CSIS BRIEFS

Russia's Shadow War Against the West

Seth G. Jones

MARCH 2025

THE ISSUE

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 attacks nearly tripled between 2023 and 2024. Russia's primary targets have included transportation, government, critical infrastructure, and industry, and its main weapons and tactics have included explosives, blunt or edged instruments (such as anchors), and electronic attack. Despite the increase in Russian attacks, Western countries have not developed an effective strategy to counter these attacks.

INTRODUCTION

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. The number of Russian attacks in Europe 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 (or GRU), was likely responsible for many of these attacks, either directly by their own officers or indirectly through recruited agents. The GRU and other Russian intelligence agencies frequently recruited local assets to plan and execute sabotage and subversion missions. Other operations relied on Russia's "shadow fleet," commercial ships used to circumvent Western sanctions, for undersea attacks.

The data indicate that Russia poses a serious threat to the United States and Europe and that the Russian government, including President Vladimir Putin, cannot be trusted. Roughly 27 percent of the attacks were against transportation targets (such as trains, vehicles, and airplanes), another 27 percent were against government targets (such as military bases and officials), 21 percent were against critical infrastructure targets (such as pipelines, undersea fiber-optic cables, and the electricity grid), and 21 percent were against industry (such as defense companies). Many of these targets had links to Western aid to Ukraine, such as companies producing or shipping weapons and other matériel to Ukraine. Russia also used a variety of weapons and tactics. The most common (35 percent) involved explosives and incendiaries. Other weapons and tactics included blunt or edged instruments (27 percent), such as anchors used to cut undersea fiber-optic cables; electronic attack (15 percent); and the weaponization of illegal immigrants (8 percent).

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. 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 defense). While these efforts are necessary, they are not sufficient. NATO countries should develop a calibrated *offensive* campaign against Russia that includes several components: escalating sanctions against Moscow; targeted offensive cyber operations against important Russian military and commercial targets; information and influence operations targeting the populations of Russia and its partners, such as Belarus; and more aggressive actions against assets valuable to Russia, such as its shadow fleet. In short, NATO should design a campaign to escalate the costs on Russia should the country continue such operations.

To better understand Russian actions, this brief asks several questions. What are Russian objectives in conducting these attacks? What are the main tactics and targets of Russian actions? And what should the United States and other Western countries do to better deter and counter Russian activity?

To answer these questions, the analysis utilizes several sources of data. Most importantly, it builds and analyzes a database of Russian destructive attacks and plots between January 2022 and March 2025, including date, location, target, weapon, and other information.[1] In addition, it supplements this database with an overview of historical Russian and Soviet activity. It also utilizes data from other sources, such as CSIS's database of hundreds of cyber incidents since 2006. Finally, it uses information from interviews with U.S. and European government officials.

The rest of this brief is divided into five sections. The first provides an overview of actions below the threshold of conventional warfare, including their historical use by the Soviet Union and Russia. The second section assesses Russian motivations for conducting this type of warfare, including the benefits and drawbacks. The third examines the main Russian actors involved in planning and executing its shadow war, from the Kremlin to the GRU and local recruits. The fourth section analyzes the primary trends in Russia's actions, including geographic location, targets, and weapons. And the fifth outlines policy implications for the United States and its allies.

RUSSIAN SHADOW WARS: THE HISTORICAL CONTEXT

Actions below the threshold of conventional warfare have long been an important component of statecraft.[2] U.S. military doctrine refers to these types of actions as "irregular warfare" or "irregular activities," while European governments have frequently referred to these actions as "hybrid warfare" or "hybrid threats."[3] Others have used different terms to capture some or all of these actions, such as gray zone activity, political warfare, asymmetric conflict, unconventional warfare, and low-intensity conflict.[4] These types of activities involve using tools of statecraft below the threshold of conventional warfare to shift the balance of power in their favor. Examples include:

- Information and influence operations, including psychological operations and propaganda.
- Offensive cyber operations and electronic warfare.
- Support to state and non-state partners, such as guerrillas and proxy forces.
- Covert and clandestine actions by intelligence and special operations forces, including sabotage and subversion.
- Economic coercion.[5]

Russia and the Soviet Union have a rich tradition of conducting this type of warfare. During the Cold War, the Soviet Union developed an aggressive campaign to influence populations across the globe in ways that aided Soviet interests and undermined the United States and its allies, which was best captured in the phrase "active measures" (or активные меры).[6] Led by the KGB, the Soviet Union's premier spy agency, active measures included several types of activities:

- Written and oral disinformation (or дезинформация), including "gray" (unattributed) and "black" (falsely attributed) propaganda.
- The use of agents of influence, including foreign academics and media assets.
- Clandestine radio stations.
- The use of foreign political parties and international front groups to pursue Soviet national security objectives.
- Support for international revolutionary and terrorist organizations, including national liberation movements.
- Political blackmail and kidnapping.
- Targeted assassinations, including the killing of defectors.[7]

Soviet active measures focused primarily on the United States, which it referred to as the main opponent or adversary (or главный противник), though the KGB and other Soviet agencies, such as the GRU, also focused on Western European and other countries in order to undermine U.S. influence and alliances. As one former Warsaw Pact intelligence operative noted:

> Target No. 1 was the United States. . . . The objective was to hurt the United States wherever and whenever it was possible, to weaken the positions of the United States and Western Europe, to create new rifts within the NATO Alliance, to weaken the position of the United States in developing countries, to cause new rifts between the United States and developing countries, to disinform the United States and the Western allies about the military strength of the Soviet bloc countries.[8]

The documents collected by Vasili Mitrokhin, an archivist for the Soviet Union's foreign intelligence service who defected to the West just as the Cold War ended, provide some of the most illuminating insights into Soviet active measures. As one KGB analysis explained, "The main value of all Active Measures lies in the fact that it is difficult to check the veracity of the information conveyed and to identify the real source. Their effectiveness is expressed as a coefficient of utility, when minimum expenditure and effort achieves maximum end results."[9] In addition to active measures, the Soviet Union and more recently Russia also used such strategies and tactics as denial and deception (or маскировка) and information confrontation (or информационное противоборство).[10]

RUSSIAN STRATEGY

Today, Russian active measures support the following types of foreign policy objectives:

- Influencing public opinion through psychological operations in Europe, the United States, and other countries to support Russian interests.
- Coercing governments, companies, or individuals to stop taking specific actions, particularly curbing military and other assistance to Ukraine.
- Deterring countries, companies, or individuals from taking specific actions, such as escalating the type and amount of military aid 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.

These types of operations have several benefits, which make them attractive to Russian leaders. First, they allow countries to conduct coercive activities against a state below a threshold that is likely to trigger a costly or risky conventional war. Countries generally do not respond to actions below the threshold of conventional warfare by declaring war on the perpetrator. For example, Article 5 of the North Atlantic Treaty states that an armed attack against one NATO member is considered an attack on all members. But NATO governments typically do not consider active measures "an armed attack" that requires collective self-defense.[11] This means that perpetrators, including Russia, know that they can conduct these activities without causing a conventional war. As a 2024 Norwegian intelligence assessment concluded, "Any act of sabotage would most likely be performed in a manner that would make it challenging to prove who was behind it. One important reason for this is that Russia wants to avoid any situation that could trigger Article 5 of the NATO Treaty regarding collective defense."[12]

Second, these types of actions are relatively inexpensive for perpetrators. Unlike conventional war, they generally do not require vast sums of money and do not cause the perpetrator to suffer substantial casualties. Some of these actions—such as offensive cyber, electronic warfare (including GPS jamming), and influence operations—can also be done from a state's own territory, a third country, or virtual networks.

Third, these types of actions are often deniable, and targeted governments are frequently cautious—sometimes overly cautious—about attributing them due to fear of escalation. Since they may not be directly perpetrated by a government operative, countries can—and generally do—deny responsibility. Governments have frequently used a number of entities as cut-outs, such as local recruits, including criminal organizations or diaspora populations, non-governmental organizations, and companies. Russia has also used commercial vessels, such as the oil tanker *Eagle S*, which sailed under the flag of the Cook Islands, for sabotage operations.[13]

Despite these benefits, however, actions below the threshold of conventional warfare have limitations. To

Several European government agencies assessed that the Eagle S *oil tanker belonged to Russia's shadow fleet and was engaged in sabotage operations against undersea power cables.*

Photo: Jussi Nukari/AFP/Getty Images

begin with, they often have a limited impact. For example, it is difficult to conquer a country using irregular or hybrid means.[14] In addition, local assets recruited to conduct covert actions may not be professional operatives with extensive training in strategic sabotage and tradecraft beyond what their case officers can teach them, undermining the effectiveness of these operations. As the head of MI5, Ken McCallum remarked about Russian actions in Europe, "Russia's use of proxies further reduces the professionalism of their operations, and—absent diplomatic immunity—increases our disruptive options."[15] MI6 chief Richard Moore similarly noted that Russia is "having to do it through criminal elements" in Europe, which has some costs. "Criminals do stuff for cash," he noted. "They're not reliable. They're not particularly professional. . . . I think Russian intelligence services has gone a bit feral, frankly, in some of their behavior."[16]

Outsourcing actions to non-state or quasi-state actors creates a classic principal-agent problem.[17] If a group's or actor's goals are not closely aligned with that of its patron, the potential for agency loss is high and local recruits could go rogue. These types of actions can also trigger a response from the targeted government or governments, even if it is not a conventional war. Examples include economic sanctions, expulsion of government officials, the arrest and imprisonment of perpetrators, or even irregular and hybrid actions in response. Finally, these types of actions can backfire and cause a rally-around-the-flag effect in the targeted country by increasing resolve among the affected population, strengthening opposition to the sponsor's policies, and driving up military spending, as well as increasing interest in balancing alliances.

