Congressional Research Service
Informing the legislative debate since 1914

Russian Hybrid Warfare Activities in Europe: Considerations for Congress

August 11, 2026

Congressional Research Service
https://crsreports.congress.gov
R49134

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

Russian Hybrid Warfare Activities in Europe: Considerations for Congress

Following Russia's invasion of Ukraine in 2022, U.S. and European officials have accused Russia of a sustained campaign of malign activities, often referred to as *hybrid warfare*, across Europe. These attacks, which have been increasing in number and severity, include sabotage, assassinations, political interference and influence, cyberattacks, and airspace violations, among others. Russia's foreign intelligence agencies have demonstrated flexibility in conducting these attacks and adapting to European responses (such as sanctions, expulsions of intelligence officers, increased military operations and heightened intelligence scrutiny), and they are conducting more aggressive operations, which carry a greater risk of exposure. Some European officials have asserted that Russia is using hybrid warfare tactics to undermine European support for Ukraine and destabilize or complicate a unified European response to Russian policies and actions.

Continued Russian hybrid warfare activities are raising questions in both the United States and Europe about the long-term threat Russia poses to U.S. and European strategic and national security interests. Congress has introduced legislation and held multiple hearings on Russian hybrid warfare activities in Europe and other related issues. Congress may examine whether and how Russian hybrid warfare activities are affecting European threat perceptions and national security interests, U.S. military or intelligence commitments, and the overall security environment in Europe. Congress may deliberate what support, if any, to provide Europe for its responses and assess current or proposed U.S. and European responses to Russian hybrid warfare activities, including determining whether military, law enforcement, or intelligence-led strategies—or a mix of approaches—are most effective at countering Russia's hybrid warfare activities.

SUMMARY

R49134

August 11, 2026

Andrew S. Bowen, Coordinator
Analyst in Russian and European Affairs

Sarah E. Garding
Analyst in European Affairs

Derek E. Mix
Specialist in European Affairs

Catherine A. Theohary
Specialist in National Security Policy, Cyber and Information Operations

Contents

Figures

Contacts

Introduction

Since the start of Russia's full-scale invasion of Ukraine in 2022, U.S., European, and NATO officials have highlighted the continued threat Russia poses to European security.[1] Observers and European officials have expressed concern regarding the rise of Russian hybrid warfare activities.[2] In November 2025, for example, Kaja Kallas, High Representative of the European Union (EU) for Foreign Affairs and Security Policy, stated that "Russia's hybrid actions in Europe are increasingly brazen. Russia is committing state sponsored terrorism."[3] In an October 2025 speech, European Commission President Ursula von der Leyen stated, "It is a coherent and escalating campaign to unsettle our citizens, test our resolve, divide our Union, and weaken our support for Ukraine. And it is time to call it by its name. This is hybrid warfare, and we have to take it very seriously."[4] According to congressional testimony in March 2026 by General Alexus G. Grynkewich, Commander of U.S. European Command and NATO Supreme Allied Commander Europe, "we [the United States] see a fairly robust amount of what we call Russian hybrid activities or asymmetric activities ... whether it's information operations or sabotage and those types of things. There have been several incidences in the Baltics and in Poland, in particular, over the last several months since I've been in command."[5] The Russian government routinely denies responsibility for suspected attacks.[6]

Hybrid warfare activities attributed to Russia by U.S. and European officials and observers have included acts of sabotage, assassinations, airspace violations, global positioning system (GPS) jamming, the severing or damaging of critical underwater infrastructure (CUI), cyberattacks, weaponized migration, and political and election interference.[7] In May 2026, Anne Keast-Butler, Director of the United Kingdom's (UK's) Government Communications Headquarters (GCHQ), stated that "Russia is scaling up its daily hybrid activity against the UK and Europe, stretching from the seabed to cyberspace—relentlessly targeting critical infrastructure, democratic processes, supply chains and public trust."[8] According to one study, the number of Russian hybrid

[1] Lara Seligman and Yoko Kubota, "U.S. Intel Finds Putin Could Test NATO's Resolve with Limited Incursion," *Wall Street Journal*, August 6, 2026.

[2] See, for example, Council of the European Union (EU), "Statement by the High Representative on Behalf of the EU Condemning Russia's Persistent Hybrid Campaigns Against the EU, Its Member States and Partners," press release, July 18, 2025; Lara Jakes, "Europe Wants to Get the Word Out: Russia Is to Blame for Sabotage," *New York Times*, December 3, 2025; *NL Times*, "Dutch Intelligence Agencies Warn of Escalating Russian Hybrid Attacks," February 19, 2026.

[3] European Union External Action Service, "Foreign Affairs Council: Press Conference by High Representative Kaja Kallas," November 20, 2025.

[4] European Commission, "Speech by President von der Leyen at the European Parliament Plenary Debate on a United Response to Recent Russian Violations of the EU Member States' Airspace and Critical Infrastructure," press release, October 7, 2025.

[5] U.S. Congress, Senate Armed Services Committee, *To Receive Testimony on the Posture of United States European Command and United States Transportation Command in Review of the Defense Authorization Request for Fiscal Year 2027 and the Future Defense Program*, 119th Cong., 2nd sess., March 12, 2026.

[6] Due to the difficulty of attribution, definitive official Russian culpability is often difficult or impossible to prove. Culpability has been attributed to Russian officials with varying degrees of confidence—some cases are clear and well documented, whereas other cases rest on more circumstantial evidence. In this report, *Russian hybrid warfare activities* are incidents that national, U.S., NATO, or EU officials and scholars or analysts studying hybrid warfare attribute to the Russian government—again, with varying levels of evidence.

[7] Seth G. Jones, *Russia's Shadow War Against the West*, Center for Strategic and International Studies (CSIS), March 2025; Sam Jones, "Russia's Hybrid Warfare Puts Europe to the Test," *Financial Times*, December 9, 2025.

[8] Government Communications Headquarters (GCHQ), "GCHQ Annual Lecture 2026—As Delivered," transcript, May (continued...)

attacks in Europe quadrupled from 2023 to 2024; another investigation compiled at least 151 incidents of reported Russian operations from February 2022 to March 2026 (see **Figure 1**).[9]

Some Members of Congress (see, for example, H.R. 7632 and S. 3249) and U.S. officials have expressed concern regarding the rise in suspected Russian hybrid warfare activities in Europe.[10] The 119th Congress may continue to assess the scale and scope of Russian hybrid warfare activities in Europe and their implications for U.S. security interests, evaluate possible legislative options to address such activities, and conduct oversight of the executive branch's policies on this issue.

Hybrid Warfare

In the United States, according to defense analyst Frank Hoffman, the first public use of the term *hybrid warfare* by a military official was at Forum 2005, where General James Mattis presented a concept of hybrid warfare as a merger of different forms of warfare, including conventional, irregular, terrorist, and criminal.[11] Subsequent publications by General Mattis and Hoffman, particularly in Hoffman's 2007 report *Conflict in the 21st Century: The Rise of Hybrid Wars*,[12] further explored the topic.

Although there is no set definition of what tactics and activities constitute hybrid warfare, observers broadly argue that hybrid warfare is a strategy seeking to subvert and undermine an adversary's capability and is below the threshold of armed conflict. Hybrid warfare can include tactics such as information operations, economic coercion, corruption, use of proxy forces, and malicious cyber operations intended to destabilize adversaries. Prepared at the behest of the Chairman of the Joint Chiefs of Staff, joint publications are the principles that guide the employment of U.S. military forces in integrated operations. Joint Publication 1 vol.1, *Joint Warfighting*, refers to these activities as irregular warfare, defined as "a form of warfare where states and non-state actors campaign to assure or coerce states or other groups through indirect, non-attributable, or asymmetric activities, either as the primary approach or in concert with conventional warfare."[13] Other doctrinal publications view hybrid warfare as akin to information

27, 2026. https://www.gchq.gov.uk/speech/gchq-annual-lecture-2026-as-delivered. GCHQ is the UK's intelligence, security, and cyber agency.

[9] Charlie Edwards and Nate Seidenstein, *The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure*, International Institute for Strategic Studies, August 2025; Emma Burrows, "Latvia's Security Service Says 2 People Set Fire to a Train and Rail Equipment for Russia," Associated Press, March 12, 2026.

[10] Congress has held several hearings on these and related issues. See, for example, U.S. Congress, House Foreign Affairs Committee, Europe Subcommittee, *Weaponized Mass Migration: A Security Risk to Europe and the United States*, 119th Cong., 2nd sess., February 10, 2026; U.S. Congress, Senate Foreign Relations Committee, *Sabotage in the Baltic Sea, Implications for European Security, and Lessons for the Indo-Pacific*, 119th Cong., 2nd sess., April 30, 2026.

