



**Statement before the
U.S. Helsinki Commission**

“Deterrence on NATO’s Eastern Flank”

A Testimony by:

Seth G. Jones

President, Defense and Security Department, Center for Strategic and
International Studies

November 17, 2025

Chairman Wicker, Co-Chairman Wilson, and distinguished Members of the Commission, I am honored to share my views with you on the important topic of deterrence on NATO's eastern flank.¹ CSIS does not take policy positions, so the views represented in this testimony are my own and not those of my employer. In my testimony, I would like to reflect on three main points:

- The Russian government has conducted a growing campaign of sabotage and subversion against the United States and Europe designed in part to target countries, companies, and individuals that provided support to Ukraine.
- Led by the Main Intelligence Department, or GRU, Russian attacks have included bombings, drone incursions, sabotage against undersea cables and pipelines, electronic attack, and cyber operations.
- The United States and Europe need to develop a more effective strategy of defensive and offensive measures to strengthen deterrence on NATO's eastern flank and raise the costs on Moscow of continued aggression.

Russia's Growing Campaign of Aggression

Russia has engaged in an aggressive and violent campaign of sabotage below the threshold of conventional warfare led by Russia's Main Intelligence Department, or GRU. These actions have complemented Russia's conventional war in Ukraine and nuclear saber-rattling. Russia's strategy has likely been to coerce European governments and companies to stop aiding Kyiv, deter Russian soldiers and citizens from defecting to the West, sow fear and division, and undermine public support for the Ukraine war.

Russia and the Soviet Union have long been engaged in sabotage and subversion in Europe and other regions, which Moscow has historically referred to as "active measures" (or *aktivnyye meropriyatiya*). What is new, however, is the scale and scope of the attacks, as well as the nature of the targets. Following Russia's full-scale invasion of Ukraine and European and U.S. support to Kyiv, Russia significantly escalated its campaign of sabotage and subversion in Europe. According to CSIS's data set of Russian subversive attacks, the number of Russian attacks in Europe tripled between 2023 and 2024, after quadrupling between 2022 and 2023.² The data covers Russian kinetic attacks using such weapons as explosives, other incendiaries, firearms, anchors and other blunt instruments for damaging undersea fiberoptic cables and pipelines, electronic attack, and the weaponization of illegal immigrants. Russia's primary targets were critical infrastructure (such as pipelines and undersea fiberoptic cables), private industry, government, and transportation targets (such as rail lines transporting materiel to Ukraine).³

