Hybrid Threats and the Evolution of Russian Sabotage

https://www.e-ir.info/2025/08/26/hybrid-threats-and-the-evolution-of-russian-sabotage/

NINON DE BUCHET, AUG 26 2025

Since Russia's invasion of Ukraine on 24 February 2022, Europe has witnessed a sharp increase in suspected Russian sabotage attempts (Richterova et al. 2024a). These destructive attacks, primarily leveraged against NATO member states, reveal important parallels between the Kremlin's current campaign and Soviet-era sabotage doctrine. This essay will argue that state-led sabotage in the Putin era mirrors the Cold War doctrine of active measures in its reliance on the principle of escalation and choice of operational targets. However, a departure from traditional doctrine can be observed in the Russian security agencies' harnessing of information and communication technologies (ICTs) and the emergence of new avenues for exploiting Western vulnerabilities.

To make this argument, the essay will begin by looking at the continuities between Cold War and Putin-era sabotage doctrine. It will first connect the Soviet policy of active measures to the hybrid war campaign being waged against Ukraine and its allies, evaluating the extent to which Russian sabotage relies on escalatory behaviour to achieve strategic objectives. It will then consider how the Kremlin selects targets that will generate panic and sow discord within Western societies. The second part of the essay will turn to new elements of Russian sabotage, starting with the use of ICTs, which has led to an increase in the scale of operations paired with an observable decline in operational tradecraft. A further development is that, although recent discoveries reveal that Soviet sabotage doctrine deliberately targeted foreign critical infrastructure (Richterova 2024), this practice has reached new heights in recent years, namely through sabotage around undersea cable infrastructure and cyberattacks.

Although there is no agreed upon definition for this term, doctrine is understood to describe the set of institutionalised principles that inform a military's decisions on how best to carry out operations (Posen 2016, 159). The UK National Security Act (2023) defines sabotage as "activity conducted for, on behalf of, or for the benefit of a foreign power, resulting in damage to property, sites and data affecting the UK's interests, and national security" (NPSA 2024). Sabotage is a form of active measures, a Soviet term for the array of overt and covert tactics employed by the Russian security services to achieve their strategic objectives (Shultz 1984, 2). In light of the wave of sabotage plaguing the West, there is a critical need to contextualise Russia's current actions within the legacy of Soviet doctrine and the ongoing War in Ukraine. To counter Moscow's sabotage efforts, Western governments must first understand the evolution of this practice and the intentions driving it.

Continuities in Sabotage Doctrine

Recent findings from the Czech Security Service's archives shed considerable light on the Soviets' sabotage enterprise. Eastern Bloc states were encouraged to focus their efforts on states where the instruments of Western power were concentrated, such as the NATO headquarters in Belgium, or France and Germany, which were seen as pivotal players in the event of a Western-led war (Richterova 2024). By targeting key players in this manner, the Soviets hoped to strike at their adversaries while avoiding attribution and even detection (Bilal 2024). Moscow sought new and innovative ways to keep its intentions and capabilities concealed. Sabotage was thus produced as an inexpensive and relatively nonviolent approach to achieve national interests (Gioe, Lovering and Pachesny 2020, 518). Plans were laid out to strike targets that were important enough to undermine opponents' military capabilities and political resolve without triggering outright war. For example, military sites and communication lines featured prominently on the list of Soviet targets outlined in Czech archival records, and attacks were designed to resemble accidental disruptions in order to complicate attribution (Richterova et al. 2024a). Moscow's sabotage efforts therefore fulfilled a perceived need to weaken Western unity by orchestrating attacks that it could plausibly deny and which would be unlikely to elicit serious retaliatory action.