[11] Forum 2005 was the first in an annual series of events now known as Defense Forum. Forum 2005 was jointly sponsored by the U.S. Naval Institute and the Marine Corps Association. See James Mattis and Frank Hoffman, *Future Warfare: The Rise of Hybrid Wars*, https://www.usni.org/magazines/proceedings/2005/october/forum-2005-katrina-teaches-hard-lessons; and Frank Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, The Potomac Institute for Policy Studies, 2007, https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

[12] Frank Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, The Potomac Institute for Policy Studies, 2007, https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

[13] Joint Chiefs of Staff, *Joint Publication 1 vol.1 Joint Warfighting,* August 27, 2023. For more information, see CRS Report R45142, *Information Warfare: Issues for Congress*, by Catherine A. Theohary.

warfare, with its focus on exploiting the information environment.[14] Still others view hybrid warfare as a form of political warfare.[15]

For allies in NATO and Europe, hybrid warfare refers to a range of economic, political, informational, and diplomatic activities combined with conventional military activities intended to destabilize and weaken an adversary.[16] According to NATO, hybrid threats

> combine military and non-military as well as covert and overt means, including disinformation, cyber attacks, economic pressure, deployment of irregular armed groups and use of regular forces. Hybrid methods are used to blur the lines between war and peace, and attempt to sow doubt in the minds of target populations. They aim to destabilize and undermine societies.[17]

Hybrid warfare tactics can be used alongside military force during war and may include military forms of coercion, although, as noted above, analysts generally consider hybrid activities to be below the threshold of armed conflict.[18] Broadly, hybrid activities display several attributes, including the following:

- **Flexibility**. Observers regard hybrid activities as flexible and readily adaptable to fit any situation or condition. Additionally, these tactics can be discarded or adapted depending on the target's responses.
- **Ambiguity of Attribution**. Generally, maintaining a level of deniability is a key component of hybrid warfare tactics. Often, the goal is not to maintain total deniability but to ensure a level of ambiguity that complicates the target's ability to definitively (or convincingly) prove attribution. This is referred to as *strategic ambiguity*.
- **Kinetic and Non-Kinetic Actions**. Hybrid warfare tactics can encompass non-kinetic actions (e.g., weaponized migration) and more kinetic tactics (e.g., the use of irregular or proxy forces, sabotage). As such, hybrid warfare tactics can range from relatively mundane (e.g., propaganda and/or disinformation) to more extreme and kinetic activities (e.g., assassination).
- **Less Escalatory**. Due to ambiguity of attribution and the varied and often covert nature of the tactics employed, hybrid warfare is considered less escalatory than some overt military actions, in that it intentionally exploits the escalation gap, blurring the lines between war and peace, and potentially limiting the target's ability to respond.

---

[14] For more information, see CRS Report R45142, *Information Warfare: Issues for Congress*, by Catherine A. Theohary.

[15] CRS In Focus IF11127, *What Is "Political Warfare"?*, by Catherine A. Theohary and Martin A. Weiss.

[16] The concept of hybrid warfare is debated among scholars and practitioners, including whether other terms such as *non-linear war*, *asymmetric*, or *grey zone conflicts* are more appropriate. For more, see Mark Galeotti, "Hybrid, Ambiguous, and Non-Linear? How New is Russia's 'New Way of War'?" *Small Wars and Insurgencies*, vol. 27, no. 2 (2016), pp. 282-301; Geraint Hughes, "War in the Grey Zone: Historical Reflections and Contemporary Implications," *Survival*, vol. 62, no. 3 (2020), pp. 131-158; Chiara Libiseller, "Hybrid Warfare' as an Academic Fashion," *Journal of Strategic Studies*, vol. 46, no. 4 (2023), pp. 858-880.

[17] NATO, "Countering Hybrid Threats," January 29, 2026.

[18] Rory Cormac and Richard J. Aldrich, "Grey is the New Black: Covert Action and Implausible Deniability," *International Affairs*, vol. 94, no. 3 (2018), pp. 477-494; Andrew Mumford and Pascal Carlucci, "Hybrid Warfare: The Continuation of Ambiguity by Other Means," *European Journal of International Security*, vol. 8, no. 1 (2023), pp. 192-206; Bojan Pancevski, "Europe Sees Signs of Russian Sabotage but Hesitates to Blame Kremlin," *Wall Street Journal*, May 20, 2024; Joshua Rovner et al., "Sand in the Gears: Sabotage in World Politics," *European Journal of International Security*, (2025), pp. 1-20.

Some observers argue that hybrid warfare tactics are not a new trend in warfare and have a long history.[19] Observers generally note that Russia has a much longer tradition and a different conceptual understanding of hybrid warfare than current U.S. and European understandings of the concept.[20] Russian observers accordingly discuss hybrid warfare strategies in a holistic fashion and, broadly speaking, appear to consider hybrid warfare a subset of coercion rather than a new and distinct form of conflict.[21]

When Russian observers and military theorists explicitly reference the term hybrid warfare (in Russian, *gibridnaya voyna*), they are generally identifying the Western application of hybrid tactics and the changing nature of conflict or war, including the increasing role of technology and the rise in importance of non-military means of coercion.[22] For example, Russian Foreign Minister Sergei Lavrov stated at the February 2025 G20 Foreign Ministers' meeting,

> To fight rivals, they [the West] use a broad range of "hybrid-war" methods, including illegal sanctions, protectionism, theft of sovereign assets, destruction of critical infrastructure, market and pricing machinations, abuse of reserve currencies, and more. They are attempting to justify their violations of international law, including interference in the internal affairs of states, by references to a "rules-based order."[23]

Russian Intelligence and Proxies

Russia has multiple foreign intelligence agencies tasked with conducting traditional espionage operations to collect political, economic, and scientific/technological intelligence.[24] These agencies also conduct Russia's hybrid warfare activities, in addition to their traditional espionage missions.[25] Russia's three main foreign intelligence agencies are the following:

- **Foreign Intelligence Service** (SVR). Russia's primary civilian foreign intelligence agency, the SVR conducts the full range of foreign intelligence activities. These include human intelligence operations, under both official diplomatic cover (out of Russian embassies and consulates) and nonofficial cover

[19] See, for example, *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, eds. Williamson Murray and Peter Mansoor (Cambridge University Press, 2012).

[20] Russian theorists also use the terms *active measures* and *new generation warfare*, among others, to describe many of the concepts of hybrid warfare. Mark Galeotti, *Russian Political War: Moving Beyond the Hybrid* (Routledge: New York, 2019); Ofer Fridman, *Russian "Hybrid Warfare": Resurgence and Politicization* (Oxford University Press, 2022).

[21] Oscar Jonsson, *The Russian Understanding of War: Blurring the Lines Between War and Peace* (Georgetown University Press, 2019), pp. 8-16; Bilyana Lily, *Russian Information Warfare: Assault on Democracies in the Cyber Wild West* (Annapolis, MD: Naval Institute Press, 2022), pp. 20-22; Dmitry Adamsky, *The Russian Way of Deterrence: Strategic Culture, Coercion, and War* (Palo Alto: Stanford University Press, 2023); Michael Petersen et al., *Russian Concepts of Future Warfare Based on Lessons from the Ukraine War*, Center for Naval Analyses (CNA), July 2025, pp. 6-12.

[22] Bettina Renz, "Russia and 'Hybrid Warfare,'" *Contemporary Politics*, vol. 22, no. 3 (2016), pp. 283-300; Katri Pynnoniemi and Minna Jokela, "Perceptions of Hybrid War in Russia: Means, Targets, and Objectives Identified in the Russian Debate," *Cambridge Review of International Affairs*, vol. 33, no. 6 (2020), pp. 828-845; Andrew Monaghan, *Blitzkrieg and the Russian Art of War* (Manchester University Press, 2025), pp. 226-227; Gudrun Persson, *Russian Military Thought* (Georgetown University Press, 2025), pp. 130-132.

[23] Ministry of Foreign Affairs of the Russian Federation, "Foreign Minister Sergey Lavrov's Remarks on the Global Geopolitical Situation at the G20 Foreign Ministers' Meeting, Johannesburg, February 20, 2025," transcript, February 20, 2025, https://mid.ru/en/foreign_policy/news/1998882/.

[24] For more information, see CRS In Focus IF12865, *Russia's Foreign Intelligence Services*, by Andrew S. Bowen.

[25] *Economist*, "Russian Spies Are Back—And More Dangerous Than Ever," February 20, 2024.

(operations without diplomatic immunity or apparent connections to Russia), as well as cyber and information operations.

- **Main Directorate of the General Staff of the Armed Forces of the Russian Federation** (GU; also known as the GRU or Main Intelligence Directorate). Russia's military intelligence agency, the GU is tasked with collecting all levels of military intelligence (including using official and nonofficial cover), commanding Russia's *spetsnaz* brigades, and managing proxy and mercenary units.[26] The GU also has extensive cyber operations and has been linked to numerous acts of sabotage, assassinations, and assassination attempts.
- **Federal Security Service** (FSB). Russia's largest and arguably most powerful security service, the FSB is focused primarily on internal security. The FSB has gradually gained more foreign intelligence capabilities, especially in countries that were formerly part of the Soviet Union. The FSB also has been linked to cyber operations, information warfare, and assassinations of the regime's perceived political opponents both domestically and abroad.

