch. "Georgia: Brutal Police Violence Against Protesters." December 23, 2024. https://www.hrw.org/news/2024/12/23/georgia-brutal-police-violence-against-protesters.

International Republican Institute. "IRI Georgia Poll Finds Support for EU Accession High, Weariness of Russian Presence, Lack of Faith in Political Parties." April 25, 2023. https://www.iri.org/news/iri-georgia-poll-finds-support-for-eu-accession-high-weariness-of-russian-presence-lack-of-faith-in-political-parties/.

ISFED. "Russian Information Operations in the 2024 Election Cycle." April 4, 2025. https://www.isfed.ge/eng/blogi/rusuli-sainformatsio-operatsia-2024-tslis-saparlamento-archevnebtan-dakavshirebit.

Iulian Ernst. "Russian Lawmakers Warn Moldova's Nato Aspirations May Lead to Its Destruction." IntelliNews, January 25, 2023. https://www.intellinews.com/russian-lawmakers-warn-moldova-s-nato-aspirations-may-lead-to-its-destruction-267920/.

Jon Shelton. "Germany: Nearly 90% of Voters Fear Manipulation." *DW*, February 6, 2025. https://www.dw.com/en/germany-nearly-90-of-voters-fear-foreign-manipulation/a-71528481.

Jonah, Anaella. *From Soft Power to Digital Firepower: France Steps up Fight against Disinformation*. September 8, 2025. https://www.france24.com/en/france/20250908-from-soft-power-to-digital-firepower-france-steps-up-against-online-disinformation-french-response.

Jonathan Greig. "New 'Curly' Threat Actor Found Targeting Sensitive Organizations in Georgia, Moldova." The Record, August 13, 2025. https://therecord.media/curly-threat-actor-targeting-moldo-

va.

Jones, Seth G. “Russia’s Shadow War Against the West.” Center for Strategic & International Studies, March 18, 2025. https://www.csis.org/analysis/russias-shadow-war-against-west.

Joseph Matveyenko. *Assessing the Impact of Disinformation on Minority Communities in Moldova*. No. 19. Media Forward. Freedom House, 2023. https://freedomhouse.org/sites/default/files/2023-12/fh-pb_19-Disinformation-Moldova-Minorities_Eng-v2.pdf.

Julia Smirnova, Karolin Schwarz, and Saman Nazari. “Storm-1516 and R-FBI: Russian Attempts to Interfere in the German Election.” Alliance4Europe, February 13, 2025. https://alliance4europe.eu/storm-1516-german-elections.

Juurvee, Ivo, and Anna-Mariita Mattiisen. *The Bronze Soldier Crisis of 2007: Revisiting an Early Case of Hybrid Conflict*. International Centre for Defence and Security, 2020. https://icds.ee/en/the-bronze-soldier-crisis-of-2007/.

Kaitseministeerium. “Estonia to Invest over €10 Billion in Defence in 2026-2029.” July 30, 2025. https://www.kaitseministeerium.ee/en/news/estonia-invest-over-eu10-billion-defence-2026-2029.

Kaitseministeerium. “Estonia’s Military Aid to Ukraine.” April 9, 2024. https://kaitseministeerium.ee/et/abi-ukrainale.

Kamil Frymark and Michał Kędzierski. “Germany: New Law on the Protection of Critical Infrastructure.” Centre for Eastern Studies (OSW), February 4, 2026. https://www.osw.waw.pl/en/publikacje/analyses/2026-02-04/germany-new-law-protection-critical-infrastructure.

Kavanagh, Jennifer, and Jeremy Shapiro. “The Bear in the Baltics: Reassessing the Russian Threat in Estonia – European Council on Foreign Relations.” European Council on Foreign Relations, December 18, 2025. https://ecfr.eu/publication/the-bear-in-the-baltics-reassessing-the-russian-threat-in-estonia/.

Keefe, Patrick Radden. “How Putin’s Oligarchs Bought London.” *The New Yorker*, March 17, 2022. https://www.newyorker.com/magazine/2022/03/28/how-putins-oligarchs-bought-london.