Thus far, contemporary sabotage efforts appear to follow the same rationale. Operations are kept under the NATO threshold for collective-defence outlined in Article V and appear accidental and uncoordinated (Gramer and MacKinnon 2024). While it is impossible to establish the exact scope of these operations, an unprecedented number of incidents have been publicly ascribed to Russia by Western governments (Richterova et al. 2024b). Although Moscow has kept its attacks subthreshold, in line with Cold War schematics, their volume and intensity have generated significant disruptions. In 2024, Poland suffered a series of arsonous fires, one of which destroyed a shopping centre and required 200 firefighters to respond (US Army 2024). Booby-trapped parcels designed to ignite on command are believed to have caused fires at DHL logistics centres in Germany and the UK (Apps 2024). Other incidents have been reported in a variety of warehouses and weapons manufacturing facilities across Europe, the UK, and even the US (O'Carroll 2024; Kirby and Gardner 2024). The exceptional scale of suspected sabotage since 2022 raises serious concerns about the risk of escalation should tensions between Moscow and the West increase.

The escalatory character of Russian sabotage efforts is particularly evident in the intensification of attacks in tandem with major military operations. In the lead-up to the 2008 invasion, Georgian counterintelligence apprehended a GRU colonel who had established a secretive unit in South Ossetia consisting of 120 agent-saboteurs; a similar plot was uncovered in Ukraine in 2021 (Cormac 2022, 145). These operations appear to have been set in place to support the deployment of military forces. While Western services cannot know what impact the sabotage units had or how many of them may have been in operation, their existence reveals the magnitude of Russian escalation. Similarly, Moscow's annexation of Crimea in 2014 was swiftly followed by explosions in a Czech ammunition depot containing military supplies for Ukraine and in a warehouse in Vrbetice, resulting in two fatalities (Richterova et al. 2024b). These examples illustrate the strategic deployment of sabotage alongside more traditional instruments of military power, presumably with the intent of weakening adversaries' war efforts by forcing them to fight on multiple different fronts. Some experts warn that GRU-sponsored disruptions in Europe are symptomatic of a broader hybrid campaign aimed at undermining support for Ukraine (Richardson 2024; Bilal 2024). The hybrid war concept contends that Russia is attempting to reduce the power differential with NATO by combining military and non-military tactics to overwhelm Western governments (Bilal 2024). The deliberate targeting of sites of military-industrial importance supports this hypothesis, as does the inclusion of sabotage units in ground invasion plans.

A major precipitant of escalation during the Cold War and, it seems, in the current geopolitical context, is the Kremlin's conviction that its sphere of influence is under threat. Sabotage was one of the tools historically used to "neutralise the Westernisation of the surrounding countries," and the maintenance of a buffer zone around Russia's borders was considered of vital national interest (Darczewska 2017, 10). This thinking has trickled down from Soviet doctrine. It provided the rationale behind Putin's decision to invade Ukraine in 2022, which the Kremlin has framed as a response to Western encroachment (Dickinson 2022). Even diplomatic responses to Russian aggression may add fuel to the fire. To illustrate, the most recent upsurge in sabotage activity is partly believed to have been retaliation for the expulsion of some 750 undercover Russian operatives from Europe following the Ukraine invasion (Richardson 2024). The scale and intensity of attacks therefore reflect Moscow's appraisal of the political landscape. Sabotage aimed at countering Western influence in the Russian Federation's borderlands is carefully calibrated according to the level of escalation Moscow seeks to achieve. This also means that increased support for Ukraine will likely be met with more destructive and deliberate attacks.

The second major continuity between Cold War and Putin-era doctrine is the targeting of structures and individuals deemed of posing a threat to Russian foreign policy objectives. Soviet operational targets included items of key industrial importance such as water reservoirs, chemical plants, and storage facilities (Richterova 2024). Although there is no confirmation of such attacks being carried out in the past, evidence of GRU involvement in physical "incidents" against Western critical infrastructure is present and growing. In June 2024, break-ins at water treatment facilities in Finland aligning with Russian sabotage tactics were flagged by authorities (Recorded Future 2024). These now appear to have spread to Sweden, where residents in the district of Bollnas were instructed to boil drinking water as a safety measure after a break-in on October 13th (Apps 2024). Similar precautions were taken following the contamination of the water supply on a military base just outside Cologne in August 2024; a spokesperson for the German defence ministry warned of a “serious indication” of Russian sabotage (Connolly 2024). Low-level operations of this kind generate fear and mistrust and mimic the escalatory doctrine outlined in Czech records, which Moscow exported to Soviet Bloc countries.

