CNA

MAY 2025

Quantity Has a Quality All of Its Own

The Transformation of Russian Intelligence Operations Since the Ukraine Invasion

Elena Grossfeld

IOP-2025-U-041545-Final

CNA

Abstract

This report examines a shift in Russian intelligence from precision operations toward a broader, quantity-driven strategy that has become visible since Russia's 2022 full-scale invasion of Ukraine. Russia's increasing sabotage, intelligence collection, and influence efforts highlight the systemic factors driving this departure from the Cold War–era KGB approach. This shift aligns with broader trends in Russian military and strategic thinking, echoing the "meat grinder" tactics Russia has used in warfare in Ukraine and drawing comparisons to high-performance systems, in which multiples of cheap, off-the-shelf components are employed to achieve strategic goals rather than higher cost, more precise parts. This report also explores the implications of this shift for Russian intelligence efficacy and resource management, as well as for the future of Russian intelligence operations, ultimately arguing that Russia's growing reliance on mass-scale, less specialized tactics could redefine the effectiveness and scope of its intelligence efforts moving forward.

APPROVED FOR PUBLIC RELEASE. Unlimited distribution. **May 2025**

This report is part of a series generously funded by a grant from the Carnegie Corporation of New York.

This work was performed under Specific Authority Contract No. G-19-56503.

Cover image: Russian Presidential Administration, Dec. 19, 2016.

Approved by: **May 2025**

David Knoll, Research Program Director
Countering Threats and Challenges Program
Strategy, Policy, Plans, and Programs Division

Request additional copies of this document through inquiries@cna.org.

Executive Summary

Since the full-scale invasion of Ukraine, Russian intelligence operations have shifted toward a mass-scale approach, focusing on sabotage, intelligence collection, and influence efforts. This transformation is driven by Russia's expanding operational demands, even as it is constrained by mass expulsions of intelligence officers and the urgency to ramp up operations. In response, Russian intelligence has prioritized quantity over quality, relying on multiple cheap, inefficient, and nonprofessional resources. Sheer numbers compensate for inefficiency, and anonymity provides an added layer of plausible deniability.

A key driver of this shift has been the Kremlin's efforts to undermine Western support for Ukraine, which disrupted Russia's plans for a quick victory. Russian intelligence—Russia's primary strategic tool since the Soviet era—was tasked with imposing costs on the North Atlantic Treaty Organization (NATO), shaping public opinion, disrupting arms shipments, and gathering intelligence. However, with diminished capabilities and a decline in professionalism, Russian intelligence has moved away from precision-driven, professionalized operations to a mass-scale, decentralized model that mirrors broader trends in Russian military strategy. This change aligns with Russian military and strategic thinking, in which materiel shortages are compensated by sheer numbers and indifference to casualties. This transformation has significant implications for intelligence efficacy, resource management, and global security.

The shift from quality to quantity

Historically, Soviet intelligence operations during the era of the KGB (the Russian Committee for State Security) were marked by precision and the use of highly trained operatives. These operations focused on high-value targeted objectives such as the infiltration of foreign governments, high-profile assassinations, and covert activities.[1] After the disintegration of the Soviet Union in 1991, Russian intelligence largely maintained this approach throughout the post–Cold War period. Although subtle changes might have begun to emerge during Russia's initial operations in Ukraine in 2014, the dramatic shift became unmistakable during the full-scale invasion in 2022. In recent years, Russia's intelligence operations have increasingly prioritized quantity over precision, mirroring a broader trend in its military strategy, particularly the "meat grinder" tactics that favor overwhelming force over precision. The shift also reflects a high-performance systems design approach in which multiple low-cost, off-the-shelf components replace expensive, custom-built solutions to achieve strategic goals.

Surge in sabotage, intelligence collection, and influence operations

Russian intelligence has long been Russia's primary tool for achieving strategic results, with sabotage

[1] The KGB (1954–1991) was established as a successor to previous security agencies such as the NKVD (the People's Commissariat for Internal Affairs, 1934–1946) and the VChK (the All-Russian Extraordinary Commission, 1917–1922).

being one of its main methods. The rise in sabotage operations targeting critical infrastructure, military sites, transportation networks, and manufacturing and storage facilities reflects the shift from precision to mass-scale tactics. These operations are wide-ranging and indiscriminate, with targets spanning from vital infrastructure—such as water treatment facilities in Finland—to retail locations, such as IKEA stores in Lithuania and Poland. Designed to undermine the West's support for Ukraine while remaining below the threshold of active warfare, these attacks highlight the scale and ambition of Russian intelligence efforts. This wave of sabotage has been accompanied by intensified influence operations and intelligence gathering, complementing campaigns of disinformation, cyberattacks, and manipulation of public opinion, reaching unprecedented levels and threatening NATO cohesion.

Expansion of Russian intelligence activities

The surge in Russian intelligence operations has the potential to expand Russia's global reach, driven by recruitment across diverse populations, including refugees, ethnic Russians, Russia sympathizers, and criminals. Social media, encrypted channels such as Telegram, and anonymous online recruitment underscore the decentralized and cost-effective nature of these activities. Cryptocurrency facilitates covert payments, bypassing traditional financial systems. This approach closely mirrors Islamist terrorist recruitment, relying on vulnerable individuals, encrypted communication channels, and financial or ideological incentives to recruit agents.

Implications for intelligence efficacy and global security

The shift toward quantity-driven intelligence tactics poses significant challenges for global law enforcement and counterintelligence efforts. Although mass-scale, less specialized operations reduce precision and increase the risk of failure, they can cause widespread damage, casualties, and fear. From a broader security perspective, the shift from quality to quantity in Russian intelligence operations threatens regional stability and could have far-reaching consequences for global security.

Recommendations

To counter Russia's growing intelligence capabilities and mitigate the risks posed by the shift in Russian intelligence strategies, we offer the following recommendations:

1. **Strengthen intelligence collaboration and integration.** Enhanced coordination and information sharing among NATO and its allies will enable a unified and proactive response to Russian intelligence activities, facilitating quicker identification and disruption of sabotage or intelligence-gathering activities.

2. **Improve attribution and analysis capabilities.** A key challenge to Russia's evolving tactics is the difficulty in timely attribution. Improving attribution techniques and accelerating disclosure will enable faster, more coordinated responses, reducing the effectiveness of Russian covert operations.

3. **Enhance monitoring of social media and encrypted communication platforms.** Enhanced monitoring of messaging and social media platforms used by Russian intelligence for recruiting is critical. Similarly, it is essential to engage with platform providers to ensure speedy cooperation with law enforcement and counterintelligence agencies. Preventing cryptocurrency trading bots from operating on noncompliant crypto exchanges restricts Russia's ability to conduct untraceable financial operations. It is also crucial to continuously identify platforms suitable for recruitment to anticipate and counter shifts in Russian intelligence operations.

4. **Develop outreach programs in vulnerable communities.** Raising awareness of Russian intelligence recruitment tactics among vulnerable communities—such as ethnic Russians, Ukrainian refugees, and migrant populations—by expanding outreach programs and strengthening collaboration with local law enforcement enhances vigilance and facilitates identification and disruption of recruitment attempts for sabotage or espionage.

5. **Emphasize rapid disclosure and public awareness.** Rapid disclosure of suspected Russian sabotage or influence attempts enhances public awareness and strengthens response efforts. Timely investigations and public attribution help counter disinformation, limit the effects of influence operations, and prevent the spread of misinformation. Public awareness campaigns reinforce resilience against manipulation.

6. **Adapt to the evolving nature of warfare and intelligence.** Russia's growing focus on mass-scale intelligence operations calls for NATO and its allies to reevaluate current counterintelligence strategies. Governments and international bodies need to adapt to a landscape in which quantity-driven, decentralized operations are increasingly common. Effective responses require flexibility in resource management, intelligence gathering, and counterintelligence strategies to address the growing complexity of Russian intelligence operations.

Conclusion

The shift in Russian intelligence operations reflects increased operational demands coupled with capability constraints. The move from precision-driven specialized operations to mass-scale, low-cost strategies signals a fundamental transformation in how Russia conducts intelligence operations. Although this shift poses significant challenges to global security, the international community can adapt to and mitigate the risks by enhancing collaboration, improving attribution capabilities, and adjusting strategies to counter Russia's growing reliance on quantity-driven intelligence. By doing so, NATO and its allies can better safeguard both regional and global stability in the face of evolving threats.

PAGE INTENTIONALLY BLANK

Table of Contents

PAGE INTENTIONALLY BLANK

Introduction

Just as Russia's invasion of Ukraine prompted the West to reassess long-held beliefs about the Russian military, the recent surge in Russian sabotage, influence operations, and other intelligence activities demands that the West reevaluate Russian intelligence. Russia's shift toward a strategy focused on quantity over quality marks a sharp departure from traditional intelligence methods and carries profound implications for global security.

During the Cold War, Soviet intelligence was viewed as a highly trained, professional force that excelled at intelligence activities and active measures and ran tightly coordinated operations orchestrated by Moscow. However, recent developments point to a significant departure from this disciplined model. Following the disintegration of the Soviet Union in 1991, Russian intelligence largely continued operating in familiar patterns, engaging in activities made familiar to the West during the Cold War, with no major visible transformation. Although some changes were visible in 2014, the full-scale invasion of Ukraine in 2022 marked a decisive break from past practices, shifting toward mass-scale, decentralized, and less professionalized intelligence operations. The days of highly orchestrated, ideologically driven operations are over. Instead, intelligence officers who are unconcerned with risks and indifferent to consequences devise haphazard activities to be carried out by a motley crew of untrained, unprofessional gig economy workers. These operatives have little regard for operational security or ideological commitment, functioning as disposable assets controlled from afar and managed through anonymous messengers.

The spike in operations carried out on behalf of the Kremlin suggests a shift in Russian intelligence toward prioritizing quantity over quality. This shift

Russia's shift toward a strategy focused on quantity over quality marks a sharp departure from traditional intelligence methods and carries profound implications for global security.

resembles the infamous Russian "meat grinder" approach in Ukraine, in which bodies are thrown at a problem in overwhelming numbers rather than with strategic precision. Although this shift from quality to quantity may seem to align with the dialectical materialist principle asserting that quantitative changes can eventually lead to qualitative ones, ideology is unlikely to be driving the surge in operations carried out by untrained personnel outside traditional intelligence frameworks. A more plausible explanation is that systemic incentives, operational needs, and the new constraints placed on Russian intelligence after the full-scale invasion of Ukraine have forced this change. The benefits of a quantity-driven gig economy model—such as scaling operations and overwhelming adversaries—resemble principles from high-performance systems design, in which success comes from replication rather than precision.

The recent surge in Russian intelligence activities has raised significant concerns among North Atlantic Treaty Organization (NATO) allies, intelligence

communities, and law enforcement agencies in the West. Viewing itself as under attack by the West, Russia appears to be revisiting its Cold War–era playbook. However, this time there is a notable shift in focus—from prioritizing high-quality, precise intelligence operations to prioritizing quantity. Sabotage operations, a part of the Soviet-era approach, are now a central element of Russia's broader efforts to undermine NATO support for Ukraine, demonstrating the same shift in focus from specialized high-precision operations to a more quantity-driven approach.

This occasional paper examines the shift in priorities of Russian intelligence operations, analyzing the surge in sabotage, intelligence collection, and influence operations to explore the systemic factors driving this change, particularly in the context of Russia's full-scale invasion of Ukraine.

This occasional paper examines the shift in priorities of Russian intelligence operations, analyzing the surge in sabotage, intelligence collection, and influence operations to explore the systemic factors driving this change, particularly in the context of Russia's full-scale invasion of Ukraine. The paper examines how Russian intelligence has moved away from the precision and specialized operations of the Cold War–era KGB (the Russian Committee for State Security) and suggests that this shift aligns with broader trends in Russian strategic thinking, including the long-standing meat grinder tactics in military operations. This approach mirrors high-performance systems design, where lower-cost, off-the-shelf components replace expensive custom-built ones to achieve performance goals. Ultimately, the paper examines the implications of this shift for Russian intelligence efficacy and resource management, as well as for the future of Russian intelligence operations.

The first section, "Russian Sabotage: Distorted Echoes of the Cold War," compares the current Russian intelligence approach to sabotage with the KGB's approach to sabotage during the Cold War. Russia's sabotage, espionage, and influence operations are an evolving adaptation to modern constraints; the country's success in leveraging the gig economy to recruit untrained operatives through digital platforms highlights the benefits of the newer model. This section contrasts the current recruitment patterns with the more precise, coordinated, and ideologically driven operations and recruitment demands of the KGB during the Cold War.

The second section, "Influence Operations: Same Song, Off-Key," explores the shift in influence operations from the highly controlled, ideologically driven strategies of the Cold War to the broader, more indiscriminate approach of Russian intelligence today. Despite this shift, the goals of Russian intelligence still align with those of the KGB: sowing discord and destabilizing adversaries. They continue to use familiar methods, such as exploiting racial tensions and manipulating public sentiment, but where the KGB's operations were ideologically grounded and precise, their current methods are neither.