Kiel Institute. “Ukraine Support Tracker - A Database of Military, Financial and Humanitarian Aid to Ukraine.” December 10, 2025. https://www.kielinstitut.de/topics/war-against-ukraine/ukraine-support-tracker/.

Kofman, Michael. “Russian Hybrid Warfare and Other Dark Arts.” War on the Rocks, March 11, 2016. https://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/.

Kohv, Marek. “Estonia’s Robust Security Posture: Dispelling the ‘Is Narva Next?’ Narrative.” International Centre for Defense and Security, July 21, 2025. https://icds.ee/en/estonias-robust-security-posture-dispelling-the-is-narva-next-narrative/.

Lake, Jon. “Drone Activity over US Air Bases Blamed on Russian Agents.” Aerospace Global News, February 27, 2025. https://aerospaceglobalnews.com/news/drone-activity-over-us-air-bases-

blamed-on-russian-agents/.

Laura Daniels. “Russian Active Measures in Germany and the United States: Analog Lessons From the Cold War.” War on the Rocks, September 27, 2017. https://warontherocks.com/2017/09/russian-active-measures-in-germany-and-the-united-states-analog-lessons-from-the-cold-war/.

Lawless, Jill, and Danica Kirka. “Britain Boots 23 Russian Diplomats over Spy Poisoning.” AP News, March 14, 2018. https://apnews.com/article/db50f6e2d32b4f7482d32beee9a31c76.

Le Figaro. “Tags de cercueils liés au conflit ukrainien : plusieurs Moldaves seront jugés en février.” October 9, 2025. https://www.lefigaro.fr/international/tags-de-cercueils-lies-au-conflit-ukrainien-plusieurs-moldaves-seront-juges-en-fevrier-20251009.

Le Monde. “Bergerac : Un Drone a Survolé Un Site Produisant Des Tonnes de Poudre Pour l’armée Française, Une Enquête Ouverte.” November 11, 2025. https://www.lemonde.fr/economie/article/2025/11/11/bergerac-un-drone-a-survole-illegalement-un-site-de-production-de-poudre-de-la-societe-eurenco-une-enquete-ouverte_6653022_3234.html.

Le Monde. “Estonia Says Russia Flew Three Fighter Jets over Its Airspace.” September 20, 2025. https://www.lemonde.fr/en/russia/article/2025/09/19/estonia-says-russia-flew-three-fighter-jets-over-its-airspace_6745560_140.html.

Le Monde. “France: Two Moldovans Charged over Coffin Graffiti in Paris.” June 23, 2024. https://www.lemonde.fr/en/france/article/2024/06/22/france-two-moldovans-charged-over-coffin-graffiti-in-paris_6675480_7.html.

Le Monde. “Georgians celebrate EU candidate status.” December 15, 2023. https://www.lemonde.fr/en/international/article/2023/12/15/georgians-celebrate-eu-candidate-status_6347639_4.html.

Le Monde. “La Russie a Désigné La France Comme « son Principal Adversaire En Europe », Selon Le Chef d’état-Major Français.” July 11, 2025. https://www.lemonde.fr/international/article/2025/07/11/la-russie-a-designe-la-france-comme-son-principal-adversaire-en-europe-selon-le-chef-d-etat-major-francais_6620666_3210.html.

Lehberger, Roman, Sven Röbel, and Wolf Wiedmann-Schmidt. “Deutschlandweite Sabotageserie offenbar von Russland gesteuert.” *Der Spiegel*, February 5, 2025. https://www.spiegel.de/panorama/justiz/hunderte-autos-beschaedigt-deutschlandweite-sabotageserie-offenbar-aus-russland-gesteuert-a-7625e908-2f28-4ef8-bb69-35e5bacd6125.

Light, Felix. “Protesters Clash with Georgian Police over Government’s EU Application Delay.” *Reuters*, November 29, 2024. https://www.reuters.com/world/europe/georgia-says-it-will-not-enter-eu-membership-talks-until-2028-snub-brussels-2024-11-28/.

