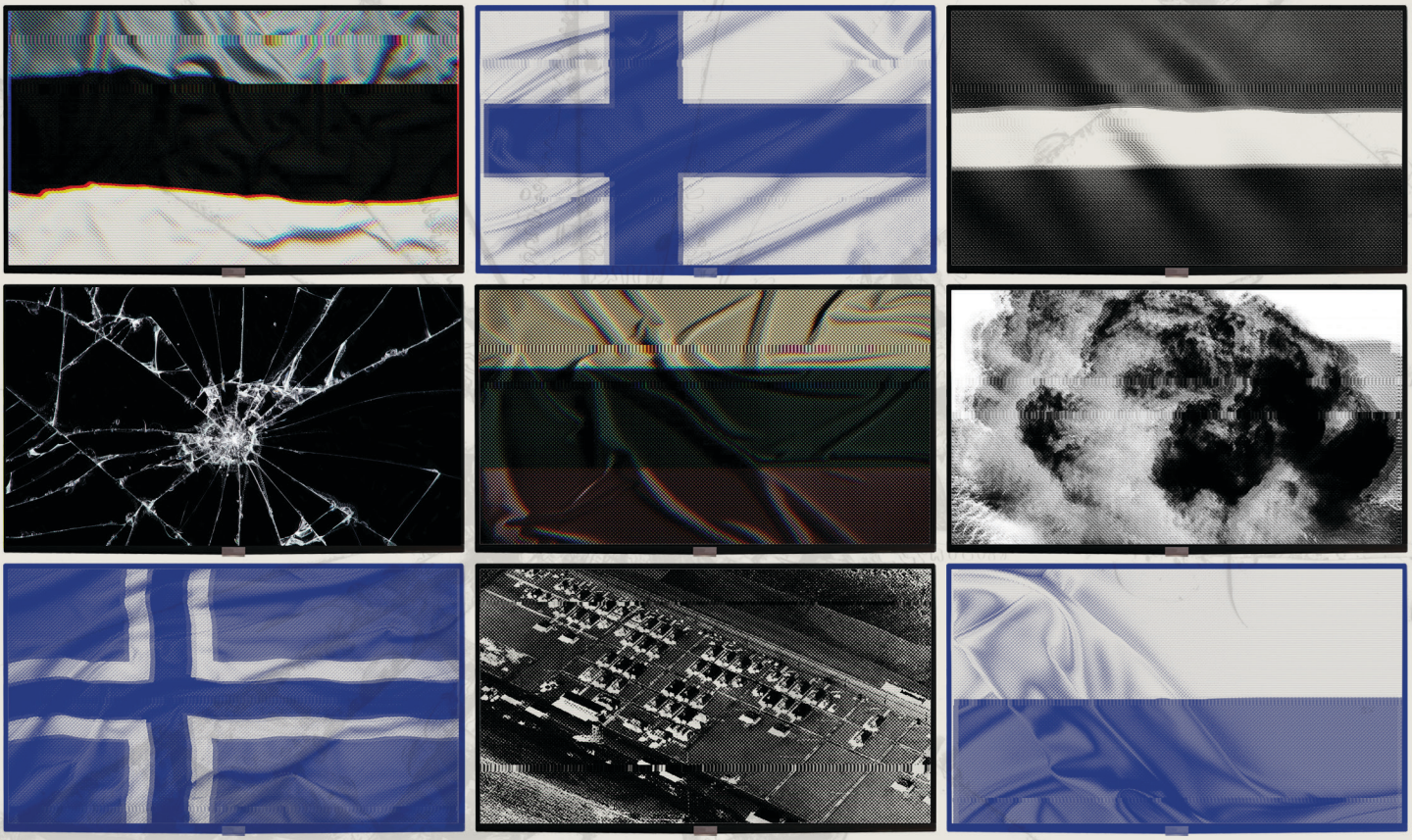
THREAT ANALYSIS

RUSSIA

Recorded Future®

By Insikt Group®

November 14, 2024



Russian Sabotage Activities Escalate Amid Fraught Tensions

Russia is very likely intensifying its sabotage operations across Europe to damage NATO countries' military, economic, and political capabilities in response to their support for Ukraine.