The third section, "Decoding the Shift," analyzes factors, among them operational constraints, the decline in professionalism, and the need for rapid scaling in response to geopolitical pressure, that are driving the shift in Russian intelligence practices. In combination with historical and systemic influences, those drivers have contributed to the prioritization of quantity over quality in intelligence operations.

The concluding section, "Quantity over Quality: Implications for Global Security and Intelligence Collaboration," discusses the broader consequences of Russia's quantity-driven intelligence approach for global security and explores the risks associated with the surge in Russian operations, as well as potential consequences such as destabilization, civilian casualties, and effects on international relations. This section outlines the ramifications of these tactics and the new challenges they present for NATO and Western intelligence agencies as they strive to safeguard regional and global stability. Despite the limited success of these quantity-driven operations, their effects are already significant, underscoring the need for a coordinated response. In its final paragraphs, the section offers recommendations for responding to Russia's evolving intelligence operations approach.

Russian Sabotage: Distorted Echoes of the Cold War

Reports of accidents and near-accidents suspected to be the result of Russian sabotage operations now appear with alarming regularity, their frequency increasing continuously since the onset of Russia's full-scale invasion of Ukraine. What began a decade ago as a handful of carefully targeted sabotage operations—executed by dedicated GRU (Special Forces of the Main Directorate) operatives—against arms and munitions depots supplying Russia's adversaries has since become a veritable flood, covering civilian infrastructure, businesses, and military installations.

Recent waves of Russian sabotage have cast a wide net, targeting both vital infrastructure and more ordinary sites in Europe, the United Kingdom, and potentially the US.[2] Among the critical infrastructure targets were water treatment facilities in Finland and critical transportation hubs and power lines in Norway.[3] Russia also targeted industrial and manufacturing facilities—both those unrelated to Ukraine war efforts, such as a telecommunications company in Lithuania; a paint factory in Wroclaw, Poland; and an Ikea store in Vilnius, and those directly supporting the war, such as Mesko arms factory in Poland, Diehl weapons factory in Berlin, and a munitions factory in Wales—and Ukrainian businesses in London.[4] US military bases in Germany and NATO military

Recent waves of Russian sabotage have cast a wide net, targeting both vital infrastructure and more ordinary sites in Europe, the United Kingdom, and potentially the US. Among the critical infrastructure targets were water treatment facilities in Finland and critical transportation hubs and power lines in Norway.

[2] Isabel van Burgen, "Mysterious Accidents at US, Ally's Defense Facilities Spark Sabotage Fears," *Newsweek*, Apr. 19, 2024, https://www.newsweek.com/us-nato-defense-facilities-ukraine-russia-sabotage-1892099.

[3] Insikt Group, *Russian Sabotage Activities Escalate amid Fraught Tensions*, 2024, https://www.recordedfuture.com/research/russian-sabotage-activities-escalate-amid-fraught-tensions; Sigmund Brandvold, "Norwegian Intelligence Assessment on Russian Interference," The Jamestown Foundation, Nov. 9, 2024, https://jamestown.substack.com/p/norwegian-intelligence-assessment.

[4] AlexandruC4 (@AlexandruC4), "Law enforcement authorities have detained two Spanish nationals who were planning to carry out a terrorist act in the city of Šiauliai in northern Lithuania," Post, X, Nov. 20, 2024, 3:09 p.m., https://x.com/AlexandruC4/status/1859358524125610264; "Poland Arrests Nine Suspects over Alleged Russian Sabotage Plot," *Guardian*, May 20, 2024, https://www.theguardian.com/world/article/2024/may/20/poland-arrests-nine-suspects-over-alleged-russian-sabotage-plot; Insikt Group, *Russian Sabotage Activities Escalate*; Souad Mekhennet et al., "Russia Recruits Sympathizers Online for Sabotage in Europe, Officials Say," *Washington Post*, July 10, 2024, https://www.washingtonpost.com/world/2024/07/10/russia-sabotage-europe-ukraine/; Leo Chiu, "Explosion Rocks UK Munitions Factory in South Wales," *Kyiv Post*, Apr. 18, 2024, https://www.kyivpost.com/post/31331; Emine Sinmaz, "Briton Charged with Aiding Russia and Planning Arson Against Ukraine-Linked Business in UK," *Guardian*, Apr. 26, 2024, https://www.theguardian.com/uk-news/2024/apr/26/man-charged-conducting-hostile-activity-uk-benefit-russia.

bases in the Baltics were among the known targets of Russian sabotage.[5] The European rail network became a prime target for sabotage, ranging from plans to derail trains transporting Western arms to Ukraine to thousands of hacking attempts aimed at compromising railway signaling systems.[6] On several occasions, explosives-laden packages were shipped by air and exploded on the ground in shipping facilities, narrowly avoiding detonation in the air. These were reportedly dry runs aimed at sabotaging flights to the US and Canada.[7] In 2024, a veritable epidemic of incidents involving damage to major underwater communication cables and power transmission lines in the Baltic Sea were carried out by a range of ships, some of which appear to belong to Russia's "shadow fleet" of tankers transporting oil in defiance of sanctions.[8]

Taken together, these diverse acts of sabotage reveal a clear pattern of Russian sabotage operations. Broadly aligning with the principles of the KGB's Cold War sabotage doctrine, the current approach nonetheless suggests significant changes in strategy, tactics, and use of resources.[9] As multiple states raise alarms about the growing danger of escalation, the surge in Russian sabotage activities organized around gig economy principles and carried out by nontraditional and untrained operatives who are recruited via messenger apps, FSB-designed gaming platforms, and the dark net and paid through anonymous wire transfers and cryptocurrencies continues to grow.[10] In the decade before 2022, only a handful of sabotage acts occurred, but at least 50 have occurred since 2022, and 70 suspicious incidents took place in Europe in 2024 alone.[11]

---

[5] "German Secret Services Alarmed by Russian Threat," Voice of America, Oct. 14, 2024, https://www.voanews.com/a/7822201.html; Carina Huppertz et al., "'Make a Molotov Cocktail': How Europeans Are Recruited Through Telegram to Commit Sabotage, Arson, and Murder," OCCRP, Sept. 26, 2024, https://www.occrp.org/en/investigation/make-a-molotov-cocktail-how-europeans-are-recruited-through-telegram-to-commit-sabotage-arson-and-murder.

[6] Greg Miller, Loveday Morris, and Mary Ilyushina, "Russia Recruited Operatives Online to Target Weapons Crossing Poland," *Washington Post*, Aug. 18, 2023, https://www.washingtonpost.com/world/2023/08/18/ukraine-weapons-sabotage-gru-poland/; Carl Deconinck, "'Russia Trying to Sabotage European Railways,' Says Czech Transport Minister," Brussels Signal, Apr. 5, 2024, https://brusselssignal.eu/2024/04/russia-trying-to-sabotage-european-railways-says-czech-transport-minister/.

[7] Paul Kirby and Frank Gardner, "Mystery Parcel Fires Were 'Test Runs' to Target Cargo Flights to US, Says Poland," BBC, Nov. 5, 2024, https://www.bbc.com/news/articles/c07912lxx33o.

[8] John Leicester and Emma Burrows, "At Least 11 Baltic Cables Have Been Damaged in 15 Months, Prompting NATO to Up Its Guard," AP News, Jan. 28, 2025, https://apnews.com/article/nato-france-russia-baltic-cables-ships-damage-764964a275530915c2cc5af1125ec125; Matthew Powell, "Suspected Baltic Sea Cable Sabotage by Russia's 'Shadow Fleet' Is Ramping Up Regional Defence," University of Portsmouth, Jan. 28, 2025, https://www.port.ac.uk/news-events-and-blogs/blogs/academic-expertise/suspected-baltic-sea-cable-sabotage-by-russias-shadow-fleet-is-ramping-up-regional-defence; Michelle Wiese Bockmann, "Russia-Linked Cable-Cutting Tanker Seized by Finland 'Was Loaded with Spying Equipment,'" Lloyd's List, Dec. 27, 2024, https://www.lloydslist.com/LL1151955/Russia-linked-cable-cutting-tanker-seized-by-Finland-was-loaded-with-spying-equipment.

[9] Daniela Richterova, "The Long Shadow of Soviet Sabotage Doctrine?," War on the Rocks, Aug. 19, 2024, https://warontherocks.com/2024/08/the-long-shadow-of-soviet-sabotage-doctrine/.

[10] John T. Psaropoulos, "As War Rages, Russia Activates Soviet Sabotage Plans in Europe: Experts," Al Jazeera, May 29, 2024, https://www.aljazeera.com/news/2024/5/29/as-ukraine-war-rages-russia-activates-sabotage-plans-in-europe-experts; John Vandiver, "Russian Sabotage Is Escalating Risk of Greater Conflict in Europe, Army's Williams Says," *Stars and Stripes*, Oct. 15, 2024, https://www.stripes.com/theaters/europe/2024-10-15/russian-sabotage-us-army-nato-15515862.html; Daniela Richterova et al., "Russian Sabotage in the Gig-Economy Era," *The RUSI Journal* 169, no. 5 (2024), doi: 10.1080/03071847.2024.2401232; "Orders to Set Ukrainian Armed Forces Vehicles on Fire Appeared on the Darknet. Four Jeeps of Ukrainian Fighters Were Burned in One Night [В даркнете появились заказы на поджог машин ВСУ. За одну ночь были сожжены четыре джипа украинских бойцов — «Важные истории»]," The Insider, July 10, 2024, https://theins.ru/news/272991; Richterova et al., "Russian Sabotage in the Gig-Economy Era," p. 16.

[11] Agenstvo Novosti (agentstvonews), "Россия могла осуществить не менее 50 гибридных операций против 13 стран Европы с начала войны," Telegram post, Jan. 4, 2025, https://t.me/agentstvonews/8726; Emil Rottbøll and Kenneth Holm-Dahlin, "PET opruster markant mod russisk skyggekrig: Truslen fra fysisk sabotage i Danmark er skærpet," Berlingske, Jan. 30, 2025, https://www.berlingske.dk/content/item/1824430.

However, unlike previous GRU operations, such as the detonation of an ammunition depot in Bulgaria in 2011 and explosion of an ammunition depot in the Czech Republic in 2014 (both aimed at preventing munitions from reaching Russia's adversaries), these recent efforts have yielded questionable results, with many either failing or quickly being attributed to their perpetrators.[12] The approach used by the Russian military in Ukraine—throwing bodies at a problem—has led to similarly predictable outcomes for Russian intelligence. These temporary laborers, unburdened by ideology, paid per assignment, and motivated by financial incentives, are drawn from a variety of sources, including ethnic Russians and expatriates residing in the West, Ukrainian refugees, teenagers directed to use quest games for missile strikes, and small-time criminals acting as intermediaries to find and vet new recruits.[13] Despite obvious drawbacks, such as the vulnerability of open platforms to counterintelligence efforts and the short-term nature of engagement, which forces Russian intelligence operatives to seek new recruits constantly, this recruitment model allows Russian intelligence to conduct operations remotely by relying on a decentralized and often unreliable workforce. In Ukraine, both the FSB (Federal Security Service) and the GRU have been recruiting Ukrainians looking for "easy money" on Telegram channels and dating apps to assist Russian war efforts by placing explosives, conducting battle damage assessment (BDA), and providing targeting assistance for Russian drones and missiles.[14] In the Baltics, Russia-ordered operations ranged from setting fire to a museum dedicated to documenting the Soviet occupation and vandalizing national monuments to spying on a NATO air base.[15]

In cyberwarfare, long considered a key tool in Russian intelligence's disruptive strategy, the shift toward a quantity-driven approach has been noted. Precise numbers of total Russian cyberattacks and cyber espionage efforts are not readily available, but data from Ukraine reveal a recurring pattern of preference for quantity at the expense of quality. Although the number of cyberattacks in Ukraine grew, the sharp drop in high-severity incidents indicates a systemic shift in focus on quantity at the cost of achieving meaningful results.[16] Favoring symbolic high-volume operations designed to create an appearance of success, often at the expense of careful preparation or strategic outcomes, this approach generates persistent disruption in target systems despite the limited strategic effect of individual operations.[17] Since Russia's involvement in Ukraine began in

[12] Richterova et al., "Russian Sabotage in the Gig-Economy Era," p. 19.

[13] Oleg Sokolenko, "В ФРГ предъявили обвинения предполагаемым российским шпионам," dw.com, Dec. 30, 2024, https://www.dw.com/ru/v-frg-predavili-obvinenia-predpolagaemym-rossijskim-spionam/a-71187895; Jarek (@jarek_jakimczyk) Jakimczyk, "Podejrzany o #szpiegostwo," Post, X, Oct. 18, 2024, 4:58 a.m., https://x.com/jarek_jakimczyk/status/1847230750501867923; Darina Antoniuk, "Ukraine Uncovers Russian Spy Network Recruiting Teens for Espionage," The Record, Dec. 13, 2024, https://therecord.media/ukraine-sbu-espionage-campaign-russia; Holger Roonemaa and Inga Springe, "From Kyiv to Riga: Russian Sabotage Operations in the Baltics," Re:Baltica, July 10, 2024, https://en.rebaltica.lv/2024/07/2970/.