Lowe, Christian. “Russian Protesters ‘Lay Siege’ to Estonian Embassy.” *Reuters*, August 9, 2007. https://www.reuters.com/article/world/russian-protesters-lay-siege-to-estonian-embassy-idUSL03545498/.

Lucas, Edward. “Britain’s New Spy Chief Has a New Mission.” Foreign Policy, March 5, 2026. https://foreignpolicy.com/2026/01/23/mi6-sis-blaise-metreweli-intelligence-espionage-britain-russia/.

Maitland, Eva, Alice Lee, and Madeline Roache. “New Kremlin-Linked Influence Campaign Targeting Moldovan Elections Draws 17 Million Views on X and Infects AI Models.” *NewsGuard*, September 26, 2025. https://www.newsguardtech.com/special-reports/kremlin-linked-influence-campaign-targets-moldovan-elections-infects-ai-models.

Maitland, Eva, Madeline Roache, and Alice Lee. “Russia’s Matryoshka Propaganda Machine Picks New Target, Pushing 39 False Claims Against Moldova Over Past Three Months.” *NewsGuard*, July 15, 2025. https://www.newsguardtech.com/special-reports/russia-matryoshka-propaganda-moldova.

Margarita Antidze and Andrew Osborn. “Georgia and Russia Trade Blame over Unrest as Crisis Brews.” *Reuters*, June 21, 2019. https://www.reuters.com/article/world/georgia-and-russia-trade-blame-over-unrest-as-crisis-brews-idUSKCN1TM0O0/.

Market Design – Moldova Energy Profile. International Energy Agency, 2021. https://www.iea.org/reports/moldova-energy-profile/market-design.

Matsiuk, Iryna. “The Kremlin’s Shadow: Strategy and Tactics of Russian Interference in the Baltic States Elections.” Blue Europe, September 3, 2025. https://www.blue-europe.eu/analysis-en/full-reports/the-kremlins-shadow-strategy-and-tactics-of-russian-interference-in-the-baltic-states-elections/.

Mattis, James N., and Frank Hoffman. “Future Warfare: The Rise of Hybrid Wars.” U.S. Naval Institute, November 1, 2005. https://www.usni.org/magazines/proceedings/2005/november/future-warfare-rise-hybrid-wars.

McCarthy, Michael, Matthew Moyer, and Brett Venable. “Deterring Russia in the Gray Zone.” *Books, Monographs & Collaborative Studies*, March 20, 2019. https://press.armywarcollege.edu/monographs/379.

Mchugh, David. “Finland Stops Russia-Linked Vessel over Damaged Undersea Power Cable in Baltic Sea.” *AP News*, December 26, 2024. https://apnews.com/article/eu-finland-estonia-baltic-sea-power-cable-6741ef1ce9130602abac6214d7297717.

“Men Who Organised Russia-Backed Arson at London Warehouse Jailed.” *Counter Terrorism Policing*, October 24, 2025. https://www.counterterrorism.police.uk/men-who-organised-russia-backed-arson-at-london-warehouse-jailed/.

Morton, Becky, Jonathan Beale, and Damian Grammaticas. “UK Warns Putin after Russian Spy Ship Seen near British Waters.” *BBC*, January 23, 2025. https://www.bbc.com/news/articles/cqjv7qgpw28o.

Müller, Franziska, and Gavin Blackburn. “Russian Border Guards Briefly Cross into Estonian Territory, Foreign Ministry Says.” *Euronews*, December 18, 2025. http://www.euronews.com/2025/12/18/russian-border-guards-briefly-cross-into-estonian-territory-foreign-minis-

try-says.

Munich Airport. “Press: Another Drone Sighting at Munich Airport.” October 4, 2025. https://www.munich-airport.com/press-another-drone-sighting-at-munich-airport-35720233.

Natia Seskuria. “Georgia Elections 2024: Can Georgia Repair Its Relations With the EU and United States?” Foreign Policy, October 25, 2024. https://foreignpolicy.com/2024/10/25/georgia-elections-us-china-russia-eu-integration-diplomacy/.