In addition to an increased number of attacks, the tactics and nature of Russian hybrid warfare operations have changed.[27] Since 2022, Russia's intelligence agencies reportedly have become more aggressive, conducting more public and kinetic attacks.[28] U.S., European, and NATO officials have identified the GU, in particular, as the most aggressive and brazen Russian intelligence agency.[29] According to the Special Inspector General for Operation Atlantic Resolve, "Russian intelligence and security services—particularly the General Staff Main Intelligence Directorate—almost certainly [have] continued to attempt arson and sabotage operations throughout Europe to degrade NATO cohesion and discourage support for Ukraine."[30]

The UK's domestic intelligence agency, MI5, has estimated that between 2022 and 2024, at least 750 Russian diplomats and suspected intelligence officers have been expelled across Europe, hampering Russian intelligence operations and capabilities.[31] Despite these expulsions, Russian intelligence agencies reportedly have demonstrated flexibility and adaptability in conducting operations by contracting with or outsourcing to proxies and for-hire agents.[32] This contract

[26] GU *spetsnaz* units are specialized light infantry units that conduct battlefield reconnaissance and sabotage missions.

[27] Bart Schuurman, "Russia Is Stepping Up Its Covert War Beyond Ukraine," *Foreign Policy*, January 10, 2025; Elena Grossfeld, *Quantity Has a Quality All of Its Own: The Transformation of Russian Intelligence Operations Since the Ukraine Invasion*, CNA, May 2025; Raphael Minder, "Poland Probes Record Number of Russian Espionage Cases," *Financial Times*, May 6, 2026.

[28] Kevin Riehle, "The Ukraine War and the Shift in Russian Intelligence Priorities," *Intelligence and National Security*, vol. 29, no. 3 (2024), pp. 458-474; Jack Watling et al., *The Threat from Russia's Unconventional Warfare Beyond Ukraine, 2022-2024*, Royal United Services Institute (RUSI), February 20, 2024; Sean M. Wiswesser, *Tradecraft, Tactics, and Dirty Tricks: Russian Intelligence and Putin's Secret War* (Naval Institute Press, 2026).

[29] For example, "the Main Directorate of the General Staff of the Russian Armed Forces (GRU), which are specially trained to carry out sabotage operations and assassinations, [will] highly likely continue to plan and coordinate operations of this nature." Lithuania Ministry of Defense and State Security Department of the Republic of Lithuania, *2026 National Threat Assessment*, p. 26. Also see, UK Foreign, Commonwealth and Development Office, "UK Sanctions Russian Spies at the Heart of Putin's Malicious Regime," press release, July 18, 2025; Joshua Yaffa, "To Build a Fire," *The New Yorker*, February 2, 2026.

[30] Special Inspector General-Operation Atlantic Resolve, *Operation Atlantic Resolve: Including U.S. Government Activities Related to Ukraine, January 1, 2026-March 31, 2026*, Report to Congress, p. 11.

[31] Security Service, MI5, "Director General Ken McCallum Gives Latest Threat Update," press release, October 8, 2024. Also see, Henry Foy and Andy Bounds, "EU to Curb Russian Diplomats' Travel as Suspected Spy Attacks Mount," *Financial Times*, October 7, 2025.

[32] Thomas Escritt and Sarah Marsh, "Russia Buying Spies to Make Up for Expelled Diplomats, German Agency Says," (continued...)

approach may help Russian intelligence agencies compensate for the loss of intelligence officers in Europe and could increase deniability, as such agents may have little direct connection to Russia and may be considered disposable by Russian intelligence services.[33] Contractors, however, may be less effective than intelligence officers, as for-hire agents and proxies may have little training or experience in conducting espionage.[34]

Proxies may range from individuals recruited for a single operation to organized crime networks used for assassinations or complex sabotage attempts.[35] According to European officials, some proxies may be unaware they are working for Russian intelligence or be used for specific operations and then discarded.[36] One recent study of 145 Russian "low-level agents" recruited for sabotage found that proxies were often part of networks (albeit compartmentalized) with tasks ranging from ferrying orders to conducting complex operations such as sabotage.[37] Additionally, the study found that these "low-level agents" were used for multiple operations and that the level of deniability and tradecraft varied, sometimes due to poor tradecraft by the agents or the Russian intelligence agencies themselves.[38]

Russian Hybrid Warfare Tactics and Activities in Europe

U.S. and European awareness of Russian hybrid warfare increased after Russia's initial invasion of Ukraine in 2014. During that operation, Russia used irregular forces and Russian soldiers, also known as "little green men," who did not wear insignia and denied any affiliation with Russia.[39] The Russian government's use of hybrid warfare has continued since its full-scale invasion of Ukraine in 2022, amid continuing Russian denials.[40] For example, in April 2026, the UK government detailed a covert Russian effort "to conduct hybrid warfare activities against the UK and its Allies" using specialized submarines to surveil CUI in and around the UK, possibly for

Reuters, June 18, 2024; Norwegian Police Security Service, *National Threat Assessment 2026*, February 6, 2026, pp. 13-14; Daniel Richterova, "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, 2025.

[33] Shaun Walker, "These People Are Disposable': How Russia Is Using Online Recruits for a Campaign of Sabotage in Europe," *Guardian*, May 4, 2025; Sky News, "Three People Arrested in London on Suspicion of Assisting Russian Spy Agencies," October 23, 2025.

[34] Max Colchester, "Inside Jan Marsalek's Chaotic Russian Spy Ring," *Wall Street Journal*, March 8, 2025.

[35] Mark Galeotti, *Gangster at War: Russia's Use of Organized Crime as an Instrument of Statecraft*, Global Initiative Against Organized Crime, November 2024; Kacper Rekawek et al., *Russia's Crime-Terror Nexus: Criminality as a Tool of Hybrid Warfare in Europe*, International Centre for Counter-Terrorism, September 2025; Marion Solletty, "$500 and a Trip Abroad: How Recruits End Up in Russian Sabotage Training Camps," *Politico*, March 25, 2026; Michael Holden and Sam Tobin, "Amateur Saboteurs: The Young Men Carrying Out Attacks for Gangs, Russia and Iran," Reuters, June 15, 2026.

[36] Daniela Richterova et al., "Russian Sabotage in the Gig-Economy Era," *RUSI Journal*, vol. 169, no. 5 (2024), pp. 10-21; Federal Office for the Protection of the Constitution, "Joint Information Campaign on 'Low-Level Agents' Launched," press release, September 2, 2025, https://www.verfassungsschutz.de/SharedDocs/kurzmeldungen/DE/2025/2025-09-02-informationskampagne.html; Finnish Security and Intelligence Service, "How to Recruit a Saboteur," *National Security Overview 2026,* https://supo.fi/en/how-to-recruit-a-saboteur.

[37] Bart Schuurman, "Russia's Low-Level Agents: Characteristics, Roles and Organisational Structure of Covert Operatives in Europe, 2022-2025," *European Security*, 2026, pp. 1-22.

[38] Schuurman, "Russia's Low-Level Agents," pp. 16-17.

[39] Carl Schreck, "From 'Not Us' to 'Why Hide It': How Russia Denied Its Crimea Invasion, Then Admitted It," RFE/RL, February 26, 2019.

[40] Edwards and Seidenstein, *Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure*; Reuters, "Kremlin Accuses Poland of 'Russophobia' After Warsaw Blames Railway Sabotage on Russia," November 18, 2025.

future sabotage.[41] Then-UK Defense Minister John Healey stated at a press conference, "And to President Putin, I say this: we see you, we see your activity over our cables and pipelines. And you should know that any attempt to damage them will not be tolerated, and will have serious consequences."[42] NATO has also stated that hybrid threats could trigger NATO's Article 5 mutual defense clause in the North Atlantic Treaty.[43]

The EU has expanded its awareness of and responses to hybrid warfare activities, including from Russia.[44] In February 2026, the European Parliament adopted a resolution on EU strategic defense and security partnerships that emphasized "the particular security concerns of EU Member States on its eastern flank, which face direct threats from Russian aggression and hybrid warfare."[45] As of July 2026, the EU had sanctioned 26 entities and more than 100 individuals for supporting Russia's destabilizing activities, including cyberattacks.[46]

Several analysts have posited that Russia has various motivations for conducting hybrid warfare activities in Europe, including testing target responses and imposing costs on or straining resources of target countries.[47] NATO, EU, and U.S. officials assert that Russia's increased use of hybrid warfare activities is at least partly in response to Western support for Ukraine and designed to undermine transatlantic unity.[48] Other observers surmise that Russia is adopting hybrid warfare tactics as a form of asymmetric conflict given its conventional military inferiority relative to the United States and NATO.[49] According to the U.S. Defense Intelligence Agency,

> Moscow uses indirect actions to compete with the West and overcome military overmatch by exploiting asymmetry to advance Russian interests without incurring the costs of full-scale warfare. Moscow also employs covert action, information operations, cyberactivities, airspace violations, and proxies to undermine Ukraine's war effort, compete against the

[41] UK Ministry of Defence, "Defence Secretary No9 Speech," transcript, April 9, 2026.