[14] SBU (SBUkr), "СБУ затримала агента російського гру," Telegram post, Sept. 9, 2024, https://t.me/SBUkr/12858; SBU (SBUkr), "СБУ затримала коригувальника фсб, якого завербували через сайти знайомств," Telegram post, Oct. 9, 2024, https://t.me/SBUkr/13073; SBU (SBUkr), "СБУ та Нацполіція затримали неповнолітніх агентів рф, які підірвали вибухівки поблизу двох райвідділів поліції у Харкові," Telegram post, Dec. 16, 2024, https://t.me/SBUkr/13599; *How Russian Spies Use Cell Phones as OPs*, Tradecraft Sunday, Posted by Spy Collection (YouTube, Dec. 22, 2024), Video, https://www.youtube.com/watch?v=C-TiHFcAJtk.

[15] Huppertz et al., "Make a Molotov Cocktail."

[16] State Service of Special Communications and Information Protection of Ukraine, *Russian Cyber Operations: APT Activity Report H1 2024*, Sept. 2024, https://cip.gov.ua/en/news/cyber-operations-rf-h1-2024-report.

[17] Gavin Wilde, *Russia's Countervalue Cyber Approach: Utility or Futility?*, Carnegie Endowment for International Peace, Feb. 2024, https://carnegieendowment.org/research/2024/02/russias-countervalue-cyber-approach-utility-or-futility?lang=en.

2014, Russian intelligence has ramped up its cyber operations, expanding recruitment efforts by drawing in students from technical colleges, farming out work to private companies, and enlisting cybercriminals to support its war efforts.[18] Although both the personnel count and the volume of cyberattacks have apparently increased, there has been no corresponding improvement in results beyond high demands for defender resources and resilience as Ukraine adjusted to periodic disruption of digital services.

This operational strategy, deliberately erratic in its execution and focused on quantity at the expense of quality, could not be more different from the Cold War–era approach demonstrated by Soviet intelligence.

This operational strategy, deliberately erratic in its execution and focused on quantity at the expense of quality, could not be more different from the Cold War–era approach demonstrated by Soviet intelligence. Unlike present efforts, the KGB's sabotage operations were meticulously planned, with carefully selected targets designed to disrupt the West's military plans and political stability in the event of escalating conflict. Until such escalation occurred, the KGB engaged in more subtle and covert tactics, using active measures to manipulate public opinion, influence foreign governments, and destabilize adversaries.

The KGB's sabotage doctrine determined three primary goals for its operations: demoralizing the public, weakening the adversary's military and economic capacities, and sowing discord among allied nations.[19] A dedicated KGB directorate was tasked with identifying appropriate targets in Europe and North America, including critical infrastructure and communication systems. The directorate planned and prepared sabotage operations to be carried out by both Soviet agents and local "resistance" groups, set up arms caches, and planned future operations aimed at wreaking havoc, such as poisoning water systems, assassinating leaders, and blowing up military installations.[20] The success of the KGB's planned sabotage operations depended on the professionalism of its operatives, who were carefully selected and rigorously educated to ensure that their expertise and ideological commitment aligned with the KGB's operational objectives.

Today, Russian intelligence recruiting approaches differ from those Russia used during the Cold War. Ideological alignment and education were viewed as critical to the effectiveness and loyalty of KGB agents, both Soviet and foreign. Seen by some at the time as an ideological beacon lighting the way to a better life for the masses, the Soviet Union had many foreign agents working for them who collaborated for purely ideological reasons, an option that is no longer available to contemporary Russia. Soviet

[18] Andrei Soldatov and Irina Borogan, *Russian Cyberwarfare: Unpacking the Kremlin's Capabilities*, Center for European Policy Analysis, Sept. 2022, https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/; Patrick Howell O'Neill, "U.S. Sanctions Russian Companies Linked to FSB," CyberScoop, June 11, 2018, https://cyberscoop.com/russian-sanctions-fsb-digital-security-erpscan/; "Treasury Targets Corruption and the Kremlin's Malign Influence Operations in Moldova," US Department of the Treasury, Oct. 26, 2022, https://home.treasury.gov/news/press-releases/jy1049.

[19] "The Long Shadow of Soviet Sabotage Doctrine?"

[20] Christopher M. Andrew and Vasilij N. Mitrochin, *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB* (New York: Basic Books, 2001), p. 359; Oleg Kalugin, *Spymaster: My Thirty-Two Years in Intelligence and Espionage Against the West* (New York: Basic Books, 2009), p. 147.

citizens selected as agents for operations in the West had to be well-versed in Marxism-Leninism, the decisions of the Communist Party of the Soviet Union (CPSU) Central Committee, and Soviet foreign policy goals. They were also expected to understand the political climate in their destination country and be able to discuss the advantages of socialism and the drawbacks of capitalism. Upon their return, they were required to report on their missions.[21] Equally important was the "ideological and political education" of foreign agents, particularly those recruited to act as acquisition agents (those tasked with recruiting others), which required additional training in communications and secure operations.[22]

Those recruited for financial incentives or through blackmail were subjected to even greater scrutiny and oversight. Because agent recruitment was the ultimate goal of intelligence officers, KGB textbooks emphasized the importance of studying candidates thoroughly and building personal rapport, acknowledging the lack of motivation among those recruited under duress and stressing the need for constant monitoring to ensure continued cooperation.[23] Continuous personal communication with agents was considered essential for an intelligence officer, an approach that starkly contrasts with an anonymously run Telegram channel.[24]

Every operational task related to covert intelligence collection—"aimed at gathering specific and relevant information about a target individual or group, important enemy objects, their activities, and specific characteristics"—required professionalism and careful preparation.[25] In current Russian intelligence practice, by contrast, untrained agents are sent to photograph important NATO military installations equipped with rented devices under their real names and are prone to writing down assignments on paper only to lose it.[26] This shift away from precision and quality, evident in Russia's sabotage efforts, extends to other areas of Russian intelligence as well, including influence operations, in which similar tactics of scale and impersonal execution are used.

[21] Ju Ju Petkevicius, *Recommendations of the 1st Department of the LSSR KGB Concerning the Preparation of the Agency for Work Abroad*, KGB, 1981, KGB Documents, https://www.kgbdocuments.eu/documents/recommendations-of-the-1st-department-of-the-lssr-kgb-concerning-the-preparation-of-the-agency-for-work-abroad/.

[22] KGB, *Working with Agents Rabota s Agenturoj* (1970); KGB, *Acquisition and Training of Agent Recruiters* (Higher Intelligence School of the Committee for State Security, 1988).

[23] KGB, *Recruitment of Agents Verbovka Agentury* (1969).

[24] KGB, *Communication with Agents* (Higher Intelligence School of the Committee for State Security).

[25] Lt. Colonel I. A. Stepanov, *Iz Opyta Provedenia Operativnykh Ustanovok*, Kafedra Spezialnoi Distsiplini I (Moscow: Higher School of KGB 101, 1965).

[26] "From Kyiv to Riga."

Influence Operations: Same Song, Off-Key

Russians are once again conducting influence operations, but their methods have changed significantly from previous eras. A rehash of the KGB's old playbook is once again in demand—Russian intelligence is seeking to actively shape public sentiment in the West and increase societal tensions. Today, multiple Russian intelligence agencies have sprung into action, aiming to instill fear and uncertainty about the future and incite protests against Western support for Ukraine. Protests organized and funded by Russian intelligence taking place across Europe were attended by a "roving troupe of Russian hirelings" who, coincidentally, were also recruiting people online to be photographed for a fee.[27]

In a similar manner, the Russian intelligence approach to influence operations has shifted toward broader, less targeted tactics. Gone is the highly coordinated, ideologically driven strategy of the past, focused on precision and long-term influence. In its place, contemporary Russian tactics prioritize high-volume, fast-paced initiatives aimed at sowing discord and distrust without concern for a coherent narrative. New technologies have enabled the rapid scaling of these operations, allowing the recruitment of unwitting operatives who may be unaware of or indifferent to the operations' true objectives. Russian disinformation—although deserving separate analysis because of its scope—clearly demonstrates a similar shift from quality to quantity.

In cases in which Russian intelligence cannot organize its own protests, it is quick to exploit genuine demonstrations for causes completely unrelated to its targets. By placing operatives with Ukraine-related posters and slogans, Russian intelligence ensures that the photographs produced are spread far and wide to amplify their message.

In cases in which Russian intelligence cannot organize its own protests, it is quick to exploit genuine demonstrations for causes completely unrelated to its targets. By placing operatives with Ukraine-related posters and slogans, Russian intelligence ensures that the photographs produced are spread far and wide to amplify their message.[28] This tactic allows Russian intelligence to hijack authentic public

[27] Christo Grozev, Roman Dobrokhotov, and Michael Weiss, "'Morality and Ethics Should Play No Part': Leaks Reveal How Russia's Foreign Intelligence Agency Runs Disinformation Campaigns in the West," The Insider, July 4, 2024, https://theins.ru/en/politics/272870.

[28] Thomas Eydoux, Margaux Farran, and Le Monde's Video Investigation Team, "How Russia Is Staging Fake Protests in Europe to Discredit Ukraine," *Le Monde*, May 7, 2023, https://www.lemonde.fr/en/international/article/2023/05/07/how-russia-is-staging-fake-protests-in-europe-to-discredit-ukraine_6025808_4.html.

sentiment and manipulate perceptions, furthering its agenda while maintaining a façade of grassroots support.

Other incidents orchestrated by Russian intelligence aimed to exacerbate societal tensions and sow unrest. These included the desecration of monuments, attempts to manipulate public sentiment by placing coffins under the Eiffel Tower, drawings of Stars of David in Paris to incite fear, planned provocations at public events, and attempts to intimidate and physically attack dissidents.[29]

Despite their high volume, these influence operations have yet to produce any visible results. The majority of EU governments remain committed to continuing military and other aid to Ukraine, and public opinion in Europe and the United States—reflected in recent polls—shows sustained support for Ukraine despite Russian disinformation efforts. Although Russia's current approach is characterized by an often broad and indiscriminate manner, a similar focus on shaping public opinion and destabilizing adversaries was a hallmark of Soviet-era intelligence tactics, albeit carried out with more caution and professionalism. Aimed at undermining Soviet adversaries, the KGB's influence operations were a critical tool in its broader strategy of covert influence. These operations sought to shape public sentiment and increase societal tensions; contemporary Russian intelligence faithfully executes the same tactics.

Then as now, capitalizing on racial tensions is among the favorite tactics of Russian influence operations. The KGB dispatched letters to African diplomats in the United Nations designed to appear as though from racist Americans, delivered antisemitic letters to Jewish leaders, and paid agents to vandalize synagogues and desecrate Jewish cemeteries in New York and Washington.[30] Their success in sparking a wave of antisemitic actions in West Germany was especially fruitful, leaving Bonne to struggle with grave international repercussions.[31] However, unlike today, Cold War–era influence operations were far less likely to be immediately attributed to Soviet intelligence.[32]

Relying on a long tradition of active measures, the KGB's influence operations were ideologically grounded, carefully vetted, and consistent, designed

---

[29] Aušra Mindaugas, Indrė Makaraitytė, and LRT Investigation Team, "International Investigation: Russian Special Forces Change Tactics in the Baltics," LRT, Oct. 30, 2024, https://www.lrt.lt/en/news-in-english/19/2401273/international-investigation-russian-special-forces-change-tactics-in-the-baltics; Kim Willsher, "Russian Interference Suspected After Coffins Draped with Tricolour Placed at Eiffel Tower," *Guardian*, June 3, 2024, https://www.theguardian.com/world/article/2024/jun/03/russian-interference-suspected-coffins-at-eiffel-tower-paris; "France Investigates Foreign Connection to Daubing of Stars of David," Reuters, Nov. 7, 2023, https://www.reuters.com/world/europe/france-investigates-foreign-connection-daubing-stars-david-2023-11-07/; Christo Grozev, Michael Weiss, and Roman Dobrokhotov, "Красная звезда Мишлен. The Insider выявил повара-агента, готовившего провокации на Олимпиаде в Париже, он арестован," The Insider, July 25, 2024, https://theins.ru/politika/273341; "Attack on Navalny Aide Was Work of Russian Special Services, Says Lithuania Counter-Intelligence," Reuters, Mar. 14, 2024, https://www.reuters.com/world/europe/attack-navalny-aide-was-work-russian-special-services-says-lithuania-counter-2024-03-14/.

[30] Kalugin, *Spymaster*, p. 54.

[31] US Department of State Global Engagement Center, *More than a Century of Antisemitism: How Successive Occupants of the Kremlin Have Used Antisemitism to Spread Disinformation and Propaganda*, Jan. 2024, https://www.state.gov/wp-content/uploads/2024/01/GEC-Special-Report-More-than-a-Century-of-Antisemitism.pdf.

