Sabotage as a â??New Normalâ?•

Description

> *â??Efforts will be made in such countries to disrupt national self-confidence, to hamstring measures of national defense, to increase social and industrial unrest, to stimulate all forms of disunity.â?• â??George Kennan, The Long Telegram*

Since 2022, there has been a spate of high-profile sabotage attacks across Europe: a suspicious fire in Berlin, explosions at a Bulgarian arms factory, and damage to undersea communications cables chief among them. This brazen campaign of sabotage, presumably perpetrated or sponsored by Russian security services, proxies, and the occasional unwitting, manipulated recruit, are at a â??level previously unseenâ?• according to German foreign intelligence service director Bruno Kahl. Similarly, Ken McCallum, the head of Britainâ??s MI5, said that â??The GRU in particular is on a sustained mission to generate mayhem on British and European streets.â?• Russian-backed attacks on energy and transportation infrastructure are not limited to Ukraine, but now also extend across Europe.

While the frequency of incidents has slowed, neither NATO nor Ukraine are likely to see a total cessation of events given the relatively low risk, high reward nature of modern sabotage. Acts of sabotage are likely to persist as a characteristic of the European security environment and anticipate upticks leading to elections and other key events. Sabotage is the new normal.

Positive but Misleading Trends

Sabotage has, as of late, been used synonymously with the somewhat murky and contentious term Russian hybrid operations, inviting ambiguity and vagueness. â??Hybrid warfareâ?• can range from the spectacularâ??such as the 2024 attempted assassination of Germanyâ??s Rheinmetall CEOâ??to the disruptive but more criminal in nature, such as the acts of arson against property of current British Prime Minister Keir Starmer, in addition to sabotage. However, it is important to isolate the growing pattern of Russian-backed sabotage with a precise definition in order to identify its distinctive effects and purposes.

The term sabotage is best used in the traditional sense: to refer to attacks or incidents that cause physical damage to, or the destruction of, military (and, increasingly, civil) infrastructure and equipment. The inclusion of civilian infrastructure is the most concerning characteristic in a departure to what has long been a primarily military endeavor. However, currently nothing appears to be off-limits

as undersea telecommunications cables that enable the global economy by way of transporting gas, data, and power across bodies of water and borders become targets.

In what might be perceived as a positive trend, two recent reports indicate a decline in Russian sabotage attacks. Leading American political scientist and author Seth Jones noted in a March CSIS report that Russian attacks in Europe quadrupled between 2022 and 2023, then nearly tripled again between 2023 and 2024. But, Mr. Jones noted a precipitous drop-off in the first six months of 2025, with only four incidents qualifying as sabotage or attempted sabotage by Russia. The International Institute for Strategic Studies (IISS) also said in an August 2025 report that sabotage operations this year had declined, but that the threat remained as Europeans struggled to coordinate a response.

The West has not been totally passive, and the decline is likely due at least in part to the reinvigorated efforts to counter this threat. As Radio Free Europe Radio Liberty notes, some European powers have â??expelled dozens of Russian intelligence officers, many working under diplomatic cover, dating back to before the Ukraine invasion.â?•

Proving that Western actions are driving the decline in sabotage activities is difficult , however. Measuring deterrence is particularly challenging, as it requires correlating actions taken or messages issued to successfully deterring an actor. In short, it is inherently difficult to prove a negative. The downwards trend in sabotage could just as likely be tied to the increased role President Donald Trump is playing during Ukraine-Russia negotiations, given the enmity between Presidents Zelensky and Putin.

While these reports reflect a positive trend for the West, it would be wrong to be lulled into a false sense of security. Increased coordination may have already helped Europe move beyond the high-water mark of Russian-sponsored sabotage, but the threat remains. Sabotage will likely prove to be too tempting to ignore for a revisionist power such as Russia, given its proven track record of disrupting the West for what is a relatively low cost.

The Siren Song of Sabotage: Low Risk, High Reward

Russia simply gets too much from this bad behavior to stop. Even without knowing the inner workings of the Kremlin, it is a safe assumption that the primary aim of the post-2022 sabotage campaign has been to diminish the Westâ??s support for Ukraine. This goal, at least, appears to still be unrealized, but the disruption has secondary effects that benefit Moscow. Acts of sabotage, regardless of their size or efficacy, keep European governments off-kilter as constituents question leaders who fail to protect the power grid. As a result, sabotage distracts Western powers even if it doesnâ??t achieve the larger strategic aim of sapping the Westâ??s support for Ukraine. These attacks target Allied unity as they

undermine Western resilience and coherence between Allies regarding what constitutes an appropriate response. While intelligence sharing has increased, it is difficult to coordinate a unified response, even between treaty allies.

In addition to the political benefits of diminishing support for Ukraine, Moscowâ??s sabotage campaign serves concrete military ends as well. In some cases, sabotage has the tactical impact of destroying military resources intended for Kyiv, or at least slowing their delivery. In some cases, Moscow may be setting conditions for any potential military eventuality, such that the destruction of military and some civilian infrastructure certainly serves that purpose. Moscow will see little downside to accelerating in any post-deal future.

Implausible Deniability: A Golden Age of Sabotage?

A golden age of sabotage may be upon us, as modern society makes it easier, cheaper, faster, and safer than ever to recruit someone, witting or otherwise, to commit acts of sabotage. Intelligence agencies can now recruit individuals remotely using messaging apps such as Telegram, as was the case with Englishman Dylan Earl, who was recruited to set fire to a warehouse holding equipment bound for Ukraine by a handler he never met in person.

