Crisis of Secrecy: The Weaponisation of Ambiguity in Covert Action

Written by Ninon de Buchet

The strategic utility of covert action has traditionally been grounded in its ability to cause effects in a plausibly deniable manner (Duffield 2024, 4). However, recent transformations in the media and information environments have sparked a 'crisis of secrecy' with far-reaching implications for covert operations (Aldrich and Richterova 2018, 1003). Western governments' ascription of a wide range of attacks to the Russian state since 2014, for instance, exemplify the growing implausibility of denial. Intelligence scholars have attributed this heightened risk of exposure to a variety of factors, the principal one being changes in the information landscape which have enabled investigative journalists to expose foreign interference, occasionally even rivalling domestic intelligence agencies in their attribution efforts (Cormac 2017, 170). Some have concluded that the decline of plausible deniability will nullify the benefits of covert activity (Cormac and Aldrich 2018, 493). Drawing on examples of suspected and confirmed Russian covert operations since the annexation of Crimea, this essay will argue that denial has largely become implausible due to credible attribution by non-state intelligence professionals using publicly available analytical technologies. It will further argue that the deterioration of secrecy in this domain has created new avenues for Russia to conduct operations below the threshold of armed conflict with NATO while cultivating an image of impunity.

The first section of the essay will explore how the proliferation of open-source and forensic investigation techniques has led to significant advances in the attribution and monitoring of Russian covert operations in Western Europe, particularly those undertaken as part of the Kremlin's alleged 'hybrid war' against NATO. These attribution efforts are supported by globalised information flows, which facilitate greater interaction between independent media organisations and broader civil society. The second section will discuss how Russia has embraced implausible deniability. It will show that while sophisticated attribution efforts have significantly enhanced NATO's collective response to hybrid warfare, the Kremlin has countered this by exploiting the strategic ambiguity generated by unacknowledged yet identifiable kinetic operations. As the essay will demonstrate, this dynamic has both positive and negative implications for the international security environment.

Covert action refers to any policy in support of national interests abroad that a state undertakes while keeping its involvement concealed (Daughtery 2004, 13). Aldrich and Cormac (2018, 482) note the crucial distinction between plausibly deniable action, referring to operations that are neither apparent

nor acknowledged, and implausibly deniable action, referring to ones that are apparent but not acknowledged. A key element of covert operations is that they allow governments to achieve results "by methods short of war" (Mitrovich 2021, 391). This is reflected in the growing scholarship on hybrid war, a concept developed by the US military to describe the combination of political and military threats to achieve greater effects (Galeotti 2016, 286). Russia, whose integrated use of military and non-military means can be traced back to the Soviet doctrine of active measures, is now widely understood to be waging an aggressive hybrid warfare campaign against NATO member states (Bilal 2024; Richardson 2024). This essay will therefore focus on Russian covert action aimed at weaponising strategic ambiguity and sowing discord in Western societies, most notably through physical sabotage, assassinations, and disinformation operations.

Western media organisations and digital investigation techniques

The main challenge to plausible deniability in covert action arises from the proliferation of open-source intelligence (OSINT) tools and concurrent emergence of non-state actors capable of producing and disseminating intelligence. Public, widespread access to big data analytics and open source methodologies has made contemporary counterintelligence functions significantly more effective (Lord 2015, 668). While this work is primarily associated with the intelligence services, public media organisations can also assume counterintelligence-like functions, as evidenced by the award-winning investigations undertaken by groups like Bellingcat and Der Standard (Huppertz et al. 2024). The ability to conduct operations in secret, which has diminished in the information age, is further compromised by the increasingly skilled public sector application of investigative methods to detect and expose state interference (Cormac and Aldrich 2018, 486). In this manner, the ability to produce and disseminate intelligence has effectively been extended to civil society. Bellingcat's report on the 2018 Salisbury poisonings stands out as a seminal example of a journalistic organisation applying OSINT and forensic-like methods to expose foul play by a foreign intelligence service (Bellingcat Investigation Team 2018). Reporters used leaked Russian government databases containing passport registration data to identify anomalies in the suspects' documents. More importantly, the organisation found that the GRU had been furnishing operatives with consecutively numbered passports for nearly a decade (Riehle 2024, 871). Revelations like this one enhance attribution and inform future detection and monitoring efforts, as will be shown further in the essay. The multiplication of potential sources of exposure means that plausible deniability is significantly harder to achieve and maintain for intelligence services.