[32] "Vandals Again Desecrate Jewish Cemetery," *New York Times*, June 4, 1977, https://www.nytimes.com/1977/06/04/archives/vandals-again-desecrate-jewish-cemetery.html.

to damage the reputation and image of adversary states while advancing Soviet foreign policy goals.[33] These operations were often run by specialists in Department A at KGB headquarters and coordinated with the ideologues of the International Department at the CPSU.[34] To create the appearance of mass support in capitalist states, influence operations were coordinated with friendly organizations such as the World Peace Council and foreign communist parties, which helped generate the illusion of a lack of foreign intervention.[35]

In modern Russia, the surge in sabotage and influence operations prioritizing quantity over quality appears to be an attempt to compensate for the reduced effectiveness. Because Russian influence operations reflect a departure from the carefully orchestrated operations of the KGB, understanding the driving forces behind this shift requires examining several key factors, such as the need for rapid operational scaling and the decline in professionalism and ideological commitment.

[33] E. A. Gorbunov, "«ДЕЗИНФОРМАЦИЯ... УВЕЛИЧИВАЕТ И ОБЕСПЕЧИВАЕТ УСПЕХ КОМПАНИИ: Документы российских архивов о первых шагах работы по советской дезинформации. 1922–1925 гг.»," Almanakh "Rossiya. XX Vek" Arkhiv Aleksandra N. Yakovleva, accessed Sept. 19, 2024, https://www.alexanderyakovlev.org/almanah/inside/almanah-intro/1000406; Christopher Andrew and Oleg Gordievsky, *KGB: The Inside Story of Its Foreign Operations from Lenin to Gorbachev* (New York: Perennial, 1991), p. 463; Andrew and Gordievsky, *KGB*, pp. 503–505.

[34] Wayne Lambridge, *A Note on KGB Style*, CIA, https://www.cia.gov/resources/csi/static/Note-on-KGB-Style.pdf.

[35] Andrew and Gordievsky, *KGB*, pp. 503–505.

Decoding the Shift

Western support for Ukraine, which enabled the country to resist Russian aggression and undermined Russia's plans for a quick victory, prompted Russian leadership to direct Russia's intelligence services to focus on undercutting this support. Russian intelligence has been the "Kremlin's principal strategic tool, exalted over the military" since the Soviet era and remains the central instrument of statecraft, a legacy that continues to shape post-Soviet Russia's pursuit of its strategic objectives.[36] Russian intelligence aimed to impose costs, influence public opinion in NATO states, disrupt arms shipments, and gather intelligence on NATO locations critical to supporting Ukraine while also collecting intelligence within Ukraine to support Russian military operations. The combination of increased demand for intelligence collection, sabotage, and influence operations; reduced operational capabilities after the invasion; the decline in professionalism; and reliance on Cold War–era tactics forced Russian intelligence to adopt an approach that ultimately prioritized quantity over quality.

Russian intelligence has been the "Kremlin's principal strategic tool, exalted over the military" since the Soviet era and remains the central instrument of statecraft, a legacy that continues to shape post-Soviet Russia's pursuit of its strategic objectives.

The reduction in operational capacity came as a response to prolonged Russian belligerence and aggression. What started as a brief honeymoon period between Russia and the West after the end of the Cold War, during which Russian intelligence operatives were stationed under diplomatic cover in the West in great numbers, ended with mass expulsion of these operatives. The first wave, which began after former Russian double agent Sergei Skripal and his daughter Yulia were poisoned with a military-grade nerve agent in the United Kingdom in 2018, intensified after the invasion of Ukraine, reducing the Russian diplomatic presence in Europe by 600, of which 400 were judged to be spies.[37]

[36] Yaacov Falkov, "Intelligence-Exalting Strategic Cultures: A Case Study of the Russian Approach," *Intelligence and National Security* 37, no. 1 (2022), doi: 10.1080/02684527.2021.1978135.

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

Russian illegals fared no better; several were arrested, and others managed to escape before arrest.[38] Opportunistic collection was similarly hindered as travel from Russia to the West declined, visas were no longer issued, and Russian airlines were banned from flying over Europe, forcing out seconded intelligence officers stationed in Russian companies under cover.[39] Despite these challenges, Russian intelligence found it necessary to not only continue its operations but also expand in both Europe and Ukraine, necessitating a shift in its approach.

Unable to rely on its own workforce of professional operatives for its sabotage, influence, and intelligence collection operations, Russian intelligence turned to tasking gig economy workers recruited on Telegram and other messaging applications popular among refugees, Russia sympathizers, small-time criminals, and others looking for a quick buck without asking too many questions.[40] This gig economy pattern provides the necessary flexibility and speed in recruiting for operations that are separated into atomic tasks, reducing the need for specialized training while maintaining compartmentalization among agents.[41] It also echoes a long-standing strategy rooted in both Russian and Soviet military tradition known as the "meat grinder," that is, "'using mass to overwhelm defensive positions and achieve tactical gains.'"[42] Based on the premise of abundant manpower, a fundamental principle since the days of the Russian empire, its ultimate goal is to overwhelm and exhaust the opponent. Russian intelligence's adoption of this principle, in which success is measured in not only specific tactical wins but also sustained disruption and pressure, relies on expendable agents recruited through "trash fishing."[43] The scalability and low cost ensure a constant state of below-the-threshold conflict with the aim of avoiding escalation while still destabilizing adversaries.

Despite reduced operational capacity in the West, the need to compensate for technological and capability gaps has driven increased demand for Russian intelligence collection. Russia's declining space capabilities have significantly affected its invasion of Ukraine. Unreliable satellites, insufficient coverage, and inferior sensors—combined with delays in image processing, coordination, and information delivery—have deprived the Russian military of critical intelligence, contributing to

---

[38] The term *illegals* refers to intelligence agents who operate under the guise of normal jobs, rather than under diplomatic cover. Shaun Walker, "Russian Spies Sentenced in Slovenia After Pleading Guilty," *Guardian*, July 31, 2024, https://www.theguardian.com/world/article/2024/jul/31/russian-spies-sentenced-slovenia-court-prisoner-exchanges; Dan Sabbagh, "Russian Spy Caught Trying to Infiltrate War Crimes Court, Says Netherlands," *Guardian*, June 16, 2022, https://www.theguardian.com/law/2022/jun/16/russian-spy-caught-trying-to-infiltrate-war-crimes-court-says-netherlands; Christo Grozev, "Socialite, Widow, Jeweller, Spy: How a GRU Agent Charmed Her Way into NATO Circles in Italy," Bellingcat, Aug. 25, 2022, https://www.bellingcat.com/news/2022/08/25/socialite-widow-jeweller-spy-how-a-gru-agent-charmed-her-way-into-nato-circles-in-italy/.

[39] "European Union: Council Suspends Visa Facilitation Agreement with Russia," Library of Congress, Sept. 20, 2022, https://www.loc.gov/item/global-legal-monitor/2022-09-20/european-union-council-suspends-visa-facilitation-agreement-with-russia/; Anastasia Dagaeva, "Turbulent Times: How Russian Airlines Are Weathering the Storm," Carnegie Politika, Mar. 28, 2023, https://carnegieendowment.org/russia-eurasia/politika/2023/02/turbulent-times-how-russian-airlines-are-weathering-the-storm?lang=en; Sergei Kanev, "Отлетались. Как из-за войны с Украиной развалилась резидентура ГРУ в «Аэрофлоте» и где теперь эти шпионы," The Insider, June 9, 2023, https://theins.info/obshestvo/262031.

[40] Richterova et al., "Russian Sabotage in the Gig-Economy Era."

[41] Richterova et al., "Russian Sabotage in the Gig-Economy Era," p. 16.

[42] Paul Adams, "Russia's 'Meat-Grinder' Tactics Bring Battlefield Success - but at Horrendous Cost," BBC, Dec. 6, 2024, https://www.bbc.com/news/articles/c0ewneynypwo; Becky Alexis-Martin, "Russia's 'Meat Grinder' Tactics in Ukraine Have Proved Effective in Past Wars – but at Terrible Cost," The Conversation, Oct. 21, 2024, http://theconversation.com/russias-meat-grinder-tactics-in-ukraine-have-proved-effective-in-past-wars-but-at-terrible-cost-241688.

[43] Huppertz et al., "Make a Molotov Cocktail."

operational inefficiencies and civilian casualties.[44] These limitations have led to inferior targeting and complicated BDA. Although reports indicate that China has assisted the Russian war effort by providing geospatial intelligence and remote sensing data, gaps in satellite intelligence, along with institutional constraints hindering effective integration on the battlefield, continue to pressure Russian intelligence to fill intelligence, surveillance, and reconnaissance (ISR) deficiencies.[45]

The ongoing challenges in collecting actionable intelligence on arms shipments into Ukraine and on Western military and industrial facilities supporting Ukraine's war efforts have been among the drivers for the recruitment of gig economy workers in Ukraine, Poland, and Germany.[46] To satisfy this need, workers were tasked with planting cell phones and installing cameras in strategic locations to compensate for the lack of up-to-date satellite imagery. This shift to using gig economy workers highlights the adaptability of Russian intelligence in response to high-tech intelligence gaps, further underscoring the trend toward prioritizing quantity over quality in operations.

This shift to using gig economy workers highlights the adaptability of Russian intelligence in response to high-tech intelligence gaps, further underscoring the trend toward prioritizing quantity over quality in operations.

Organizational culture contributes to this shift. Known for its preference for loyalty over professionalism, the Russian intelligence system is structured to prioritize action over results. Intelligence failures, whether due to poor operational security or inadequate strategic assessments before the Ukraine invasion, are often overlooked, whereas those who follow orders diligently are rewarded.[47] These rewards come in various forms, from organizational incentives for meeting quotas to financial benefits gained through corruption.[48] This organizational culture reinforces the shift toward a quantity-driven intelligence strategy, which diminishes the focus on effectiveness and promotes the use of untrained operatives.

---

[44] Elena Grossfeld, "Russia's Declining Satellite Reconnaissance Capabilities and Its Implications for Security and International Stability," *International Journal of Intelligence and CounterIntelligence* 38, no. 1 (2025), doi: 10.1080/08850607.2024.2330848; Volya, "«Половина попаданий ракетами по гражданским из-за сбоев в работе техники и плохой подготовки. Вторая половина — осознанные удары»," Telegraph, May 5, 2022, https://telegra.ph/Polovina-popadanij-raketami-po-grazhdanskim-iz-za-sboev-v-rabote-tehniki-i-plohoj-podgotovki-Vtoraya-polovina--osoznannye-udary-05-05.

[45] Roman Kolodii, Giangiuseppe Pili, and Jack Crawford, "Hi-Tech, High Risk? Russo-Chinese Cooperation on Emerging Technologies," RUSI, Mar. 1, 2024, https://www.rusi.org/explore-our-research/publications/commentary/hi-tech-high-risk-russo-chinese-cooperation-emerging-technologies.

[46] Miller, Morris, and Ilyushina, "Russia Recruited Operatives Online."

[47] Margarita Zavadskaya and Jussi Lassila, "The Kremlin's Dilemma: Effectiveness Versus Loyalty in the Case of Prigozhin's Wagner PMC," PONARS Eurasia, Oct. 21, 2024, https://www.ponarseurasia.org/the-kremlins-dilemma-effectiveness-versus-loyalty-in-the-case-of-prigozhins-wagner-pmc/; Huw Dylan, David V. Gioe, and Elena Grossfeld, "The Autocrat's Intelligence Paradox: Vladimir Putin's (Mis)Management of Russian Strategic Assessment in the Ukraine War," *The British Journal of Politics and International Relations* 25, no. 3 (2023), doi: 10.1177/13691481221146113; Irina Borogan and Andrei Soldatov, "Ирина Бороган и Андрей Солдатов: Как меняются спецслужбы и что угрожает политической эмиграции?," Sapere Aude, 2024, https://sapere.online/irina-borogan-i-andrej-soldatov-kak-menyayutsya-spetssluzhby-i-chto-ugrozhaet-politicheskoj-emigratsii/.

[48] "The Shadow of the KGB and Recruitment Failures: Archaic Methods of Russian Intelligence Services Were the Main Cause of the Largest War in Europe in the Last 70 Years [Тень КГБ и провал вербовки: архаичные методы российских спецслужб стали главной причиной самой крупной войны в Европе за последние 70 лет]," Re: Russia, Dec. 4, 2023, https://re-russia.net/review/236/.