Russian sabotage activities are very likely calibrated to remain in the "gray zone" to avoid a direct war while achieving Russia's strategic objectives.

Insikt Group found three plausible Russian sabotage acts in Finland and Poland from a dataset of 21 incidents occurring in June 2024 in six European countries bordering Russia.

Executive Summary

Russia is very likely intensifying sabotage operations across Europe as part of its broader hybrid warfare strategy that augments its conventional military operations in Ukraine with deniable and subversive actions against Ukraine's allies. This is almost certainly underpinned by North Atlantic Treaty Organization (NATO) countries' support for Ukraine in its active conflict with Russia — which the Kremlin has increasingly warned could put NATO at war with Russia — and because Russia perceives that it is in a passive phase of war with Western countries. In June 2024 alone, Insikt Group identified three plausible acts of Russian sabotage across Finland and Poland targeting critical infrastructure from a broader dataset of 21 incidents of interest in six European countries that border Russia (Estonia, Finland, Latvia, Lithuania, Norway, and Poland). These three incidents align closely with Russia's sabotage strategy and tactics — which have very likely remained consistent since the Soviet Union, with the exception of technological advances and associated new opportunities to conduct sabotage — as well as documented Russian sabotage operations.

The very likely expanded scope of Russian sabotage operations in Europe poses significant risks to European critical infrastructure, military capabilities, and political stability. Russia's sabotage operations almost certainly seek to destabilize NATO allies, degrade NATO's war-fighting capacity, and disrupt NATO support to Ukraine (such as targeting military assets NATO committed to providing to Ukraine), among other objectives. Without adequate countermeasures, Russia's sabotage operations could lead to significant disruptions in target countries, undermining national security and NATO's support to Ukraine.

As relations between Russia and the West will almost certainly remain at a low point, Russia is very likely to engage in more effective sabotage operations, including the destruction of critical infrastructure facilities. As Russian hybrid operations continue to evolve, European nations must be prepared to counter a wide array of covert threats that extend beyond traditional military confrontations. NATO governments and allies should bolster their intelligence-sharing about Russian covert activities, increase critical infrastructure security, and closely monitor likely targets for signs of escalation in hybrid activities.

Key Findings

- Russia is very likely intensifying its sabotage operations across Europe to damage NATO countries' military, economic, and political capabilities in response to their support for Ukraine.
- Sabotage operations are carried out by various Russian special operations forces, including the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU) Spetsnaz forces and GRU agent networks, in many cases using rudimentary equipment to obfuscate attribution.

- Current Russian sabotage activities are very likely calibrated to remain in the "gray zone" and avoid crossing the threshold of war while ensuring that Russia's objectives to undermine its adversaries are achieved.
- Russian sabotage objectives and tactics have very likely remained consistent since the Soviet Union, with the exception of technological advances and opportunities to conduct sabotage, as illustrated by recent documented Russian sabotage incidents.
- Three incidents in June 2024 were plausibly the result of Russian sabotage operations based on assessment criteria informed by Russian sabotage objectives and tactics, documented Russian sabotage incidents, the strategic value of the targeted entity, government statements, and other factors.
- As relations between Russia and the West will almost certainly remain fraught, Russia is very likely to increase the destructiveness and lethality of its sabotage operations without crossing the threshold of war with NATO, as discussed in the Gerasimov doctrine.
- Future Russian sabotage operations will likely adapt to new technologies and domestic political situations, with a growing emphasis on plausible deniability, for example, by recruiting or supporting domestic violent extremists to conduct sabotage operations.