RUSSIAN ACTORS

Russian covert operations against the West are part of its foreign policy, and decisionmaking for them is centralized in the Kremlin and led by an experienced hand in covert action, President Vladimir Putin. As an operative in the KGB, Putin served in the station (or резидентура) in Dresden, East Germany, and helped spearhead active measures against West Germany.[18] He later became head of the Federal Security Service (FSB), a successor to the KGB involved in countering foreign intelligence services, combating organized crime, and ensuring economic and financial security.

Putin has long supported strategies and tactics below the threshold of conventional warfare.

Within the Kremlin, there have been several reforms regarding the organization and implementation of active measures. Around 2022, Russian Presidential First Deputy Chief of Staff Sergey Kiriyenko established the Committees of Special Influence, which is responsible for assigning Russian special services with specific tasks in target countries. In addition, activities such as violent provocations are authorized by a committee of the National Security Council under the guidance of its secretary, Sergei Shoigu.[19]

The main Russian organization involved in active measures is the GRU, headed by Admiral Igor Kostyukov. In addition, Andrei Averyanov, deputy head of the GRU, is likely responsible for overseeing all active measures other than those targeting Ukrainian territory. Averyanov established the Service for Special Activities, which includes three main entities: Unit 29155, Unit 54654, and a headquarters and planning department for coordinating the Service for Special Activities.[20]

Sergey Kiriyenko, Russian Presidential First Deputy Chief of Staff

Photo: Contributor/Getty Images

Sergei Shoigu, Secretary of Russia's National Security Council

Photo: SOPA Images/Getty Images

Igor Kostyukov, Director of the GRU

Photo: Anadolu/Getty Images

Andrey Averyanov, Deputy Director of the GRU

Photo: Contributor/Getty Images

GRU Unit 29155 is the most well known of these entities. It is also referred to as the 161 Intelligence Specialists Training Centre (Центр подготовки специалистов специального назначения), or 161 Centre. Soviet leaders established the unit in 1963 and brought together human intelligence and special operations personnel. Today, some evidence suggests that the 161 Centre is organized into a headquarters unit, three training units, an operational planning unit, three operational units, a financial and logistical unit, and a supply unit. It deploys personnel to Europe and other locations for active intelligence under partial legalization. For Russia's special services, "legalization" involves the establishment of a cover identity that allows an individual to conduct covert activity in a target country or countries. Depending on the duration of the activity, Russia divides legalization into "full" and "partial" categories. Full legalization generally means that an operator stays in place for an indefinite period of time, while partial legalization assumes a short-term stay and basic levels of scrutiny by the target government's intelligence or law enforcement services.[21]

GRU Unit 29155 was linked to the March 2018 nerve agent poisoning in the United Kingdom of Sergei Skripal, a former GRU officer that had worked for British intelligence and then defected, along with his daughter. The unit was also likely behind the September 2020 poisoning of Russian opposition politician Aleksei Navalny; a campaign to provide money to Taliban-linked militants in Afghanistan to target foreign forces, including potentially U.S. troops; a failed coup attempt in Montenegro in 2016; and the poisoning of Bulgarian arms dealer Emilian Gebrev, his son, and his business manager in 2015.[22]

GRU Unit 54654 is designed to build a network of illegal operatives operating under full legalization. The unit recruits individuals with prior military service or other backgrounds—including foreign students studying at Russian universities. It also recruits contractors through front companies, keeps their names and personally identifiable information out of government records, and embeds its officers in Russian ministries unrelated to defense or in private companies.[23]

There are other GRU organizations involved in subversive activities—particularly cyber operations—such as GRU Unit 26165 (also referred to as Fancy Bear) and GRU Unit 74455 (also referred to as Sandworm).[24] The United States and European Union have sanctioned a wide range of GRU operatives for their involvement in clandestine activity. For example, the European Union sanctioned Nikolay Alexandrovich Korchagin, Vitaly Shevchenko, and Yuriy Fedorovich Denisov from GRU Unit 29155 for their involvement in cyberattacks against Estonia.[25] The United States also sanctioned GRU officer Valery Korovin for his involvement in influence operations targeting the 2024 U.S. presidential election.[26]

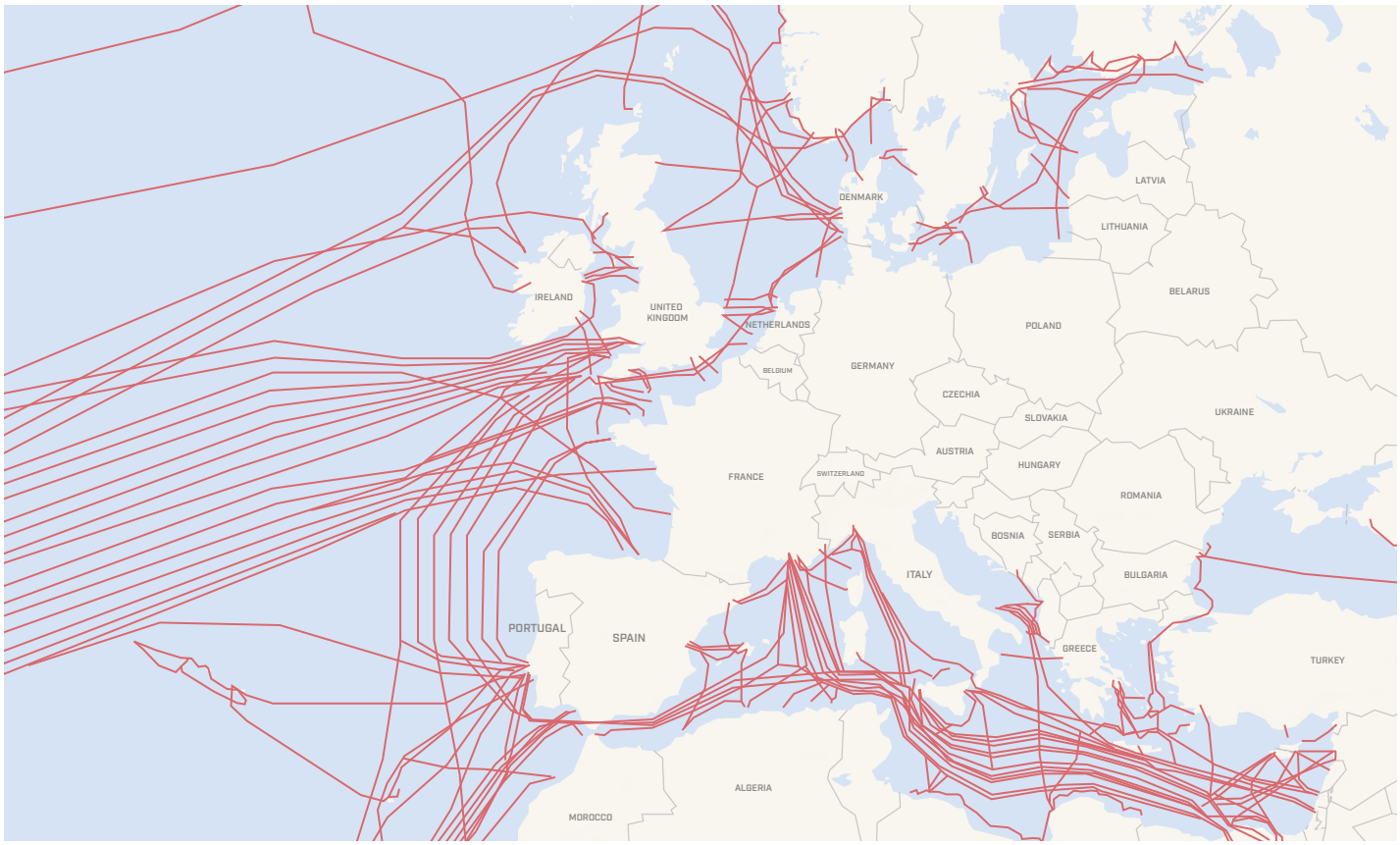
Russia's Foreign Intelligence Service (SVR), the Main Directorate for Deep Sea Research (GUGI), and the FSB have also been involved in active measures in Europe, the United States, and other countries. SVR cyber units, such as Nobelium (also known as Advanced Persistent Threat 29, the Dukes, Cozy Bear, and Midnight Blizzard), have conducted a wide range of cyberattacks against U.S. and European targets.[27] As Microsoft assessed in one attack, their cyber analysts identified "Russian threat actor Midnight Blizzard sending a series of highly targeted spear-phishing emails to individuals in government, academia, defense, non-governmental organizations, and other sectors."[28] The SVR's Nobelium unit was involved in the massive data breach of SolarWinds, a company based in Austin, Texas, that made network monitoring software. The SolarWinds supply chain attack gave Russia the ability to spy on and disrupt more than 18,000 computer systems across the globe, including in the U.S. Departments of Commerce, State, Defense, and the Treasury.[29]

GUGI is a secretive Russian agency belonging to the Russian Ministry of Defense that operates submarines and vessels that can engage in sabotage, such as cutting undersea fiber-optic cables, collecting intelligence, and conducting other operations.[30] There are currently 16 cables running under the Atlantic that connect the United States with mainland Europe. They are primarily operated by such companies as Google, Microsoft, France's Alcatel Submarine Networks, and China's Huawei Marine Networks. Submarine cables are critical for global communication and account for roughly 95 percent of all transatlantic data traffic. These cables are vulnerable to subversion and sabotage, even from the anchors on ships.[31] When ships drag anchors on the bottom of the seabed, it can either completely sever cables or cause partial damage that over time leads to deterioration—and ultimate failure—of the cable.[32] As a result, Russia does not even need to use GUGI's specialized equipment to disrupt these cables.