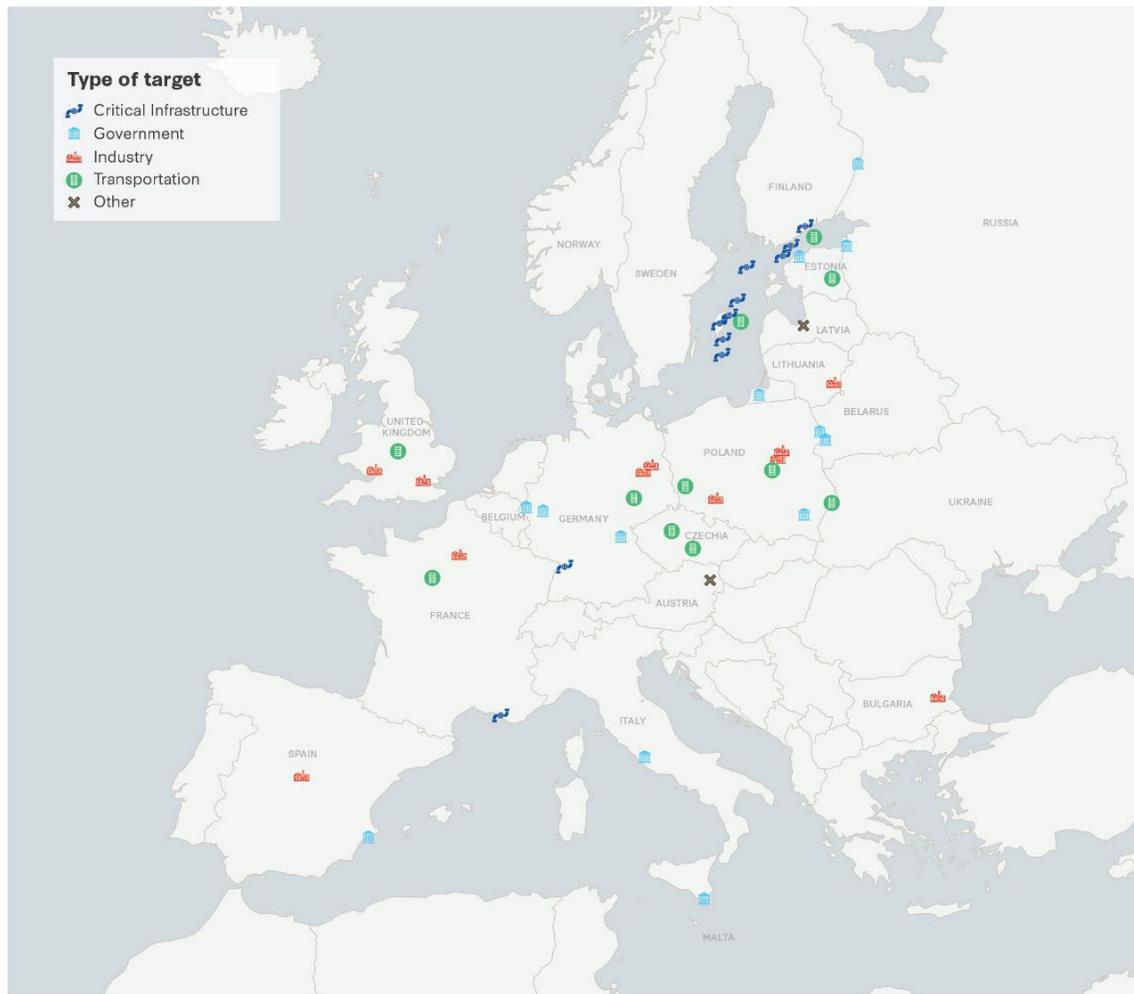
¹ The analysis and recommendations in this report draw extensively from the following forthcoming article: Seth G. Jones, "Russia's Sabotage Campaign in Europe," *Survival*, vol. 67, no. 6, December 2025–January 2026.

² The data come from the Center for Strategic and International Studies.

³ For other data sets see, for example, Edwards and Seidenstein, *The Scale of Russian Sabotage Operations against Europe's Critical Infrastructure*; Benedicte Dobbinga, "Research: Europe Increasingly Targeted by Russian Sabotage," Leiden University, January 25, 2025, <https://www.universiteitleiden.nl/en/news/2025/01/research-europe-increasingly-targeted-by-russian-sabotage>; and U.S. Helsinki Commission Staff, *Spotlight on the Shadow War: Inside Russia's Attacks on NATO Territory* (Helsinki, Finland: U.S. Helsinki Commission, December 2024), <https://www.csce.gov/publications/spotlight-on-the-shadow-war-inside-russias-attacks-on-nato-territory/>.

As Figure 1 highlights, Russian sabotage occurred across much of Europe, with a few important caveats. Russian intelligence services generally stayed away from countries that had close relations with the Kremlin and whose governments shied away from aid to Ukraine. For example, there were no recorded attacks against Hungary or Serbia, which retain relatively close relations with the Kremlin. Russia also did not conduct attacks against several European states that remained largely neutral in the Ukraine war, such as Switzerland. Instead, the attacks were concentrated against countries that supplied weapons or other materiel to Ukraine, sheltered Russian defectors, or otherwise conducted actions against Kremlin interests (including Finland and Sweden’s decision to join NATO after Russia’s full-scale invasion of Ukraine).

Figure 1: Location of Russian Sabotage in Europe, 2022- 2025



Source: CSIS analysis.

CSIS | DEFENSE AND SECURITY
DEPARTMENT

Companies that produced, transported, or stored materiel destined for Ukraine were a common target of Russian activity. In May 2024, for example, Russian intelligence was likely behind a massive fire at a Diehl Group factory in Berlin, which manufactured IRIS-T surface-to-air

missiles used in Ukraine.⁴ The attackers used electric massagers implanted with a magnesium-based flammable substance to explode bombs at DHL logistics hubs in 2024 near Leipzig, Germany; Birmingham, England; and Jablonow, Poland. These plots may have been a test run to figure out how to get such incendiary devices aboard planes.⁵ Indeed, Polish prosecutor Katarzyna Calow-Jaszewska concluded that Russia's goal was to "test the transfer channel for such parcels, which were ultimately to be sent to the United States of America and Canada."⁶