In directing its recruitment efforts toward messaging and social media, Russian intelligence promotes a practice reminiscent of Cold War–era norms and accountability. KGB recruitment was highly professionalized, but its officers still operated within a Soviet bureaucratic system and were required to meet annual quotas in accordance with socialist principles.[49] It stands to reason that a similar approach, sans the professionalization, still governs Russian intelligence organizations today, prioritizing numbers over operational capabilities. An additional advantage of volume-based recruiting is that it provides Russian intelligence agencies, known for their corruption, with opportunities to siphon off portions of the funds allocated for agent payments.[50]

However, this approach is not without its drawbacks. As the failed sabotage and influence attempts in Europe testify, mass recruiting focused on cost rather than capability does not necessarily contribute to operational success because the lack of skills or motivation among recruits often leads to botched missions. Although Soviet intelligence operated within a quota-driven system, their professionalism, structured training, and adherence to high operational standards contrast with today's reliance on unskilled, expendable operatives, which prioritizes volume over success. Thus, the Stars of David paint job in Paris, in which the perpetrators were caught in the act, was quickly exposed as a Russia-instigated and -financed operation, undermining efforts to present it as a grassroots antisemitic act.[51] Similarly, two Spaniards planning arson at production facilities in Lithuania were detained before reaching their target destination.[52] Nonetheless, even in their failure, sabotage and influence operations still manage to be effective—at least in the psychological and physical domains. In this way, the focus on quantity does seem to yield qualitative changes, albeit perhaps in ways that were not initially intended. The decline in professionalism is another factor that leads to prioritizing quantity over quality, shifting the focus from achieving effective outcomes to simply increasing the number of operations.

As the failed sabotage and influence attempts in Europe testify, mass recruiting focused on cost rather than capability does not necessarily contribute to operational success because the lack of skills or motivation among recruits often leads to botched missions.

The willingness of Russian intelligence to compromise the quality of operations for sheer quantity could be driven by an additional factor. The decline of professionalism among Russian intelligence operatives created an environment in which less importance is placed on operational effectiveness and mission integrity, and operational failures are overlooked or accepted as part of the process.

[49] Lambridge, *A Note on KGB Style*.

[50] Irina Borogan and Andrei Soldatov, "FSB Gamekeepers Turn Poachers in Putin's Crime-Riddled State," Center for European Policy Analysis, Jan. 10, 2024, https://cepa.org/article/fsb-gamekeepers-turn-poachers-in-putins-crime-riddled-state/; Mark Galeotti, *Putin's Hydra: Inside Russia's Intelligence Services*, European Council on Foreign Relations, 2016, https://www.jstor.org/stable/resrep21577.

[51] Hugh Schofield, "Star of David Graffiti in Paris - the Russian Connection," BBC, Nov. 8, 2023, https://www.bbc.com/news/world-europe-67360768.

[52] "Two Spanish Nationals Detained for Plotting Terrorist Act in Lithuania's Šiauliai," LRT, Nov. 19, 2024, https://www.lrt.lt/en/news-in-english/19/2417915/two-spanish-nationals-detained-for-plotting-terrorist-act-in-lithuania-s-siauliai.

This shift, which is more cultural than a mere result of resource constraints, reinforces the broader trend toward a quantity-driven intelligence approach. The incompetence among the operatives recruited by Russian intelligence is undeniable, and similar criticisms have been directed at the intelligence officers themselves. The decline in professionalism within Russian intelligence organizations has been lamented by former operatives and acknowledged by supervisors. The recent string of failures—the FSB's sloppy poisoning attempts on Alexei Navalny, Vladimir Kara-Murza, and others; the capture of an assassin in broad daylight in Berlin; the failed assassination attempt on a former Russian intelligence officer in Florida; and the botched attempt on the lives of Skripal and his daughter leading to the death of an innocent citizen, among others—stands in stark contrast to the Soviet practice of "wet affairs."[53]

In a departure from the KGB's careful avoidance of operations deemed likely to produce significant long-term repercussions or damage to its reputation, Russian intelligence today has no such qualms, which speaks for itself.[54] "Gross incompetence," "outrageous sloppiness," and "they might as well have worn Budyonovkas" were just some of the unflattering assessments of failed GRU operations as early as 2018.[55] The disregard for operational security, both at home and abroad, confirms the decline in standards within Russian intelligence, which is made worse by the open rivalry among Russian intelligence organizations, each trying to outdo the other with underhanded tactics.[56] This decline has been further exacerbated by the continuous dynastic hiring practices of Russian intelligence organizations, in which loyalty and personal connections have replaced rigorous training and ideological commitment.[57] The lack of meaningful external oversight beyond presidential supervision for the FSB and SVR and the General Staff's oversight of the GRU all but guarantees that no lessons will be learned beyond those that the management prefers, contributing to the erosion of professionalism within these agencies.[58]

Although the emphasis on quantity in Russian intelligence operations might resemble the Marxist belief that increasing quantity can eventually lead to

---

[53] Natalia Antonova, "Russia's Security Agencies Are Both Terrifying and Incompetent," *Foreign Policy*, Jan. 15, 2021, https://foreignpolicy.com/2021/01/15/russia-security-agencies-terrifying-incompetent-fsb/; "FSB Abroad [ФСБ за границей]," Dossier Center, Feb. 17, 2020, https://fsb.dossier.center/abroad/; Ronen Bergman, Adam Goldman, and Julian E. Barnes, "Russia Sought to Kill Defector in Florida," *New York Times*, June 19, 2023, https://www.nytimes.com/2023/06/19/us/politics/russia-spy-assassination.html; CIA, *Soviet Use of Assassination and Kidnapping*, 1964, https://www.archives.gov/files/research/jfk/releases/104-10021-10115.pdf.

[54] Kalugin, *Spymaster*, pp. 185–87.

[55] The *budenovka* (Russian: будёновка) was a distinctive woolen hat worn by the Red Army from 1918 to 1940 characterized by its pointed shape, earflaps, and red star emblem. Designed by artist Viktor Vasnetsov and named after cavalry commander Semyon Budyonny, it became an iconic symbol of the Soviet era despite being replaced by more practical headgear after its use during the Russian Civil War. For more examples of Russian responses to intelligence failures, see Dmitry Volcheck [Дмитрий Волчек], "'Putin's Special Services Are in Disarray': The FSB Is Haunted by the GRU's Foreign Assets, Which Are Underground Business Empires [«В путинских спецслужбах бардак» ФСБ не дают покоя зарубежные активы ГРУ, которые представляют собой подпольные бизнес-империи]," Крым. Реалии, Oct. 14, 2018, https://ru.krymr.com/a/v-putnskih-specslujbah-bardak/29541981.html.

[56] Bellingcat Investigation Team, "FSB Team of Chemical Weapon Experts Implicated in Alexey Navalny Novichok Poisoning," Bellingcat, Dec. 14, 2020, https://www.bellingcat.com/news/uk-and-europe/2020/12/14/fsb-team-of-chemical-weapon-experts-implicated-in-alexey-navalny-novichok-poisoning/; Gordon Corera, "Russian GRU Spy Tried to Infiltrate International Criminal Court," BBC, June 16, 2022, https://www.bbc.com/news/world-europe-61831961; Volcheck, "'Putin's Special Services Are in Disarray.'"

[57] Borogan and Soldatov, "Ирина Бороган и Андрей Солдатов."

[58] Andrei Soldatov and Irina Borogan, "о прокурорском надзоре за ФСБ," Agentura.Ru Livejournal, July 7, 2011, https://agentura.livejournal.com/43291.html; Gordon Bennett, "The SVR: Russia's Intelligence Service," Federation of American Scientists Intelligence Resource Program, 2000, https://irp.fas.org/world/russia/svr/c103-gb.htm.

qualitative changes—a concept proposed by Georg Wilhelm Friedrich Hegel, further developed by Karl Marx and Friedrich Engels in dialectical materialism, and endorsed by Vladimir Lenin—this shift is unlikely to be driven by a renewed embrace of Marxist ideology.[59] The current model of Russian intelligence operations resembles John von Neumann's concept of building reliable systems from unreliable components, in which success is achieved through redundancy.[60] By combining the outputs of multiple redundant components, the system becomes more reliable, even if individual components may be less dependable. A variant of this approach has been used in computing systems design, particularly by companies offering online services such as e-commerce and social media platforms. As demand for computer power surged with the adoption and availability of the internet, more functions became available online, such as shopping, search, and many others. Although companies addressed initial growth by purchasing more powerful and, incidentally, expensive servers, the demand far outpaced the capacity of even the largest servers. The answer came from the scale-out approach, in which systems were split among many smaller and cheaper machines to meet the growth in demand. This shift leveraged redundancy—many smaller commodity components working together—to achieve greater scalability at a fraction of the cost.[61]

The parallels to Russian intelligence are striking—just as the scale-out approach in technology relies on cheaper, mass-produced components to address growing demands for capacity, Russian intelligence has increasingly relied on recruiting low-cost operatives at scale. This approach provides the flexibility necessary to address the surge in operational demand, such as that resulting from the escalation of operations related to Ukraine, but also leverages economies of scale, reducing the cost per operation and avoiding extensive training or specialized expertise. Although Russian intelligence's adoption of this scaling model is unlikely to be the result of diligent research of system architecture design patterns, the resemblance suggests that this quantity-based approach is viable and provides benefits similar to those of scalable distributed systems in technology.

However, this approach is not without its drawbacks. Redundancy-based designs require extensive coordination and careful integration; they can backfire if not implemented properly, and Russian intelligence's approach has encountered similar setbacks. These include increased operational complexity, failures due to lack of synchronization, and added pressures to operate at a higher tempo or in less secure conditions.[62] In addition to its effects on Russian intelligence practices, the quantity-first shift, driven by operational constraints, systemic incentives, and other factors, has far-reaching implications for global security and international intelligence cooperation.

---

[59] Robert L. Carneiro, "The Transition from Quantity to Quality: A Neglected Causal Mechanism in Accounting for Social Evolution," *Proceedings of the National Academy of Sciences* 97, no. 23 (2000), doi: 10.1073/pnas.240462397; Vladimir Il'ich Lenin, *Государство и революция* (1919), Google Books, https://www.google.com/books?id=be7gAAAAMAAJ.

[60] Claude E. Shannon, "Von Neumann's Contributions to Automata Theory," *Bulletin of the American Mathematical Society* 64, no. 3 (1958), https://www.ams.org/bull/1958-64-03/S0002-9904-1958-10214-1/.

[61] Amin Vahdat et al., "Scale-Out Networking in the Data Center," *IEEE Micro* 30, no. 4 (2010), https://ieeexplore.ieee.org/abstract/document/5550998/?casa_token=56TTO9em5CUAAAAA:JIY47nVYXBmUPgkD8HiMaR39JRHCTDfRTjyomJuODAtNH9nT7oVaNDyfkJdEcZa_J-Ay_Y.

[62] Scott D. Sagan, "Learning from 'Normal Accidents,'" *Organization & Environment* 17, no. 1 (2004), https://www.jstor.org/stable/26162452.

Quantity over Quality: Implications for Global Intelligence and Security

Russia's shift to a quantity-driven intelligence approach has introduced new risks and challenges for global security, necessitating a readjustment of intelligence collaboration and countermeasures. Despite frequent operational failures, the effectiveness of this approach lies in its scalability, adaptability, and persistence—allowing Russian intelligence to sustain operational tempo, overwhelm adversaries with volume rather than precision, and exploit opportunities as they arise. Given Russia's constraints—reduced professionalism, a shrinking pool of trained operatives, and an urgent need for continuous operations—this model remains viable, reflecting the principles of von Neumann's design and the scaling-out model adopted in technology. The sheer volume of attempts ensures that some operations succeed, making this strategy difficult to counter. Unless the conditions driving this shift change, it is likely to persist, shaping long-term intelligence and security dynamics.

The high volume of Russian sabotage and influence operations orchestrated from afar and executed by unprofessional agents carries the risk of destabilizing and straining NATO relations in unintended ways, particularly because some states have been affected more than others.

The high volume of Russian sabotage and influence operations orchestrated from afar and executed by unprofessional agents carries the risk of destabilizing and straining NATO relations in unintended ways, particularly because some states have been affected more than others.[63] The Baltic states are especially vulnerable to sabotage because Russia perceives the region to be strategically important and desires to strengthen and expand its influence there to preserve access to the Baltic Sea. Although the Baltic states' membership in the European Union and NATO likely prevents Russia from conducting a full military invasion, it does not provide the same deterrence against sabotage.[64] Despite the geographic differences, no NATO states, including the US, should feel overly secure. Russia's ability to reach sympathetic or financially motivated actors, such as the German-Russian dual citizen arrested for casing a US military base in Germany and the small-time criminals tried in Lithuania for vandalizing a museum, is transferrable to the US, as evidenced by the arrest of a Kazakh migrant affiliated with the

[63] Shashank Joshi, "Russian Spies Are Back—and More Dangerous Than Ever," *The Economist*, Feb. 20, 2024, https://www.economist.com/international/2024/02/20/russian-spies-are-back-and-more-dangerous-than-ever.

[64] David V. Gioe, Marina Miron, and Marc Ozawa, "Reassessing NATO's Deterrence and Defence Posture in the Baltics: Rebalancing Strategic Priorities to Counter Russian Hybrid Aggression," *Defense & Security Analysis* 41, no. 1 (2025), doi: 10.1080/14751798.2024.2424935.