EUROPEAN VOICES

- Richard Moore, head of MI6, the United Kingdom's foreign intelligence agency: "We have recently uncovered a staggeringly reckless campaign of Russian sabotage in Europe, even as Putin and his acolytes resort to nuclear saber-rattling, to sow fear about the consequences of aiding Ukraine, and challenge Western resolve in so doing."[33]
- Ken McCallum, head of MI5, the United Kingdom's domestic intelligence agency: "The GRU in particular is on a sustained mission to generate mayhem on British and European streets: we've seen arson, sabotage and more. Dangerous actions conducted with increasing recklessness."[34]
- Anne Keast-Butler, director of GCHQ, the United Kingdom's main cyber agency: The United Kingdom "is increasingly concerned about growing links between the Russian intelligence services and proxy groups to conduct cyber attacks—as well as physical surveillance and sabotage operations."[35]
- Thomas Haldenwang, head of the Federal Office for the Protection of the Constitution, or BfV, Germany's domestic intelligence agency: "We have been observing aggressive actions by the Russian intelligence services for some time now. Russia is using the entire toolbox, from influencing political discussions to cyber attacks on critical infrastructure to sabotage on a significant scale."[36]
- Bruno Kahl, head of the Bundesnachrichtendienst, or BND, German's foreign intelligence agency: "Whether we like it or not, we are in direct confrontation with Russia."[37]
- Donald Tusk, prime minister of Poland, "Russia was planning acts of air terror, not only against Poland but against airlines around the world."[38]
- An analysis by the Polish Ministry of Foreign Affairs: "The Russian Federation is waging a hybrid war against Poland. This includes cyberattacks and assaults at Poland's eastern frontier, which is also the Schengen areas' border."[39]
- Radoslaw Sikorski, Polish foreign minister: "I have information that the Russian Federation is behind sabotage attempts both in Poland and allied countries."[40]
- Tomasz Siemoniak, Polish interior minister, "We are facing a foreign state that is conducting hostile and—in military parlance—kinetic action on Polish territory. There has never been anything like this before."[41]
- An analysis by NATO: "NATO Allies are deeply concerned about recent malign activities on Allied territory, including those resulting in the investigation and charging of multiple individuals in connection with hostile state activity affecting Czechia, Estonia, Germany, Latvia, Lithuania, Poland, and the United Kingdom. These incidents are part of an intensifying campaign of activities which Russia continues to carry out across the Euro-Atlantic area, including on Alliance territory and through proxies. This includes sabotage, acts of violence, cyber and electronic interference, disinformation campaigns, and other hybrid operations. NATO Allies express their deep concern over Russia's hybrid actions, which constitute a threat to Allied security."[42]
- Vice Admiral Nils Andreas Stensoenes, head of the Norwegian Intelligence Service (NIS): "The risk level has changed. We believe sabotage is more likely, and we see acts of sabotage happening in Europe now which indicate that they (the Russians) have moved a bit on that scale."[43]
- Kaja Kallas, prime minister of Estonia: "There's a shadow war going on against our societies. The aim of Russia's influence operations is to influence our democratic decision making. By making these events public, we raise awareness so that these operations would not have the effect Russia is hoping for."[44]

Figure 1: European Underwater Fiber-Optic Cables



Source: "Submarine Cable Map 2022," Telegeography, https://submarine-cable-map-2022.telegeography.com/ (CC BY-SA 4.0 DEED); and "How Can We Protect the Internet's Undersea Cables?," World Economic Forum, November 4, 2015, https://assets.weforum.org/wp-content/uploads/2015/11/151104-submarine-cablesinternet-worldmap.png.

Finally, Russia uses a wide range of non-state or quasi-state actors to conduct active measures. The significant expulsion of Russian spies from Europe since 2022 has, in part, forced Moscow to rely on other networks, though governments have long used non-state or quasi-state entities for actions below the threshold of conventional warfare. One example is criminal organizations.[45] As Ken McCallum, head of MI5, explained, "The more eye-catching shift this year has been Russian state actors turning to proxies for their dirty work, including private intelligence operatives and criminals from both the UK and third countries."[46] In addition, the GRU and other Russian organizations have frequently relied on local recruits, sometimes referred to as "disposable agents."[47] In some cases, Russia has recruited these individuals on Telegram channels, through chat functions of popular online games, or through other online locations.[48] The GRU and other organizations have recruited Russian-speaking, and on some occasions technologically savvy, young men between 20 and 30 years old. Some may be ideologically motivated and support Russia, while others may simply do it for the money.[49]

Russia has also used commercial ships, including its "shadow fleet," to conduct active measures such as sabotage.[50] The shadow fleet emerged as a way for Russia to circumvent Western-imposed sanctions on Russian oil transported by sea. To skirt the restrictions, the Kremlin invested billions of dollars in a fleet of tankers whose ownership is difficult to trace to Russia. Many sail under the flags of other nations—such as Gabon, Liberia, the Marshall Islands, and Panama—and sell to buyers in countries like China and India.[51] According to one assessment, approximately 70 percent of Russia's oil is being transported by so-called shadow tankers.[52] Russia has used other civilian vessels for intelligence collection and sabotage, including its vast commercial fishing fleet and marine research ships. Some of the ships are relatively modern, longer than 300 feet, and equipped with sonar and other technology that allows them to scan the seabed. Such vessels have mapped critical subsea infrastructure around Europe and identified potential targets.[53]

RUSSIAN ACTIONS

Russia has conducted a wide range of active measures in Europe. This section is divided into four areas: (1) overall trends, (2) targets, (3) weapons, and (4) geographic area. It relies on several data sources. The first is a CSIS database of Russian subversive actions between January 2022 and March 2025, including date, location, target, weapon type, and other information. The data cover Russian attacks and plots that had (or were intended to have) physical effects, such as weapons and tactics using explosives, other incendiaries, firearms, and anchors for cutting undersea fiber-optic cables. Attribution is always difficult for active measures. To be included in the database, CSIS identified at least three credible sources for the direct or indirect involvement of the Russian government, interviewed government and non-government experts, and asked several experts to review the data and analysis. In addition, CSIS assessed the level of confidence for each incident.[54]

The CSIS database excluded several types of activities. For example, most Russian cyber operations were excluded. It is virtually impossible to build a comprehensive unclassified database of cyber operations, since cyberattacks do not necessarily have a physical effect (such as a warehouse blowing up, an individual assassinated, or a cable cut) and the targets (such as foreign government agencies and companies) have numerous incentives *not* to publicly acknowledge the attacks. In addition, Russia and other state actors frequently perpetrate cyber operations to collect intelligence, not necessarily to impose a cost on a foreign state or other entity. However, the CSIS database did include those incidents where Russian cyber or electronic warfare attacks had an observable physical effect. These types of attacks are designed to disrupt critical infrastructure, such as power grids, water systems, and transportation networks that can lead to power outages, disruptions, or physical harm.

The CSIS database also excluded Russian disinformation campaigns, such as election interference and efforts to sow discord or otherwise influence the populations or governments in Europe, the United States, and other locations. Much like cyberattacks, it is virtually impossible to build a comprehensive unclassified database of information or influence campaigns since attacks frequently do not have a physical effect and the targets have numerous incentives not to publicly acknowledge the attacks. Nevertheless, Moscow has developed an aggressive campaign to interfere with democratic elections in individual countries and European Parliament elections, co-opt politicians for elite capture, and spread disinformation.[55] As noted previously in this analysis, the Soviet Union and such organizations as the KGB have a rich history of disinformation campaigns and other active measures.

OVERALL TRENDS IN ATTACKS

The most significant finding from the data is that the number of Russian attacks in Europe nearly tripled between 2023 (12 attacks) and 2024 (34 attacks), after quadrupling between 2022 (3 attacks) and 2023. As noted in more detail below, Russian agencies orchestrated attacks in 2024 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.

What factors caused this dramatic increase? While it is difficult to know with certainty, there are likely several factors.

First, it appears that Russia made a strategic decision to escalate its shadow war in Europe in response to U.S. and European aid to Ukraine. Many of the targets were linked to Ukraine in some capacity. Examples range from a Russian military defector assassinated in Spain to a series of companies—such as BAE Systems, Rheinmetall, German Diehl Group, and EMCO—that produce weapons for Ukraine. As a Norwegian intelligence assessment concluded, one of the primary Russian targets in Norway includes "actors involved in arms donations and the training of Ukrainian personnel. They are especially at risk of being targeted because arms deliveries could have a direct impact on the battlefield in Ukraine."[56] There were also no recorded incidents against several countries that did not provide significant aid to Ukraine, such as Hungary and Serbia, which suggests that Moscow was deliberate in where it conducted attacks—as well as where it did *not* conduct attacks.