The proliferation of investigative technologies is compounded by the unprecedented level of interconnectivity between members of the public. The globalised nature of Western society in particular means that citizens are politically conscious and can communicate easily with each other, reporters, and government personnel (Joseph and Poznansky 2017, 321). This means that individuals in a state targeted by a covert action can witness the event unfolding and collect digital evidence in real time. This makes it very challenging for states to successfully achieve plausible deniability. To illustrate, during the 2014 intervention in Eastern Ukraine, photos taken on personal smartphones and shared on social media provided incontrovertible proof that Russian troops had been deployed in the region (Szoldra 2014). Thus, any individual with a cell phone can potentially expose an act of foreign interference. When thousands of pieces of evidence of the same event are put together, this can trigger a global response against the state conducting the operation.

Non-state intelligence producers such as investigative reporters rely extensively on evidence gathered from Information and Communication Technology (ICTs) within a target state. Poznansky (2022, 524) found that decisionmakers are highly aware of the exposure risks posed by ICTs, and are consequently more cautious when authorising a covert action in a society with dense ICT networks. Cover identities of intelligence operatives are particularly vulnerable. Significant advancements in data analytics have made it possible to aggregate and process vast sums of information on a given individual's 'digital exhaust,' which refers to the residual traces left behind by a person's digital activity (Lord 2015, 669). Digitalisation renders anonymity increasingly elusive. This creates particular challenges for intelligence professionals charged with conducting covert operations. To remain undetected, operatives must now work twice as hard to conceal their actions in both the analogue and digital spheres. The emergence of other technologies tying an individual's biological attributes to their identity, such as facial and fingerprint scanners and biometric data, further complicates "the long-term defensibility of cover aliases" (Cunliffe 2021, 7). The emergence and proliferation of these technologies, paired with the risk of exposure from OSINT-enabled reporting, have the effect of calling into question the longevity of plausible deniability.

The Russian state appears highly attuned to the risks posed by these technologies. According to Watling, Danylyuk and Reynolds (2024, 9), the GRU recently identified three major vulnerabilities in its ability to organise unconventional operations; the main one constitutes intelligence personnel's "vulnerability to identification through modern analytical techniques," such as geolocation of mobile phones using advertising data. It is easy to understand the Russian intelligence agencies' growing concern about the unmasking of its operatives in Europe. In the past ten years, a number of high-profile

sabotage cases have been attributed to GRU's Unit 29155, including destabilisation operations in Moldova (2015) and a failed coup attempt in Montenegro (2016), to name just a few (Hamilton 2024). Bellingcat investigators, for instance, used open-source information to track the communications and movements of members of the military unit (Adami 2022). Their work has been instrumental in identifying patterns and vulnerabilities in the unit's operational procedures, such as the aforementioned consecutive number series in the cover passports of the two operatives responsible for the Salisbury poisonings. By looking for similar patterns in other suspected cases of politically motivated assassinations, reporters succeeded in tracing several international operations back to GRU (Bellingcat Investigation Team 2019b). In this manner, media organisations' attribution of covert actions can create a domino effect. The revelation of certain vulnerabilities in an adversary's procedures can help unravel the wider picture. This improves Western decisionmakers' understanding of broader Russian strategic aims. The findings from Bellingcat's investigations were key to prompting European governments to acknowledge Russia's resort to hybrid war tactics in the aftermath of the Crimean annexation (Pancevski 2024).

In addition to enhancing public attribution and facilitating linkages between superficially unrelated attacks, journalistic organisations' deployment of open source and forensic investigative methods supports the sustained monitoring of Russian covert activities. To illustrate, the Dutch investigative outlet Follow the Money has uncovered and disseminated vital insights on Russia's sophisticated scheme to evade the Western sanctions put in place after its 2022 invasion of Ukraine (OCCRP 2025). The investigation, which is ongoing, brings together 40 journalists from 13 different newsrooms all around the world (Henley 2025). Reporters sift through minute discrepancies in digital maritime databases to trace Russia's acquisition and recirculation of oil tankers (Follow the Money 2025). Similarly, a joint investigation by Politico and SourceMaterial used satellite imagery and shipping data to uncover the exact points where vessels illegally carrying Russian oil stopped along major trade routes to discharge (SourceMaterial and Politico 2024).