Russian intelligence was likely behind other infrastructure attacks in Europe. There was an explosion linked to Russian intelligence at a warehouse in Spain that stored communications equipment bound for Ukraine.⁷ There was also an explosion in Kazanluk, Bulgaria that killed three people at the plant of Bulgarian defense company Arsenal, which manufactured small arms, artillery pieces, and ammunition. In 2023, explosions went off in the ammunition warehouses of the Bulgarian arms manufacturer and trader EMCO, only days after Bulgaria announced it would officially join the coalition to supply shells to Ukraine.⁸

Russian security services allegedly targeted specific individuals, including executives from companies involved in aiding Ukraine, journalists that investigated Russian activity, Russian defectors to the West, and government (including Ukrainian) officials. Russian operatives in Spain likely assassinated Maksim Kuzminov, a Russian helicopter pilot who defected to Ukraine from Russia in August 2023. Several months before the attack, Russian state television reported that the GRU had "been given the order" to assassinate Kuzminov.⁹ Shortly after the assassination, the head of Russia's foreign intelligence service, Sergei Naryshkin, called Kuzminov a "traitor and criminal" who was a "moral corpse at the very moment when he planned his dirty and terrible crime."¹⁰ In 2024 in Lithuania, Russian intelligence services likely targeted Leonid Volkov, a Russian citizen and former close aide of now-deceased Russian opposition leader Alexei Navalny.¹¹ Another incident involved the vandalization of a car belonging to Estonian Minister of the Interior Lauri Läänemets, who had repeatedly been critical

⁴ "Germany: Fire Breaks out at Berlin Metal Factory," Deutsche Welle, May 4, 2024, <https://www.dw.com/en/germany-fire-breaks-out-at-berlin-metal-factory/a-68992842>.

⁵ Bojan Pancevski, Thomas Grove, Max Colchester, Daniel Michaels, "Russia Suspected of Plotting to Send Incendiary Devices on U.S.-Bound Planes," *Wall Street Journal*, November 4, 2024, <https://www.wsj.com/world/russia-plot-us-planes-incendiary-devices-de3b8c0a>; Sam Jones, John Paul Rathbone, and Richard Milne, "Russian Plotting Sabotage Across Europe, Intelligence Agencies Warn," *Financial Times*, May 5, 2024, <https://www.ft.com/content/c88509f9-c9b-d-46f4-8a5c-9b2bdd3c3dd3>.

⁶ Paul Kirby and Frank Gardner, "Mystery Fires Were Russian 'Test Runs' to Target Cargo Flights to U.S.," BBC, November 5, 2024, <https://www.bbc.com/news/articles/c07912lxx33o>.

⁷ David Ignatius, "Russia Is Punching Back at NATO in the Shadows," *Washington Post*, June 21, 2024, <https://www.washingtonpost.com/opinions/2024/06/21/russia-nato-ukraine-sabotage-attacks/>.

⁸ Krassen Nikolov, "Explosions at Bulgarian Arms Factory Set to Export to Ukraine," Euractiv, June 26, 2023, <https://www.euractiv.com/section/politics/news/explosions-at-bulgarian-arms-factory-set-to-export-to-ukraine/>.

⁹ Miguel González and Carlos E. Cué, "Gunmen Sent by Moscow Killed Defector Sheltering in Alicante, Spanish Intelligence Services Say," *El País*, February 22, 2024, <https://english.elpais.com/international/2024-02-22/gunmen-sent-by-moscow-killed-defector-sheltering-in-alicante-spanish-intelligence-services-say.html>; "Russia Spy Chief Calls Military Pilot Who Defected to Ukraine a 'Moral Corpse' after Report Murder in Spain," CBS News, February 20, 2024, <https://www.cbsnews.com/news/russia-maxim-kuzminov-defector-found-dead-villajoyosa-spain/>.

¹⁰ Lauri Gozzi, "Russian Pilot Maxim Kuzminov Who Defected to Ukraine 'Shot Dead' in Spain," BBC, February 20, 2024, <https://www.bbc.com/news/world-europe-68337794>.