Necsutu, Madalin. “Moldovans Face Bomb Threats and Cyberattacks.” Institute for War and Peace Reporting, September 5, 2022. https://iwpr.net/global-voices/moldovans-face-bomb-threats-and-cyberattacks.

Nicolas Quénel. *Allô, Paris ? Ici Moscou. Plongée Au Cœur de La Guerre de l’information*. Denoël, 2023.

Omand, David. “Hybrid CoE Working Paper 2: From Nudge to Novichok: The Response to the Skripal Nerve Agent Attack Holds Lessons for Countering Hybrid Threats.” The European Centre of Excellence for Countering Hybrid Threats, April 2018. https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-2-from-nudge-to-novichok-the-response-to-the-skripal-nerve-agent-attack-holds-lessons-for-countering-hybrid-threats/.

Pancevski, Bojan, Alistair MacDonald, and Bertrand Benoit. “U.S., Germany Foil Russian Plot to Kill Defense Executive.” *Wall Street Journal*, July 12, 2024. https://www.wsj.com/world/europe/u-s-germany-foil-russian-plot-to-kill-defense-executive-9cc497f3.

Paul, Christopher. “Confessions of a Hybrid Warfare Skeptic: What Might Really Be Interesting but Hidden Within the Various Conceptions of Gray Zone Conflict, Ambiguous Warfare, Political Warfare, and Their Ilk.” *Small Wars Journal*, March 3, 2016. https://archive.smallwarsjournal.com/index.php/jrnl/art/confessions-of-a-hybrid-warfare-skeptic.

Peleschuk, Dan. “Moldovan Police Launch Sweeping Raids over Alleged Russian Meddling.” *Reuters*, September 22, 2025. https://www.reuters.com/world/moldovan-police-raid-over-100-targets-russian-meddling-investigation-2025-09-22/.

Police and Border Guard Board. “Saatse Boot Transit Route Closed.” October 16, 2025. https://www.politsei.ee/en/the-vaerska-saatse-road.

Ponomareva, Viktoriia. “Changing Channels: How Three Years of Kremlin Propaganda Bans in the EU Have Affected Russian-Speaking Audiences.” The Insider, March 18, 2025. https://theins.ru/en/politics/279746.

Presidency of the Republic of Moldova. “President Maia Sandu’s Address in the Context of the Parliamentary Elections of September 28, 2025.” September 22, 2025. https://presedinte.md/eng/discursuri/adresarea-presedintei-maia-sandu-in-contextul-alegerilor-parlamentare-din-28-septembrie-2025.

Propastop (Estonian Defence League). “Why Did the Bomb Threat Cause Panic among Tallinn’s Russian Community but Not among Estonians?” November 20, 2025. https://www.propastop.org/

en/2025/11/20/why-did-the-bomb-threat-cause-panic-among-tallinns-russian-community-but-not-among-estonians/.

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

Radio Free Europe/Radio Liberty. “Moldova Accuses Moscow In Wave Of Vandalism In Capital Ahead Of Vote.” September 28, 2024. https://www.rferl.org/a/moldova-vandalism-russia-trained/33138585.html.

Radio Free Europe/Radio Liberty. “Moldovan Police Say They Foiled Russian-Backed Unrest Plot.” March 12, 2023. https://www.rferl.org/a/moldova-police-foil-russian-plot-unrest/32314304.html.

Rainsford, Sarah. “Moldova Election: Russian Cash-for-Votes Flows into Ukraine’s Neighbour as Nation Heads to Polls.” *BBC*, October 20, 2024. https://www.bbc.com/news/articles/c23kdjxxx1jo.

Ramani, Samuel. “Why Russia Is a Geopolitical Winner in Mali’s Coup.” Foreign Policy Research Institute, September 16, 2020. https://www.fpri.org/article/2020/09/why-russia-is-a-geopolitical-winner-in-malis-coup/.