Targets are also frequently selected for their potential to sow discord and exploit fissures within Western societies. In the 1960’s, a smear campaign against West Germany conducted by the KGB’s 13th Department involved painting swastikas in public spaces and setting synagogues on fire (CIA 1964, 6). Sixty years later, in a near mirror parallel, graffitied red hands appeared on the Holocaust Memorial in Paris and blue Stars of David were stencilled on French buildings (Chrisafis 2024). These incidents, paired with the discovery of three coffins bearing the words “French soldiers of Ukraine” under the Eiffel Tower in June 2024, are being investigated as part of a Russian destabilisation operation (Reynaud, Leloup and Albertini 2024). The most recent of these acts of strategic vandalism coincides with French President Emmanuel Macron’s pledge to provide Ukraine with Mirage fighter jets (Le Monde with AP 2024). Sabotage operations are therefore ramping up in accordance with the escalation of tensions and their aim, much as it was during the Cold War, is to strike targets in a manner that aggravates societal rifts and ultimately weakens support for Ukraine.

Divergences in Sabotage Doctrine

The previous section established escalatory measures and target selection as the principal continuities in sabotage doctrine. The essay will now turn to divergences from Cold war-era doctrine. The first relates to the Russian security services’ reliance on ICTs, particularly Internet platforms. This transformation is most visible in recruitment practices: instead of hiring highly capable “agent-saboteurs” to carry out operations, Russian agencies have shifted to an ad-hoc, ‘gig economy’ model “powered by and through ICT interfaces” (Richterova et al. 2024b, 15). Recruiters now rely on social media and encrypted messaging platforms to access a much wider pool of would-be saboteurs, thereby reducing operational costs (Richterova et al. 2024a). This differs sharply from Cold War-era recruitment of agents-of-influence, which usually required multiple years (Shultz 1984, 167). The shift to a gig-economy approach is further supported by the OCCRP-led “Ivanov” reporting project, in which journalists investigated a Telegram account called “Privet Bot” and found that the account, which had been linked to the recruitment of Europeans with pro-Russian views, used a pre-programmed menu to suggest targets and inquire after potential agents’ military experience, motivations, and willingness to carry out an attack (Huppertz et al. 2024). The emergence of new communications technologies has precipitated a transformation in sabotage doctrine by streamlining recruitment efforts and reducing their costs. Furthermore, it has led to a significant increase in the scale of operations, as evidenced by the wave of arsons, strategic vandalism, and other forms of sabotage reported by governments since 2022.

The Russian security agencies’ increasing reliance on ICTs has been accompanied by a discernible downturn in operational tradecraft. Riehle (2024, 871) contends that the surge in clandestine actions attributed to Russia in recent years is partly due to GRU incompetence: in the case of the Internet Research Agency’s disinformation campaign during the 2016 US election, Facebook ads were paid for in rubles and contained flagrant grammatical errors. Although harnessing ICTs has enabled Moscow to effectuate operations on an unprecedented scale, attacks are often poorly executed and increasingly being traced back to Russian intelligence. Much of today’s sabotage is automated and conducted via trolls and bots; the same could not be said for the Soviet enterprise, which employed controlled sources, appropriate cover, and meticulous deployment tactics (Gioe, Lovering, and Pachesny 2020, 533). Although rising attribution can partly be blamed on poor tradecraft, it is also an indicator of Russian indifference to public opinion regarding its actions (Riehle 2024, 864). The decline of plausible deniability within sabotage doctrine reflects Moscow’s increasingly belligerent attitude towards the West.