¹¹ Cat McGowan, "Leonid Volkov: Three Arrested Over Attack on Navalny Ally," BBC, April 19, 2024, <https://www.bbc.com/news/world-europe-68854314>.

of the Russian war in Ukraine.¹² Lithuania’s internal security service assessed that “the Russian special service had coordinated a hybrid operation against the security of [Estonia]” with the goal of spreading fear in the country.¹³

Russia was also involved in several plots that failed: one in Poland targeting Ukrainian President Volodymyr Zelensky; one in Austria against Bulgarian investigative journalist and director of the Bellingcat investigative reporting group Christo Grozev; one in Germany targeting Armin Papperger, the chief executive officer of Rheinmetall; one in the UK against Russian dissident Evgeny Chichvarkin who was allegedly delivering supplies to Ukraine; and one in France against Vladimir Osechkin, a Russian defector who was involved in exposing human rights abuses in Russian prisons.¹⁴

In addition, Russia targeted military bases and other government facilities tied to Ukraine, including locations where NATO military personnel and contractors trained Ukrainian forces. German prosecutors charged three Russian-German nationals—Dieter Schmidt and two accomplices—for acting as secret agents for Russia and plotting bombing and arson attacks against U.S. military bases in Germany. Schmidt allegedly participated in other sabotage plots, including taking pictures of military installations with an aim to endanger national security.¹⁵ At the U.S. base in Grafenwoehr, for example, NATO trained Ukrainian troops to operate M1 Abrams main battle tanks.

Maritime, land, and air transportation hubs were a focus of Russian sabotage, including those connected to Ukraine. Germany experienced a series of railway cable-cutting attacks, while Sweden experienced three separate train derailments on its “Iron Ore Line” attributed to Russian actions.¹⁶ In addition, Russia conducted multiple attacks against Poland’s rail system, particularly rail lines that transported materiel to Ukraine.¹⁷ Russia also targeted airplanes through electronic attack.

¹² Michael Schwirtz and Julian E. Barnes, “Russia Plotted to Put Incendiary Devices on Cargo Planes, Officials Say,” *New York Times*, November 5, 2024, <https://www.nytimes.com/2024/11/05/world/europe/russia-plot-dhl-planes.html>; Sam Jones, John Paul Rathbone, and Richard Milne, “Russian Plotting Sabotage Across Europe, Intelligence Agencies Warn,” *Financial Times*, May 5, 2024, <https://www.ft.com/content/c88509f9-c9bd-46f4-8a5c-9b2bdd3c3dd3>.

¹³ “Estonia Detains 10 People Suspected of Committing Sabotage on Orders from Russia,” *Radio Free Europe / Radio Liberty*, February 21, 2024, <https://www.rferl.org/a/estonia-detains-10-sabotage-russia/32828650.html>.

¹⁴ “Four Men Charged in France with Plotting Assassination of Russian Dissident,” *Le Monde*, October 16, 2025, https://www.lemonde.fr/en/international/article/2025/10/16/france-arrests-four-men-suspected-of-plotting-the-assassination-of-a-russian-dissident_6746501_4.html.

¹⁵ Matthew M. Burke, “Trio Charged in Germany for Pro-Russia Plot Targeting U.S. Bases in Bavaria,” *Stars and Stripes*, December 31, 2024, <https://www.stripes.com/branches/army/2024-12-31/dual-nationals-charged-spying-russia-16331452.html>.

¹⁶ Daniel Safford, “Man Admits Arson Over London Fire Linked to Russia,” *BBC*, October 25, 2024, <https://www.bbc.com/news/articles/cvgexrw3x2xo>; Keir Giles, “Russian Disruption in Europe Points to Patterns of Future Aggression,” *Chatham House*, May 1, 2024, <https://www.chathamhouse.org/2024/05/russian-disruption-europe-points-patterns-future-aggression>.

¹⁷ Andy Greenberg, “The Cheap Radio Hack That Disrupted Poland’s Railway System,” *Wired*, August 27, 2023, <https://www.wired.com/story/poland-train-radio-stop-attack/#:~:text=12%3A06%20PM-,The%20Cheap%20Radio%20Hack%20That%20Disrupted%20Poland's%20Railway%20System,broadcast%20with%20%2430%20in%20equipment;Loveday%20Morris,Poland%20Investigates%20Train%20Mishaps%20for%20Possible%20Russian>