Rasmussen, Louise. “Suspected Drones Seen over French Military Intelligence Base, Armed Forces Say.” *Reuters*, December 9, 2025. https://www.reuters.com/world/europe/suspected-drones-seen-over-french-military-intelligence-base-armed-forces-say-2025-12-09/.

Raufoglu, Alex. “Baltic Countdown: Estonia Warns Russia Will Return With More Troops, Equipment in ‘Two Years or Less.’” Kyiv Post, November 18, 2025. https://www.kyivpost.com/post/64408.

Rekawek, Kacper, Julian Lanchès, Maria Zotova, and Donald Bowser. “Russia’s Crime-Terror Nexus: Criminality as a Tool of Hybrid Warfare.” International Centre for Counter-Terrorism, September 30, 2025. https://icct.nl/publication/russias-crime-terror-nexus-criminality-tool-hybrid-warfare.

Republic of Moldova: 2021 Article IV Consultation and Requests for an Arrangement under the Extended Fund Facility and an Arrangement under the Extended Credit Facility-Press Release; Staff Report; and Statement by the Executive Director for the Republic of Moldova. International Monetary Fund, 2022. https://www.imf.org/en/publications/cr/issues/2022/01/04/republic-of-moldova-2021-article-iv-consultation-and-requests-for-an-arrangement-under-the-511622.

Reuters. “Germany Warns of Russian Disinformation Targeting Election.” February 21, 2025. https://www.reuters.com/world/europe/germany-warns-russian-disinformation-targeting-election-2025-02-21/.

Reuters. *Moldova Bans Another Pro-Russian Party from Sunday’s Vote*. September 27, 2025. https://www.reuters.com/world/moldova-bans-another-pro-russian-party-sundays-vote-2025-09-27.

Reuters. “Moldova Declares Russian Deputy PM Rogozin Persona Non Grata.” August 2, 2017. https://www.reuters.com/article/world/moldova-declares-russian-deputy-pm-rogozin-perso-

na-non-grata-idUSKBN1AI1MY/.

Reuters. "Moldova Says Russian Agents Spent 200 Mln Euro to Rig Votes Last Year." April 2, 2024. https://www.reuters.com/world/europe/moldova-says-russian-agents-spent-200-mln-euro-rig-votes-last-year-2025-04-02/.

Reuters. "Putin Orders Suspension of Passenger Flights from Russia to Georgia." June 21, 2019. https://www.reuters.com/article/world/putin-orders-suspension-of-passenger-flights-from-russia-to-georgia-idUSKCN1TM2IE/.

Reuters. "Russia Must Not Be Humiliated despite Putin's 'historic' Mistake, Macron Says." June 4, 2022. https://www.reuters.com/world/europe/russia-must-not-be-humiliated-despite-putins-historic-mistake-macron-2022-06-04/.

Reuters. "Russia Set to Resume Imports of Georgian Wine and Water." February 4, 2013. https://www.reuters.com/article/business/russia-set-to-resume-imports-of-georgian-wine-and-water-idUSL5N0B4737/.

Revue Nationale Stratégique 2025. Secrétariat général de la défense et de la sécurité nationale, 2025. http://www.sgdsn.gouv.fr/publications/revue-nationale-strategique-2025.

Riigi Kaitseinvesteeringute Keskus. "Baltic Defence Line." January 2024. https://www.kaitseinvesteeringud.ee/en/baltic-defence-line/.

Riigikogu. "The Riigikogu Established a Committee of Investigation for Russia's Influence Activities." January 21, 2026. https://www.riigikogu.ee/en/news-from-committees/constitutional-committee/the-riigikogu-established-a-committee-of-investigation-for-russia-s-influence-activities/.

Robin Emmott. "Russia Using Gas to Bully Moldova, Says EU." *Reuters*, October 28, 2021. https://www.reuters.com/business/energy/gas-being-weaponised-against-moldova-eu-says-2021-10-28/.