Methodology

To identify plausible examples of Russian sabotage in six European countries bordering Russia (Estonia, Finland, Latvia, Lithuania, Norway, and Poland), we first reviewed primary and secondary sources on Soviet and Russian sabotage activities to identify and extract sabotage objectives and tactics. Specifically, we reviewed works by GRU defector Viktor Suvorov (born Vladimir Rezun), Committee for State Security (KGB) defector Vasilii Mitrokhin, M. Drobov's book *Small War: Guerilla Warfare and Sabotage*, as well as declassified United States (US) documents on Soviet Spetsnaz forces, such as the Voroshilov lectures.[1][2][3][4][5] Various Russian military and intelligence agencies conduct sabotage; however, publicly available information primarily details GRU Special Operations Forces (Spetsnaz) tactics. As such, Russian sabotage tactics detailed in this report are primarily derived from information pertaining to Spetsnaz, though similar tactics are likely used by other Russian threat actors that conduct sabotage.

Second, we illustrated how Russian sabotage goals and tactics have very likely remained consistent since the Soviet Union by comparing documented recent GRU sabotage activities to the identified Soviet GRU Spetsnaz sabotage tactics.

Third, after establishing Soviet sabotage tactics as relevant and applicable to modern Russian sabotage operations, we reviewed the most widely read online news outlets in each country, as well as emergency service reports (**Appendix A**) to identify any incidents of fire, mechanical failures,

[1] Viktor Suvorov, *Spetsnaz: The inside Story of the Soviet Special Forces* (W. W. Norton & Company, 1988).
[2] Christopher M. Andrew, *The Sword and the Shield: the Mitrokhin Archive and the Secret History of the KGB* (Basic Books, 1999).
[3] *https://sprotyvg7[.]com.ua/wp-content/uploads/2024/01/M.A.Добров.-Малая-война.-Партизанство-и-деверсии.pdf*
[4] M A Drobov, *Малая война : партизанство и диверсии [Small War: Guerilla Warfare and Sabotage]* (State Military Publishing House, 1931).
[5] *http://www.патриот43[.]рф/statics/content/documents/files/99/%20подготовка%20спецназа%20Ардашев%20A.A..pdf*

explosions, power cuts, or any other unexplained incidents in June 2024 affecting critical infrastructure (defined in **Appendix B**).[6] [7] We focused on events that resulted in physical damage to property; we did not look at any instances of cyber and electronic interference, disinformation campaigns, or other hybrid operations. Our research is not intended to be comprehensive, as some potential sabotage instances may not be reported publicly or may affect non-critical infrastructure. Moreover, while we focused on potential Russian sabotage incidents in six European countries in June 2024, this selection of countries and timeframe is intended to serve as a representative example. Russian sabotage incidents have almost certainly occurred and continue to take place outside of this scope as tensions between Russia and the West continue to rise.

Fourth, we evaluated these incidents to identify three examples that could have plausibly been instances of Russian sabotage. We evaluated these incidents based on criteria informed by the aforementioned Russian sabotage objectives, tactics, and information derived from documented sabotage operations. It is exceptionally difficult to attribute incidents to Russian sabotage based solely on publicly available information, and incidents can happen for many reasons (for example, because of mechanical failures or human error leading to fires and explosions). Nevertheless, we sought to demonstrate how criteria informed by Russian sabotage objectives, tactics, and operations can be used to identify plausible instances of Russian sabotage.

Russia's Ongoing "Shadow War" in Europe

Since the start of Russia's full-scale invasion of Ukraine in February 2022, European governments have increasingly accused Russia of engaging in hybrid warfare against the West, including carrying out sabotage activities. Notably, on May 2, 2024, NATO issued a public statement accusing Russia of carrying out "sabotage, acts of violence, cyber and electronic interference, disinformation campaigns, and other hybrid operations … across the Euro-Atlantic area". Similarly to NATO's public statements, Western government leaders have also made statements describing Russia's hybrid warfare in Europe: [8]