Russia conducted attacks against targets in and around two countries—Finland and Sweden—that joined NATO following Russia’s full-scale invasion of Ukraine. Finnish investigators assessed that a Chinese-registered ship operated by a Russian crew damaged two undersea data cables and a gas pipeline in the Baltic Sea with its anchor. The ship was trailed by the *Sevmorput*, a Russian nuclear-powered cargo ship.¹⁸ In addition, an oil tanker likely dragged its anchor and damaged a cable in the Gulf of Finland.¹⁹ The *Vezen*, a Maltese-flagged ship, damaged an undersea fiber-optic cable linking Latvia and Sweden. Armed police parachutists from Sweden promptly boarded the ship.²⁰ Yet another ship, which had a Russian captain, cut undersea cables in the Baltic Sea off the coast of Sweden and Finland.²¹

Russia and Belarus weaponized illegal immigrants against several border countries, such as Finland, Poland, Latvia, Lithuania, and Norway. In November 2023, for instance, Finland closed its border with Russia following a surge of border crossings instigated by Russia. In the summer of 2024, Poland experienced a surge of nearly 400 illegal border crossings per day. These border crises were likely orchestrated to pressure state institutions, drain resources, and fuel anti-migrant rhetoric exploited by far-right parties across Europe.²²

Finally, Russian services aggressively collected intelligence about potential future targets. Russia flew drones over numerous European countries, including critical infrastructure, defense production facilities, and airports in Germany; airports and other areas in Denmark and Norway; and critical infrastructure in Poland, Romania, Latvia, Lithuania, and Estonia. In Germany, for example, security authorities reported significant intelligence, surveillance, and reconnaissance by drones—some of which they assessed were Russian—over critical infrastructure and military

Connection,” *Washington Post*, August 28, 2023, <https://www.washingtonpost.com/world/2023/08/28/poland-hacking-trains-russia/>.

¹⁸ Bojan Pancevski, “Europe Sees Signs of Russian Sabotage but Hesitates to Blame Kremlin,” *Wall Street Journal*, May 20, 2024, <https://www.wsj.com/world/europe/europe-sees-signs-of-russian-sabotage-but-hesitates-to-blame-kremlin-72598d4b>.

¹⁹ Mike Eckel, “A Russian Airline Bomb Plot? What We Know About the Polish PM’s Accusations,” *Radio Free Europe / Radio Liberty*, January 15, 2025, <https://www.rferl.org/a/poland-russia-tusk-airline-bomb-plot/33277035.html>; Johanna Lemola and Lynsey Chutel, “Finland Says Vessel Suspected of Cutting Cable May Be Part of Russia’s ‘Shadow Fleet,’” *New York Times*, December 26, 2024, <https://www.nytimes.com/2024/12/26/world/europe/finland-estonia-cables-russia.html>.

²⁰ Edward Lucas, “Russia’s War Beneath the Waves Threatens Us All,” *Times* (London), January 29, 2025, <https://www.thetimes.com/comment/columnists/article/russias-war-beneath-the-waves-threatens-us-all-tx6khr2fg>; 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, <https://carnegieendowment.org/emissary/2024/12/baltic-sea-internet-cable-cut-europe-nato-security?lang=en>; Elisabeth Braw, “Suspected Sabotage by a Chinese Vessel in the Baltic Sea Speaks to a Wider Threat,” Atlantic Council, November 21, 2024, <https://www.atlanticcouncil.org/blogs/new-atlanticist/suspected-sabotage-by-a-chinese-vessel-in-the-baltic-sea-speaks-to-a-wider-threat/>.

²¹ “Danish Military Monitors a Chinese-Flagged Bulk Carrier After Undersea Data Cables Were Ruptured,” Associated Press, November 21, 2024, <https://apnews.com/article/denmark-sweden-finland-germany-lithuania-china-yi-peng-undersea-cables-d3af1bf7e68ff060bb6e669f24425fd0>.

²² U.S. Helsinki Commission Staff, *Spotlight on the Shadow War*; Jon Richardson, “How and Why Russia Is Conducting Sabotage and Hybrid-War Offensive,” Australian Strategic Policy Institute, November 5, 2024, <https://www.aspistrategist.org.au/how-and-why-russia-is-conducting-sabotage-and-hybrid-war-offensive/>; Taub, “Russia’s Espionage War in the Arctic.”

installations, including transit routes and naval, air force, and army bases.²³ Some of this activity may have been routine espionage, though some of it was likely intelligence collection for potential future sabotage operations.