Second, Russia may have increased its attack tempo because there were few, if any, costs for its actions. Russian leaders knew they could get away with attacks—including an escalation in attacks—without paying a major price.

TARGETS

Russia's most frequent targets in Europe were in the transportation sector (27 percent), such as trains and airplanes (including through GPS jamming), and against government targets (27 percent), such as government officials, military bases, and border crossings. Russia also conducted attacks on critical infrastructure (21 percent), such as pipelines and undersea fiber-optic cables, and industry (21 percent), such as defense companies.

Figure 2: Targets of Russian Attacks in Europe, 2022–2025

Source: CSIS analysis.

Maritime, land, and air transportation targets were a major focus of Russian active measures. Germany experienced a railway cable-cutting attack in 2022. In addition, Russia conducted multiple attacks against Poland's rail system.[57] Russia also targeted airplanes through electronic attack.

Critical infrastructure attacks were also a focus of Russian operations, including undersea cables and pipelines. Finnish investigators assessed that the *Newnew Polar Bear*, a Chinese-registered ship operated by a Russian crew, damaged two subsea data cables and a gas pipeline in the Baltic Sea with its anchor. The ship was trailed by the *Sevmorput*, a nuclear-powered merchant ship owned by the Russian government.[58] In addition, the *Eagle S*, an oil tanker, apparently dragged its anchor and damaged a cable in the Gulf of Finland.[59] The *Vezhen*, a Maltese-flagged ship, damaged an undersea fiber-optic cable linking Latvia and Sweden. Armed police parachutists from Sweden promptly boarded the ship.[60] Finally, the Chinese ship *Yi Peng 3*, which had a Russian captain, cut an undersea cable on its journey through the Baltic Sea.[61]

The use of some Chinese cargo ships, with Russian crew, is noteworthy because China has also engaged in attacks against Taiwan's undersea fiber-optic cables.[62] Taiwan has approximately 14 international underwater submarine cables and 10 domestic ones, as well as limited satellite access in low Earth orbit, making it vulnerable to a subversive campaign. In January 2025, for example, a Chinese-owned vessel cut an undersea fiber-optic cable near Taiwan's Keelung Harbor.[63] While it is unclear to what degree Russia and China have cooperated and shared lessons, both countries have adopted a similar tactic (the use of commercial vessels) against similar targets (undersea cables and pipelines).

Private industry, especially the defense industry, was also a common target of Russian activity. The two largest European donors of military aid to Ukraine—Germany and the United Kingdom—experienced attacks on numerous defense manufacturing plants.[64] In May 2024, for example, a major fire broke out at a Diehl Group factory in Berlin, which manufactures IRIS-T surface-to-air missiles used in Ukraine.[65] A month earlier, there was an explosion at a weapons manufacturing site in South Wales belonging to BAE Systems, the United Kingdom's largest arms manufacturer, which has supplied ammunition, weapons, and other defense equipment to Ukraine.[66] A BAE investigation into the incident found no evidence of sabotage.

Russian sabotage occurred in other countries as well. There was an explosion linked to Russian services at a warehouse in Spain that stored communications equipment bound for Ukraine.[67] Less than a year earlier, 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.[68]

Russia also targeted several types of individuals that cut across government and industry sectors: corporate executives, including ones involved in supplying weapons and other matériel to Ukraine; journalists that investigated Russian activity; Russian defectors to the West, including a Russian soldier; and Ukrainian officials. Several were assassination plots that failed: one in Poland targeting Ukrainian President Volodymyr Zelensky; one in Austria against Bul-

garian investigative journalist and director of the Bellingcat investigative reporting group Christo Grozev; and one in Germany targeting Armin Papperger, the chief executive officer of Rheinmetall, a large producer of artillery and tanks that had sent shells to Ukraine.[69] The assassination plot against Papperger was one of the first instances in which Russia attempted to take lethal action against a Western citizen who had no previous connection to Moscow.[70]

There were several other attacks against individuals. One was the assassination in Spain of Maksim Kuzminov, a Russian helicopter pilot who defected from Russia in August 2023. Another was the 2024 assault in Lithuania on Leonid Volkov, a Russian citizen and former close aide of now-deceased Russian opposition leader Alexei Navalny. The assailants, who Lithuanian intelligence assessed were likely "Russian organized," broke Volkov's arm but failed to kill him.[71] Another incident involved the vandalization of a car belonging to Estonian Minister of the Interior Lauri Läänemets.[72]

In addition, German prosecutors charged three Russian-German nationals—Dieter Schmidt, Alexander J., and Alex D.—with acting as secret service agents for Russia and plotting bombing and arson attacks against U.S. military bases in Germany. Dieter Schmidt also allegedly participated in other sabotage operations, including taking pictures of military installations with an aim to endanger national security.[73] The U.S. bases had connections to Ukraine. At the U.S. base in Grafenwoehr, Germany, Ukrainian troops were being trained to operate M1 Abrams tanks.[74]

TACTICS AND WEAPONS

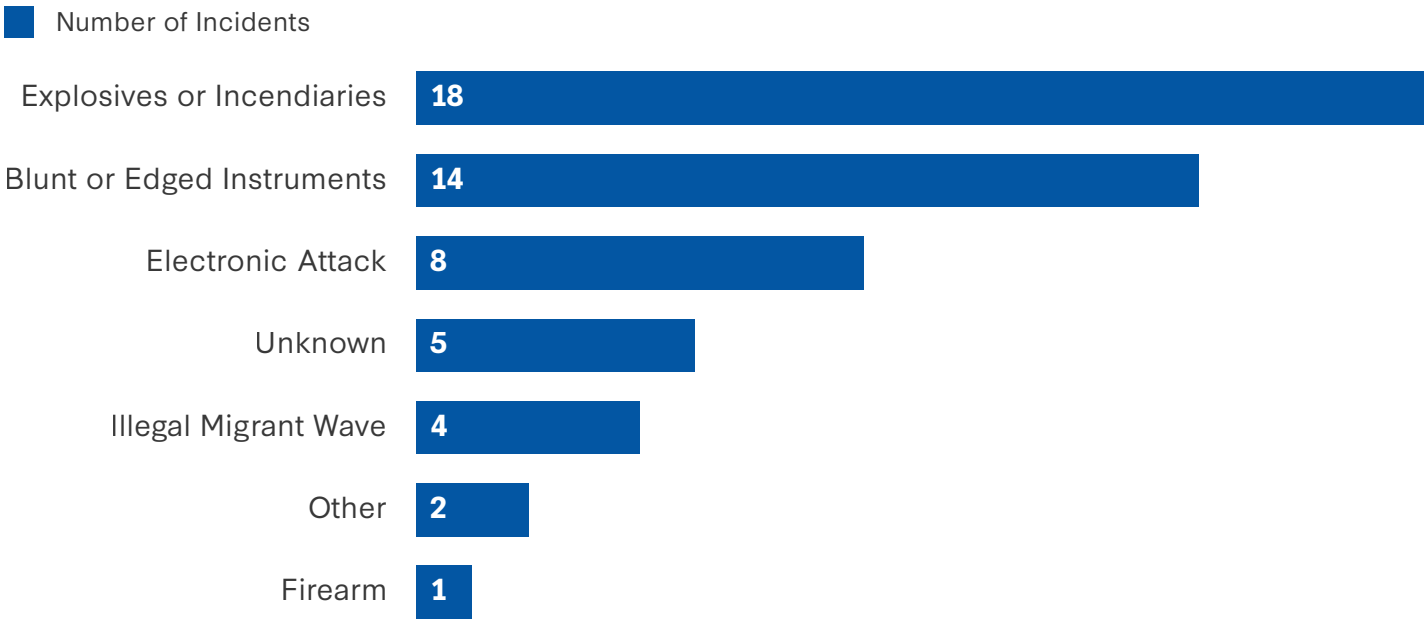
The most frequent type of weapon used in Russia's shadow war were explosives or incendiaries (35 percent), including bombs; blunt or edged instruments (27 percent), such as anchors; and electronic attack (15 percent). The next most common were the weaponization of illegal immigrants (8 percent) and the use of firearms (2 percent). Russia's use of weapons that kill, injure, or destroy property suggests that Moscow seeks to send a clear message to deter or coerce behavior, such as sending weapons to Ukraine. But the attacks had few casualties, indicating that Russia wants to keep the costs low and maximize deniability. The low level of violence has also allowed Moscow to escalate if necessary.

One of the most innovative weapons in Russian attacks was the use of electric massagers implanted with a magnesium-based flammable substance that exploded at DHL logistics hubs in 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.[75]

Captain Maksim Kuzminov, a Russian helicopter pilot, defected to Ukraine in August 2023. Russian operatives likely assassinated Kuzminov in Spain in February 2024.

Photo: NurPhoto/Getty Images

Figure 3: Weapons Used in Russian Attacks in Europe, 2022–2025



Source: CSIS analysis.