The second major development in contemporary sabotage doctrine relates to the emergence of new tactics to damage critical infrastructure. Rising levels of global interconnectedness have exacerbated Western vulnerability to undersea cable disruptions and cyberattacks, both of which have been deployed with growing intensity in recent years. Although there is no evidence of Russia intentionally cutting underwater cables, it has been systematically mapping infrastructure in the North and Baltic Seas (Schaller 2024, 204). In February 2023, Dutch intelligence warned that Moscow was undertaking acts of espionage and sabotage against the country’s key maritime facilities, including cable networks (Hancock and Sheppard 2023; Gupte et al. 2023). This is in itself nothing new: during the

Cold War, the Soviets employed a number of surveillance vessels and frequently co-opted civilian fishing fleets for sabotage missions (Schaller 2024, 206). This practice is still in effect, with Russia using commercial ships to conceal its clandestine activities (Stroobants 2024). However, reliance on undersea cables has only grown in the digital age, exacerbating Western vulnerability in the event of a sabotage-related loss of connectivity. An interruption in government communications due to severed cable networks would be especially dangerous in a crisis (Bateman 2024). Taking into consideration the War in Ukraine and threat of Russia-NATO military escalation, sabotage of undersea cable infrastructure is more likely and poses a greater risk than it did during the Cold War.

Cyberattacks have also emerged as a major new avenue for sabotage. The 2007 Russia-backed DDoS attack on Estonia lasted 22 days and resulted in a loss of service for many government servers (Devanny, Goldoni, and Medeiros 2022, 38). In 2016, Russian hackers targeted Ukrainian electrical grids, causing a major power outage in Kyiv (Riehle 2024, 870). Soon after the 2022 invasion, a massive cyberattack launched by Moscow disabled over sixty Ukrainian government websites, and a similar operation in late 2023 left twenty-four million Ukrainians without access to internet or phone services (Cwalina 2024). These operations reveal the profound implications that cyber-sabotage can have on critical information and energy infrastructure. Loss of power and connectivity, especially during a military crisis, pose a serious threat to states' ability to function, making these attacks an attractive option for Moscow in its hybrid campaign against NATO.

Conclusion

This essay has drawn on an array of suspected and confirmed cases of Russian sabotage in Europe to make the argument that contemporary sabotage mirrors Cold War era doctrine in two principal regards. The first is the Kremlin's ramping up of operations in accordance with the political calculations of the day, illustrated by recently uncovered Soviet documents and the surge in attacks since the 2022 invasion of Ukraine. The second is a target selection process aimed at spreading confusion and fear amongst Western populations. However, sabotage doctrine has also undergone tremendous changes, notably in its increasing reliance on ICTs, which has allowed low-level, low-cost attacks to proliferate, and in its relentless mapping of critical maritime infrastructure and cyber-enabled sabotage operations. Although there are many other important similarities and differences between the two eras of state-led sabotage, these have been deemed most relevant in the context of the War in Ukraine and the intensification in both scale and magnitude of Moscow's sabotage enterprise.

Bibliography

Abrams, Steve. 2016. "Beyond Propaganda: Soviet Active Measures in Putin's Russia." *Connections* 15 (1): 5-31.

Apps, Peter. 2024. "Russia's Suspected Sabotage Campaign Steps Up in Europe." *Reuters*, October 21. https://www.reuters.com/world/russias-suspected-sabotage-campaign-steps-up-europe-2024-10-21/.

Bateman, Aaron. 2024. "Undersea Cables and the Vulnerability of American Power." *Engelsberg Ideas*, May 7. https://engelsbergideas.com/essays/undersea-cables-and-the-vulnerability-of-american-power/.

Bellingcat. 2022. "Socialite, Widow, Jeweller, Spy: How a GRU Agent Charmed Her Way Into NATO Circles in Italy." August25.https://www.bellingcat.com/news/2022/08/25/socialite-widow-jeweller-spy-how-a-gru-agent-charmed-her-way-into-nato-circles-in-italy/.

Bilal, Arsan. 2024. "Russia's Hybrid War against the West." *NATO Review*, April 26. https://www.nato.int/docu/review/articles/2024/04/26/russias-hybrid-war-against-the-west/index.html.

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

CIA. 1964. "Soviet Use of Assassination and Kidnapping (Approved for Release)." *CIA Historical Review Program*, vol. 19, no. 3. https://www.cia.gov/resources/csi/studies-in-intelligence/archives/vol-19-no-3/soviet-use-of-assassination-and-kidnapping/.