[42] Ibid.

[43] Article 5 states, "an armed attack against one or more of them … shall be considered an attack against them all." CRS Legal Sidebar LSB11256, *The North Atlantic Treaty: U.S. Legal Obligations and Congressional Authorities*, by Karen Sokol; NATO, "NATO Foreign Ministers Chart Way Forward in Addressing Russian Sabotage," press release, December 4, 2024; Richard Milne, "NATO Considers Being 'More Aggressive' Against Russia's Hybrid Warfare," *Financial Times*, December 1, 2025; NATO, *Countering Hybrid Threats*, January 29, 2026.

[44] European Parliamentary Research Service, "EU Response to Hybrid Threats," July 2026.

[45] European Parliament, *EU Strategic Defence and Security Partnerships*, P10_TA (2026)0040, February 11, 2026, https://www.europarl.europa.eu/doceo/document/TA-10-2026-0040_EN.html. The vote was adopted with 440 votes to 119, with 85 abstentions.

[46] Council of the EU, "Russian Cyber-Attacks and Destabilizing Activities: Council Sanctions Nine Individuals and Four Entities," press release, July 13, 2026; European Council/Council of the EU, "Russia's Hybrid Activities: EU Sanctions," July 13, 2026.

[47] These motivations are not mutually exclusive and can include elements of several, as well as changes over time depending on conditions. Economist, "Why Russia's Micro-Aggressions Against Europe Are Proliferating," October 2, 2025; Emma Burrows, "Russia Wants to Drain Europe's Investigative Resources with Its Sabotage Campaign, Officials Say," Associated Press, December 18, 2025; Mikhail Troitskiy, "Tacit Coercion and Its Dilemmas: Russia and the West," *Survival*, vol. 67, no. 1 (2026), pp. 77-90.

[48] NATO's 2024 *Washington Summit Declaration* stated, "Russia has also intensified its aggressive hybrid actions against Allies, including through proxies, in a campaign across the Euro-Atlantic area... Russia's behavior will not deter Allies' resolve and support to Ukraine. We will also continue to support our partners most exposed to Russian destabilization, as they strengthen their resilience in the face of hybrid challenges that are also present in our neighborhood." NATO, *Washington Summit Declaration*, July 10, 2024.

[49] Kristin Ven Bruusgaard, "Deterrence Asymmetry and Strategic Stability in Europe," *Journal of Strategic Studies*, vol. 47, no. 3 (2024), pp. 334-362.

West, and test NATO capabilities and resolve while remaining under the threshold of direct armed conflict.[50]

Additionally, there may be an element of competition and entrepreneurial experimentation by the Russian intelligence agencies conducting these activities, with the Russian political leadership setting broad goals and granting Russian intelligence agencies some freedom on how to achieve those goals or desired objectives. Anonymity may also encourage engagement in high-risk "gray zone" activities.

According to the Office of the Director of National Intelligence's *2026 Annual Threat Assessment*, "Russia's gray zone tools include cyber-attacks, disinformation and influence operations, energy market manipulation, military intimidation, and sabotage. Russia often hides and denies its role, complicating U.S. efforts to counter it."[51]

Alleged Russian hybrid warfare tactics throughout Europe have included the following:

- **Sabotage.** Russia has been accused of orchestrating multiple sabotage operations, including damaging or severing CUI in the Baltic Sea, planting a series of explosive packages on cargo aircraft, and committing arson.[52] In 2024, U.S. and European authorities accused the GU of planting at least four explosive packages on international air freight shipping networks.[53] European authorities also reportedly have arrested numerous individuals accused of using drones to spy on U.S. military installations and routes for supplying security assistance to Ukraine; some observers suspect Russia aims to use the intelligence for sabotage.[54] In August 2026, a drone collided with an aircraft and another drone carrying explosives was discovered at Leipzig/Halle Airport in Germany, a major center for Ukrainian and NATO logistics.[55] There have been particular concerns that Russia has been involved in both cutting undersea telecommunication and energy cables in the Baltic Sea and mapping locations of other CUI for possible

[50] Statement by Lieutenant General James Adams, Defense Intelligence Agency, U.S. Congress, House Armed Services Committee, Intelligence and Special Operations Subcommittee, *Defense Intelligence Enterprise – Challenges, Priorities, and Resourcing for Fiscal Year 2027*, 119th Cong., 2nd sess., April 16, 2026.

[51] Office of the Director of National Intelligence, *2026 Annual Threat Assessment*, March 2026, p. 27.

[52] Lara Jakes, "Drones, Exploding Parcels and Sabotage: How Hybrid Tactics Target the West," *New York Times*, January 4, 2025; John Leicester and Emma Burrows, "11 Baltic Cables Damaged in 15 Months, Pushing NATO to Boost Security," Associated Press, January 28, 2025; Bertrand Benoit, "Germany Foils Alleged Russian Plot to Mail Incendiary Devices," *Wall Street Journal*, May 14, 2025; Emma Burrows, "UK Court Convicts Three Men over Arson Attack Authorities Say Was Organized by Russian Intelligence," Associated Press, July 8, 2025; Michael Schwirtz and Tomas Dapkus, "Lithuania Says It Broke Up Russian Sabotage and Murder Plots," *New York Times*, May 1, 2026.

[53] Michael Weiss and Kato Kopaleishvili, "Revealed: How Russia's GRU Plotted Europe's Parcel Explosions," *VSquare*, September 17, 2025; Lithuania Prosecutor General, "A Group of Individuals Who Organized and Planned to Commit Four Terrorist Acts with Hybrid Goals Has Been Identified and Detained," press release, September 17, 2025, https://prokuraturos.lt/lt/isaiskinta-ir-sulaikyta-asmenu-grupe-organizavusi-ir-planavusi-ivykdyti-keturis-teroro-aktus-turincius-hibridiniu-tikslu-with-english-translation/11619; Jessica Rawnsley, "Russia Was Behind Parcel Fires in UK and Europe, Investigators Say," BBC, March 6, 2026.

[54] Kate Connolly, "Three Men on Trial in Germany Accused of Russian Sabotage Plot," *Guardian*, May 20, 2025; Julian E. Barnes and Eric Schmitt, "Russian Drones Are Flying over U.S. Weapons Routes in Germany, Officials Say," *New York Times*, August 28, 2025; Emma Burrows, "Latvia's Security Service Says Two People Set Fire to a Train and Rail Equipment for Russia," Associated Press, March 12, 2026.

[55] Some observers suspect Russian culpability. Daniel Michaels, "Explosive Drone at German Airport Marks New Threat for Europe," *Wall Street Journal*, August 6, 2026; Sam Jones, "Explosive Drone at Germany Airport Raises 'Hybrid Threat," *Financial Times*, August 7, 2026.

sabotage operations.[56] In January 2025, NATO launched a new mission, Baltic Sentry, to increase its presence in the Baltic Sea and enhance the alliance's ability to protect CUI.[57]

- **Assassinations.** Since 2014, Russia has been linked to various assassinations and assassination attempts overseas.[58] Russia has been accused of the poisoning of former Russian military intelligence officer Sergei Skripal and his daughter in the UK in 2018, the murders of former Chechen rebel commander Zelimkhan Khangoshvili in Germany in 2019 and Russian defector Maksim Kuzminov in Spain in February 2024, and planned assassinations of Armin Papperger, the CEO of German defense firm Rheinmetall and of Russian human rights activist Vladimir Osechkin in France.[59]
- **Cyberattacks.** In addition to cyber espionage, which exploits cyberspace in order to gain access to sensitive data, Russia allegedly has carried out cyberattacks and other malicious cyber operations against critical infrastructure, governments, and essential services (including an April 2025 cyberattack on a Norwegian dam resulting in the opening of floodgates and a December 2025 cyberattack against 30 energy facilities in Poland).[60] Russian cyber actors also reportedly have sought to penetrate infrastructure and government networks, possibly in preparation for sabotage and targeted attacks on logistics networks used for transporting foreign assistance to Ukraine.[61]
- **Airspace Violations.** In 2025 and 2026, Russia reportedly engaged in airspace violations of NATO countries, including with drones and fighter aircraft.[62] Drone sightings have been reported across Europe, including near airports, resulting in multiple airport shutdowns and flight disruptions; some European officials

[56] Max Colchester and Bojan Pancevski, "The Deep-Sea Battle over the World's Data Cables Is Heating Up," *Wall Street Journal*, January 23, 2025; Victoria Jack et al., "Europe's New War with Russia: Deep Sea Sabotage," *Politico*, April 7, 2025; Romina Bandura and Thomas Bryja, *The Strategic Future of Subsea Cables: Irish Case Study*, CSIS, July 23, 2025; Caspar Hobhouse, "On a War Footing: Securing Critical Energy Infrastructure," *European Union Institute for Security Studies*, August 25, 2025; Helen Warrell et al., "The Russian Spy Ship Stalking Europe's Subsea Cables," *Financial Times*, September 26, 2025.