Offense and Defense

Russia has engaged in nuclear saber rattling during the Ukraine war as a coercive tool, conducted conventional military operations in Ukraine, and orchestrated sabotage and subversion in Europe. Moving forward, the threat from Russian sabotage in Europe is serious and likely to persist. In response, the United States and Europe should conduct a mix of defensive and offensive measures to strengthen deterrence, mitigate the impact of Russian actions, and impose costs on Russia for a continuing campaign.

Strengthening defenses includes several components. The first is increasing intelligence sharing, reconnaissance, and surveillance between military, intelligence, and law enforcement agencies against Russian sabotage and subversion. Some of this has already occurred. NATO created a Maritime Centre for the Security of Critical Undersea Infrastructure to enhance intelligence collection across member states.²⁴ In addition, Europe and the United States have heightened patrols and surveillance efforts in the Baltic, North, and Mediterranean Seas. NATO established Baltic Sentry and then Eastern Sentry to increase intelligence collection in the air, land, surface, and subsurface domains.²⁵ While useful, NATO countries will need to adapt to Russian changes in strategies and tactics. Russia is developing new uncrewed and autonomous systems, electronic warfare technology, and cyber and space-based capabilities. It is also recruiting using evolving methods, such as using online gaming platforms.

Second, Europe and the United States need to expand capabilities to counter and deter Russian sabotage. Examples include increasing integrated air and missile defense, deploying additional armed drones along Russia's borders with NATO countries, and expanding counter-drone capabilities for uncrewed and autonomous air, surface, subsurface, and ground systems. The European Union should significantly expedite its efforts to implement several efforts designed to

²³ "Fifty Shades of Grey Zone: Why Russia's Micro-Aggressions Against Europe Are Proliferating," *Economist*, October 2, 2025, <https://www.economist.com/briefing/2025/10/02/why-russias-micro-aggressions-against-europe-are-proliferating>; "Drohnenflüge über kritischer Infrastruktur und Militäranlagen auf Rekordniveau" [Drone Flights Over Critical Infrastructure and Military Installations at Record Levels], *Der Spiegel*, March, 14, 2025, <https://www.spiegel.de/panorama/spionage-drohnenfluege-ueber-kritischer-infrastruktur-und-militaeranlagen-auf-rekordniveau-a-81bb73d4-9d9f-43db-8ec6-d6969781c36c>; Christopher F. Schuetze, "3 Are Arrested in Russia-Linked Sabotage Plot, Germany Says," *New York Times*, May 14, 2025, <https://www.nytimes.com/2025/05/14/world/europe/3-are-arrested-in-russia-linked-sabotage-plot-germany-says.html>.

²⁴ NATO, "NATO Defence Ministers Launch Initiative to Enhance Maritime Surveillance Capabilities," October 12, 2023, https://www.nato.int/cps/en/natohq/news_219441.htm?selectedLocale=en.

²⁵ NATO, "NATO Launches 'Baltic Sentry' to Increase Critical Infrastructure Security," January 14, 2025, https://www.nato.int/cps/en/natohq/news_232122.htm; Christina Anderson and Amelia Nierenberg, "Sweden Suspects 'Gross Sabotage' After Damage to Cable Under Baltic Sea," *New York Times*, January 27, 2025, <https://www.nytimes.com/2025/01/27/world/europe/cable-baltic-sea-sweden-damage.html>; "NATO Ships in Baltic Sea Could Be Replaced by Drones"; Michael Swirtz, "A Polish Soldier, an Unusual Radar Dot and Then NATO Jets," *New York Times*, September 20, 2025, <https://www.nytimes.com/2025/09/20/world/europe/poland-drones-russia-nato.html>.

defend against Russian and other external threats: the Eastern Flank Watch, the European Drone Defence Initiative, the European Air Shield, and the European Space Shield.

With help from such countries as China and Iran, the Russian industrial base will likely produce uncrewed systems with longer range, higher payloads, greater autonomy, and more sophisticated capabilities for conducting electronic attack. In some cases, countries may need to conduct kinetic responses to Russian attacks. In September 2025, NATO scrambled Polish F-16 and Dutch F-35 fighter jets over Polish territory and shot down several Russian drones, including armed drones that resembled Shahed attack drones and lightweight Gerbera drones made with foam and plywood.²⁶ Companies in Israel, Europe, the United States, Australia, and other locations have also made progress in developing directed energy systems, which will be helpful to defend against Russian incursions.²⁷ NATO countries should also ease rules on the ability of pilots to shoot down Russian drones.