Connable, Ben, Stephanie Young, Stephanie Pezard, Andrew Radin, Raphael Cohen, Katya Migacheva, and James Sladden. 2020. *Russia's Hostile Measures: Combating Russian Gray Zone Aggression Against NATO in the Contact, Blunt, and Surge Layers of Competition*. RAND Corporation. https://doi.org/10.7249/RR2539.

Connolly, Kate. 2024. "Germany Investigates Possible Attack on Water System at Military Base." *The Guardian*, August 14. https://www.theguardian.com/world/article/2024/aug/14/germany-investigates-possible-attack-on-water-system-at-military-base.

Cormac, Rory. 2023. *How to Stage a Coup: And Ten Other Lessons from the World of Secret Statecraft* . Paperback edition. London: Atlantic Books.

Cwalina, Aleksander. 2024. "Concerns Grow over Possible Russian Sabotage of Undersea Cables." *Atlantic Council*, September 12. https://www.atlanticcouncil.org/blogs/ukrainealert/concerns-grow-over-possible-russian-sabotage-of-undersea-cables/.

Darczewska, Jolanta, and Piotr Żochowski. 2017. "Active Measures: Russia's Key Export." *OSW Point of View 64*, May 30. https://www.osw.waw.pl/en/publikacje/point-view/2017-05-30/active-measures-russias-key-export.

Devanny, Joe, Luiz Rogerio Franco Goldoni, and Breno Pauli Medeiros. 2022. "Strategy in an Uncertain Domain." *Journal of Strategic Security* 15, no. 2: 34-47.

Dewey, Karl. 2022. "Poisonous Affairs: Russia's Evolving Use of Poison in Covert Operations."*The Nonproliferation Review* 29 (4–6): 155–76.

Dickinson, Peter. 2022. "NATO, Nazis, Satanists: Putin is Running Out of Excuses for His Imperial War."*Atlantic Council*, November 8. https://www.atlanticcouncil.org/blogs/ukrainealert/nato-nazis-satanists-putin-is-running-out-of-excuses-for-his-imperial-war/.

Galeotti, Mark. 2019. "Active Measures: Russia's Covert Geopolitical Operations." *Marshall Center Security Insight*, no. 31, June 2019. https://www.marshallcenter.org/en/publications/security-insights/active-measures-russias-covert-geopolitical-operations-0.

Gioe, David V., Richard Lovering, and Tyler Pachesny. 2020. "The Soviet Legacy of Russian Active Measures: New Vodka from Old Stills?" *International Journal of Intelligence and CounterIntelligence* 33 (3): 514–39. https://doi.org/10.1080/08850607.2020.1725364.

Gramer, Robbie, and Amy Mackinnon. 2024. "Russia Ramps Up Sabotage Operations in Europe." *Foreign Policy*, June 13. https://foreignpolicy.com/2024/06/13/russia-sabotage-attacks-europe-espionage-hybrid-arson/.

Gupte, Eklavya, Stuart Elliott, Henry Edwardes-Evans, and Rosemary Griffin. 2023. "Dutch Intelligence Warns of Russian Sabotage Against Its Key Maritime, Energy Facilities." *S&P Global*, February 20. https://www.spglobal.com/commodity-insights/en/news-research/latest-news/crude-oil/022023-dutch-intelligence-warns-of-russian-sabotage-against-its-key-maritime-energy-facilities.

Hancock, Alice, and David Sheppard. 2023. "Netherlands Warns of Russian Attempts to Sabotage Its Energy Infrastructure." *Financial Times*, February 20. https://www.ft.com/content/ec436b8f-d00f-4525-b6e0-174cc9abaea4.

Hoiback, Harald. 2013. *Understanding Military Doctrine: A Multidisciplinary Approach*. 1st ed. Cass Military Studies. Milton Park, Abingdon, Oxon: Routledge.