- In June 2024, Polish Interior Minister Tomasz Siemoniak stated that "Poland has arrested eighteen people over the past six months on various allegations of pursuing hostile activities or planning sabotage on behalf of Russia and neighboring Belarus". At least ten individuals were involved in planning sabotage operations across Poland, and at least one "was involved in an alleged plot to assassinate Ukraine's president".
- In May 2024, Torgils Lutro, the head of the Norwegian Police Security Service in Western Norway, stated that his service has "uncovered hostile, unwanted Russian intelligence activities since the invasion of Ukraine in 2022". Lutro also stated that Russian agents "may have been preparing for acts of sabotage" with potential targets including "Haakonsvern, northern Europe's largest naval base, as well as crucial oil, gas, and power facilities in the region".

[6] Insikt Group based its assessment of the most popular news outlets based on several media landscape reports, including Reuters Institute for the Study of Journalism (RISJ), the BBC, and Media Landscapes.
[7] Analysts heavily relied on Google Translate to translate articles into English.
[8] *https://www.baltictimes.com/we_have_information_that_acts_of_sabotage_may_recur___lithuanian_president/*

- In May 2024, Estonian Prime Minister Kaja Kallas further stated that Russia is conducting a "shadow war" against the West.
- In May 2024, Finnish Prime Minister Petteri Orpo stated that Russia "uses all kinds of hybrid tools against the West, against Europe".
- In March 2024, Finland's Security and Intelligence Service, SUPO, stated that "Russia's actions remain the greatest threat to Finland's national security, with Russia treating Finland as [an] unfriendly state, and as a target for espionage and malign influence activities".
- In March 2024, Darius Jauniškis, the Head of the Lithuanian State Security Department, stated, "Security services of Russia and Belarus engage in intense activities against Lithuania seeking to sow division, mislead, spy, cause chaos and make the work of institutions difficult".
- In February 2024, the Estonian Internal Security Service arrested ten individuals on suspicion of sabotage under the direction of Russian intelligence services. According to the Estonian Internal Security Service, the sabotage operations involved "damaging property and defacing monuments, including an attack on the car of Interior Minister Lauri Läänemets and a vehicle belonging to Andrei Šumakov, editor of news website Delfi".
- In February 2024, Norwegian intelligence services identified Russia as the main threat to the country. According to the Norwegian Intelligence Service, "foreign powers" seek to gain access to critical infrastructure and value chains, which can be used "to disrupt supply chains, identify vulnerabilities and ultimately carry out physical or digital sabotage". The report also stated that Russia poses a direct threat to Norway's oil and gas infrastructure, both "physically and in the digital domain".
- In October 2023, SUPO reported that the Russian "threat of intelligence and influencing operations against critical infrastructure has increased".

Russian Military Doctrine and Sabotage Strategy

In 2013, Russian Chief of the General Staff General Valery Gerasimov gave a speech at the General Meeting of the Academy of Military Sciences, outlining a new perspective on warfare.[9] In his speech, Gerasimov introduced the concept of permanent conflict as "a whole-of-government warfare that transcends boundaries between peace- and wartime, best described as a fusion of various elements of soft and hard power across various domains". This concept — which later became known as "the Gerasimov Doctrine" — is closely associated with the concept of hybrid warfare, a fusion of conventional and irregular warfare, including the use of influence operations. Essentially, the Gerasimov Doctrine posits that even during "peacetime" or a "passive phase of war", nations engage in hostilities that are below the threshold of war — often referred to as the "gray zone". These activities can include sabotage, cyberattacks, economic coercion, sanctions, embargoes, lawfare, and others. The wartime or "active phase of a conflict" involves using conventional military forces along with unconventional means to achieve military objectives.