[57] NATO, "NATO Launches 'Baltic Sentry' to Increase Critical Infrastructure Security," January 14, 2025; *Economist*, "A Rash of Baltic Cable-Cutting Raises Fears of Sabotage," January 6, 2026.

[58] Emma Burrows and John Leicester, "Russia Is Ramping Up Its Attempts to Kill Opponents in Europe, Intelligence Officials Say," Associated Press, May 7, 2026.

[59] Christopher F. Schuetze, "Russian Is Convicted in Murder of Chechen Man in Berlin Park," *New York Times*, December 18, 2021; Drew Hinshaw et al., "Russians Keep Turning Up Dead All over the World," *Wall Street Journal*, March 3, 2024; Noemie Bisserbe and Matthew Luxmoore, "The Attempted Assassination of a Russian Dissident Is Foiled in France," *Wall Street Journal*, October 17, 2025.

[60] Council of the EU, "Cyber-Attacks: Three Individuals Added to EU Sanctions List for Malicious Cyber Activities Against Estonia," press release, January 27, 2025; Miranda Bryant, "Russian Hackers Seized Control of Norwegian Dam, Spy Chief Says," *Guardian*, August 14, 2025; Raphael Minder, "Russian Hackers Target Polish Hospitals and City Water Supply," *Financial Times*, September 16, 2025; A. J. Vicens, "Polish Officials Blame Russian Domestic Spy Agency for December 29 Cyberattacks," Reuters, January 30, 2026.

[61] Vicky Wonf and Frances Mao, "Russia Accused of EU and NATO Cyber-Attacks," BBC, September 9, 2024; State Security Department of the Republic of Lithuania, *2025 National Threat Assessment*, February 14, 2025; Netherlands Military Intelligence and Security Service, *2024 Public Annual Report*, April 22, 2025.

[62] Ben Makuch, "Swedish Jets Intercept Russian Aircraft in Two Separate Incidents," *Politico*, June 13, 2026; Emma Burrows, "Russia Waged a Drone Campaign in Europe, Likely Using Shadow Ships, Report Says," Associated Press, July 2, 2026.

suspect Russia of orchestrating these incidents.[63] In September 2025, NATO launched Eastern Sentry, a "flexible, multi-domain activity that is enhancing NATO's vigilance along the entire eastern flank."[64]

- **GPS Jamming.** Russia has been accused of conducting GPS jamming in key air and maritime spaces.[65] Since 2022, officials of NATO states neighboring Russia have accused Russia of interfering with aircraft navigation in the Baltic Sea region by jamming GPS signals.[66]
- **Election/Political Interference and Influence Operations.** Russia has been suspected of conducting numerous election and political interference operations. European officials have accused Russia of engaging in information manipulation to influence campaigns; corrupting European politicians; and conducting illicit campaign financing in multiple European countries, including France, Germany, Poland, Montenegro, Bulgaria, and Moldova.[67]
- **Weaponized Migration.** A 2024 EU policy document described weaponized migration as a hybrid warfare tactic "whereby Russia and Belarus artificially and illegally facilitate illegal migration flows towards the EU's external borders ... with the objective of destabilising our societies and undermining the unity of the European Union."[68] Since 2021, tens of thousands of migrants, primarily individuals from or transiting Middle Eastern countries, have traveled to Russia and Belarus and have subsequently attempted to enter the EU illegally through Poland, Lithuania, Latvia, and Finland.[69]

[63] Richard Milne and Henry Foy, "Russia's Hybrid War Is 'Only the Beginning,' Warns Danish PM," *Financial Times*, October 1, 2025; Reuters, "Russia's Suspected 'Hybrid War' Puts European Air Defenses to the Test," November 5, 2025.

[64] NATO Supreme Headquarters Allied Powers Europe (SHAPE), "Eastern Sentry," https://shape.nato.int/operations/operations-and-missions/eastern-sentry; Mitchell McCluskey and Lauren Kent, "NATO Launches 'Eastern Sentry' Operation in Response to Russian Drone Incursions," CNN, September 12, 2025.

[65] Riley Mellen and Eric Schmitt, "Russian Satellites Have Been Jamming GPS Signals Across Europe, Scientists Say," *New York Times*, June 5, 2026.

[66] Konstantin Eggert, "GPS Jamming in the Baltic Region: Is Russia Responsible?" *Deutsche Welle*, May 5, 2024; Andrius Sytas, "Russia Can Falsify GPS Signals Deep into Europe, Lithuania Says," Reuters, May 26, 2026.

[67] European Parliament, "MEPs Call for a Firm Response to Counter Russian Interference," press release, April 25, 2024; John Irish, "European Election: How the EU Says Russia Is Spreading Disinformation," Reuters, June 3, 2024; Oana Popescu-Zamfir, "Russian Interference: Coming Soon to an Election Near You," Carnegie Endowment, February 13, 2025; Jeanna Smialek, "Russian Meddling Fails to Swing a Pivotal Election in Europe," *New York Times*, September 28, 2025; Catherine Belton, "To Tilt Hungarian Election, Russians Proposed Staging Assassination Attempt," *Washington Post*, March 21, 2026.

[68] European Commission, "Communication from the Commission to the European Parliament and the Council on Countering Hybrid Threats from the Weaponisation of Migration and Strengthening Security at the EU's External Borders," December 11, 2024.

[69] European Commission, "Communication from the Commission to the European Parliament and the Council on Countering Hybrid Threats from the Weaponisation of Migration and Strengthening Security at the EU's External Borders."

Figure 1. Selected Suspected Russian Hybrid Warfare Attacks in Europe, 2018-2025

Sources: Graphic by CRS. Data from Charlie Edwards and Nate Seidenstein, *The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure*, International Institute for Strategic Studies, August 2025; Armed Conflict Location and Event Data Project, http://www.acleddata.com; U.S. Congress, Joint Commission on Security and Cooperation in Europe (U.S. Helsinki Commission), *Shadow War: Inside Russia's Attacks on NATO Territory*, 118th Cong., 2nd sess., December 12, 2024; Bart Schuurman, "Russian Operations Against Europe Dataset," Harvard Dataverse (2024), https://doi.org/doi:10.7910/DVN/TQ0FMQ.

Selected European Case Studies

As discussed above and depicted in **Figure 1**, European officials and policy analysts have determined that Russia has engaged in hybrid warfare activity targeting countries across Europe. This section provides case studies of documented or alleged Russian hybrid warfare activity in Poland, the three Baltic states (Lithuania, Latvia, and Estonia), Romania, and Bulgaria. All six of these countries are located on NATO's eastern flank along the Baltic Sea or the Black Sea, two regions that both NATO and Russia regard as strategically important. The six countries have provided military and other support to Ukraine and have prioritized efforts to deter potential Russian aggression against NATO territory. The countries' geographic proximity to Russia or Russia's ally Belarus makes them comparatively more exposed to certain cross-border tactics (e.g., weaponized migration and air space violations) and to direct and indirect impacts of Russia's war against Ukraine.

Poland

Analysts have observed that Russia frequently targets Poland with a range of hybrid warfare tactics, including the following:

- **Cyberattacks and Influence Campaigns.** Polish officials reportedly accused Russia of attempting to interfere in Poland's 2025 presidential election by spreading disinformation on the internet and conducting cyberattacks against critical infrastructure.[70] Press reports indicated that in a May 2025 speech prior to the election, Polish Deputy Prime Minister and Digital Affairs Minister Krzysztof Gawkowski stated, "We are currently witnessing unprecedented Russian interference in the electoral process."[71] Gawkowski also reportedly asserted that the GU had doubled information and cyber activities targeting Poland compared with the previous year.[72]
- **Espionage and Sabotage.** In April 2025, Poland's Internal Security Agency reported that since Russia's 2022 invasion of Ukraine, the agency had detained 44 people in relation to spying or sabotage on behalf of Russia or Belarus.[73] Those apprehended included Russians, Belarussians, Ukrainians, and Poles accused or convicted of engaging in a range of hybrid warfare activity, including an arson attack against a Warsaw shopping center, surveillance of sensitive military locations, and plans to attack railways carrying supplies for Ukraine.[74] On November 16, 2025, two separate attacks damaged Polish rail lines in what Polish Prime Minister Donald Tusk called "an unprecedented act of sabotage."[75] Polish authorities suspect two Ukrainian citizens working for the FSB of carrying out the attacks; the suspects reportedly fled into Belarus after the incidents.[76]
- **Weaponized Migration.** As noted above, some analysts and European officials assert that Russia and its ally Belarus have sought to use migration to destabilize the EU, including Poland. Many of the migrants arriving at the EU's eastern border reportedly originate in Middle Eastern countries, hold Russian visas, and are assisted by Belarusian security services.[77] Polish Prime Minister Tusk has described these migration flows as "state-led operations involving the regimes in Minsk and Moscow."[78]

[70] See, for example, Mariusz Marszałkowski, "Defence24 Days 2025: The Largest Defence and Security Conference in CEE Has Started," Defence24, May 6, 2025.