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."[76] German police who tested models of the incendiary devices noted that that once the magnesium ignited, it would have been difficult to extinguish with the firefighting systems on most airplanes.[77] Fires also targeted warehouses and other targets across Europe, from the United Kingdom to Poland.[78]

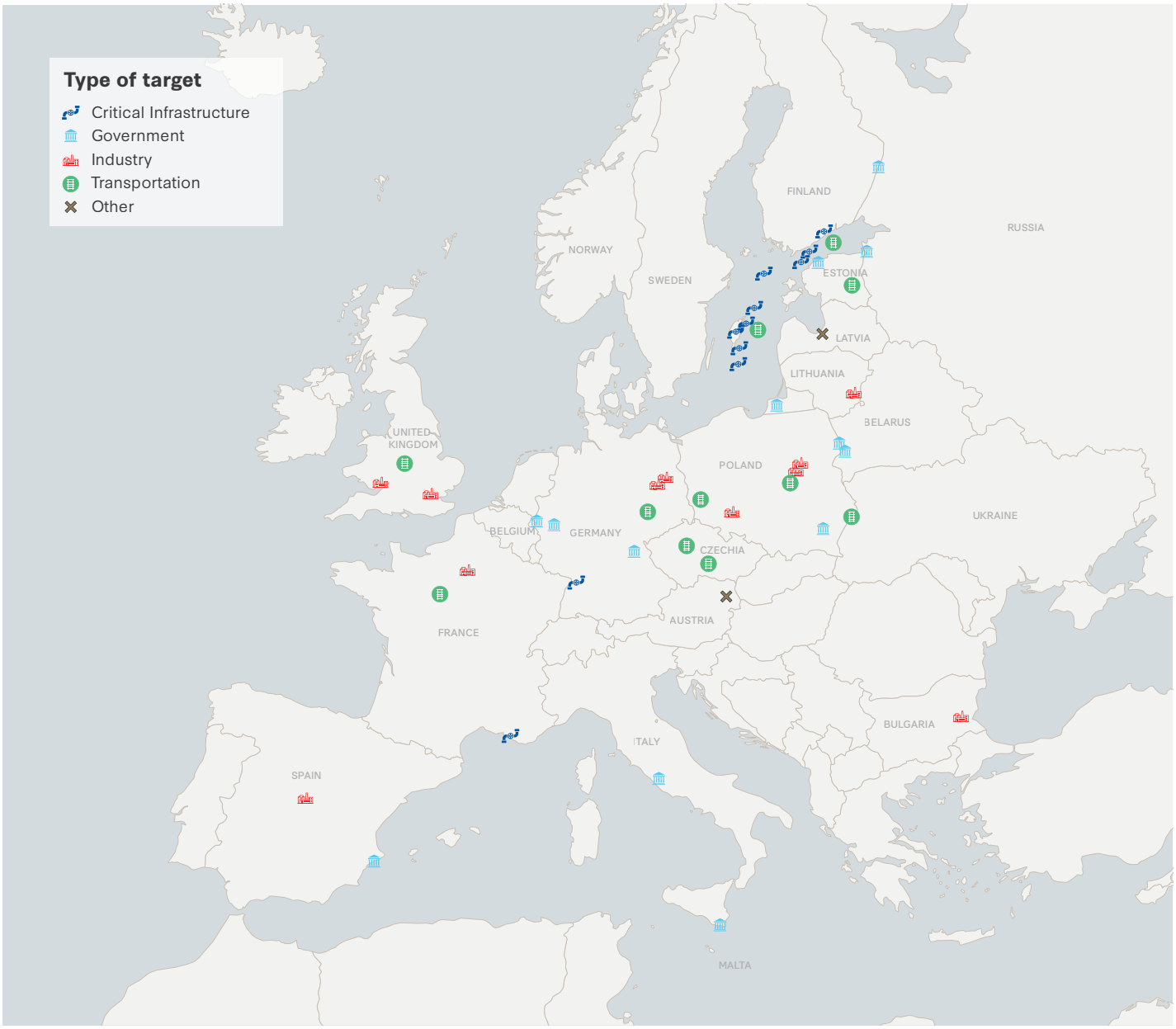
Russian agencies utilized electronic attack and cyber operations with physical effects against transportation targets. Estonia, Finland, Lithuania, Norway, and Poland all reported specific incidents of deliberate GPS signal jamming from Russia, which led to navigation errors, flight deviations, and communication breakdowns—endangering the lives of those on board.[79] Several countries, such as Poland, also reported cyberattacks against transportation targets, such as rail lines. More broadly, Russian-linked actors conducted hundreds of cyberattacks against targets in Europe, the United States, and other regions to collect intelligence, deface websites, orchestrate a denial of service, and occasionally conduct sabotage, according to a broader CSIS database of cyber incidents between 2006 and 2025 where losses were greater than a million dollars.[80]

Finally, Russia and Belarus weaponized illegal immigrants against several border countries, such as Finland, Latvia, Lithuania, Norway, and Poland. In 2021, Belarusian leader Alexander Lukashenko threatened to "flood" the European Union with "drugs and migrants," and then his government sent thousands of migrants from Iraq and other countries to the borders of Latvia, Lithuania, and Poland in 2021 and 2022.[81] In November 2023, Finland closed its border with Russia following a surge of border crossings instigated by Russia; 900 third-country nationals arrived in Finland without valid documentation in November alone. In the summer of 2024, Poland experienced a surge to nearly 400 illegal border crossings a 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.[82]

GEOGRAPHIC AREA

Russia conducted attacks throughout Europe, as indicated in Figure 4. However, the attacks were largely concentrated in NATO's eastern flank, such as Estonia, Finland, Latvia, Lithuania, and Poland, as well as waters like the Baltic Sea. In addition, Russia targeted countries that supplied weapons or other matériel to Ukraine or sheltered Russian defectors, such as Bulgaria, France, Germany, Spain, and the United Kingdom. There were no recorded attacks against countries with closer relations with Russia, such as Hungary or Serbia. Russia also did not conduct attacks against several other European states, such Greece, Portugal, Romania, and Switzerland.[83]

Figure 4: Geographic Area of Russian Attacks, 2022–2025



Source: CSIS analysis.

GOING ON OFFENSE

Russian active measures are not just a European problem, but a U.S. problem as well. The GRU and other organizations have plotted attacks against U.S. bases in Europe, including in Germany, and mapped undersea transatlantic fiberoptic cables that connect the United States and Europe. In addition, Russian military and intelligence agencies have also conducted offensive cyberattacks, disinformation, and other active measures against the United States both at home and abroad.

Russia's escalation of its shadow war indicates a Western failure to impose sufficient costs on Moscow. Some European leaders have refrained from attributing attacks to Moscow because they fear further escalation.[84] The United States and European countries have largely focused on defensive measures to deter or counter Russian actions. Examples include:

- Increasing intelligence sharing among Western military, intelligence, and law enforcement agencies.[85] In February 2023, for instance, NATO created an Undersea Infrastructure Coordination Cell to assess vulnerabilities and coordinate efforts between NATO governments and the private sector.

- Heightening patrols and surveillance. NATO established the Baltic Sentry operation to protect underwater cables and pipelines by enhancing the alliance's surface, sub-surface, and air presence in strategic locations. The operation involved frigates, maritime patrol aircraft, submarine satellites, remotely operated vehicles, drones, and other surveillance assets.[86]
- Strengthening national resilience by hardening critical infrastructure, including protecting oil and gas pipelines, warehouses, and cyber networks. For example, the European Union and NATO established an EU-NATO Task Force on Resilience of Critical Infrastructure.[87] Several countries, such as Finland, Sweden, the Baltic states, and Poland, have also adopted measures to strengthen resilience.

In addition, there have been some actions designed to impose costs on Russia. Examples include:

- Closing Russian consulates, such as the one in Poznan, Poland.[88]
- Expelling Russian government officials, including over 750 diplomats and intelligence officials between February 2022 and October 2024.[89]
- Denying diplomatic visa applications to potential Russian spies.[90]
- Arresting and prosecuting perpetrators of attacks, such as Dylan Earl for allegedly sabotaging Ukrainian businesses in east London, Alexander Suranovas (also known as Igor Prudnikov) for his apparent involvement in the DHL bombing plot, Dieter Schmidt and his colleagues for plotting bombing and arson attacks against U.S. bases in Germany, alleged GRU operative Mikhail Mikushin (also known José Assis Giammaria) who was arrested by Norway for subversive activities, and Siergey S. for his apparent involvement in arson attacks in Poland.[91]
- Closing borders, such as the decision by Finland in November 2023 to close its 830-mile (1,340-kilometer) border with Russia in part because of Russia's weaponization of illegal immigrants.
- Imposing limited sanctions on individuals, companies, and other perpetrators of active measures. 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.[92]

Defense is necessary, but not sufficient. These actions are not particularly costly for Russia and are unlikely to coerce Moscow into ending, or even reducing, its active measures. Western countries have decided not to impose more significant costs for several reasons. First, some leaders have worried that a more robust response would cause further Russian escalation. As one analysis concluded, "Western leaders are reluctant to call for a larger military response to these attacks, which could trigger uncontained escalation."[93] Second, some have opposed a more robust response because they argue that the West is not "at war" with Russia. As one assessment summarized, "the West may be limited in the kinds of counteroperations it can launch in the face of continued acts of Russian sabotage. For one thing, the United States and its allies cannot easily respond in kind, because they are not officially at war with Russia."[94]

Unlike authoritarian countries such as Russia, this logic assumes that democratic countries cannot—or should not—conduct forceful actions against Russia because they are not involved in a declared war. Yet these concerns are largely fallacious, and they reflect a mindset of self-deterrence. Russia, not Europe or the United States, chose to escalate a shadow war in Europe. In fact, a failure to respond will likely increase the likelihood of a protracted Russian campaign.