These investigative enterprises, undertaken by independent Western media, display the strategic dividends yielded by global communication flows. The interconnectedness of journalists across the world facilitates cooperation, making the difficult task of monitoring Russia's vast sanctions evasion efforts comparatively more manageable. Moreover, these research projects and the collective response that their revelations elicit from civil society ultimately foster a sense of unity in the face of Russian aggression. Public attribution of covert operations, particularly those involving violent sabotage,

assassination, or economic warfare, serves a strategic purpose by furthering the narrative that NATO members must work together to resist the Kremlin's intimidation tactics.

The rampant use of open-source tools and information to attribute covert activity is further demonstrated by reporting on Russian sabotage of critical infrastructure at sea. In April 2023, a team of journalists from Finland, Denmark, Sweden and Norway revealed the existence of a large-scale programme run by Moscow "to systematically map critical infrastructure and its vulnerabilities" in the Baltic and North Seas (Schaller 2024, 204). Although the Kremlin's current efforts primarily consist of espionage and non-kinetic operations, they are intended to set the stage for future acts of sabotage (Schaller 2024, 202). The documentary produced by these journalists, who used oceanographic databases to track the movements of Russian vessels, represents a prime example of ICT-enabled investigations threatening the Kremlin's plausible deniability.

Despite Russian officials' assertions that the ships were there for research, the reporters identified dangerous and sustained patterns of GPS manipulation, suggesting that the vessels were taking measures to keep their locations secret (Camut 2023; Connolly 2023). This reflects the level of scrutiny achieved by journalistic OSINT producers. Their work challenges Moscow's counter-claims and deceptive narratives by amassing overwhelming evidence of foul play, thereby undermining the Russian state's ability to plausibly deny involvement. Moreover, their findings corroborate disclosures from several Nordic governments warning of increased Russian sabotage activity around critical infrastructure in the North Sea (NATO News 2025). This illustrates how information issued by both civilian intelligence professionals and state intelligence agencies can have mutually reinforcing effects, which in turn can be highly advantageous to lend credibility to attribution efforts. As the next section will discuss, this is particularly significant in today's contested information environment and in the context of Russia's increasing weaponisation of strategic ambiguity to conduct operations short of war.

Russian hybrid warfare and strategic ambiguity

The previous section established how advances in ICTs, particularly open-source and forensic investigation techniques, have empowered Western media organisations in their efforts to credibly attribute covert operations to the Russian state. The essay will now discuss how the decline of plausible deniability has affected Russia's sabotage enterprise against the West. Plausible deniability's existence on a continuum presents opportunities for states to operate in a space of ambiguity. Cormac and Aldrich (2018, 482) advance the notion that "covert action is less about plausible deniability and more

about non-acknowledged intervention as performance." This idea is reinforced by Russia's strategic use of ambiguous yet ultimately recognisable activities to undermine NATO. A notable example of this is Putin's insistence that the 'little green men' in Crimea were local self-defence units when they were in fact Russian soldiers deployed there to support the annexation of the region (Long 2024, 490). The Kremlin's disavowal, while thoroughly unconvincing in the eyes of the international community, served to prevent a military confrontation with NATO. This was followed by a public admission from Putin that the soldiers were Russian just one year later (Walker 2015). This episode illustrates the porous nature of deniability in contemporary military affairs. Whereas states have historically attempted to keep their involvement in covert action secret, Russia's recent behaviour suggests a willingness to be caught in a lie.