In the context of Russia's modern military doctrine, sabotage is conducted during both passive and active phases of a perpetual conflict. According to Suvorov, in the lead-up to war, Russian intelligence

[9] *https://www.avnrf[.]ru/attachments/article/534/AVN-1(42)_maket_001-184.pdf*

forces proactively conduct sabotage operations to destroy the adversary's military, economic, and political capabilities.[10] Similarly, Russian intelligence operatives carry out sabotage operations during the active phase of a conflict to continuously weaken enemy capabilities. Given Russia is currently in an active conflict with Ukraine, with Western countries arming and providing support to Ukraine, Russia is almost certainly conducting sabotage operations in line with its overarching military strategy to weaken the capabilities of Ukraine and its allies. More broadly, Russia perceives that it is in a passive phase of war with Western countries, and as such, it is almost certainly engaging in further hostilities that are below the threshold of war, including sabotage operations.[11]

Spetsnaz Sabotage Objectives

GRU defector Suvorov, KGB defector Mitrokhin, and author Drobov emphasize that Soviet and Russian intelligence agencies have historically engaged in sabotage to incapacitate an adversary's military, economic, and political capabilities both before and immediately following the start of a direct conflict.[12] [13] [14] Suvorov notes that such operations aim to neutralize the adversary's strategic and tactical nuclear forces, eliminate decision-makers at all levels, and dismantle essential infrastructure, including communication, transportation, energy, and food systems, though operations this severe are very likely reserved to large-scale war as defined in Russia's military doctrine.[15] In the context of current geopolitical tensions between NATO and Russia, Russia's sabotage operations are almost certainly designed to destabilize NATO allies, degrade NATO's war-fighting capacity, disrupt NATO support to Ukraine (such as by targeting military assets NATO committed to providing to Ukraine), weaken the alliance's collective security by targeting critical infrastructure, overwhelming emergency services, and instill fear in local populations.

It is important to note that not all sabotage operations are designed to cause significant physical damage. The primary objective remains to undermine the adversary's military, economic, and political capabilities. In some cases, operations are intended to achieve this by affecting local security, overwhelming emergency services, instilling fear in the population, and lowering morale. For example, certain actions like graffitiing a military base in Estonia (as described in the **Latvian Sabotage Squad** section of this report) are very likely intended to affect morale and create fear among the enemy population rather than inflict direct damage on the base itself.

To better characterize and understand different sabotage operations, Drobov suggested dividing sabotage activities into four distinct types based on their objectives:

---

[10] Viktor Suvorov, *Spetsnaz: The inside Story of the Soviet Special Forces* (W. W. Norton & Company, 1988), 4–9.
[11] Russia's thinking concerning the targeting of an enemy's critical infrastructure using overt military means is best described in Russia's Strategic Operation for the Destruction of Critically Important Targets (SODCIT). This strategy posits that the Russian military should target the enemy's critically important assets to counter threats and prevent further aggression. In this, Russia seeks to inflict decisive damage to the enemy's critical infrastructure, including targeted killings of decision-makers, to deter further escalation of a conflict. The deliberate targeting of an adversary's infrastructure by conventional military means mirrors an objective of Russia's sabotage operations.
[12] M A Drobov, *Малая война: партизанство и диверсии [Small War: Guerilla Warfare and Sabotage]* (State Military Publishing House, 1931).
[13] Viktor Suvorov, *Spetsnaz: The inside Story of the Soviet Special Forces*.
[14] Christopher M. Andrew, *The Sword and the Shield: the Mitrokhin Archive and the Secret History of the KGB* (Basic Books, 1999).
[15] *http://scrf[.]gov[.]ru/security/military/document129/*

1. Economic sabotage, which targets infrastructure crucial to the economy;
2. Political sabotage, which involves influence operations;
3. Military sabotage, which focuses on key military installations; and
4. Terror, which entails the assassination of high-profile decision-makers within the enemy state[16]

Spetsnaz Sabotage Tactics

Although various Russian military and intelligence agencies can conduct sabotage, publicly available information primarily highlights operations conducted by the Russian and Soviet GRU Special Operations Forces, known as Spetsnaz.[17] The GRU's Spetsnaz units are specifically trained to carry out special operations, including sabotage missions. Within Spetsnaz, units specifically trained for sabotage are organized into sabotage and reconnaissance groups (Диверсионно-разведывательная группы; DRG). To carry out sabotage activities, Spetsnaz DRG operatives infiltrate adversary states, both in peacetime and wartime, and conduct sabotage, primarily using basic weapons and rudimentary means to complicate attribution. Spetsnaz operatives can also recruit and use agents (or a network of agents) to assist operatives in carrying out sabotage operations.