Wagner Group crossing into the US from Mexico in possession of a drone.[65] The expanding Russian intelligence presence in Mexico further highlights the Kremlin's reach and the growing threat to all states deemed unfriendly by the Kremlin.[66]

Russia's adoption of quantity-driven intelligence operations poses significant security risks, increasing both physical damage and geopolitical tensions. The reliance on low-cost, untrained agents conducting high-volume operations raises the likelihood of infrastructure damage and civilian casualties, as seen in recent break-ins to Finnish water treatment facilities and arson attacks on critical transportation hubs in Norway.[67] Beyond immediate security threats, these operations exacerbate geopolitical tensions with other states.[68] For example, although the Chinese ship Newnew Polar Bear damaged infrastructure in the Baltic Sea, the Baltic states were constrained by international law, which guarantees freedom of navigation on the high seas and requires the cooperation of the flag state to detain and board vessels.[69] Concerned about provoking retaliation, they refrained from boarding the ship, fearing that China and Russia might retaliate by using similar tactics in other regions, such as Taiwan Strait. This highlights a growing challenge: although international law guarantees freedom of navigation in international waters, it remains ill-equipped to address emerging security threats posed by hybrid operations. In addition to geopolitical consequences, attacks on critical infrastructure could have severe long-term effects, such as disrupting the European energy supplies.[70] As Russia continues to employ a quantity-driven approach, the risks of both immediate damage and broader strategic instability will only grow.[71]

The similarities of Russian intelligence recruiting and Islamist terrorist group recruiting illustrate the complexity of countering these operations. Both target untrained individuals through platforms such as Telegram and the dark web, preserving anonymity while using cryptocurrencies for payments and purchases.[72] Preventing both is difficult, as illustrated by the difficulties that counterterrorist forces face in preventing radicalization and lone wolf attacks. The lessons learned in attempts to counter Russian disinformation campaigns further demonstrate the scale of the challenge, emphasizing the need for enhanced strategies modeled on those used to prevent jihadi radicalization and recruitment to safeguard regional and global stability.

Despite the higher volume of activities, Russia-directed operations often suffer from limited tactical

---

[65] Mekhennet et al., "Russia Recruits Sympathizers Online"; Huppertz et al., "Make a Molotov Cocktail"; Carl Schreck et al., "A Wagner Mercenary Who Crossed U.S.-Mexican Border Was Honored in Russia Weeks Before Arrest," Radio Free Europe/Radio Liberty, Jan. 11, 2025, https://www.rferl.org/a/wagner-veteran-timur-praliev-detained-us-mexico-border-russia/33271493.html.

[66] Dan De Luce and Owen Hayes, "Back to the Cold War: Russia Uses Mexico as a Hub for Spying on the U.S.," NBC News, Sept. 21, 2024, https://www.nbcnews.com/investigations/cold-war-russia-uses-mexico-hub-spying-us-rcna171819.

[67] Elisabeth Braw, "Is Russia Trying to Poison Finland's Water?," *Foreign Policy*, July 26, 2024, https://foreignpolicy.com/2024/07/26/russia-sabotage-poison-finland-water-treatment/; Insikt Group, *Russian Sabotage Activities Escalate*.

[68] Sophia Besch and Eric Brown, "A Chinese-Flagged Ship Cut Baltic Sea Internet Cables. This Time, Europe Was More Prepared," Carnegie Emissary, Dec. 3, 2024, https://carnegieendowment.org/emissary/2024/12/baltic-sea-internet-cable-cut-europe-nato-security?lang=en.

[69] Elisabeth Braw, "Will Denmark Expose Chinese-Russian Sabotage in the Baltic?," *Foreign Policy*, Nov. 21, 2024, https://foreignpolicy.com/2024/11/20/will-denmark-expose-chinese-russian-sabotage-in-the-baltic/.

[70] "Norwegian Intelligence Assessment."

[71] Insikt Group, *Russian Sabotage Activities Escalate*.

[72] Michael Chertoff, Patrick Bury, and Daniela Richterova, "Bytes Not Waves: Information Communication Technologies, Global Jihadism and Counterterrorism," *International Affairs* 96, no. 5 (2020), doi: 10.1093/ia/iiaa048.

success due to the reliance on untrained operatives and the inherent challenges in executing complex missions. However, questions remain about the true scope of Russian intelligence efforts given the number of sabotage and espionage cases prosecuted in the West and the many more that likely remain undiscovered. The sheer volume of operations, combined with the difficulty in quickly attributing incidents, creates an effective strategic advantage for Russia. Even if individual operations fail, the cumulative effect complicates countermeasures and enables Russia to benefit from being credited with operations that it did not carry out, growing its already significant reputation for conducting covert and disruptive activities.[73] This quantity-over-quality approach proves strategically effective despite the varying success of individual operations.

As Russian intelligence continues to adapt to changing geopolitical and operational environments, maintaining its role as the Kremlin's primary strategic tool and supporting Russia's ongoing invasion of Ukraine, the long-term implications for global security are clear, underscoring the need for a unified and adaptive response.

As Russian intelligence continues to adapt to changing geopolitical and operational environments, maintaining its role as the Kremlin's primary strategic tool and supporting Russia's ongoing invasion of Ukraine, the long-term implications for global security are clear, underscoring the need for a unified and adaptive response.

Recommendations

Mitigating the risks posed by Russia's evolving intelligence strategies requires a proactive and adaptive approach. Enhanced coordination and information sharing among NATO and its allies will enable a unified and proactive response to Russian intelligence activities, facilitating quicker identification and disruption of sabotage or intelligence-gathering activities. Strengthening intelligence collaboration and integration across counterintelligence and law enforcement agencies will improve the ability to detect and neutralize threats more efficiently.

A key challenge to Russia's evolving tactics is the difficulty in timely attribution. Improving attribution techniques and enhancing analytical capabilities will enable faster, more coordinated responses while reducing the effectiveness of Russian covert operations. Strengthening intelligence analysis ensures that Russia's evolving strategies are better understood and countered effectively.

The use of social media, encrypted messaging platforms, and cryptocurrency has further complicated counterintelligence efforts. Enhanced monitoring of these platforms disrupts Russian intelligence recruitment and operational activities. Engaging with platform providers to ensure cooperation with law enforcement and counterintelligence agencies addresses the misuse of encrypted communication channels for intelligence gathering and sabotage coordination. In addition, restricting cryptocurrency trading bots from operating on noncompliant exchanges reduces Russia's ability to engage in untraceable financial

[73] Aurelien Breeden and Catherine Porter, "After French Rail Sabotage, Some See Signs of a Murky 'Ultraleft,'" *New York Times*, Aug. 7, 2024, https://www.nytimes.com/2024/08/07/world/europe/france-olympics-sabotage-anarchists.html.

transactions that support covert intelligence activities. Ongoing identification of emerging platforms suitable for recruitment remains important because Russian intelligence continues to adapt its methods to evade detection.

Raising awareness of Russian intelligence recruitment tactics among vulnerable communities—such as ethnic Russians, Ukrainian refugees, and migrant populations—can enhance vigilance and facilitate the identification and disruption of recruitment attempts for sabotage or espionage. Expanding outreach programs and strengthening collaboration with local law enforcement will also play a crucial role in reducing the effectiveness of Russian intelligence efforts.

Rapid disclosure of suspected Russian sabotage or influence attempts is essential for countering disinformation and minimizing their impact. Timely investigations and public attribution enhance transparency, strengthen resilience against manipulation, and reduce the effectiveness of influence operations. Public awareness campaigns further prevent misinformation from spreading and bolster societal resistance to Russian intelligence efforts.

The growing focus on mass-scale intelligence operations calls for a reevaluation of current counterintelligence strategies. Governments and international bodies need to adapt to a landscape where quantity-driven, decentralized operations are increasingly common. Effective responses require flexibility in resource management, intelligence gathering, and counterintelligence strategies to address the growing complexity of Russian intelligence operations.

Conclusion

Russia's shift toward a quantity-driven intelligence approach marks a departure from the traditional KGB model of high-quality, coordinated operations while still implementing aspects of its Cold War–era playbook. Contemporary Russian intelligence now focuses on high volumes of operations carried out by untrained agents recruited anonymously via messenger apps and social media, essentially creating a gig economy–driven sabotage marketplace. This approach has led to a surge in sabotage and influence operations. Driven by a decline in professionalism, increased operational demands, and the need for rapid scaling, the quantity-driven approach moves away from the carefully planned and specialized operations of Soviet-era intelligence. In addition, the absence of meaningful control within Russian intelligence, a departure from the strict oversight once exercised by the Party over the KGB, has created a permissive atmosphere, allowing unconstrained operations. The focus on "throwing people at a problem" is rooted in both historical practices, namely the infamous meat grinder approach, and modern geopolitical realities, particularly the ongoing conflict in Ukraine. This strategy has mimicked the scale-out model seen in computer systems design, alongside von Neumann's principle of building reliable systems from unreliable components. Russia's adoption of this model presents growing challenges to global security with long-term implications for regional and global stability.

This approach enables Russian intelligence to scale its operations in response to operational demands and constraints and therefore carries increased risks for the international community. In carrying out these operations, untrained agents could contribute to destabilization in key regions, straining NATO relations and exacerbating geopolitical tensions.

Although not all operations succeed, those that fall short of their immediate objectives still have a profound effect by sowing fear, undermining public confidence, and straining the resources of law enforcement and the intelligence community.

The reliance on digital recruitment networks adds another layer of complexity to the challenges Western intelligence agencies face.

Although not all operations succeed, those that fall short of their immediate objectives still have a profound effect by sowing fear, undermining public confidence, and straining the resources of law enforcement and the intelligence community. Russia will likely persist in its adoption of this model, continuously expanding and refining its approach, unless significant changes occur in the operational environment or the political calculus driving its intelligence strategies.

For NATO and its allies, the need to adapt is urgent. The scale of Russian intelligence operations demands a more unified, proactive response. It is crucial to strengthen intelligence collaboration, improve attribution techniques, and adapt

countermeasures to mitigate the risks posed by Russia's evolving tactics. In addition, monitoring social media platforms and messaging apps such as Telegram, which has largely avoided cooperation with law enforcement until recently, is essential. Encouraging platform owners to align their policies with law enforcement and counterintelligence efforts is key, especially because some platforms have stated that they will cooperate in cases of criminal activities that violate terms of service. However, it remains unclear whether counterintelligence will be included in such cooperation—this issue should be clarified and prioritized. Furthermore, the response time of social media and messaging platforms must be swift enough to prevent the spread of Russian intelligence activities. Equally important is establishing monitoring for platforms known for their messaging functionality, such as Discord, in case Russian intelligence activities shift there. Cryptocurrency trading bots should be prevented from operating through crypto exchanges that do not abide by anti–money laundering and "know your customer" regulations. Strengthening outreach programs to communities, particularly Ukrainian refugees and ethnic Russians, is crucial to allow counterintelligence and law enforcement to be aware of local developments and potential threats. Rapid disclosure of influence and sabotage attempts is essential, as are timely attribution and publicizing of these actions. At the same time, the international community must also reconsider the broader implications for global security, particularly as new technologies and unconventional recruitment methods further complicate traditional intelligence practices. Ultimately, the ability to counter Russia's growing intelligence capabilities will depend on the international community's willingness to unite and adapt to this new era of warfare, in which quantity often takes precedence over quality and the risks of destabilization continue to grow.

Although some former KGB officers claim that "Russian intelligence today is a sorry shadow of [its] old days," the goal of Russian intelligence remains unchanged: to "weaken, deceive, confuse, injure, damage and destroy the other side."[74] We have been here before.

[74] John H. Hedley and Henry R. Appelbaum, "US Intelligence and the End of the Cold War," *Studies in Intelligence* 44, no. 3 (2000), https://www.cia.gov/readingroom/docs/DOC_0001445139.pdf.

References

Adams, Paul. "Russia's 'Meat-Grinder' Tactics Bring Battlefield Success - but at Horrendous Cost." BBC. Dec. 6, 2024. https://www.bbc.com/news/articles/c0ewneynypwo.

Agenstvo Novosti (agentstvonews). "Россия могла осуществить не менее 50 гибридных операций против 13 стран Европы с начала войны." Telegram post. Jan. 4, 2025. https://t.me/agentstvonews/8726.

AlexandruC4 (@AlexandruC4). "Law enforcement authorities have detained two Spanish nationals who were planning to carry out a terrorist act in the city of Šiauliai in northern Lithuania." Post. X. Nov. 20, 2024, 3:09 p.m. https://x.com/AlexandruC4/status/1859358524125610264.

Alexis-Martin, Becky. "Russia's 'Meat Grinder' Tactics in Ukraine Have Proved Effective in Past Wars – but at Terrible Cost." The Conversation. Oct. 21, 2024. http://theconversation.com/russias-meat-grinder-tactics-in-ukraine-have-proved-effective-in-past-wars-but-at-terrible-cost-241688.

Andrew, Christopher, and Oleg Gordievsky. *KGB: The Inside Story of Its Foreign Operations from Lenin to Gorbachev*. New York: Perennial, 1991.