Holden, Michael and Gabriel Stargardter. 2024. “UK Intelligence Chief Accuses Russia of

‘Staggeringly Reckless’ Sabotage Campaign.” *Euronews*, November 29. https://www.euronews.com/2024/11/29/uk-intelligence-chief-accuses-russia-of-staggeringly-reckless-sabotage-campaign.

Huppertz, Carina, Artur Izumrudov, Laurin Lorenz, Ilya Lozovsky, Bastian Obermayer, Holger Roonemaa, Fabian Schmid, and Marta Vunš. 2024. “’Make a Molotov Cocktail’: How Europeans Are Recruited Through Telegram to Commit Sabotage, Arson, and Murder.” *Organized Crime and Corruption Reporting Project (OCCRP) Investigation*, September 26. https://www.occrp.org/en/investigation/make-a-molotov-cocktail-how-europeans-are-recruited-through-telegram-to-commit-sabotage-arson-and-murder.

Kaitsepolitseiamet. “Estonian Internal Security Service Apprehended Suspects for Wrecking CarsBelonging to Minister of Internal Affairs and a Journalist.” n.d. https://kapo.ee/en/media/estonian-internal-security-service-apprehended-suspects-wrecking-cars-belonging-minister/.

Karlsen, Geir Hågen. 2019. “Divide and Rule: Ten Lessons about Russian Political Influence Activities in Europe.” *Humanities & Social Sciences Communications* 5 (1): 1-14.

Kirby, Paul and Frank Gardner. 2024. “Mystery Fires Were Russian ‘Test Runs’ to Target Cargo Flights to US.”*BBC News*, November 6. https://www.bbc.com/news/articles/c07912lxx33o.

Kofman, Michael, and Matthew Rojansky. 2015. “A Closer Look at Russia’s ‘Hybrid War.’” *Kennan Cable*, no. 7, April 2015. https://www.wilsoncenter.org/publication/kennan-cable-no7-closer-look-russias-hybrid-war.

Lanoszka, Alexander. 2016. “Russian Hybrid Warfare and Extended Deterrence in Eastern Europe.” *International Affairs* 92 (1): 175–95.

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

Lucas, Edward. 2024. “New Normal: Impunity for Russian Active Measures.” *CEPA*, September 29. https://cepa.org/article/new-normal-impunity/.

Lynskey, Dorian. 2023. “Russia’s Long History of Smears, Sabotage and Barefaced Lies.” *The Spectator*, August 12. https://www.spectator.co.uk/article/russias-long-history-of-smears-sabotage-and-barefaced-lies/.

Nehring, Christopher. 2021. “Active and Sharp Measures: Cooperation between the Soviet KGB and Bulgarian State Security.” *Journal of Cold War Studies* 23 (4): 3–33. https://doi.org/10.1162/jcws_a_01038.

NPSA. 2024. “Countering the Threat of Sabotage Operations to UK Interests and National Security.” October 7. https://www.npsa.gov.uk/countering-sabotage.

O’Carroll, Lisa. 2024. “Europe on High Alert After Suspected Moscow-Linked Arson and Sabotage.” *The Guardian*, May 30. https://www.theguardian.com/world/article/2024/may/30/europe-on-high-alert-after-suspected-moscow-linked-arson-and-sabotage.

Pompeo, Michael R. 2020. “The United States Condemns Russian Cyber Attack Against the Country of Georgia.” *US Department of State Press Statement*, February 20. https://2017-2021.state.gov/the-united-states-condemns-russian-cyber-attack-against-the-country-of-georgia/.

Posen, Barry R. 2016. “Foreword: Military Doctrine and the Management of Uncertainty.” *Journal of Strategic Studies* 39 (2): 159–73. https://doi.org/10.1080/01402390.2015.1115042.

Recorded Future. 2024. “Russian Sabotage Activities Escalate Amid Fraught Tensions.” November 14. https://www.recordedfuture.com/research/russian-sabotage-activities-escalate-amid-fraught-tensions.

Reynaud, Florian, Damien Leloup, and Antoine Albertini. 2024. “Coffins at the Eiffel Tower: Suspicions Point to Another Case of Russian Interference.” *Le Monde*, June 3. https://www.lemonde.fr/en/pixels/article/2024/06/03/coffins-at-the-eiffel-tower-suspicions-point-to-another-case-of-russian-interference_6673608_13.html.