Spetsnaz Operatives

Soviet and Russian intelligence, including Spetsnaz, have historically infiltrated adversary nations using cover identities such as diplomats, athletes, and tourists to conduct sabotage operations, as detailed by Suvorov, Mitrokhin, and Drobov. These tactics, which involve embedding covert operatives under diplomatic and civilian covers, are a model Russia very likely continues to use today.

Suvorov, Mitrokhin, and Drobov extensively discussed Soviet and Russian efforts to infiltrate adversary nations before direct conflict, with the intent to carry out sabotage operations. [18] [19] [20] Suvorov, in particular, detailed how the Soviet Union and Russia used diplomatic missions, athletic competitions, tourists, and businessmen as covers to deploy operatives in adversary nations to prepare and execute covert operations.[21] He noted that the Soviet Union and Russia could enhance their diplomatic presence in these nations by replacing all staff with Spetsnaz officers. Suvorov cited the Soviet invasion of Czechoslovakia in 1968 as an example. According to Suvorov, prior to the military invasion, the Soviet government deployed Spetsnaz officers disguised as "tourists" to Czechoslovakia, who then took control of Prague Airport in advance of Soviet military aircraft arrivals.

Mitrokhin also documented the Soviet Union's use of saboteurs in foreign states, specifically highlighting the actions of Iosif Romualdovich Grigulevich, alias Teodoro B. Castro.[22] Grigulevich was a Soviet secret police (NKVD) operative who used his foreign Communist networks to conduct global sabotage and assassination operations for the Stalinist government. According to Mitrokhin, Grigulevich

[16] M A Drobov, *Малая война: партизанство и диверсии*.
[17] *http://www.патриот43[.]рф/statics/content/documents/files/99/%20подготовка%20спецназа%20Ардашев%20А.А..pdf*
[18] M A Drobov, *Малая война: партизанство и диверсии [Small War: Guerilla Warfare and Sabotage]* (State Military Publishing House, 1931).
[19] Viktor Suvorov, *Spetsnaz: The inside Story of the Soviet Special Forces.*
[20] Christipher M. Andrew, *The Sword and the Shield: the Mitrokhin Archive and the Secret History of the KGB.*
[21] Viktor Suvorov, *Spetsnaz: The inside Story of the Soviet Special Forces.*
[22] Christopher M. Andrew, *The Sword and the Shield: the Mitrokhin Archive and the Secret History of the KGB,* 162–175.

trained saboteurs during the Spanish Civil War, played a leading role in the operations to assassinate Leon Trotsky in Mexico, and managed a residency for training saboteurs in Argentina during World War II, specializing in the sabotage of ships and cargoes destined for Germany. Grigulevich also maintained a false identity through GRU's illegals program and became a high-ranking Costa Rican diplomat. Grigulevich's role as an overseas operative reflects a model for covert operations across international borders that Russia very likely continues today.

GRU Illegals Program

The GRU's Illegals program is designed to embed Russian intelligence operatives in foreign states under a false identity.[23] [24] The GRU goes to great lengths to train its illegal operatives for up to five years, create fake but believable identities in target countries, and establish cover stories to blend into the local environment. The illegals, following the establishment of their new identities, collect intelligence on the target state.

Spetsnaz Weapons

Plausible deniability is essential for Russian special operations forces when conducting sabotage, leading them to use basic, easily accessible weapons and methods like arson or explosions triggered by easily obtainable explosives to obscure their involvement.[25] The use of weapons unique to Russia and its allies would undermine Spetsnaz's objective of deniability, as analysis of the material used in an operation could support attribution to Russia.