Andrew, Christopher M., and Vasilij N. Mitrochin. *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB*. New York: Basic Books, 2001.

Antoniuk, Darina. "Ukraine Uncovers Russian Spy Network Recruiting Teens for Espionage." The Record. Dec. 13, 2024. https://therecord.media/ukraine-sbu-espionage-campaign-russia.

Antonova, Natalia. "Russia's Security Agencies Are Both Terrifying and Incompetent." *Foreign Policy*. Jan. 15, 2021. https://foreignpolicy.com/2021/01/15/russia-security-agencies-terrifying-incompetent-fsb/.

"Attack on Navalny Aide Was Work of Russian Special Services, Says Lithuania Counter-Intelligence." Reuters. Mar. 14, 2024. https://www.reuters.com/world/europe/attack-navalny-aide-was-work-russian-special-services-says-lithuania-counter-2024-03-14/.

Bellingcat Investigation Team. "FSB Team of Chemical Weapon Experts Implicated in Alexey Navalny Novichok Poisoning." Bellingcat. Dec. 14, 2020. https://www.bellingcat.com/news/uk-and-europe/2020/12/14/fsb-team-of-chemical-weapon-experts-implicated-in-alexey-navalny-novichok-poisoning/.

Bennett, Gordon. "The SVR: Russia's Intelligence Service." Federation of American Scientists Intelligence Resource Program. 2000. https://irp.fas.org/world/russia/svr/c103-gb.htm.

Bergman, Ronen, Adam Goldman, and Julian E. Barnes. "Russia Sought to Kill Defector in Florida." *New York Times*. June 19, 2023. https://www.nytimes.com/2023/06/19/us/politics/russia-spy-assassination.html.

Besch, Sophia, and Eric Brown. "A Chinese-Flagged Ship Cut Baltic Sea Internet Cables. This Time, Europe Was More Prepared." Carnegie Emissary. Dec. 3, 2024. https://carnegieendowment.org/emissary/2024/12/baltic-sea-internet-cable-cut-europe-nato-security?lang=en.

Borogan, Irina, and Andrei Soldatov. "FSB Gamekeepers Turn Poachers in Putin's Crime-Riddled State." Center for European Policy Analysis. Jan. 10, 2024. https://cepa.org/article/fsb-gamekeepers-turn-poachers-in-putins-crime-riddled-state/.

Borogan, Irina, and Andrei Soldatov. "Ирина Бороган и Андрей Солдатов: Как меняются спецслужбы и что угрожает политической эмиграции?" Sapere Aude. 2024. https://sapere.online/irina-borogan-i-andrej-soldatov-kak-menyayutsya-spetssluzhby-i-chto-ugrozhaet-politicheskoj-emigratsii/.

Brandvold, Sigmund. "Norwegian Intelligence Assessment on Russian Interference." The Jamestown Foundation. Nov. 9, 2024. https://jamestown.substack.com/p/norwegian-intelligence-assessment.

Braw, Elisabeth. "Is Russia Trying to Poison Finland's Water?" *Foreign Policy*. July 26, 2024. https://foreignpolicy.com/2024/07/26/russia-sabotage-poison-finland-water-treatment/.

Braw, Elisabeth. "Will Denmark Expose Chinese-Russian Sabotage in the Baltic?" *Foreign Policy*. Nov. 21, 2024. https://foreignpolicy.com/2024/11/20/will-denmark-expose-chinese-russian-sabotage-in-the-baltic/.

Breeden, Aurelien, and Catherine Porter. "After French Rail Sabotage, Some See Signs of a Murky 'Ultraleft.'" *New York Times*. Aug. 7, 2024. https://www.nytimes.com/2024/08/07/world/europe/france-olympics-sabotage-anarchists.html.

Carneiro, Robert L. "The Transition from Quantity to Quality: A Neglected Causal Mechanism in Accounting for Social Evolution." *Proceedings of the National Academy of Sciences* 97, no. 23 (2000): 12926–31. doi: 10.1073/pnas.240462397.

Chertoff, Michael, Patrick Bury, and Daniela Richterova. "Bytes Not Waves: Information Communication Technologies, Global Jihadism and Counterterrorism." *International Affairs* 96, no. 5 (2020): 1305–25. doi: 10.1093/ia/iiaa048.

Chiu, Leo. "Explosion Rocks UK Munitions Factory in South Wales." *Kyiv Post*. Apr. 18, 2024. https://www.kyivpost.com/post/31331.

CIA. *Soviet Use of Assassination and Kidnapping*. 1964. https://www.archives.gov/files/research/jfk/releases/104-10021-10115.pdf.

Corera, Gordon. "Russian GRU Spy Tried to Infiltrate International Criminal Court." BBC. June 16, 2022. https://www.bbc.com/news/world-europe-61831961.

Dagaeva, Anastasia. "Turbulent Times: How Russian Airlines Are Weathering the Storm." Carnegie Politika. Mar. 28, 2023. https://carnegieendowment.org/russia-eurasia/politika/2023/02/turbulent-times-how-russian-airlines-are-weathering-the-storm?lang=en.

De Luce, Dan, and Owen Hayes. "Back to the Cold War: Russia Uses Mexico as a Hub for Spying on the U.S." NBC News. Sept. 21, 2024. https://www.nbcnews.com/investigations/cold-war-russia-uses-mexico-hub-spying-us-rcna171819.

Deconinck, Carl. "'Russia Trying to Sabotage European Railways,' Says Czech Transport Minister." Brussels Signal. Apr. 5, 2024. https://brusselssignal.eu/2024/04/russia-trying-to-sabotage-european-railways-says-czech-transport-minister/.

Dylan, Huw, David V. Gioe, and Elena Grossfeld. "The Autocrat's Intelligence Paradox: Vladimir Putin's (Mis)Management of Russian Strategic Assessment in the Ukraine War." *The British Journal of Politics and International Relations* 25, no. 3 (2023): 385–404. doi: 10.1177/13691481221146113.

"European Union: Council Suspends Visa Facilitation Agreement with Russia." Library of Congress. Sept. 20, 2022. https://www.loc.gov/item/global-legal-monitor/2022-09-20/european-union-council-suspends-visa-facilitation-agreement-with-russia/.

Eydoux, Thomas, Margaux Farran, and Le Monde's Video Investigation Team. "How Russia Is Staging Fake Protests in Europe to Discredit Ukraine." *Le Monde*. May 7, 2023. https://www.lemonde.fr/en/international/article/2023/05/07/how-russia-is-staging-fake-protests-in-europe-to-discredit-ukraine_6025808_4.html.

Falkov, Yaacov. "Intelligence-Exalting Strategic Cultures: A Case Study of the Russian Approach." *Intelligence and National Security* 37, no. 1 (2022): 90–108. doi: 10.1080/02684527.2021.1978135.

"France Investigates Foreign Connection to Daubing of Stars of David." Reuters. Nov. 7, 2023. https://www.reuters.com/world/europe/france-investigates-foreign-connection-daubing-stars-david-2023-11-07/.

"FSB Abroad [ФСБ за границей]." Dossier Center. Feb. 17, 2020. https://fsb.dossier.center/abroad/.

Galeotti, Mark. *Putin's Hydra: Inside Russia's Intelligence Services*. European Council on Foreign Relations. 2016. https://www.jstor.org/stable/resrep21577.

"German Secret Services Alarmed by Russian Threat." Voice of America. Oct. 14, 2024. https://www.voanews.com/a/7822201.html.

Gioe, David V., Marina Miron, and Marc Ozawa. "Reassessing NATO's Deterrence and Defence Posture in the Baltics: Rebalancing Strategic Priorities to Counter Russian Hybrid Aggression." *Defense & Security Analysis* 41, no. 1 (2025): 145–65. doi: 10.1080/14751798.2024.2424935.

Gorbunov, E. A. "«ДЕЗИНФОРМАЦИЯ... УВЕЛИЧИВАЕТ И ОБЕСПЕЧИВАЕТ УСПЕХ КОМПАНИИ: Документы российских архивов о первых шагах работы по советской дезинформации. 1922–1925 гг.»." Almanakh "Rossiya. XX Vek" Arkhiv Aleksandra N. Yakovleva. Accessed Sept. 19, 2024. https://www.alexanderyakovlev.org/almanah/inside/almanah-intro/1000406.

Grossfeld, Elena. "Russia's Declining Satellite Reconnaissance Capabilities and Its Implications for Security and International Stability." *International Journal of Intelligence and CounterIntelligence* 38, no. 1 (2025): 1–30. doi: 10.1080/08850607.2024.2330848.

Grozev, Christo. "Socialite, Widow, Jeweller, Spy: How a GRU Agent Charmed Her Way into NATO Circles in Italy." Bellingcat. Aug. 25, 2022. https://www.bellingcat.com/news/2022/08/25/socialite-widow-jeweller-spy-how-a-gru-agent-charmed-her-way-into-nato-circles-in-italy/.

Grozev, Christo, Roman Dobrokhotov, and Michael Weiss. "'Morality and Ethics Should Play No Part': Leaks Reveal How Russia's Foreign Intelligence Agency Runs Disinformation Campaigns in the West." The Insider. July 4, 2024. https://theins.ru/en/politics/272870.

Grozev, Christo, Michael Weiss, and Roman Dobrokhotov. "Красная звезда Мишлен. The Insider выявил повара-агента, готовившего провокации на Олимпиаде в Париже, он арестован." The Insider. July 25, 2024. https://theins.ru/politika/273341.

Hedley, John H., and Henry R. Appelbaum. "US Intelligence and the End of the Cold War." *Studies in Intelligence* 44, no. 3 (2000). https://www.cia.gov/readingroom/docs/DOC_0001445139.pdf.

How Russian Spies Use Cell Phones as OPs. Tradecraft Sunday. Posted by Spy Collection. YouTube, Dec. 22, 2024. Video. https://www.youtube.com/watch?v=C-TiHFcAJtk.

Howell O'Neill, Patrick. "U.S. Sanctions Russian Companies Linked to FSB." CyberScoop. June 11, 2018. https://cyberscoop.com/russian-sanctions-fsb-digital-security-erpscan/.

Huppertz, Carina, Artur Izumrudov, Laurin Lorenz, Ilya Lozovsky, Bastian Obermayer, Holger Roonemaa, Fabian Schmid, and Marta Vunš. "'Make a Molotov Cocktail': How Europeans Are Recruited Through Telegram to Commit Sabotage, Arson, and Murder." OCCRP. Sept. 26, 2024. https://www.occrp.org/en/investigation/make-a-molotov-cocktail-how-europeans-are-recruited-through-telegram-to-commit-sabotage-arson-and-murder.

Insikt Group. *Russian Sabotage Activities Escalate amid Fraught Tensions*. 2024. https://www.recordedfuture.com/research/russian-sabotage-activities-escalate-amid-fraught-tensions.

Jakimczyk, Jarek (@jarek_jakimczyk). "Podejrzany o #szpiegostwo." Post. X. Oct. 18, 2024, 4:58 a.m. https://x.com/jarek_jakimczyk/status/1847230750501867923.

Joshi, Shashank. "Russian Spies Are Back—and More Dangerous Than Ever." *The Economist*. Feb. 20, 2024. https://www.economist.com/international/2024/02/20/russian-spies-are-back-and-more-dangerous-than-ever.

Kalugin, Oleg. *Spymaster: My Thirty-Two Years in Intelligence and Espionage Against the West*. New York: Basic Books, 2009.

Kanev, Sergei. "Отлетались. Как из-за войны с Украиной развалилась резидентура ГРУ в «Аэрофлоте» и где теперь эти шпионы." The Insider. June 9, 2023. https://theins.info/obshestvo/262031.

KGB. *Acquisition and Training of Agent Recruiters*. Higher Intelligence School of the Committee for State Security, 1988.

KGB. *Communication with Agents*. Higher Intelligence School of the Committee for State Security.

KGB. *Recruitment of Agents Verbovka Agentury*. 1969.

KGB. *Working with Agents Rabota s Agenturoj*. 1970.

Kirby, Paul, and Frank Gardner. "Mystery Parcel Fires Were 'Test Runs' to Target Cargo Flights to US, Says Poland." BBC. Nov. 5, 2024. https://www.bbc.com/news/articles/c07912lxx33o.

Kolodii, Roman, Giangiuseppe Pili, and Jack Crawford. "Hi-Tech, High Risk? Russo-Chinese Cooperation on Emerging Technologies." RUSI. Mar. 1, 2024. https://www.rusi.org/explore-our-research/publications/commentary/hi-tech-high-risk-russo-chinese-cooperation-emerging-technologies.

Lambridge, Wayne. *A Note on KGB Style*. CIA. https://www.cia.gov/resources/csi/static/Note-on-KGB-Style.pdf.

Leicester, John, and Emma Burrows. "At Least 11 Baltic Cables Have Been Damaged in 15 Months, Prompting NATO to Up Its Guard." AP News. Jan. 28, 2025. https://apnews.com/article/nato-france-russia-baltic-cables-ships-damage-764964a275530915c2cc5af1125ec125.