Royal Navy. "Royal Navy Activated Twice in Two Weeks to Intercept Russian Ships in UK Waters." November 24, 2025. https://www.royalnavy.mod.uk/news/2025/november/24/20251124-royal-navy-tracks-russian-ships-including-research-ship-yantar.

Russian Invasion of Ukraine Narrative Report: Germany. Global Disinformation Index, 2023. https://www.disinformationindex.org/.

Rutenberg, Jim. "RT, Sputnik and Russia's New Theory of War." *The New York Times*, September 13, 2017. https://www.nytimes.com/2017/09/13/magazine/rt-sputnik-and-russias-new-theory-of-war.html.

Ruy, Donatienne. "Did Russia Influence Brexit?" Center for Strategic & International Studies, July 21, 2020. https://www.csis.org/blogs/brexit-bits-bobs-and-blogs/did-russia-influence-brexit.

Sabbagh, Dan. "Spy Ring Plotted to Obtain Details from Phones of Ukrainians at US Airbase in Germany, UK Court Hears." *The Guardian*, December 3, 2024. https://www.theguardian.com/uk-news/2024/dec/03/spy-ring-plotted-to-obtain-details-from-phones-of-ukrainians-at-us-air-

base-in-germany-uk-court-hears.

Saman Nazari, Eto Buziashvili, Victoria Olari, et al. “Still Marching on(Line): How R-FBI Targets Moldova’s Elections.” Alliance4Europe, September 26, 2025. https://alliance4europe.eu/still-marching-online-how-r-fbi-targets-moldovas-elections.

Samkharadze, Nino. “Georgian Dream’s Populist Conservatism: Fight to Legitimise and Hold On to Power.” *GIP*, no. 68 (March 2017). https://gip.ge/publication-post/georgian-dreams-populist-conservatism-fight-to-legitimise-and-hold-on-to-power/.

Santos, Sofia Ferreira. “Third Man Charged over Fires at Homes Linked to Keir Starmer.” *BBC*, May 21, 2025. https://www.bbc.com/news/articles/c8xgg7rr1q8o.

Sauer, Pjotr, and Shaun Walker. “Explosive Sex Toys and Cosmetics: The Story behind the DHL Parcels Plot.” *The Guardian*, May 5, 2025. https://www.theguardian.com/world/2025/may/05/explosive-sex-toys-and-cosmetics-the-story-behind-the-dhl-parcels-plot.

Schaaf, Matthew, and Andrew Rogan. “A Lesson in Resilience: Moldova’s Resistance to Election Interference.” International Foundation for Electoral Systems, December 17, 2025. https://www.ifes.org/publications/lesson-resilience-moldovas-resistance-election-interference.

Schofield, Hugh. “Russia Link Suspected in Eiffel Tower Coffin Mystery.” *BBC*, June 3, 2024. https://www.bbc.com/news/articles/cldd7n97dvro.

Schuetze, Christopher F. “Germany Accuses Russia of Sabotage, Cyberattacks and Disinformation.” World. *The New York Times*, December 12, 2025. https://www.nytimes.com/2025/12/12/world/europe/germany-russia-cyberattacks-sabotage-hybrid-war.html.

Seely, Robert. “Defining Contemporary Russian Warfare: Beyond the Hybrid Headline.” *RUSI Journal* 162, no. 1 (2017): 50–59. https://doi.org/10.1080/03071847.2017.1301634.

Shlapak, David A., and Michael Johnson. *Reinforcing Deterrence on NATO’s Eastern Flank: Wargaming the Defense of the Baltics*. RAND Corporation, 2016. https://www.rand.org/pubs/research_reports/RR1253.html.

Smolentceva, Natalia. “Estonians Prepare to Defend Themselves against Russia.” *DW*, December 10, 2024. https://www.dw.com/en/estonian-volunteers-prepare-for-potential-russian-attack/a-70436904.

Sorg, Alexander. “Force de l’Europe: How Realistic Is a French Nuclear Umbrella?” War on the Rocks, March 24, 2025. https://warontherocks.com/2025/03/force-de-leurope-how-realistic-is-a-french-nuclear-umbrella/.