[71] As quoted in Mariusz Marszałkowski.

[72] *PolskieRadio*, "Poland Faces 'Unprecedented' Russian Election Interference: Deputy PM," May 6, 2025.

[73] *Polska Agencja Prasowa*, "Poland Detains Ukrainian Suspected of Spying for Russia," April 1, 2025.

[74] *TVP World*, "Poland to Close Russian Consulate After Evidence Kremlin Ordered 2024 Arson Attack," May 12, 2025; Anjou Kang-Stryker and Janusz Bugajski, *Poland on the Frontlines Against Russia's Shadow War*, Jamestown Foundation, *Eurasia Daily Monitor*, May 8, 2025.

[75] Aaron Weiner, "Rail Explosion in Poland Was 'Sabotage,' Prime Minister Says," *Washington Post*, November 17, 2025.

[76] Meduza, "Poland Links Railways Sabotage to Two Ukrainians Working for Russia's FSB," November 18, 2025.

[77] Henry-Laur Allik, "Poland, Baltics Step up Border Controls amid Migrant Crisis," *Deutsche Welle*, June 16, 2024.

[78] Chancellery of the Prime Minister, Republic of Poland, "Poland Effectively Protects the EU Border," March 22, 2025.

- **Airspace Violations.** In September 2025, Polish and other NATO aircraft shot down several Russian drones that entered Poland's airspace.[79] Poland continues to intercept Russian planes that violate its airspace.[80]

Baltic States

Analysts have observed that Russia has become more aggressive in employing hybrid threats against the Baltic states (Estonia, Latvia, and Lithuania) since 2022, employing tactics such as the following:[81]

- **Information Operations.** Russian influence efforts against the Baltic states typically attempt to polarize society by portraying the Baltic states as illegitimate and dysfunctional, NATO and the United States as imperial powers, and Baltic governments as Russophobe fascist regimes that fuel the war in Ukraine while oppressing their ethnic Russian populations.[82]
- **Cyberattacks.** The Baltic states regularly experience distributed denial-of-service (DDoS) attacks and other disruptive cyberattacks that EU and Baltic state authorities attribute to pro-Russia hacker groups. [83] Such cyberattacks often target critical infrastructure and the websites of public services, media, and the financial and transportation sectors.
- **Vandalism and Acts of Violence.** Baltic state authorities have suspected Russian security services' involvement in numerous instances of vandalism against monuments, memorials, and national or pro-Ukraine symbols. In March 2024, the chief of staff of the late Russian opposition leader Alexei Navalny was attacked with a hammer outside of his home in Lithuania's capital city, Vilnius, an incident that Lithuanian intelligence reportedly characterized as probably "Russian-organized and implemented."[84]
- **Sabotage and Arson.** European officials reportedly suspected Russian security services of planting incendiary devices aboard commercial cargo aircraft in July 2024 after packages originating in Lithuania ignited at handling facilities in Germany and the UK.[85] Lithuanian officials also suspected Russia's involvement in a large fire at a warehouse in Vilnius in May 2024.[86] Since 2023, there have been several incidents in which vessels linked to Russia allegedly have damaged

[79] NATO, "Statement by NATO Secretary General Mark Rutte on the Violation of Polish Airspace by Russian Drones," September 10, 2025; Michael Schwirtz, "A Polish Soldier, an Unusual Radar Dot and Then NATO Jets," *New York Times*, September 20, 2025; Robert Hamilton, "NATO's Air Defense Dilemma," *War on the Rocks*, September 25, 2025; Thomas Grove and Daniel Michaels, "Suspected Russian Drone Incursions Expose Gaps in NATO Defenses," *Wall Street Journal*, September 26, 2025.

[80] Reuters, "Poland Says It Intercepts Russian Aircraft over Baltic Sea," May 13, 2026.

[81] Henrik Praks, *Russia's Hybrid Threat Tactics Against the Baltic Sea Region: From Disinformation to Sabotage*, The European Centre of Excellence for Countering Hybrid Threats, May 2024.

[82] Indrė Makaraitytė and Mindaugas Aušra, "Moscow's Propaganda in Baltics Achieves Limited Success—LRT Investigation," *Lithuanian National Radio and Television*, August 5, 2024.

[83] See, for example, Republic of Estonia Information System Authority, *Cyber Security in Estonia 2026*, February 11, 2026.

[84] Sarah Rainsford, "Leonid Volkov: Navalny Ally Blames Putin Henchmen for Attack in Lithuania," BBC, March 13, 2024.

[85] RFE/RL, "Parcels That Exploded in Europe Reportedly Part of Russian Plot," November 5, 2024.

[86] Jurga Bakaitė and Evelina Knutovič, "Who Is Behind 'Sabotages and Diversions' in Lithuania and Poland?," *Lithuanian National Radio and Television*, May 23, 2024.

underwater infrastructure in the Baltic Sea by dragging their anchors across the seabed (see text box below).

- **Airspace Violations**. In September 2025, NATO F-35 fighter aircraft intercepted Russian MiG-31 fighters violating the airspace of Estonia.[87]

Sabotage of Critical Undersea Infrastructure

In 2023 and 2024, U.S. and NATO authorities reportedly alerted allies of increased Russian military activity near undersea cables, warning that Russia was "actively mapping" undersea infrastructure. In April 2026, then-UK Defense Secretary John Healey held a press conference where he announced that the UK, along with Norway and other allies, identified a Russian submarine operation over the last several weeks conducting "hybrid warfare activities against the UK and its Allies, specifically around Critical Undersea Infrastructure." Secretary Healey said that the specialist submarines belonged to Russia's Main Directorate of Deep Sea Research (GUGI). GUGI is a specialist branch of the Russian military (directly under the command of the Russian Ministry of Defense and separate from the Russian Navy) operating numerous specialized submarine, undersea, and surface vessels. GUGI's primary missions are reconnaissance and maritime intelligence collection, including surveillance of foreign naval assets and management of underwater surveillance systems. GUGI also may have the capabilities to conduct undersea sabotage, including severing or disabling undersea infrastructure.

In several incidents, vessels have allegedly damaged undersea infrastructure in the Baltic Sea by dragging their anchors across the seabed. News reports indicated at least six instances of suspected sabotage or disruption to undersea cables in the Baltic Sea in December 2025 and January 2026. For example, in December 2025, Finnish authorities detained a cargo vessel flying the flag of St. Vincent and the Grenadines that was suspected of damaging an undersea telecommunications cable connecting Finland and Estonia; the vessel had sailed from St. Petersburg, Russia. In December 2024, Finnish authorities seized a Cook Islands-registered oil tanker, which had departed the nearby Russian port of Ust-Luga, on suspicion of damaging several data cables and an undersea power cable linking Finland and Estonia. Finnish authorities brought criminal charges against several of the ship's officers.

Investigators have linked at least two incidents of suspected sabotage to vessels registered in the People's Republic of China (PRC, or China), which were possibly linked to Russia. In November 2024, regional governments reported that undersea communications cables connecting Lithuania to Sweden, and Germany to Finland, respectively, had been physically cut within hours of each other. As authorities investigated the incident, German Defense Minister Boris Pistorius stated, "No one believes that these cables were cut accidentally." Investigations subsequently centered on a PRC-flagged cargo ship sailing from a Russian port. Some observers suspect that Russian intelligence services, rather than the PRC government, were behind the incident.

In October 2023, the Balticconnector pipeline that links the gas infrastructure of Estonia and Finland suffered unexplained damage, with the pipeline shutting down due to a major leak. China's government later admitted that a Hong Kong-flagged cargo ship caused the damage with its anchor, claiming that the incident was an accident due to a storm. Regional officials have expressed skepticism that the damage was caused accidentally.