Lenin, Vladimir Il'ich. *Государство и революция*. 1919. Google Books. https://www.google.com/books?id=be7gAAAAMAAJ.

Mekhennet, Souad, Catherine Belton, Emily Rauhala, and Shane Harris. "Russia Recruits Sympathizers Online for Sabotage in Europe, Officials Say." *Washington Post*. July 10, 2024. https://www.washingtonpost.com/world/2024/07/10/russia-sabotage-europe-ukraine/.

Miller, Greg, Loveday Morris, and Mary Ilyushina. "Russia Recruited Operatives Online to Target Weapons Crossing Poland." *Washington Post*. Aug. 18, 2023. https://www.washingtonpost.com/world/2023/08/18/ukraine-weapons-sabotage-gru-poland/.

Mindaugas, Aušra, Indrė Makaraitytė, and LRT Investigation Team. "International Investigation: Russian Special Forces Change Tactics in the Baltics." LRT. Oct. 30, 2024. https://www.lrt.lt/en/news-in-english/19/2401273/international-investigation-russian-special-forces-change-tactics-in-the-baltics.

"Orders to Set Ukrainian Armed Forces Vehicles on Fire Appeared on the Darknet. Four Jeeps of Ukrainian Fighters Were Burned in One Night [В даркнете появились заказы на поджог машин ВСУ. За одну ночь были сожжены четыре джипа украинских бойцов — «Важные истории»]." The Insider. July 10, 2024. https://theins.ru/news/272991.

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

Petkevicius, Ju Ju. *Recommendations of the 1st Department of the LSSR KGB Concerning the Preparation of the Agency for Work Abroad*. KGB. 1981. KGB Documents. https://www.kgbdocuments.eu/documents/recommendations-of-the-1st-department-of-the-lssr-kgb-concerning-the-preparation-of-the-agency-for-work-abroad/.

"Poland Arrests Nine Suspects over Alleged Russian Sabotage Plot." *Guardian*. May 20, 2024. https://www.theguardian.com/world/article/2024/may/20/poland-arrests-nine-suspects-over-alleged-russian-sabotage-plot.

Powell, Matthew. "Suspected Baltic Sea Cable Sabotage by Russia's 'Shadow Fleet' Is Ramping Up Regional Defence." University of Portsmouth. Jan. 28, 2025. https://www.port.ac.uk/news-events-and-blogs/blogs/academic-expertise/suspected-baltic-sea-cable-sabotage-by-russias-shadow-fleet-is-ramping-up-regional-defence.

Psaropoulos, John T. "As War Rages, Russia Activates Soviet Sabotage Plans in Europe: Experts." Al Jazeera. May 29, 2024. https://www.aljazeera.com/news/2024/5/29/as-ukraine-war-rages-russia-activates-sabotage-plans-in-europe-experts.

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

Richterova, Daniela, Elena Grossfeld, Magda Long, and Patrick Bury. "Russian Sabotage in the Gig-Economy Era." *The RUSI Journal* 169, no. 5 (2024): 10–21. doi: 10.1080/03071847.2024.2401232.

Roonemaa, Holger, and Inga Springe. "From Kyiv to Riga: Russian Sabotage Operations in the Baltics." Re:Baltica. July 10, 2024. https://en.rebaltica.lv/2024/07/2970/.

Rottbøll, Emil, and Kenneth Holm-Dahlin. "PET opruster markant mod russisk skyggekrig: Truslen fra fysisk sabotage i Danmark er skærpet." Berlingske. Jan. 30, 2025. https://www.berlingske.dk/content/item/1824430.

Sabbagh, Dan. "Russian Spy Caught Trying to Infiltrate War Crimes Court, Says Netherlands." *Guardian*. June 16, 2022. https://www.theguardian.com/law/2022/jun/16/russian-spy-caught-trying-to-infiltrate-war-crimes-court-says-netherlands.

Sagan, Scott D. "Learning from 'Normal Accidents.'" *Organization & Environment* 17, no. 1 (2004): 15–19. https://www.jstor.org/stable/26162452.

SBU (SBUkr). "СБУ затримала агента російського гру." Telegram post. Sept. 9, 2024. https://t.me/SBUkr/12858.

SBU (SBUkr). "СБУ затримала коригувальника фсб, якого завербували через сайти знайомств." Telegram post. Oct. 9, 2024. https://t.me/SBUkr/13073.

SBU (SBUkr). "СБУ та Нацполіція затримали неповнолітніх агентів рф, які підірвали вибухівки поблизу двох райвідділів поліції у Харкові." Telegram post. Dec. 16, 2024. https://t.me/SBUkr/13599.

Schofield, Hugh. "Star of David Graffiti in Paris - the Russian Connection." BBC. Nov. 8, 2023. https://www.bbc.com/news/world-europe-67360768.

Schreck, Carl, Mark Krutov, Mike Eckel, Ramazan Alpaut, and Maqpal Mukankyzy. "A Wagner Mercenary Who Crossed U.S.-Mexican Border Was Honored in Russia Weeks Before Arrest." Radio Free Europe/Radio Liberty. Jan. 11, 2025. https://www.rferl.org/a/wagner-veteran-timur-praliev-detained-us-mexico-border-russia/33271493.html.

"The Shadow of the KGB and Recruitment Failures: Archaic Methods of Russian Intelligence Services Were the Main Cause of the Largest War in Europe in the Last 70 Years [Тень КГБ и провал вербовки: архаичные методы российских спецслужб стали главной причиной самой крупной войны в Европе за последние 70 лет]." Re: Russia. Dec. 4, 2023. https://re-russia.net/review/236/.

Shannon, Claude E. "Von Neumann's Contributions to Automata Theory." *Bulletin of the American Mathematical Society* 64, no. 3 (1958): 123–29. https://www.ams.org/bull/1958-64-03/S0002-9904-1958-10214-1/.

Sinmaz, Emine. "Briton Charged with Aiding Russia and Planning Arson Against Ukraine-Linked Business in UK." *Guardian*. Apr. 26, 2024. https://www.theguardian.com/uk-news/2024/apr/26/man-charged-conducting-hostile-activity-uk-benefit-russia.

Sokolenko, Oleg. "В ФРГ предъявили обвинения предполагаемым российским шпионам." dw.com. Dec. 30, 2024. https://www.dw.com/ru/v-frg-predavili-obvinenia-predpolagaemym-rossijskim-spionam/a-71187895.

Soldatov, Andrei, and Irina Borogan. *Russian Cyberwarfare: Unpacking the Kremlin's Capabilities*. Center for European Policy Analysis. Sept. 2022. https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/.

Soldatov, Andrei, and Irina Borogan. "No прокурорском надзоре за ФСБ." Agentura.Ru Livejournal. July 7, 2011. https://agentura.livejournal.com/43291.html.

State Service of Special Communications and Information Protection of Ukraine. *Russian Cyber Operations: APT Activity Report H1 2024*. Sept. 2024. https://cip.gov.ua/en/news/cyber-operations-rf-h1-2024-report.

Stepanov, Lt. Colonel I. A. *Iz Opyta Provedenia Operativnykh Ustanovok*. Kafedra Spezialnoi Distsiplini I. Moscow: Higher School of KGB 101, 1965.

"Treasury Targets Corruption and the Kremlin's Malign Influence Operations in Moldova." US Department of the Treasury. Oct. 26, 2022. https://home.treasury.gov/news/press-releases/jy1049.

"Two Spanish Nationals Detained for Plotting Terrorist Act in Lithuania's Šiauliai." LRT. Nov. 19, 2024. https://www.lrt.lt/en/news-in-english/19/2417915/two-spanish-nationals-detained-for-plotting-terrorist-act-in-lithuania-s-siauliai.

US Department of State Global Engagement Center. *More than a Century of Antisemitism: How Successive Occupants of the Kremlin Have Used Antisemitism to Spread Disinformation and Propaganda*. Jan. 2024. https://www.state.gov/wp-content/uploads/2024/01/GEC-Special-Report-More-than-a-Century-of-Antisemitism.pdf.

Vahdat, Amin, Mohammad Al-Fares, Nathan Farrington, Radhika Niranjan Mysore, George Porter, and Sivasankar Radhakrishnan. "Scale-Out Networking in the Data Center." *IEEE Micro* 30, no. 4 (2010): 29–41. https://ieeexplore.ieee.org/abstract/document/5550998/?casa_token=56TTO9em5CUAAAAA:JIY47nVYXBmUPgkD8HiMaR39JRHCTDfRTjyomJuOODAtNH9nT7oVaNDyfkJdEcZa_J-Ay_Y.

van Burgen, Isabel. "Mysterious Accidents at US, Ally's Defense Facilities Spark Sabotage Fears." *Newsweek*. Apr. 19, 2024. https://www.newsweek.com/us-nato-defense-facilities-ukraine-russia-sabotage-1892099.

"Vandals Again Desecrate Jewish Cemetery." *New York Times*. June 4, 1977. https://www.nytimes.com/1977/06/04/archives/vandals-again-desecrate-jewish-cemetery.html.

Vandiver, John. "Russian Sabotage Is Escalating Risk of Greater Conflict in Europe, Army's Williams Says." *Stars and Stripes*. Oct. 15, 2024. https://www.stripes.com/theaters/europe/2024-10-15/russian-sabotage-us-army-nato-15515862.html.

Volcheck, Dmitry [Волчек, Дмитрий]. "'Putin's Special Services Are in Disarray': The FSB Is Haunted by the GRU's Foreign Assets, Which Are Underground Business Empires [«В путинских спецслужбах бардак» ФСБ не дают покоя зарубежные активы ГРУ, которые представляют собой подпольные бизнес-империи]." Крым. Реалии. Oct. 14, 2018. https://ru.krymr.com/a/v-putnskih-specslujbah-bardak/29541981.html.

Volya. "«Половина попаданий ракетами по гражданским из-за сбоев в работе техники и плохой подготовки. Вторая половина — осознанные удары»." Telegraph. May 5, 2022. https://telegra.ph/Polovina-popadanij-raketami-po-grazhdanskim-iz-za-sboev-v-rabote-tehniki-i-plohoj-podgotovki-Vtoraya-polovina--osoznannye-udary-05-05.

Walker, Shaun. "Russian Spies Sentenced in Slovenia After Pleading Guilty." *Guardian*. July 31, 2024. https://www.theguardian.com/world/article/2024/jul/31/russian-spies-sentenced-slovenia-court-prisoner-exchanges.

Wiese Bockmann, Michelle. "Russia-Linked Cable-Cutting Tanker Seized by Finland 'Was Loaded with Spying Equipment.'" Lloyd's List. Dec. 27, 2024. https://www.lloydslist.com/LL1151955/Russia-linked-cable-cutting-tanker-seized-by-Finland-was-loaded-with-spying-equipment.

Wilde, Gavin. *Russia's Countervalue Cyber Approach: Utility or Futility?* Carnegie Endowment for International Peace. Feb. 2024. https://carnegieendowment.org/research/2024/02/russias-countervalue-cyber-approach-utility-or-futility?lang=en.

Willsher, Kim. "Russian Interference Suspected After Coffins Draped with Tricolour Placed at Eiffel Tower." *Guardian*. June 3, 2024. https://www.theguardian.com/world/article/2024/jun/03/russian-interference-suspected-coffins-at-eiffel-tower-paris.

Zavadskaya, Margarita, and Jussi Lassila. "The Kremlin's Dilemma: Effectiveness Versus Loyalty in the Case of Prigozhin's Wagner PMC." PONARS Eurasia. Oct. 21, 2024. https://www.ponarseurasia.org/the-kremlins-dilemma-effectiveness-versus-loyalty-in-the-case-of-prigozhins-wagner-pmc/.

This report was written by CNA's Strategy, Policy, Plans, and Programs Division (SP3).

SP3 provides strategic and political-military analysis informed by regional expertise to support operational and policy-level decision-makers across the Department of the Navy, the Office of the Secretary of Defense, the unified combatant commands, the intelligence community, and domestic agencies. The division leverages social science research methods, field research, regional expertise, primary language skills, Track 1.5 partnerships, and policy and operational experience to support senior decision-makers.

About the author

Elena Grossfeld is a PhD candidate in the Department of War Studies at King's College London. She is also a member of the King's Centre for the Study of Intelligence.

Dedicated to the Safety and Security of the Nation

www.cna.org

About CNA

CNA is a not-for-profit analytical organization dedicated to the safety and security of the nation. With nearly 700 scientists, analysts, and professional staff across the world, CNA's mission is to provide data-driven, innovative solutions to our nation's toughest problems. It operates the Center for Naval Analyses—the federally funded research and development center (FFRDC) of the Department of the Navy—as well as the Institute for Public Research. The Center for Naval Analyses provides objective analytics to inform decision-making by military leaders and ultimately improve the lethality and effectiveness of the joint force. The Institute for Public Research leverages data analytics and sophisticated methods to support federal, state, and local government officials as they work to protect the homeland, the American people, and industry.

IOP-2025-U-041545-Final