Souverbie, Louise. “Russian Incursions and Hybrid Warfare: Europe Under Aerial Pressure.” IRIS, September 26, 2025. https://www.iris-france.org/en/russian-incursions-and-hybrid-warfare-europe-under-aerial-pressure/.

Spriņģe, Inga, Holger Roonemaa, and Michael Weiss. “Exclusive: Inside Russia’s Latvian Sabotage

Squad." The Insider. https://theins.ru/en/politics/272989.

Stent, Angela. *Putin's World: Russia Against the West and with the Rest*. Twelve, 2019.

Stephen Jones and Natalie Sabanadze. "Perspectives | Elections Are Not Enough: Georgia Needs a New Model of Democracy." Eurasianet, March 10, 2023. https://eurasianet.org/perspectives-elections-are-not-enough-georgia-needs-a-new-model-of-democracy.

Suc, Matthieu. "Opération « Mains Rouges » : Des Agents Provocateurs Néonazis à La Solde Du Kremlin." Mediapart, January 2, 2025. https://www.mediapart.fr/journal/international/020125/operation-mains-rouges-des-agents-provocateurs-neonazis-la-solde-du-kremlin.

Sytas, Andrius. "Estonia Says It Repelled Major Cyber Attack after Removing Soviet Monuments." *Reuters*, August 18, 2022. https://www.reuters.com/world/europe/estonia-says-it-repelled-major-cyber-attack-after-removing-soviet-monuments-2022-08-18/.

Tags de Cercueils En Lien Avec l'Ukraine: Quatre Hommes Nés En Moldavie Jugés à Paris En Février. October 9, 2025. https://www.laprovence.com/article/france-monde/34850979070970/tags-de-cercueils-en-lien-avec-lukraine-quatre-hommes-nes-en-moldavie-juges-a-paris-en-fevrier.

Tanas, Alexander. "Thousands in New Moldova Anti-Government Protest." *Reuters*, October 23, 2022. https://www.reuters.com/world/europe/thousands-new-moldova-anti-government-protest-2022-10-23/.

Tellier, Maxime. "Derrière Les Tags d'étoiles de David à Paris, Un Vaste Réseau de Désinformation Russe." *Radio France*, January 26, 2024. https://www.franceinfo.fr/enquetes-franceinfo/enquete-franceinfo-derriere-les-tags-d-etoiles-de-david-a-paris-un-vaste-reseau-de-desinformation-russe_6325623.html.

The Economist. "Armin Papperger: The German Arms Boss Russia Wants Dead." May 21, 2025. https://www.economist.com/europe/2025/03/21/armin-papperger-the-german-arms-boss-russia-wants-dead.

The Economist. "In the Kremlin's Pocket: Who Backs Putin, and Why." February 12, 2015. https://www.economist.com/briefing/2015/02/12/in-the-kremlins-pocket.

The Guardian. "MI5 Forced to 'Pare Back' Counter-Terrorism Work Due to Rogue States, Says Chief." December 6, 2024. https://www.theguardian.com/uk-news/2024/dec/06/mi5-forced-to-pare-back-on-counter-terrorism-work-due-to-hostile-states-says-agency-chief.

The Soufan Center. "Georgian Dream or Democratic Nightmare? The Struggle for Democracy Amid Voter Fraud and Russian Interference." October 30, 2024. https://thesoufancenter.org/intelbrief-2024-october-30/.

The Soufan Center. "Moldova's Gas Crisis: The Cost of Defying Russia." January 17, 2025. https://thesoufancenter.org/intelbrief-2025-january-17/.

The Soufan Center. "Winning the Battle, Not the War: Moldova's Fight Against the Kremlin's Hybrid

Arsenal." September 30, 2025. https://thesoufancenter.org/intelbrief-2025-september-30/.

"The Statement of the Ministry of Foreign Affairs of Georgia Concerning the Illegal So-Called Presidential Elections Held in the Occupied Abkhazia Region." February 15, 2025. https://mfa.gov.ge/en/statements-by-mfa/894797-saqartvelos-sagareo-saqmeta-saministros-gantskhadeba-okupirebul-aphkhazetis-regionshi-chatarebuli-uk.