Instead, NATO should complement these defensive measures with a calibrated *offensive* campaign that focuses on several elements. These actions could be integrated into broader negotiations on a peace deal with Ukraine, in which the United States or European countries threaten—either implicitly or explicitly—offensive measures if Russia continues its sabotage campaign.

First, NATO should develop and communicate a clearer strategy that involves ramping up sanctions to stop Moscow's shadow war in Europe. This approach might include increasing secondary sanctions against countries that import Russian goods, including oil and gas, as well as sanctioning additional entities and individuals involved in illegal Russian exports.

Second is an increase in NATO covert and overt actions. For example, Russia's shadow fleet, which is illegally shipping oil and gas to overseas markets, is vulnerable to seizure. Russia also has oil and gas pipelines that are vulnerable to sabotage.

Third is conducting targeted offensive cyber operations against important Russian military and commercial targets, including the networks of Russia's energy sector that are vital to Russia's economy. There was some reporting that U.S. Cyber Command briefly halted offensive cyber operations against Russia in an effort to draw President Putin into talks on Ukraine, though some Pentagon officials denied these reports.[95] Offensive cyber operations against Russia remain an important stick that can be used if Russian sabotage and subversion continues.

Fourth, NATO countries should conduct a more aggressive offensive information campaign targeting the populations of Russia and its partners, such as Belarus, devised to counter state-run media.

An offensive campaign should be designed to signal to Moscow that continued active measures in Europe will be costly. In short, a successful Western campaign needs to be coercive to change Moscow's behavior, and the pain has to appear contingent on Russian behavior. But a strategy that does not include raising the costs on Moscow is likely to fail. ■

This report was updated on March 20, 2025, to reflect findings from an internal investigation conducted by BAE Systems on the 2024 explosion at its weapons manufacturing site in South Wales.

Seth G. Jones *is president of the Defense and Security Department at the Center for Strategic and International Studies in Washington, D.C.*

The author wishes to thank Katherine Trauger, Iselin Brady, and Riley McCabe for their help in building the database and for other research assistance during the research, writing, and production phases. Thanks also to Daniel Byman and Philip Wasielewski for their reviews of the document and outstanding comments.

This brief was made possible through general funding to CSIS.

ENDNOTES

1. On other databases, see 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/.
2. See, for example, Max Boot, *Invisible Armies: An Epic History of Guerrilla Warfare from Ancient Times to the Present* (New York: W.W. Norton, 2013).
3. On irregular warfare, see U.S. Department of Defense, *Summary of the Irregular Warfare Annex to the National Defense Strategy* (Washington, DC: U.S. Department of Defense, 2020), https://media.defense.gov/2020/Oct/02/2002510472/-1/-1/0/Irregular-Warfare-Annex-to-the-National-Defense-Strategy-Summary.PDF; Charles T. Cleveland, *The American Way of Irregular Warfare: An Analytical Memoir* (Santa Monica, CA: RAND, 2020), https://www.rand.org/pubs/perspectives/PEA301-1.html; and David H. Ucko and Thomas A. Marks, *Crafting Strategy for Irregular Warfare: A Framework for Analysis and Action* (Washington, DC: National Defense University Press, July 2020). On hybrid warfare, see, for example, NATO, *Hybrid Threats and Hybrid Warfare: Reference Curriculum* (Brussels: NATO Headquarters, June 2024); and "Countering Hybrid Threats," European Commission, March 2022, https://defence-industry-space.ec.europa.eu/document/download/3b90af44-dbf6-4ea7-a24a-b6c60305c9be_en?filename=Factsheet%20-%20Countering%20Hybrid%20Threats.pdf.
4. See, for example, Hal Brands, *The Twilight Struggle: What the Cold War Teaches Us about Great-Power Rivalry Today* (New Haven: Yale University Press, 2022); Kathleen H. Hicks et al., *By Other Means, Part I: Campaigning in the Gray Zone* (Washington, DC: CSIS, 2019), https://www.csis.org/analysis/other-means-part-i-campaigning-gray-zone; Tim Weiner, *The Folly and the Glory: America, Russia, and Political Warfare 1945-2020* (New York: Henry Holt, 2020); Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020); Linda Robinson et al., *Modern Political Warfare: Current Practices and Possible Responses* (Santa Monica, CA: RAND 2018), https://www.rand.org/pubs/research_reports/RR1772.html; Frank G. Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges," National Defense University, *PRISM*, vol. 7, no. 4, 2018, 31–47, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1983462/examining-complex-forms-of-conflict-gray-zone-and-hybrid-challenges/; George F. Kennan, "Organizing Political Warfare," April 30, 1948, History and Public Policy Program Digital Archive; and Hal Brands and Toshi Yoshihara, "How to Wage Political Warfare," *National Interest*, December 16, 2018, https://nationalinterest.org/feature/how-wage-political-warfare-38802.
5. See, for example, Seth G. Jones, *Three Dangerous Men: Russia, China, Iran, and the Rise of Irregular Warfare* (New York: W.W. Norton, 2021); Hicks, *By Other Means;* and Robinson, *Modern Political Warfare*.
6. See, for example, Christopher Andrew and Vasili Mitrokhin, *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB* (New York: Basic Books, 1999); and Rid, *Active Measures*.
7. Soviet Covert Action (the Forgery Offensive), Hearings before the Subcommittee on Oversight of the Permanent Select Committee on Intelligence, U.S. House of Representatives, 96th Cong. (February 1980) (statement of John McMahon, Deputy Director for Operations, Central Intelligence Agency), https://books.google.com/books?id=Wbq13FASztIC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false.
8. Statement of Ladislav Bittman, Former Deputy Chief of the Disinformation Department of the Czechoslovak Intelligence Service, "Soviet Covert Action (The Forgery Offensive)," Hearings Before the Subcommittee on Oversight of the Permanent Select Committee on Intelligence, U.S. House of Representatives (Washington, DC: U.S. Government Printing Office, 1980), 43–44.
9. "KGB Active Measures in Southwest Asia in 1980-82," Wilson Center Digital Archive, Contributed to CWIHP by Vasili Mitrokhin and first published in CWIHP Bulletin 14/15, April 2004, https://digitalarchive.wilsoncenter.org/document/110013.
10. See, for example, Лата В. Ф., Анненков В. А., Моисеев В. Ф. [V.F. Lata, V.A. Annenkov, V.F. Moiseev], Информационное противоборство: система терминов и определений [Information Confrontation: A System of Terms and Definitions], Вестник Академии военных наук [*Bulletin of the Academy of Military Sciences*], No. 2, 2019; and Ben Taub, "Russia's Espionage War in the Arctic," *New Yorker*, September 9, 2024, https://www.newyorker.com/magazine/2024/09/16/russias-espionage-war-in-the-arctic.
11. "The North Atlantic Treaty," NATO, April 4, 1949, https://www.nato.int/cps/en/natohq/official_texts_17120.htm.
12. Norwegian Police Security Service (PST), *National Threat Assessment 2024* (Oslo: PST, 2024), 23, https://www.pst.no/globalassets/2024/nasjonal-trusselvurdering-2024/nasjonal-trusselvurdering-2024_engelsk_web_.pdf.
13. Anne Kauranen, "Baltic Sea Sabotage Crew Were Poised to Cut More Cables When Caught, Finland Says," Reuters, January 15, 2025, https://www.reuters.com/world/europe/oil-tanker-sabotage-crew-were-poised-cut-more-cables-when-caught-finland-says-2025-01-13/; and John Grady, "Finland Seizes Russian Oil Tanker After Suspected Undersea Fiber-Optic Cable Sabotage," USNI News, December 27, 2024, https://news.usni.org/2024/12/27/finland-seizes-russian-oil-tanker-after-suspected-undersea-fiber-optic-cable-sabotage.
14. See, for example, Philip Wasielewski, "Modern Russian Statecraft: Neither New Nor Hybrid, Part One," *Small Wars Journal*, December 12, 2021, https://smallwarsjournal.com/2021/12/12/modern-russian-statecraft-neither-new-nor-hybrid-part-one/; and Philip Wasielewski, "Modern Russian Statecraft: Neither New Nor Hybrid, Part Two," *Small Wars Journal*, January 21, 2022, https://smallwarsjournal.com/2022/01/21/modern-russian-statecraft-neither-new-nor-hybrid-part-two-post-soviet-and-still-soviet/.

15. Ken McCallum (speech, Counter Terrorism Operations Center, London, October 8, 2024), https://www.mi5.gov.uk/director-general-ken-mccallum-gives-latest-threat-update.

16. "DCIA William Burns and MI6 Chief Richard Moore," Central Intelligence Agency, September 7, 2024, https://www.cia.gov/static/DCIA_Bill_Burns_MI6_Chief_Richard_Moore_with_FT_Editor_Roula_Khalaf_Transcript.pdf.