Richardson, Jon. 2024. “How and Why Russia is Conducting Sabotage and Hybrid-War Offensive.”*The Strategist – Australian Strategic Policy Institute*, November 5. https://www.aspistrategist.org.au/how-and-why-russia-is-conducting-sabotage-and-hybrid-war-offensive/.

Richterova, Daniela, Elena Grossfeld, Magda Long, and Patrick Bury. 2024a. “A New Era of Russian Sabotage?” *KCSI Insights*, November 4. https://kcsi.uk/kcsi-insights/a-new-era-of-russian-sabotage.

Richterova, Daniela, Elena Grossfeld, Magda Long, and Patrick Bury. 2024b. “Russian Sabotage in the Gig-Economy Era.” *The RUSI Journal* 169 (5): 10–21. https://doi.org/10.1080/03071847.2024.2401232.

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

Riehle, Kevin P. 2024. “Ignorance, Indifference, or Incompetence: Why Are Russian Covert Actions So Easily Unmasked?” *Intelligence and National Security* 39 (5): 864–78.

Roehjell, Dag. 2024. “Contemporary Russian Threat Perception — Has Anything Really Changed Since 1917?”*The Journal of Slavic Military Studies,* 37 (2): 143-167.

Romerstein, Herbert. 2001. “Disinformation as a KGB Weapon in the Cold War.” *Journal of Intelligence History* 1 (1): 54–67. https://doi.org/10.1080/16161262.2001.10555046.

Rosengren, Oscar. 2022. “Russian Active Measures in Norway: A Situational Assessment.” *Grey Dynamics* , November 10. https://greydynamics.com/russian-active-measures-in-norway-a-situational-assessment/.

Rumer, Eugene. 2019. “The Primakov (Not Gerasimov) Doctrine in Action.”*Carnegie Endowment for International Peace*, June 5. https://carnegieendowment.org/research/2019/06/the-primakov-not-gerasimov-doctrine-in-action?lang=en.

Samorukov, Maksim and Vuk Vuksanovic. 2023. “Untarnished by War: Why Russia’s Soft Power Is So Resilient in Serbia.” *Carnegie Endowment for International Peace*, January 18. https://carnegieendowment.org/russia-eurasia/politika/2023/01/untarnished-by-war-why- russias-soft-power-is-so-resilient-in-serbia?lang=en.

Shevchenko, Vitaly. 2024. “Russia Blamed for GPS Interference Affecting Flights in Europe.” *BBC News*, May 2. https://www.bbc.co.uk/news/articles/cne900k4wvjo.

Shultz, Richard H., and Roy Godson. 1984. *Dezinformatsia: Active Measures in Soviet Strategy*. Washington: *Pergamon Press.*

Stroobants, Jean-Pierre. 2024. “In the North Sea, Russia Conceals Espionage Activities With Commercial Ships.”*Le Monde*, June 22. https://www.lemonde.fr/en/international/article/2024/06/22/in-the-north-sea-russia-conceals-espionage-activities-with-commercial-ships_6675426_4.html.

The Baltic Sentinel. 2024. “Russian Military Intelligence Linked to Sabotage Attack on Estonian Interior Minister’s Vehicle.” December 5. https://balticsentinel.eu/8148455/russian-military-intelligence-linked-to-sabotage-attack-on-estonian-interior-minister-s-vehicle.

US Army. 2024. “Safeguarding the U.S. Defense Industrial Base and Private Industry Against Sabotage.” November 21.https://www.army.mil/article/281519/ncsc_acic_and_partners_provide_security_guidance_to_u_s_defense_industrial_base_regarding_russian_sabotage_activity_in_europe.

Vernetti, Lorenzo. 2024. “Active Measures: Russian Shadow Games in the Digital Age.” *Grey Dynamics*, August 28. https://greydynamics.com/active-measures-russian-shadow-games-in-the-digital-age/.