Tim Zadorozhnyy. *Estonian Defense Minister on NATO's Response to Russian Threats*. Kyiv Independent. 2025. https://www.youtube.com/watch?v=KKRN1cQUmLw.

Tom Balmforth and Alexander Tanas. "Moldova's Sandu Decries 'unprecedented' Meddling as EU Referendum Goes to Wire." *Reuters*, October 20, 2024. https://www.reuters.com/world/europe/moldova-votes-election-eu-referendum-shadow-alleged-russian-meddling-2024-10-20/.

Tran, Mark. "Enter Sarkozy the Peacemaker." *The Guardian*, August 12, 2008. https://www.theguardian.com/world/2008/aug/12/georgia.russia4.

Tsurkan, Kate. "Moldova Casts Blame on Russia for Attempts to Disrupt Pivotal Parliamentary Elections." *The Kyiv Independent*, September 28, 2025. https://kyivindependent.com/moldovas-election-infrastructure-targeted-in-mass-cyber-attacks-during-consequential-parliamentary-elections/.

Tuhina, Gjeraqina. "Two Years Into EU Ban, Russia's RT And Sputnik Are Still Accessible Across The EU." *Radio Free Europe/Radio Liberty*, February 3, 2024. https://www.rferl.org/a/russia-rt-sputnik-eu-access-bans-propaganda-ukraine-war/32803929.html.

Tzu, Sun. "The Art of War." Accessed January 30, 2026. https://classics.mit.edu/Tzu/artwar.html.

Van Puyvelde, Damien. "Hybrid War – Does It Even Exist?" NATO Review, May 7, 2015. https://web.archive.org/web/20241125174159/https://www.nato.int/docu/review/articles/2015/05/07/hybrid-war-does-it-even-exist/.

Vignal, François. "Ukraine : Comment Expliquer l'évolution d'Emmanuel Macron Face à La Russie ?" Public Sénat, March 2024. https://www.publicsenat.fr/actualites/international/ukraine-comment-expliquer-levolution-demmanuel-macron-face-a-la-russie.

Vladimir Socor. "Moldova Outlaws Shor's Russophile Party, but the Threat Persists (Part One)." Jamestown, June 21, 2023. https://jamestown.org/moldova-outlaws-shors-russophile-party-but-the-threat-persists-part-one/.

Walker, Shaun. "'These People Are Disposable': How Russia Is Using Online Recruits for a Campaign of Sabotage in Europe." *The Guardian*, May 4, 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.

Whewell, Tim. "The Great Moldovan Bank Robbery." *BBC*, June 18, 2015. https://www.bbc.com/news/magazine-33166383.

Wilkinson, Isabella, and Tamar Dekanosidze. “Georgia Must Bolster Resilience to Information Warfare.” Chatham House, March 8, 2023. https://www.chathamhouse.org/2022/03/georgia-must-bolster-resilience-information-warfare.

Yorke, Harry. “Revealed: Russia’s Secret War in UK Waters.” *The Times*, April 5, 2025. https://www.thetimes.com/uk/defence/article/russia-secret-war-uk-waters-submarines-dpbzphfx5.

Министерство иностранных дел Российской Федерации. “The Concept of the Foreign Policy of the Russian Federation.” March 31, 2023. https://www.mid.ru/ru/detail-material-page/1860586/?lang=en.

Официальное опубликование правовых актов. “Указ Президента Российской Федерации От 02.07.2021 № 400 ‘О Стратегии Национальной Безопасности Российской Федерации.’” July 2, 2021. http://publication.pravo.gov.ru/Document/View/0001202107030001.

The Soufan Center is a 501c3 non-profit organization

THE SOUFAN CENTER

156 W 56th Street
New York, NY
10019

Phone
+1 646-248-6486
Email
info@thesoufancenter.org
Website
www.thesoufancenter.org