17. See, for example, Daniel Byman and Sarah E. Kreps, "Agents of Destruction? Applying Principal-Agent Analysis to State-Sponsored Terrorism," *International Studies Perspectives* 11, no. 1 (February 2010): 1-18, https://doi.org/10.1111/j.1528-3585.2009.00389.x; Idean Salehyan, Kristian Skrede Gleditsch, and David Cunningham, "Explaining External Support for Insurgent Groups," *International Organization* 65, no. 4 (Fall 2011): 709–744, https://www.cambridge.org/core/journals/international-organization/article/abs/explaining-external-support-for-insurgent-groups/5BD53FA2D095F6B6283AEEC6DF895DDE; Darren G. Halkins et al., eds., *Delegation and Agency in International Organizations* (New York: Cambridge University Press, 2006); and Idean Salehyan, "The Delegation of War to Rebel Organizations," *Journal of Conflict Resolution* 54, no. 3 (2010): 493–515, https://www.jstor.org/stable/27820997.

18. Rid, *Active Measures*, 330.

19. Watling, Danylyuk, and Reynolds, *The Threat from Russia's Unconventional Warfare*, 8; and "Russian Spies Are Back—and More Dangerous Than Ever," *The Economist*, February 24, 2024, https://www.economist.com/international/2024/02/20/russian-spies-are-back-and-more-dangerous-than-ever.

20. Watling, Danylyuk, and Reynolds, *The Threat from Russia's Unconventional Warfare*; "Russian Spies Are Back—and More Dangerous Than Ever," *The Economist*; and Mark Krutov, Sergei Dobrynin, Mike Eckel, and Carl Schreck, "Russian Wedding Photos Highlight Novichok Suspect's Security Ties," Radio Free Europe/Radio Liberty, October 14, 2019, https://www.rferl.org/a/member-of-the-wedding-russian-nuptials-highlight-novichok-suspect-s-intelligence-ties/30216231.html.

21. Michael Weiss, Christo Grosev, and Roman Dobrokhotov, "The Enemy Within: How Russia's GRU Agents Blend in with Human Rights Activists, Journalists, and Filmmakers," *The Insider*, February 4, 2024, https:// theins.ru/en/politics/268886; and Watling, Danylyuk, and Reynolds, *The Threat from Russia's Unconventional Warfare*.

22. Author interviews with U.S. and European officials, 2024 and 2025.

23. Watling, Danylyuk, and Reynolds, *The Threat from Russia's Unconventional Warfare*, 9-11; and "Russian Spies Are Back—and More Dangerous Than Ever," *The Economist*.

24. National Cyber Security Centre, "UK and Allies Uncover Russian Military Unit Carrying Out Cyber Attacks and Digital Sabotage for the First Time," press release, September 5, 2024, https://www.ncsc.gov.uk/news/uk-allies-uncover-russian-military-carrying-out-cyber-attacks-digital-sabotage.

25. 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, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202500171.

26. U.S. Department of the Treasury, "Treasury Sanctions Entities in Iran and Russia That Attempted to Interfere in the U.S. 2024 Election," press release, December 31, 2024, https://home.treasury.gov/news/press-releases/jy2766.

27. See, for example, "Joint Cybersecurity Advisory," U.S. Federal Bureau of Investigation (FBI), U.S. Cybersecurity & Infrastructure Security Agency (CISA), U.S. National Security Agency (NSA), Polish Military Counterintelligence Service (SKW), CERT Polska (CERT.PL), and the UK National Cyber Security Centre (NCSC), December 13, 2023, https://www.cisa.gov/sites/default/files/2023-12/aa23-347a-russian-foreign-intelligence-service-svr-exploiting-jetbrains-teamcity-cve-globally_0.pdf.

28. "Midnight Blizzard Conducts Large-Scale Spear-Phishing Campaign Using RDP Files," Microsoft, October 29, 2024, https://www.microsoft.com/en-us/security/blog/2024/10/29/midnight-blizzard-conducts-large-scale-spear-phishing-campaign-using-rdp-files.

29. White House, "Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government," press release, April 15, 2021, https://ru.usembassy.gov/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/; and CISA, "Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency," press release, January 5, 2021, https://www.cisa.gov/news-events/news/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure-security-agency-0.

30. Sidharth Kaushal, "Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure," RUSI, May 25, 2023, https://rusi.org/explore-our-research/publications/commentary/stalking-seabed-how-russia-targets-critical-undersea-infrastructure; and Jim Sciutto, "Exclusive: U.S. Sees Increasing Risk of Russian 'Sabotage' of Key Undersea Cables by Secretive Military Unit," CNN, September 6, 2024, https://www.cnn.com/2024/09/06/politics/us-sees-increasing-risk-of-russian-sabotage-undersea-cables/index.html.

31. Mark Scott, "Will Russia Attack Undersea Internet Cables Next?," *Politico*, September 29, 2022, https://www.politico.eu/article/everything-you-needto-know-about-the-threat-to-undersea-internet-cables/.

32. Ellie Moore "Anchor Damage to Offshore Cables," University of Cambridge, Department of Engineering, May 31, 2017, https://www-geo.eng.cam.ac.uk/system/files/documents/2017MooreE.pdf.

33. Sir Richard Moore (speech, Paris, November 29, 2024), https://www.gov.uk/government/speeches/speech-by-sir-richard-moore-chief-of-sis-29-november-2024.

34. McCallum (speech, Counter Terrorism Operations Center).

35. Pancevski, "Europe Sees Signs."

36. Kayali et al., "Europe Is Under Attack from Russia."

37. "Germany: Spy Chiefs Warn of Increasing Russian Threat," *Deutsche Welle*, October 14, 2024, https://www.dw.com/en/germany-spy-chiefs-warn-of-increasing-russian-threat/a-70493640.

38. Eckel, "A Russian Airline Bomb Plot?"

39. Poland Ministry of Public Affairs, "Minister of Foreign Affairs Decides to Close Russian Consulate in Poznań," press release, October 22, 2024, https://www.gov.pl/web/diplomacy/minister-of-foreign-affairs-decides-to-close-russian-consulate-in-poznan.

40. "Poland Orders Closure of Russian Consulate in Poznan and Expels 10 Employees," Euro News, October 24, 2024, https://www.euronews.com/my-europe/2024/10/24/poland-orders-closure-of-russian-consulate-in-poznan-and-expels-10-employees.

41. "Poland Tightens Ukraine Aid Hub Security Over Sabotage Concerns," Bloomberg, May 23, 2024, https://www.bloomberg.com/news/articles/2024-05-23/poland-tightens-ukraine-aid-hub-security-over-sabotage-concerns.

42. NATO, "Statement by the North Atlantic Council on Recent Russian Hybrid Activities," press release, May 2, 2024, https://www.nato.int/cps/en/natohq/official_texts_225230.htm.

43. Nerijus Adomaitis, "Norway's Spy Chief Sees Russia More Likely to Attempt Sabotage," Reuters, September 11, 2024, https://www.reuters.com/world/europe/norways-spy-chief-sees-russia-more-likely-attempt-sabotage-2024-09-10/.

44. Jim Sciutto, "Estonia Thwarts 'Shadow War' Attack, Prime Minister Kaja Kallas Tells CNN," CNN, February 20, 2024, https://www.cnn.com/2024/02/20/europe/russia-shadow-war-attack-estonia-kallas-intl/index.html.

45. Laura Kayali et al., "Europe Is Under Attack from Russia. Why Isn't It Fighting Back?," *Politico*, November 25, 2024, https://www.politico.eu/article/europe-russia-hybrid-war-vladimir-putin-germany-cyberattacks-election-interference/.

46. McCallum (speech, Counter Terrorism Operations Center).

47. Julian E. Barnes, "Russia Steps Up a Covert Sabotage Campaign Aimed at Europe," *New York Times*, May 26, 2024, https://www.nytimes.com/2024/05/26/us/politics/russia-sabotage-campaign-ukraine.html; and Kayali et al., "Europe Is Under Attack from Russia."

48. 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.

49. Robbie Gramer and Amy Mackinnon, "Russia Ramps Up Sabotage Operations in Europe," *Foreign Policy*, June 13, 2024, https://foreignpolicy.com/2024/06/13/russia-sabotage-attacks-europe-espionage-hybrid-arson/; and Kayali et al., "Europe Is Under Attack from Russia."

50. Norwegian Police Security Service, *National Threat Assessment 2024*, 22.

51. 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.

52. Benjamin Hilgenstock, Anatoliy Kravtsev, Yuliia Pavystska, and Anna Vlaysuk, *Creating "Shadow-Free" Zones: Proposal for the Implementation of an Insurance Requirement to Address Key Environmental Risks* (Kyiv: Kyiv School of Economics, KSE Institute, October 2024), https://kse.ua/wp-content/uploads/2024/10/Shadow_free_zones_October_2024_final.pdf; and Benjamin Hilgenstock, Oleksii Hrybanovskii, and Anatoliy Kravtsev, *Assessing Russia's Shadow Fleet: Initial Build-Up, Links to the Global Shadow Fleet, and Future Prospects* (Kyiv: Kyiv School of Economics, KSE Institute, June 2024), https://kse.ua/about-the-school/news/assessing-russias-shadow-fleet-initial-build-up-links-to-the-global-shadow-fleet-and-future-prospects/.

53. Pancevski, "Europe Sees Signs."

54. Some may wonder whether the increase in Russian attacks was caused by selection bias, such as an increase in public attention (and thus news reporting) of Russian activity. This analysis attempted to correct for such biases by interviewing U.S. and European government officials with detailed knowledge of Russian operations.