There is evidence to suggest that the decline of plausible deniability in recent years reflects an acknowledgement that unveiled covert operations yield important strategic advantages. Riehle (2024, 864) makes the argument that Russian actions display a shocking indifference to international opinion. The example of the secret services' shift to a 'gig economy' approach to sabotage, which consists of hiring amateurs to conduct low-level attacks in Western countries, corroborates this apparent downturn in Russian tradecraft (Richterova et al. 2024b). The Kremlin's resort to rudimentary sabotage practices has widened the scope of its operations across Europe at the expense of plausible deniability. This is not to say that efforts to conceal state involvement have ceased entirely. The ostensible lack of effort put into low-level sabotage operations is counter-balanced by the sophistication of many other covert activities, such as the 2021 SolarWinds computer intrusion, which took months to detect (Riehle 2024, 872). Deniability still appears to be a hallmark of Russian covert action (Richterova et al. 2024a). However, the Kremlin seems to have found a way to leverage exposure into new avenues for projecting influence. When actions go unattributed, they sow confusion in the target states. When they are traced back to their orchestrator, they reinforce the image of Moscow as a powerful force to be reckoned with.

The notion of non-acknowledged intervention as performance is not new; rather, it reflects the potential of implausibly deniable operations for states seeking to engage in aggressive posturing. By keeping operations short of war and refusing to deny or confirm involvement, a state can create an atmosphere of ambiguity whereby international actors do not know "whether a state of war exists – and if it does, who is a combatant and who is not" (Cormac and Aldrich 2018, 490). This is significant because it reduces the ability of target states to respond to attacks. Societies may experience widespread confusion as they begin to suspect every disruption of concealing foreign interference, ultimately

allowing fear to take hold (Cormac and Aldrich 2018, 491). In July 2024, European investigative reporters uncovered SVR documents containing instructions for an 'information warfare' operation aimed at "amplifying emotions like 'fear', 'panic', and horror'" amongst populations in NATO member states (Long 2024, 89). Discoveries like this one reveal the extent of Russia's use of sabotage and other kinetic operations to instil panic in its adversaries. While plausible deniability is maintained as often as possible, the unprecedented scale of the country's sabotage enterprise works to its advantage. All operations whose secrecy is compromised regain strategic value as part of Russia's broader campaign of intimidation. Thus, even 'failed' covert actions can be repurposed.

This phenomenon is exacerbated by the pluralistic character of the Western media landscape. Christo Grozev, former lead investigator for Bellingcat, noted that a major challenge with today's information environment is countering misinformation from official sources. He argues that at the onset of the War in Ukraine, European coverage of the conflict fell into the trap of false equivalence, reporting claims from Russian sources and unintentionally furthering the Kremlin's narrative that the war was a response to aggressive NATO expansion (Adami 2022). This information environment rife with claims and counterclaims creates major dilemmas for both journalists and governments. It exacerbates the threat posed by covert action, since both over and under exaggerating a foreign actor's level of involvement can have detrimental consequences for the target state. Underreporting on such cases risks fuelling narratives that are sympathetic to Moscow, while overreporting on them sends the message that the Kremlin can strike at Western countries with impunity.

Implausibly deniable actions can also serve a performative function by communicating resolve. Some scholars have pointed out the ability of such operations to convey messages about intentions that will be picked up by domestic intelligence services and shared with leaders (Cormac and Aldrich 2018, 488). A mirror process occurs when investigative organisations pick up on foreign interference and relay it to the wider public. In addition to communicating intent directly to leaders, covert operations can send a powerful message to a foreign electorate through the intermediary of reputable media outlets. Russia's actions, including the purported lack of effort in concealing some of its lower-level sabotage attempts, make sense from a narratological perspective. Duffield (2024, 4) explains that for actors seeking to influence the narrative, barely plausible deniability can present more advantages for covert action than true secrecy. Russia is visibly trying to gain the upper hand in this domain, as evidenced by its deployment of influence and kinetic operations to question the credibility and legitimacy of Western leaders, leveraging accusations of fascist or authoritarian rhetoric to erode trust in democratic institutions (Karlsen 2019, 6). These tactics represent Moscow's embrace of implausible

deniability to achieve effects, in this case to advance a dangerous narrative aimed at delegitimising Western politicians and institutions while presenting itself as the victim of NATO belittlement. In the long term, Russia is likely to continue expanding its influence through the weaponisation of ambiguity in the international security environment, as this allows it to communicate resolve and impunity without engaging in a direct military confrontation with NATO.

