Russia's Shadow War Against the West

By Seth G. Jones, President of the Defense and Security Department

KEY TAKEAWAYS

- Russia is conducting an escalating and violent campaign of sabotage and subversion against European and U.S. targets in Europe led by Russian military intelligence (the GRU), according to a new CSIS database of Russian activity.
- The number of Russian sabotage attacks in Europe nearly tripled between 2023 and 2024, after quadrupling between 2022 and 2023.
- In 2024, Russian agencies orchestrated attacks in Europe against a wide range of targets, from critical infrastructure to transportation targets, using a variety of weapons and tactics, from explosives to blunt or edged weapons such as anchors.
- Russian military and intelligence agencies have also conducted offensive cyberattacks, disinformation, and other active measures against the United States.
- The increase in attacks indicates that the West has failed to coerce Russia from stopping its campaign of sabotage and subversion. Russian attacks are not just a European problem, but a U.S. problem as well. The GRU and other organizations have conducted operations against U.S. targets, such as U.S. bases in Germany.

BACKGROUND AND CONTEXT

Russia is engaged in an aggressive campaign of subversion and sabotage against European and U.S. targets, which complement Russia's brutal conventional war in Ukraine. These actions are not likely to stop even with a peace deal in Ukraine, since the Kremlin continues to assess that the United States is its main opponent. Russia's "active measures" campaign is focused on achieving several objectives:

- **Influencing public opinion, including U.S. public opinion, to support Russian interests.**
- **Coercing governments, companies, or individuals to stop taking specific actions, particularly continuing to provide military and other assistance to Ukraine.**
- **Deterring Russian soldiers, government officials, and citizens from defecting to the West.**
- **Creating fissures between governments, especially between NATO allies.**
- **Undermining the democratic norms and values that underpin the West.**

Russia has long favored active measures, including sabotage and subversion, as a means to accomplish foreign policy objectives. But new CSIS data has identified an alarming increase in the number of attacks in Europe, which have nearly tripled between 2023 and 2024, after quadrupling between 2022 and 2023. Russia's military intelligence service, the Main Directorate of the General Staff of the Armed Forces of the Russian Federation, referred to as GRU, was likely responsible for many of these attacks, either directly by their own officers or indirectly through recruited agents.

Roughly 28 percent of Russian attacks were against transportation targets (such as trains, vehicles, and airplanes), another 28 percent were against government targets (such as military bases and officials), 20 percent were against critical infrastructure targets (such as pipelines, undersea fiber-optic cables, and the electricity grid), and 20 percent were against industry (such as defense companies). Russia also used a variety of weapons and tactics. The most common (32 percent) involved explosives and incendiaries against warehouses or companies producing or shipping material to Ukraine.

LEGISLATIVE AND POLICY IMPLICATIONS

Recently introduced legislation related to CSIS's findings include H.Res.135, which affirms that transatlantic cooperation through NATO is critical to combating the proliferation of malign influence, technologies, and destabilizing operations from adversaries like Russia; S.5365, which would require the president to notify Congress and take certain actions in response to any attempt by a country of concern (such as Russia) to affect U.S. elections; and H.R.10368, which seeks to codify in statue certain sanctions against Russia.

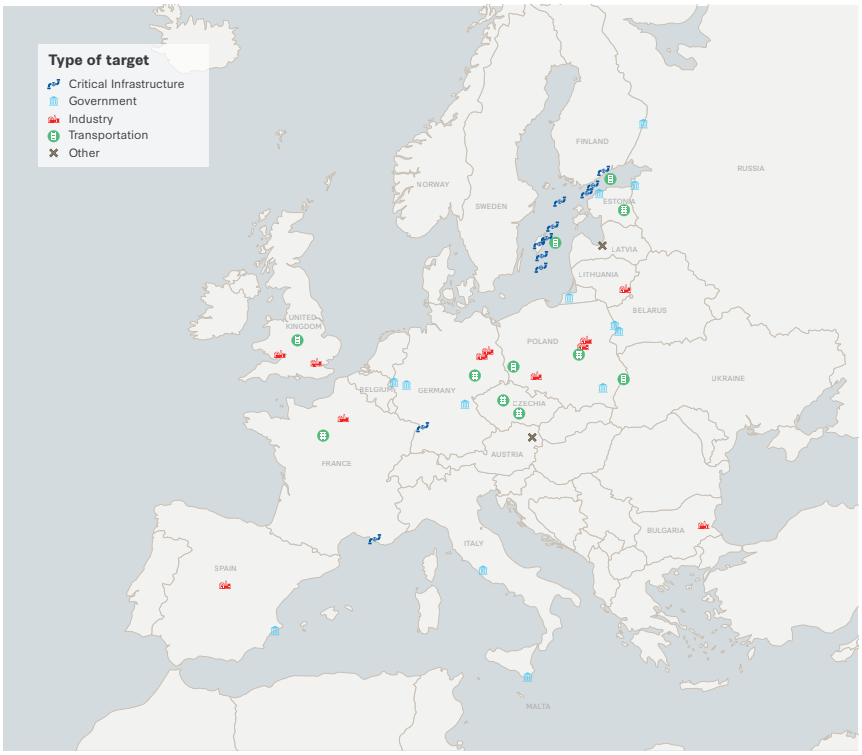
CSIS's latest findings reaffirm the urgent need to address Russia's escalating sabotage campaign with a calibrated response carried out in close collaboration with the United States' NATO allies. The CSIS database provides additional and compelling evidence in support of the proposed legislation above.

RECOMMENDATIONS

- The United States and European countries, including the European Union and NATO, have largely focused on defensive measures to counter Russian actions, such as sharing intelligence and strengthening resilience (including cyber defenses). While these efforts are necessary, they are not sufficient.
- U.S. lawmakers should outline a calibrated offensive campaign against Russia that includes escalating sanctions against Moscow if Russian sabotage and subversion continue; support for targeted offensive cyber operations against important Russian military and commercial targets; and more aggressive actions against assets valuable to Russia, such as its shadow fleet.

All views, positions, and conclusions expressed in this brief should be understood to be solely those of the author(s).

Geographic Area of Russian Attacks, 2022–2025



Source: CSIS analysis.

Additional Resources and Contact Information

Seth G. Jones, "Russia's Shadow War Against the West," CSIS, March 18, 2025, https://www.csis.org/analysis/russias-shadow-war-against-west.

"Significant Cyber Incidents," CSIS, last updated 2025, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

For more information, contact **Chloe Himmel** at 202.775.3186 or **chimmel@csis.org**.