55. See, for example, U.S. Helsinki Commission Staff, *Spotlight on the Shadow War*; U.S. Department of Justice, "Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere," press release, September 4, 2024, https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence; and 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.

56. Norwegian Police Security Service, *National Threat Assessment 2024*, 10.

57. 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; and Loveday Morris, "Poland Investigates Train Mishaps for Possible Russian Connection," *Washington Post*, August 28, 2023, https://www.washingtonpost.com/world/2023/08/28/poland-hacking-trains-russia/.

58. Pancevski, "Europe Sees Signs."

59. 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; and 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.

60. Edward Lucas, "Russia's War Beneath the Waves Threatens Us All," *The 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-cu

t-europe-nato-security?lang=en; and 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/.

61. "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.

62. Karisha Vaswami, "China Takes Russian Cable Tactics to Taiwan," Bloomberg, February 9, 2025, https://www.bloomberg.com/opinion/articles/2025-02-09/china-takes-russian-undersea-cable-tactics-to-taiwan; Jill Goldenziel, "Law Can't Stop Submarine Cable Sabotage. Russia And China Know It," Forbes, February 13, 2025, https://www.forbes.com/sites/jillgoldenziel/2025/02/13/law-doesnt-protect-undersea-cables-russia-and-china-know-it/; and Wayne Chang and Simone McCarthy, "A Cut Undersea Internet Cable Is Making Taiwan Worried About 'Gray Zone' Tactics from Beijing," CNN, January 10, 2025, https://www.cnn.com/2025/01/09/china/undersea-cable-taiwan-intl-hnk/index.html.

63. Joyu Wang, "Chinese Vessel Cuts Taiwan Internet Cable in Apparent Sabotage," *Wall Street Journal*, January 5, 2025, https://www.wsj.com/world/asia/chinese-vessel-cuts-taiwan-internet-cable-in-apparent-sabotage-81e0d3b1.

64. "Ukraine Weapons: What Arms Are Being Supplied and Why Are There Shortages?," BBC, July 18, 2024, https://www.bbc.com/news/world-europe-62002218.

65. "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.

66. Jones, Rathbone, and Milne, "Russian Plotting Sabotage"; and Leo Chiu, "Explosion Rocks UK Munitions Factory in South Wales," *Kyiv Post*, April 18, 2024, https://www.kyivpost.com/post/31331.

67. 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/.

68. 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/.

69. Daniel Safford, "Man Admits Arson Over London Fire Linked to Russia," BBC, October 25, 2024, https://www.bbc.com/news/articles/cvgexrw3x2xo; Giles, "Russian Disruption"; and Eckel, "A Russian Airline Bomb Plot?"

70. See, for example, Philip Wasielewski, "NATO Must Respond to Russian Shadow War on European Soil," The Cipher Brief, November 20, 2024, https://www.thecipherbrief.com/column_article/nato-must-respond-to-russian-shadow-war-on-european-soil.

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

72. 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; and 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.

73. 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.

74. Daniel Safford, "Man Admits Arson Over London Fire Linked to Russia," BBC, October 25, 2024, https://www.bbc.com/news/articles/cvgexrw3x2xo; Giles, "Russian Disruption"; Natasha Bertrand, "Intelligence on Russian Sabotage Threat Prompted Increase in Security at U.S. Military Bases in Europe," CNN, July 9, 2024, https://www.cnn.com/2024/07/09/politics/intelligence-russian-sabotage-threat-us-bases-europe/index.html; and Souad Mekhennet, Catherine Belton, Emily Rauhala, and Shane Harris, "Russia Recruits Sympathizers Online for Sabotage in Europe, Officials Say," *Washington Post*, July 10, 2024, https://www.washingtonpost.com/world/2024/07/10/russia-sabotage-europe-ukraine/.

75. Bojan Pancevski, Thomas Grove, Max Colchester, and 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.

76. 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.

77. Jones, Rathbone, and Milne, "Russian Plotting Sabotage."

78. Andrei Soldatov and Irina Borogan, "Putin's New Agents of Chaos," *Foreign Affairs*, August 9, 2024, https://www.foreignaffairs.com/ukraine/paris-olympics-putin-agents-chaos-andrei-soldatov-irina-borogan; Daniel Safford, "Man Admits Arson Over London Fire Linked to Russia," BBC, October 25, 2024, https://www.bbc.com/news/articles/cvgexrw3x2xo; and Giles, "Russian Disruption in Europe Points to Patterns of Future Aggression."

79. Daniel Safford, "Man Admits Arson Over London Fire Linked to Russia," BBC, October 25, 2024, https://www.bbc.com/news/articles/cvgexrw3x2xo; Giles, "Russian Disruption"; and Adrian Niță, *Navigating the Risks: Understanding GPS Jamming on Planes–Central Euro-Atlantic Pentru Reziliență - E-ARC* (Bucharest: Euro-Atlantic Resilience Centre, June 2024), https://e-arc.ro/en/2024/06/05/navigating-the-risks-understanding-gps-jamming-on-planes-2/.

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

81. See, for example, Anaïs Marin and Samantha de Bendern, *Belarus-EU Border Crisis Reveals Wider Security Threat* (London:

Chatham House, December 8, 2021), https://www.chathamhouse.org/2021/12/belarus-eu-border-crisis-reveals-wider-security-threat; and Rhoda Margesson, Derek E. Mix, and Cory Welt, "Migrant Crisis on the Belarus-Poland Border," Congressional Research Service, IF11983, December 13, 2021, https://crsreports.congress.gov/product/pdf/IF/IF11983.

82. 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/; and Taub, "Russia's Espionage War in the Arctic."

83. Pietro Bomprezzi, Ivan Kharitonov, and Christoph Trebesch, "Ukraine Support Tracker - A Database of Military, Financial and Humanitarian Aid to Ukraine," Kiel Institute for the World Economy, August 6, 2024, https://www.ifw-kiel.de/topics/war-against-ukraine/ukraine-support-tracker/.aid.

84. Pancevski, "Europe Sees Signs."

85. Ignatius, "Russia Is Punching Back at NATO in the Shadows"; and Robbie Gramer and Amy Mackinnon, "Russia Ramps Up Sabotage Operations in Europe," *Foreign Policy*, June 13, 2024, https://foreignpolicy.com/2024/06/13/russia-sabotage-attacks-europe-espionage-hybrid-arson/.

86. "NATO Launches 'Baltic Sentry' to Increase Critical Infrastructure Security," NATO, January 14, 2025, https://www.nato.int/cps/en/natohq/news_232122.htm; and 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.

87. "EU-NATO Task Force on the Resilience of Critical Infrastructure," European Commission, June 2023, https://commission.europa.eu/system/files/2023-06/EU-NATO_Final%20Assessment%20Report%20Digital.pdf; Eoin Micheál McNamara, "Reinforcing Resilience: NATO's Role in Enhanced Security for Critical Undersea Infrastructure," *NATO Review*, August 28, 2024, https://www.nato.int/docu/review/articles/2024/08/28/reinforcing-resilience-natos-role-in-enhanced-security-for-critical-undersea-infrastructure/index.html; and Kayali et al., "Europe Is Under Attack from Russia."

88. Republic of Poland, "Minister of Foreign Affairs Decides to Close Russian Consulate in Poznań," press release, October 22, 2024, https://www.gov.pl/web/diplomacy/minister-of-foreign-affairs-decides-to-close-russian-consulate-in-poznan.

89. McCallum (speech, Counter Terrorism Operations Center).

90. Ibid.

91. "Germany: Spy Chiefs Warn of Increasing Russian Threat," *Deutsche Welle*, October 14, 2024, https://www.dw.com/en/germany-spy-chiefs-warn-of-increasing-russian-threat/a-70493640; Pancevski, Grove, Colchester, and Michaels, "Russia Suspected of Plotting"; 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; "Academic Arrested in Norway as a Moscow Spy confirms His Real, Russian Name, Officials Say," Associated Press, December 14, 2023, https://apnews.com/article/norway-russia-brazilian-university-spy-1f93f5ddb7195f4b70fb394bf3403ef3; "Russian Intelligence Paid $5,000 to Recruit Arsonists in Poland," Polskie Radio, October 23, 2024, https://www.polskieradio.pl/395/7786/Artykul/3438674,russian-intelligence-paid-5000-to-recruit-arsonists-in-poland; and Leyland Cecco, "Suspected Russian Spy Arrested in Norway Spent Years Studying in Canada," *The Guardian*, October 28, 2022, https://www.theguardian.com/world/2022/oct/28/russian-spy-norway-canada-brazil-academic.

92. 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.

93. Soldatov and Borogan, "Putin's New Agents of Chaos."

94. Ibid.

95 On reporting that U.S. Cyber Command halted U.S. offensive operations see Julian E. Barnes, David E. Sanger, and Helene Cooper, "Hegseth Orders Pentagon to Stop Offensive Cyberoperations Against Russia," *New York Times*, March 2, 2025, https://www.nytimes.com/2025/03/02/us/politics/hegseth-cyber-russia-trump-putin.html. On Pentagon denials that the United States halted cyber operations, see Caitlyn Burchett, "Pentagon Denies Halting Cybersecurity Operations Against Russia," *Stars and Stripes*, March 4, 2025, https://www.stripes.com/theaters/us/2025-03-04/cyber-hegseth-pentagon-russia-17031715.html.