Sources: Charlie Cooper, "NATO Warns Russia Could Target Undersea Pipelines and Cables," *Politico*, May 3, 2023; Sidharth Kaushal, "Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure," Royal United Services Institute (RUSI), May 25, 2023; Li Beiping, "China's 'Accidental' Damage to Baltic Pipeline Viewed with Suspicion," *Voice of America*, August 17, 2024; Aleksander Cwalina, *Concerns Grow over Possible Russian Sabotage of Undersea Cables*, Atlantic Council, September 12, 2024; Oliver Moody, "Fears That Russia Was Behind Baltic Telecoms Cable 'Sabotage'," *The Times (London)*, November 19, 2024; Sophia Besch and Erik Brown, *A Chinese-Flagged Ship Cut Baltic Sea Internet Cables. This Time, Europe Was More Prepared*, Carnegie Endowment for International Peace, December 3, 2024; Sophia Besch and Erik Brown, *Securing Europe's Subsea Data Cables*, Carnegie Endowment for International Peace, December 16, 2024; Ellen Francis, "Finland Seizes Ship in Probe of Undersea Cable Damage," *Washington Post*, December 26, 2024; Amelia Nierenberg, "Finland Charges Ship's Crew Members in Slashing of Undersea Cables," *New York Times*, August 11, 2025; Economist, "A Rash of Baltic Cable-Cutting Raises Fears of Sabotage," January 6, 2026; Gavin Blackburn, "Cargo Vessel Suspected of Damaging Undersea Cable Allowed to Leave Finland," *Euronews*, January 12, 2026; UK Ministry of Defence, "Defence Secretary No. 9 Speech," transcript, April 9, 2026; UK Ministry of Defence, "UK Exposes Covert Russian Submarine Operation in and Around UK Waters," press release, April 9, 2026; Oleksandr Danylyuk, "Seabed War: Russia's Secretive Defence Units and Undersea Sabotage Architecture," RUSI, May 18, 2026.

[87] Steven Erlanger, "Russian Fighter Jets Enter Airspace of Estonia, a NATO Member," *New York Times*, September 19, 2025; NATO, "Statement by the North Atlantic Council on Recent Airspace Violations by Russia," September 23, 2025.

Romania and Bulgaria

Romania and Bulgaria, two NATO and EU member states located along the Black Sea, reportedly have faced increased Russian hybrid threats since 2022. Exposure to such tactics may have implications for both countries' internal stability, critical infrastructure, and security, as well as for the development of offshore energy resources and other strategic commercial opportunities.[88] Examples of alleged Russian hybrid threats include the following:

- **GPS Jamming.** Romanian and Bulgarian authorities have observed growing instances of GPS jamming in the Black Sea. In 2023, the press quoted Romania's then-Chief of the Defense Staff of having said that Russia was "actively and constantly" jamming GPS communications in Romania's Black Sea territorial waters.[89] Bulgarian defense officials reportedly attributed increased jamming to "radio-electric warfare systems" but reportedly declined to name the responsible party.[90]
- **Airspace Violations.** Romania, which borders Ukraine, has experienced numerous violations of its airspace by drones since 2022. According to the Romanian Ministry of Defense, Russia has carried out more than 100 attacks against Ukrainian targets near the Ukraine-Romania border since 2022.[91] In the context of these attacks, there have been 29 unauthorized incursions of Russian drones into Romania's airspace, and numerous cases of drone debris on Romanian territory.[92] In May 2026, a Russian GERAN-2 drone crashed into a residential building in Galaţi, Romania, resulting in two injuries. A Romanian nongovernmental organization asserted that coordinated social media posts in the aftermath of the crash seemingly sought to stoke fear among the public and sow doubts about official information regarding the incident.[93] In separate incidents over the course of three days in July 2026, Romanian F-16 fighter jets shot down drones that had entered Romanian airspace, at least one of which was assessed to

[88] Sofia Globe, "Security, Intelligence Agencies: Russia, Western Balkans Instability Main Threats to Bulgaria's National Security," April 28, 2025; Irina Marica, "Parliament Approves Romania's New 2025-2030 National Defense Strategy," *Romania Insider*, November 27, 2025; Matthew Boyse, prepared statement for U.S. Congress, Senate Foreign Relations Committee, Europe and Regional Security Cooperation Subcommittee, *The Future of U.S. Black Sea Strategy*, 119th Cong., 1st sess., September 30, 2025; George Scutaru, "Black Sea's Offshore Energy Potential and Its Strategic Role at a Regional and Continental Level," New Strategy Center, 2024; Bulgarian Ministry of Defence, *National Defence Strategy*, 2025.

[89] Romania Journal, "Head of the Romanian Army: Russia Is Jamming the GPS of Ships in Romanian Territorial Waters," September 29, 2023.

[90] Georgi A. Angelov, "Suspected Russian GPS Jamming Risks Fresh Dangers in Black Sea Region," RFE/RL, October 26, 2023.

[91] Ministry of National Defence, press release number 129, June 30, 2026. Also see United Nations, "Speakers Raise Alarm over Ukraine's War Spillover Effect as Security Council Discusses Reported Russian Federation Drone Crash in Romania," June 1, 2026.

[92] Ministry of National Defence, press release number 129, June 30, 2026.

[93] As described in Tamara Kaňuchová and Matei Vrabie, "Drone Incursions in Romania Were Followed by a Coordinated Online Storm," Vsquare, June 11, 2026. Original report (in Romanian) at https://funky.ong/wp-content/uploads/2026/06/Sapte-zile-doua-drone_-cum-a-fost-tinut-activ-subiectul-dronelor-in-online.pdf. A week after the drone crash in Galaţi, a few Ukrainian maritime drones that reportedly had veered off course exploded near Romania's Constanţa port. Ukrainian officials acknowledged the incident, attributing it to "enemy electronic interference." Nathan Reynolds, "Ukraine Says Sea Drone That Exploded in Constanta Veered Off Course Due to Electronic Interference," *EuroNews*, June 5, 2026.

be of Russian origin.[94] Romanian authorities summoned the Russian ambassador and expelled a Russian diplomat.[95]

- **Cyberattacks.** Romania and Bulgaria have experienced DDoS attacks and other disruptive cyberattacks that authorities and other experts attribute to pro-Russia hacker groups.[96] These cyberattacks reportedly have targeted election-related systems, other government systems, and critical infrastructure.
- **Sabotage.** In 2025, Romanian intelligence authorities reported that they had foiled a sabotage operation targeting critical infrastructure, and linked the suspect to "an extensive network of saboteurs targeting European countries, controlled through intermediaries by the Russian secret services."[97] In an ongoing criminal case, two Ukrainian nationals (suspected of being recruited and directed by Russian intelligence) face charges of attempting to sabotage the physical premises of Ukrainian courier company Nova Post in Bucharest; prosecutors reportedly have linked the case to a wider plot including sites in Poland.[98] Bulgaria's defense industry reportedly may have been the target of Russia-linked sabotage operations.[99]
- **Political Interference and Disinformation.** A 2024 study concluded that Romania is "a prime target for Russian political warfare campaigns," with Russia aiming to "create a climate of uncertainty and anxiety" in Romanian society, "fracture the cohesion of Romanian society," "erode trust in the NATO alliance and EU institutions," and weaken popular support for Ukraine.[100] Romanian authorities and other observers have accused Russia of seeking to interfere in Romanian elections through a combination of disinformation, social media manipulation, and cyberattacks.[101] Ahead of Bulgaria's April 2026 parliamentary election, a report warned that Bulgaria is one of the EU's "most permissive

[94] As of July 27, 2026, the search for debris from the other incidents was ongoing. Ministry of National Defence, press release number 150, July 27, 2026. Also see NATO, "NATO Fighter Jets Scramble, Shot Down Drone After It Enters Romanian Airspace," July 24, 2026; Minister of Foreign Affairs Oana Ţoiu (@oana_toiu), post on X, July 27, 2026.

[95] Ministry of National Defence, Ministry of Foreign Affairs (@MAERomania), post on X, July 27, 2026, https://x.com/MAERomania/status/2081718961578684848.

[96] *Romania Insider*, "Romanian President: NATO, EU, and UK Confirm Russian Cyber Attacks and Election Interference," July 22, 2025; Reuters, "Romanian State Institutions Face 10,000 Cyberattacks Daily, Defence Minister Says," March 31, 2026; RFE/RL, "Bulgarian Government Hit by Cyberattack Blamed on Russian Hacking Group," October 15, 2022; Sofia Globe, "Security, Intelligence Agencies: Russia, Western Balkans Instability Main Threats to Bulgaria's National Security," April 28, 2025.

[97] Serviciul Roman de Informatii, "SRI Foiled a Sabotage Operation Conducted by the Russian Federation on Romania's Territory," January 17, 2025.

[98] Marian Chiriac, "Romania Indicts Two Over Alleged Russian-Linked Sabotage Plot," *Balkan Insight*, April 6, 2026; Pawel Florkiewicz, "Poland, Romania Foil Russian Exploding Parcels Plot, Warsaw Says," Reuters, October 21, 2025.

[99] Bellingcat, "How GRU Sabotage and Assassination Operations in Czechia and Bulgaria Sought to Undermine Ukraine," April 26, 2021; Krassen Nikolov, "Risk of Russian Sabotage in Bulgaria, Warns Leading Investigative Journalist," *Euractiv*, January 18, 2023; Marton Dunai, "Russian Hitmen and Saboteurs Target Bulgaria's Arms Industry, Magnate Says," *Financial Times*, November 19, 2023; Nicolas Camut, "Bulgaria's Economy Minister Hints Russians Attacked Ammo Factory," *Politico*, June 26, 2023.