Conclusion

This essay has argued that the rise of open-source intelligence and digital forensics has been accompanied by the diminution of secrecy, most notably in the realm of covert action. As demonstrated through the examples of Western reporting on a wide range of assassination attempts, disinformation campaigns, and sabotage operations across Western Europe since 2014, media organisations equipped with ICT-powered investigative tools play a pivotal role in exposing Russian covert activities. The decline of plausible deniability, however, has not rendered covert action obsolete. Rather, the Russian intelligence agencies have adapted to this new strategic environment, embracing a posture that enables them to operate in the ambiguous grey space between denial and acknowledgment. This state of quasi-secrecy supports Moscow's efforts to reshape the narrative in Western societies, communicating resolve and feeding into feelings of confusion and fear to achieve effects aligned with its foreign policy interests. Thus, the crisis of secrecy marks a transformation in how states exploit exposure as a form of influence. Although Russia's hybrid war has made the international security environment more dangerous, Western attribution efforts have yielded remarkable results, highlighting the value of decisive, coordinated responses in addressing unconventional threats.

Bibliography

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

Adami, Marina. 2022. "Bellingcat's Grozev on Investigating Russia's Invasion of Ukraine." *Global Investigative Journalism Network*, March 3. https://gijn.org/resource/bellingcats-grozev-on-investigating-russias-invasion-of-ukraine/

Aldrich, Richard J, and Daniela Richterova. 2018. "Ambient Accountability: Intelligence Services in Europe and the Decline of State Secrecy." *West European Politics* 41 (4): 1003–24.

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/

Bellingcat Investigation Team. 2018. "Full Report: Skripal Poisoning Suspect Dr. Alexander Mishkin, Hero of Russia." *Bellingcat*, October 9. https://www.bellingcat.com/news/uk-and-europe/2018/10/09/full-report-skripal-poisoning-suspect-dr-alexander-mishkin-hero-russia/

Bellingcat Investigation team. 2019a. "The Dreadful Eight: GRU's Unit 29155 and the 2015 Poisoning of Emilian Gebrev." *Bellingcat*, November 23. https://www.bellingcat.com/news/uk-and-europe/2019/11/23/the-dreadful-eight-grus-unit-29155-and-the-2015-poisoning-of-emilian-gebrev/

Bellingcat Investigation Team. 2019b. "The GRU Globetrotters: Mission London." *Bellingcat*, June 28. https://www.bellingcat.com/news/uk-and-europe/2019/06/28/the-gru-globetrotters-mission-london/

Bellingcat Investigation Team. 2021a. "How GRU Sabotage and Assassination Operations in Czechia and Bulgaria Sought to Undermine Ukraine." *Bellingcat*, April 26. https://www.bellingcat.com/news/uk-and-europe/2021/04/26/how-gru-sabotage-and-assassination-operations-in-czechia-and-bulgaria-sought-to-undermine-ukraine/

Bellingcat Investigation Team. 2021b. "Senior GRU Leader Directly Involved with Czech Arms Depot Explosion." *Bellingcat*, April 20. https://www.bellingcat.com/news/2021/04/20/senior-gru-leader-directly-involved-with-czech-arms-depot-explosion/

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.

Bloch, Chase, and Roseanne W. McManus. 2024. "Denying the Obvious: Why Do Nominally Covert Actions Avoid Escalation?" *International Organization* 78 (3): 600–624.

Camut, Nicolas. 2023. "Russia Uses Civilian Boats to Spy in the North Sea, Joint Report Says." *Politico*, April 19. https://www.politico.eu/article/russia-uses-civilian-ships-to-spy-in-the-north-sea-reports/

Carson, Austin, and Michael Poznansky. 2016. “The Logic For (Shoddy) US Covert Action in Syria.” War on the Rocks, July 21. https://warontherocks.com/2016/07/the-logic-for-shoddy-u-s-covert-action-in-syria/

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. 2023. “Russian Spy Network Operating in North Sea, Investigation Claims.” *The Guardian*, April 19. https://www.theguardian.com/world/2023/apr/19/russian-spy-network-operating-in-north-sea-investigation-claims

Cormac, Rory, and Richard J. Aldrich. 2018. “Grey Is the New Black: Covert Action and Implausible Deniability.” *International Affairs (London)* 94 (3): 477–94.

Cormac, Rory. 2017. “Disruption and Deniable Interventionism: Explaining the Appeal of Covert Action and Special Forces in Contemporary British Policy.” *International Relations (London)* 31 (2): 169–91.