One emergent technique is to hire local criminals to carry out acts of sabotage, rather than sending trained intelligence agents. This tactic has been used in both England and Spain, with the head of Londonâ??s Metropolitan Police counterterrorism section noting that â??itâ??s a relatively new thing to see criminal proxies used on behalf of state actors.â?• In a period *The Economist* dubbed the â??summer of sabotageâ?• in 2024, European capitals expelled Russian spies and Moscow relied largely on local criminals as assets to accomplish disruption operationsâ??an act of either desperation or pragmatism. MI5 Chief Ken McCallum commented that the use of proxies reduced the professionalism of these operations, but the willingness to accept comparative amateurs may suggest that operational success was less important or simply harder to come by.

One Royal United Services Institute (RUSI) journal article outlines how Russian-sponsored sabotage demonstrates characteristics of a â??gig economy,â?• a primarily online marketplace for freelancers seeking short-term employment. As the RUSI report highlights, the wide breadth of recruitsâ??from engineers to hockey playersâ??reflects a change in reach and tactics for Russian security services, or at least an easier reach into varied pools of recruits.

Using criminals or â??gigâ?• saboteurs as assets or cut-outs increases deniability. Incidents of sabotage, whether theyâ??re executed by agents, criminals, freelancers, or the unwitting, fall under the umbrella of the larger â??shadow warâ?• against the West. Given the countries effected by sabotage

and its timing during the war in Ukraine, there is no real denying Moscowâ??s involvement, no matter how vociferously the Kremlin denies it. By publicly denying involvement and still sponsoring these acts, Moscow participates in implausible theater on the international stage. Aided by modern technology such as encrypted messaging apps, however, implausible deniability still serves as deniability in the eye of the beholder.

Vulnerabilities in European infrastructure, including undersea cables and digital systems, present sabotage opportunities. Moscow increasingly exploits these susceptibilities through quiet military operations and cyber-attacks, mitigating attribution and escalation dynamics through remote virtual systems, military deception, and deniability. But given the opportunities and existing Allied vulnerabilities, should state-sponsored sabotage be viewed as more than just a nuisance or disruption? Moscow may very well view modern sabotage as a new novel offset given their own strategic problem to solve: a unified and motivated NATO on their doorstep. As with the thinking behind previous â??offsetâ?• strategies, modern sabotage could be the way Russia is thinking about how to remedy their own perceived gaps against the strategic dilemma of NATOâ??s 32-flags.

The New Normal

Sabotage is a way for Moscow to test the Westâ??s red lines. It is possible that Putinâ??s regime is aiming to normalize these disruptions so that theyâ??re accepted as the status quo while avoiding entanglement into a wider conventional war. While NATO is coalescing around the challenge, there is little incentive for Moscow to stop enabling and funding acts of sabotage against both military and civilian infrastructure.

The West will need to incorporate thinking about counter-sabotage into steady-state campaigning efforts such as Baltic Sentry that dedicate multi-national efforts to respond to sabotage and build resiliency. For example, strengthening electrical grids and other infrastructure redundancies would fortify European nations against disruption and limit catastrophic risks. If sabotage events are not already incorporated into military and interagency exercises, they should beâ??their inclusion could improve Europeâ??s response to these events if the challenges to a unified response are first defined and overcome in fictional scenarios. Precision of languageâ??calling out physical sabotage separate from propaganda, cyber-attacks and other â??grey zoneâ?• activitiesâ??would help draw a line in the sand and mitigate effective sabotage.

The United States took a risk in disclosing details of Moscowâ??s invasion preparations in 2022 and intelligence assessments that could serve to spoil some sabotage operations. While Moscow would likely continue to deny accusations of sabotage, publicly linking support to actions that counter Russian objectivesâ??such as supplying Tomahawk missiles to Ukraineâ??could also serve as an indirect way

to coerce Moscow into decreasing support for sabotage.

It behooves the defense community to accept state-sponsored sabotage as part of the new normal and consider deterrent options for sabotage. Some NATO experts already assess that select Russian defense officials question NATOâ??s Article V commitment, a perspective that may change with a more robust response to Russian sabotage. While Moscow would likely continue to leverage plausible deniability, NATO messaging (or a precisely worded declaration categorizing sabotage as an offensive action) could serve as a red line that would deter more malign activity. The integration of counter-sabotage planning into Western collective defense strategy will mitigate the alarming trend of sabotage aimed at weakening Ukraine and fracturing NATO and contribute to long-term stability in Europe.

Rick Chersicla is an active-duty Army Strategist and 2025 non-resident fellow with the Irregular Warfare Initiativeâ??s (IWI) Project Europe. The views expressed in this article are those of the author and do not reflect the official policy or position of the United States Army, Department of Defense, or the United States Government.

Main Image: Generated by DALL-E, OpenAI, using descriptions of the Diehl Metall Factory fire in Berlin, Germany. Russian agents researched fire safety protocols for the building prior to the sabotage and the IRIS-T is a largely sought after varied range infrared air-to-air and surface-to-air missile system produced by Diehl.

If you value reading the Irregular Warfare Initiative, please consider supporting our work. And for the best gear, check out the IWI store for mugs, coasters, apparel, and other items.

The views expressed are those of the author and do not reflect the official position of the Irregular Warfare Initiative, Princeton Universityâ??s Empirical Studies of Conflict Project, the Modern War Institute at West Point, or the United States Government.

Date Created
2025/11/19