Additionally, GRU provides Spetsnaz operatives with extensive training on a wide array of Soviet, Russian, and Western weapons to execute their missions.[26] Their arsenal includes submachine guns, pistols, and crossbows, along with more specialized weapons such as ground-to-air missiles, various types of mines, plastic explosives, sniper rifles, and others. Suvorov also emphasized that Spetsnaz members receive training in larger weapons systems, such as heavy artillery, mortars, and infantry fighting vehicles. In addition, Spetsnaz units are trained to use Western weapons they may acquire during their operations. These units also use animals, particularly dogs and dolphins, for their scent and sonar detection capabilities.

With a wide variety of weapons at their disposal, Spetsnaz operatives likely employ different types of weapons for sabotage activities depending on the phase of a war. For example, in the "passive phase of a perpetual war", Spetsnaz almost certainly uses basic weapons and rudimentary means to complicate the target's ability to attribute the sabotage incident to Russia. However, in the "active phase of a perpetual war", Spetsnaz can use more advanced weapons systems, including Russian weapons systems, to achieve its objectives, as there is a reduced need to hide their involvement.

[23] Viktor Suvorov, *Inside Soviet Military Intelligence*, 75–83.
[24] Christopher M. Andrew, *The Sword and the Shield: the Mitrokhin Archive and the Secret History of the KGB.*
[25] *http://www.патриот43[.]рф/statics/content/documents/files/99/%20подготовка%20спецназа%20Ардашев%20А.А..pdf*
[26] Viktor Suvorov, *Spetsnaz: The inside Story of the Soviet Special Forces.* W. W. Norton & Company, 99–112.

Spetsnaz Agent Networks

Spetsnaz's Soviet-era strategy of recruiting agents and extremist groups to assist in conducting sabotage operations, enhancing the success of missions while maintaining plausible deniability, almost certainly continues today.

While Spetsnaz personnel are highly trained and undergo rigorous selection to join these special forces, Spetsnaz also recruits agents to assist in carrying out sabotage activities. [27] [28] These agents are crucial to the success of Spetsnaz missions, as they help manage logistics, obtain resources, and ensure a successful and undetected exit. Agents can be responsible for a variety of mission-critical tasks, such as establishing safe houses in advance of an operation, maintaining weapons or explosives, and supporting the overall sabotage efforts. According to Suvorov, the ideal recruit for such roles is someone who does not arouse suspicion from local law enforcement or security services and who would not be an obvious suspect in the event of an investigation. Suvorov describes the ideal candidate as

> *"a man [or woman] between 55 and 65 years of age who has never served in the military, never had access to classified information, does not own or carry weapons, is unfamiliar with hand-to-hand combat, possesses no secret equipment, does not support Communist [or broadly Russian] causes, avoids reading newspapers, was not born in the Soviet Union [or Russia], and has never interacted with Soviet citizens. This individual leads a solitary, introspective life, far from others, and works as a forester, fisherman, lighthouse keeper, security guard, or railwayman".*[29]

Spetsnaz also recruits agents to carry out sabotage activities under its direction without Spetsnaz's direct involvement. According to Suvorov, Spetsnaz specifically targets individuals who are discontented with their government and are willing "to go to extremes." [30] These recruits often include individuals and groups who strongly disagree with government policies and are prepared to take action aligned with their beliefs. For instance, Suvorov mentioned a French ecological group that, in 1982, fired Soviet-made anti-tank rockets at a nuclear power plant under construction. While Suvorov stopped short of directly attributing this incident to Spetsnaz, he emphasizes that nuclear power plants are "one of the most important targets" for Spetsnaz because they "reduce Europe's dependence on imported oil, including Soviet oil". Given the origin of the rockets fired and the strategic importance of the target, it is likely that Spetsnaz was involved in some element of the attack but leveraged the French group's own political motivation to achieve Russia's objectives.