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

Cunliffe, Kyle S. 2021. “Hard Target Espionage in the Information Era: New Challenges for the Second Oldest Profession.” *Intelligence and National Security* 36 (7): 1018–34. https://doi.org/10.1080/02684527.2021.1947555.

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.

Daugherty, William J, and Mark Bowden. 2004. *Executive Secrets: Covert Action & the Presidency*. 1st ed. New York: The University Press of Kentucky.

Devanny, Joe, Luiz Rogerio Franco Goldoni, and Breno Pauli Medeiros. 2022. "Strategy in an Uncertain Domain." *Journal of Strategic Security* 15 (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.

Downes, Alexander B., and Mary Lauren Lilley. 2010. “Overt Peace, Covert War?: Covert Intervention and the Democratic Peace.” *Security Studies* 19 (2): 266–306.

Duffield, Jack. 2024. “A Narrative Approach to Analysis of Covert Action.” *Review of International Studies*, 1–19.

Follow the Money. 2025. “The Shadow Fleet Secrets.” Investigation (Ongoing), Last Updated February 25. https://www.ftm.eu/files/the-shadow-fleet-secrets

Galeotti, Mark. 2016. “Hybrid, Ambiguous, and Non-Linear? How New Is Russia’s ‘New Way of War’?” *Small Wars & Insurgencies* 27 (2): 282–301.

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.

Galeotti, Mark. 2022. *The Weaponisation of Everything: A Field Guide to the New Way of War*. New Haven: Yale University Press.

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/.

Grozev, Christo. 2022a. “The Remote Control Killers behind Russia’s Cruise Missile Strikes on Ukraine.” Bellingcat, October 24. https://www.bellingcat.com/news/uk-and-europe/2022/10/24/the-remote-control-killers-behind-russias-cruise-missile-strikes-on-ukraine/

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

Hamilton, Fiona. 2024. “Sabotage, Spies and Sergei Skripal’s Poisoning – Behind Russia’s Secret War.” *The Times*, December 8. https://www.thetimes.com/uk/defence/article/russian-spy-unit-29155-skripal

Hastedt, Glenn. 2005. “Public Intelligence: Leaks as Policy Instruments-the Case of the Iraq War.” *Intelligence and National Security* 20 (3): 419–39.

Henley, Jon. 2025. “Shipowners Have Made £4.8bn Selling Tankers to Russian ‘Shadow Fleet’.” *The Guardian*, February 4. https://www.theguardian.com/world/2025/feb/04/us-and-european-shipowners-sold-230-ageing-tankers-to-russian-shadow-fleet

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

Joseph, Michael F, and Michael Poznansky. 2018. “Media Technology, Covert Action, and the Politics of Exposure.” *Journal of Peace Research* 55 (3): 320–35.

Karlsen, Geir Hågen. 2019. “Divide and Rule: Ten Lessons about Russian Political Influence Activities in Europe.” *Humanities & Social Sciences Communications* 5 (1): 19-.

Kragh, Martin, and Sebastian Åsberg. 2017. “Russia’s Strategy for Influence through Public Diplomacy and Active Measures: The Swedish Case.” *Journal of Strategic Studies* 40 (6): 773–816.

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

Long, Magda. 2025. “Shadows of Power beneath the Threshold: Where Covert Action, Organized Crime and Irregular Warfare Converge.” *Intelligence and National Security* 40 (1): 87–113.

Lord, Jonathan. 2015. “Undercover Under Threat: Cover Identity, Clandestine Activity, and Covert Action in the Digital Age.” *International Journal of Intelligence and Counterintelligence* 28 (4): 666–91.

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/.

Miller, Bowman H. "Open-Source Intelligence (OSINT): An Oxymoron?." *International Journal of Intelligence and Counterintelligence* 31, no. 4 (2018): 702-719.

Mitrovich, Gregory. 2021. “Covert Action and Grand Strategy.” In *The Oxford Handbook of Grand Strategy*, edited by Thierry Balzacq and Ronald R. Krebs. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198840299.013.26.

Montasari, Reza. 2023. *Countering Cyberterrorism: The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policing in US and UK National Cybersecurity*. 1st ed. Cham: Springer International Publishing, 2023.