[100] Daniel Ioniţa et al., "Norway and Romania: Navigating Information Warfare," New Strategy Center and Norwegian Institute of International Affairs, April 2024. Also see Natalie Sabanadze and Galip Dalay, "Understanding Russia's Black Sea Strategy: How to Strengthen Europe and NATO's Approach to the Region," Chatham House, July 2025.

[101] RFE/RL, "Romanian Elections Targeted By 'Aggressive Hybrid Russian Action,' Declassified Documents Show," December 4, 2024; Tim Ross and Andrei Popoviciu, "Russian Interference Claims Hit Romania's Critical Election on Voting Day," *Politico*, May 18, 2025; EU External Action Service, *4th EEAS Report on Foreign Information Manipulation and Interference Threats*, March 2026.

information environments for non-democratic malign manipulation," citing "prolonged political instability and polarization, a deeply embedded amplification infrastructure rooted in state capture, weak regulatory enforcement, and low societal resilience."[102] In anticipation of possible interference in the 2026 election, Bulgarian authorities reportedly launched an initiative to counter disinformation and hybrid threats and sought EU assistance.[103]

Considerations for Congress

Some Members of Congress have expressed concern at the reported rise in Russian hybrid warfare activities since 2022.[104] Congress may have an interest in monitoring reports of Russian hybrid warfare operations and executive branch policy via hearings, oversight engagements, and/or mandated executive branch reports.

Congress also may consider whether to maintain, strengthen, remove, or adjust sanctions on Russia's intelligence agencies and personnel in response to Russian hybrid activities. Both Congress and successive Administrations have imposed sanctions on Russia's foreign intelligence agencies, including under Section 231 of P.L. 115-44, and Executive Orders 13694 and 14024, as amended.[105]

The 2026 National Defense Authorization Act (P.L. 119-60, Section 1241) modifies the annual report on military and security developments involving the Russian Federation to include, among other things, "a list and description of all known violations by Russia of NATO airspace during the reporting period, and to the extent feasible, an evaluation of whether such incidents were intentional or unintentional" and "an assessment of the threat posed to NATO bases, critical infrastructure, and other industrial and military targets posed by Russian hybrid attacks." Also in P.L. 119-60, Section 5160 directs the Secretary of State to establish a Countering Russian Influence Fund Unit (CRIF Unit) to oversee and monitor the implementation of Section 254 of the Countering Russian Influence in Europe and Eurasia Act of 2017 (22 U.S.C. 9543) and, among other things, calls upon the Director of the CRIF Unit to "ensure that all CRIF Unit programming advances United States foreign policy and national security interests, including efforts to counter Russian aggression against sovereign countries and other nefarious kinetic and hybrid Russian activities in countries that are United States allies or partners that affect, threaten, or undermine United States interests."

[102] Rositsa Dzhekova et al., "Defending the Vote: Policy Responses to Information Warfare in Bulgaria," Center for the Study of Democracy, March 11, 2026.

[103] Antoaneta Roussi, "Bulgaria Requests EU Support to Fend Off Election Meddling in April Vote," *Politico*, April 1, 2026.

[104] See, for example, U.S. Congress, Joint Commission on Security and Cooperation in Europe (U.S. Helsinki Commission), *Shadow War: Inside Russia's Attacks on NATO Territory*, 118th Cong., 2nd sess., December 12, 2024; U.S. Congress, House Foreign Affairs Committee, Europe Subcommittee, *Hybrid Warfare in Europe Against U.S. Interests: Moscow and Beijing's Playbook*, 119th Cong., 2nd sess., December 12, 2025; U.S. Congress, House Foreign Affairs Committee, Europe Subcommittee, *Weaponized Mass Migration: A Security Risk to Europe and the United States*, 119th Cong., 2nd sess., February 10, 2026; U.S. Congress, Senate Foreign Relations Committee, *Sabotage in the Baltic Sea, Implications for European Security, and Lessons for the Indo-Pacific*, 119th Cong., 2nd sess., April 30, 2026.

[105] Countering Russian Influence in Europe and Eurasia Act of 2017, as amended (CRIEEA; P.L. 115-44, Countering America's Adversaries Through Sanctions Act [CAATSA], Title II; 22 U.S.C. 9501 et seq.); Executive Order 13694 of April 1, 2015, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," 80 *Federal Register* 18077, April 2, 2015; Executive Order 14024 of April 15, 2021, "Blocking Property with Respect to Specified Harmful Foreign Activities of the Government of the Russian Federation," 86 *Federal Register* 20249, April 19, 2021.

Successive U.S. Administrations have expelled Russian diplomats and suspected intelligence officers (reportedly over 100 between 2016 and early 2025).[106] Some media reports in 2025 indicated the second Trump Administration had engaged in discussions with Russia to allow the return of expelled Russian diplomats.[107] Congress may consider measures to conduct oversight of executive branch policy on Russia's diplomatic presence in the United States, including potential counterintelligence implications.[108]

In the 119th Congress, several other legislative measures have been introduced to address concerns about Russian hybrid warfare activities. These include the following:

- Section 1618 in H.R. 3838 would instruct the Director of National Intelligence, in coordination with the Secretary of Defense (the Secretary of Defense is using "Secretary of War" as a "secondary title" under Executive Order 14347 of September 5, 2025[109]) and the Secretary of State, to submit a "report on Russian active measures in NATO territory."
- H.R. 7632 (the SHADOW Act), would call on the Secretary of State to appoint a coordinator for "hybrid warfare accountability" and assess the threat of hybrid warfare activities to U.S. and allied interests.
- Additionally, Section 1225 in S. 4784 would instruct the Secretary of Defense to notify the appropriate committees of Congress of any "gray zone activities known or reasonably suspected to have been carried out by the Russian Federation against a North Atlantic Treaty ally."

In conducting oversight of executive branch policies and responses, Congress could evaluate whether and to what extent law enforcement, intelligence, or conventional military tools, or combinations thereof, may be deployed to counter hybrid warfare activities. Furthermore, Congress could require or request that the intelligence community submit a National Intelligence Estimate, in classified and unclassified form, on Russian hybrid warfare and intelligence operations.

Congress may also consider other policies, such as law enforcement or intelligence actions rather than conventional military operations, and conduct oversight of or seek to shape U.S. policies on NATO efforts to counter Russian hybrid threats.[110] NATO, in particular, has taken multiple steps to counter hybrid threats. For example, in 2025, NATO launched two missions, Baltic Sentry and

[106] Natasha Bertrand and Zachary Cohen, "Russia Sees Talks with U.S. as an Opening to Rebuild Its Spy Networks, Officials Say," CNN, February 28, 2025.

[107] Paul Sonne and Michael Crowley, "Plan to Return Russian Diplomats to U.S. Poses Espionage Risk," *New York Times*, March 9, 2025.

[108] Section 205 of Division N of P.L. 115-31 established an advanced notification regime for all travel by accredited diplomats and consular personnel of the Russian Federation.

[109] Executive Order 14347 of September 5, 2025, "Restoring the United States Department of War," 90 *Federal Register* 43893, September 10, 2025.

[110] For example, Estonia's internal security service calls for the aggressive prosecution and public naming of Russian operatives to deter operations. See, Estonian Internal Security Service, *Annual Review 2025-2026*; and Sam Jones, "Prosecute Russian-Sponsored Saboteurs, Estonia Tells Europe," *Financial Times*, April 27, 2026. See also Jenny Gross and Aurelien Breeden, "Romania Says It Could Invoke NATO's Article 4. What Would That Do?," *New York Times*, May 29, 2026; Sam Greene et al., *War Without End: Deterring Russia's Shadow War*, Center for European Policy Analysis, March 31, 2026.

Eastern Sentry, to monitor, deter, and respond to Russian sabotage of CUI and airspace violations.[111]

Author Information

Andrew S. Bowen, Coordinator
Analyst in Russian and European Affairs

Derek E. Mix
Specialist in European Affairs

Sarah E. Garding
Analyst in European Affairs

Catherine A. Theohary
Specialist in National Security Policy, Cyber and Information Operations

Disclaimer

[111] NATO Allied Maritime Command, "NATO's Baltic Sentry Steps Up Patrols in the Baltic Sea to Safeguard Critical Undersea Infrastructure," press release, January 14, 2025, https://mc.nato.int/media-centre/news/2025/nato-baltic-sentry-steps-up-patrols-in-the-baltic-sea-to-safeguard-critical-undersea-infrastructure; NATO, "NATO Launches 'Eastern Sentry to Bolster Posture Along Eastern Flank," press release, September 12, 2025, https://www.nato.int/en/news-and-events/articles/news/2025/09/12/nato-launches-eastern-sentry-to-bolster-posture-along-eastern-flank.