Third, the United States needs a long-term military presence in Europe focused on NATO's eastern flank to deter Russian aggression. The United States should establish 4+2 force posture with four brigade combat teams (BCTs) and two regional headquarters. Russia will likely remain a serious threat to the United States and Europe in the foreseeable future. Russian president Vladimir Putin retains the political will and intentions to expand Russian power, and Russia is reconstituting its military capabilities with help from China, Iran, and North Korea. A substantial downsizing of U.S. forces in Europe could significantly weaken deterrence and embolden Russia.²⁸

Along these lines, European militaries need to continue strengthening their own capabilities to deter Russia and—if deterrence fails—to help fight and win a major power war, particularly because of U.S. interests in the Indo-Pacific. Today, European militaries would likely have difficulty conducting operations at the high end of the conflict continuum without substantial assistance from the United States. European states still lack sufficient capabilities such as: combat support, including short-range air defense and long-range indirect fires; quantity, quality, and capabilities of ground forces, especially heavy maneuver forces; and sufficient quantities of long-range precision strike munitions.

While these defensive measures are necessary, they are not sufficient. Europe and the United States should complement defensive measures with an offensive campaign designed to raise the costs on Moscow. A successful campaign needs to be coercive, and the pain has to appear contingent on Russian behavior. A strategy that does not include raising the costs on Moscow is likely to fail. There are several components of an offensive campaign.

First is imposing additional primary and secondary economic sanctions against Russia and countries that import Russian goods, as well as sanctioning additional entities and individuals

²⁶ Michael Swirtz, "A Polish Soldier, an Unusual Radar Dot and Then NATO Jets."

²⁷ See, for example, Lara Jakes, "The Hottest New Defense Against Drones? Lasers," *New York Times*, September 18, 2025, <https://www.nytimes.com/2025/09/18/world/europe/drones-laser-weapons.html>.

²⁸ Seth G. Jones and Seamus P. Daniels, *Deterring Russia: U.S. Military Posture in Europe* (Washington: Center for Strategic and International Studies, January 27, 2025), <https://www.csis.org/analysis/deterring-russia-us-military-posture-europe>.

involved in sabotage and subversion. Europe has already conducted some useful steps. For example, the European Union sanctioned Nikolay Alexandrovich Korchagin, Vitaly Shevchenko, and Yuriy Fedorovich Denisov—operatives in GRU Unit 29155—for their alleged involvement in cyberattacks targeting Estonia.²⁹ Sanctions should be connected to Russia’s broader war in Ukraine. Russia is grappling with inflation, labor shortages, brain drain and limited paths to economic growth. The country’s economy is exposed in oil and gas, and increased sanctions against Russia’s energy sector would likely cause additional pain. Energy sanctions could be combined with sanctions against other Russian exports, such as minerals, metals, agricultural goods, and fertilizers.

Second is increasing U.S. and European proactive efforts against such targets as Russia’s shadow fleet, which is illegally shipping oil and gas to overseas markets. With U.S. assistance, including intelligence assistance, European governments should board and inspect tankers and other vessels linked to Russia’s shadow fleet. In addition, the United States and Europe should reach out to priority flag states that provide or enable logistical support to the shadow fleet and increase pressure on them to deregister sanctioned vessels. There are likely other useful steps, such as listing and sanctioning insurers and other parts of the shadow fleet ecosystem.

Third, Europe and the United States should expand broader military aid and economic assistance to Ukraine. Taking these steps are important for many reasons. But if one of Russia’s goals in using sabotage is to coerce the United States and Europe from aiding Ukraine, then increasing aid to Ukraine shows that Russia is failing to achieve some of its main goals. Examples of aid include exporting German Taurus missiles, supplying components to help Ukraine’s domestic industry develop and produce long-range missiles (such as Ukraine’s Flamingo ground-launched cruise missile) for deep strike into Russia, and using frozen Russian assets to aid Ukraine. Russia should know that the United States and Europe are willing to raise the costs if Russia continues to wage its conventional and unconventional campaigns.

It would be naive to expect that increased defensive and offensive measures will eliminate Russian aggression. They won’t. But these types of offensive and defensive measures can raise the costs on Russia, minimize the benefits for Moscow, and strengthen deterrence. In the end, that may be good enough.

²⁹ European Union, Council Decision (CFSP) 2025/171 of 27 January 2025 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, January 27, 2025, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202500171.