National Intelligence Council. 2021. “Foreign Threats to the 2020 US Federal Elections.” US Intelligence Community Assessment ICA 2020-00078D, March 10. Declassified on 15 March 2021. https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2021/3521-intelligence-community-assessment-on-foreign-threats-to-the-2020-u-s-federal-elections

NATO News. 2025. “NATO Launches ‘Baltic Sentry’ to Increase Critical Infrastructure Security.” January 14. https://www.nato.int/cps/en/natohq/news_232122.htm

OCCRP. 2025. “European Ships Keep Russia’s Shadow Fleet Afloat.” Organized Crime and Corruption Reporting Project Ongoing Investigation, February 4. https://www.occrp.org/en/investigation/european-ships-keep-russias-shadow-fleet-afloat

Pancevski, Bojan. 2024. “Europe Sees Signs of Russian Sabotage but Hesitates to Blame Kremlin.” *Wall Street Journal*, May 20. https://www.wsj.com/world/europe/europe-sees-signs-of-russian-sabotage-but-hesitates-to-blame-kremlin-72598d4b

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.

Poznansky, Michael. 2021a. “Covert Action, Espionage, and the Intelligence Contest in Cyberspace.” War on the Rocks, March 23. https://warontherocks.com/2021/03/covert-action-espionage-and-the-intelligence-contest-in-cyberspace/

Poznansky, Michael. 2021b. “The Appeal of Covert Action: Psychology and the Future of Irregular Warfare.” *Modern War Institute* – West Point, September 6. https://mwi.westpoint.edu/the-appeal-of-covert-action-psychology-and-the-future-of-irregular-warfare/

Poznansky, Michael. 2022. “Revisiting Plausible Deniability.” *Journal of Strategic Studies* 45 (4): 511–33.

Renz, Bettina. 2016. “Russia and ‘Hybrid Warfare.’” *Contemporary Politics* 22 (3): 283–300.

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/

Richterova, Daniela. 2025. “Putin’s Spies for Hire: What the UK’s Biggest Espionage Trial Revealed About Kremlin Tactics in Wartime Europe.” War on the Rocks, April 8. https://warontherocks.com/2025/04/putins-spies-for-hire-what-the-u-k-s-biggest-espionage-trial-revealed-about-kremlin-tactics-in-wartime-europe/

Rid, Thomas, and Brian Matthews. 2021. *Active Measures: The Secret History of Disinformation and Political Warfare*. Paperback edition. London: Profile Books.

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

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

Sobel, Ariel Whitfield. 2022. “All the World’s a Stage: Covert Action as Theatrical Performance.” *Intelligence and National Security* 37 (4): 569–80.

SourceMaterial and Politico. 2024. “Dark Water: How Putin’s Shadow Fleet is Illegally Dumping Oil Across the Globe.” October 17. https://www.source-material.org/putin-shadow-fleet-illegal-dumping-oil-sea/

Szoldra, Paul. 2014. “Without Realizing It, Russian Soldiers are Proving Vladimir Putin is Lying About Eastern Ukraine.” *Business Insider*, July 31. https://www.businessinsider.in/without-realizing-it-russian-soldiers-are-proving-vladimir-putin-is-lying-about-eastern-ukraine/articleshow/39390298.cms

Tucker, David. 2014. *The End of Intelligence: Espionage and State Power in the Information Age*. Redwood City: Stanford University Press.

Walker, Shaun. 2015. “Putin Admits Russian Military Presence in Ukraine for First Time.” *The Guardian*, December 17. https://www.theguardian.com/world/2015/dec/17/vladimir-putin-admits-russian-military-presence-ukraine

Watling, Jack, Oleksandr V. Danylyuk, and Nick Reynolds. 2024. “The Threat From Russia’s Unconventional Warfare Beyond Ukraine, 2022-2024.” *RUSI* Special Report, February 20. https://www.rusi.org/explore-our-research/publications/special-resources/threat-russias-unconventional-warfare-beyond-ukraine-2022-24

Windward. 2024. “Updated Report: Illuminating Russia’s Shadow Fleet.” https://windward.ai/knowledge-base/illuminating-russias-shadow-fleet/