Suvorov further asserted that Spetsnaz supports — through the provision of funds, weapons, explosives, training, and intelligence — extremist groups worldwide that share common interests with the Soviet government, particularly those with anti-Western views. Spetsnaz supports these groups to

[27] Viktor Suvorov, *Spetsnaz: The inside Story of the Soviet Special Forces*, 85–95.
[28] Viktor Suvorov, *Inside Soviet Military Intelligence* (Macmillan, 1984), 100–106.
[29] Viktor Suvorov, *Spetsnaz: The Inside Story of the Soviet Special Forces*, 87.
[30] Ibid., 89.

achieve its sabotage objectives, including destruction of an adversary's critical infrastructure. However, these extremist groups are often unaware of the Soviet government's backing, as Spetsnaz takes great care to conceal its involvement, allowing the groups to believe they are acting independently.

Suvorov's claim about the Soviet Union's support for extremists is further supported by now-declassified US intelligence reports. For example, in 1986, the CIA declassified a report titled "Soviet Support for International Terrorism and Revolutionary Violence". It stated that the Soviets "support Palestinian and other radical anti-Israeli and anti-US groups based in the Middle East; most of them use terrorism as a means of seeking political objectives".

Documented Russian Sabotage Operations

Several documented examples of Russian intelligence operatives and GRU agents conducting sabotage operations in Europe are either confirmed or currently under litigation. The following examples illustrate that Russian sabotage goals and tactics have very likely remained consistent since the Soviet Union, with the exception of technological advances and associated opportunities to carry out sabotage operations, such as disruptive and destructive cyberattacks. More historical case studies are provided in **Appendix D**.

Latvian Sabotage Squad

An article published by The Insider on July 10, 2024, revealed details about the Latvian Sabotage Squad.[31] Based on Latvian and Estonian court documents, the article alleged that a likely GRU asset, known as Alexander, used Telegram to recruit three young adults (Sergejs Hodonovičs, Martins Griķis, and Ivan Tarabanov) to carry out sabotage activities across Eastern Europe since at least January 2022.[32] These activities included arson attempts at an unidentified military base in Kyiv, Ukraine, and at Riga's Museum of the Occupation, as well as a graffiti defacement of a military complex that houses NATO's Cooperative Cyber Defence Center of Excellence. Alexander's recruits reportedly operated in three distinct jurisdictions — Ukraine, Latvia, and Estonia — underscoring the wide range of European infrastructure that could be targets of Russian sabotage.

Although The Insider offered no definitive proof that Alexander is a GRU officer, the article cited "a source familiar with the case" who suggested Alexander might be "an unwitting agent recruited by Russian military intelligence to scout others in foreign countries". The Insider indicates that in recruiting assets for sabotage operations, Russian intelligence agencies employ several layers of contacts to obfuscate their involvement. The case of the Latvian Sabotage Squad also underscores that not all sabotage operations are successful. One of the agents tasked with committing arson at a military base in Kyiv reportedly "got scared and set fire only to the building's exterior wall". Similarly, GRU agents failed to burn down Riga's Museum of the Occupation — the fire was quickly extinguished.

[31] *https://theins[.]ru/en/politics/272989*
[32] *https://theins[.]ru/en/politics/272989*

The Latvian Sabotage Squad case study closely mirrors Soviet sabotage objectives and tactics, demonstrating that Russia continues to use the same methods. The goal of the Latvian Sabotage Squad was very likely to instill fear in the local population and degrade the military capability of Ukraine, mirroring objectives outlined in Soviet-era documents, specifically conducting military and political sabotage as described by Drobov. Like Soviet operations, Russian intelligence employed local, unassuming agents to conduct low-level sabotage, such as arson and graffiti, minimizing direct attribution. The use of covert communication channels like Telegram and the multi-layered recruitment approach further align with Soviet tactics for recruiting agent networks, emphasizing plausible deniability.

Likely GRU Sabotage Operations in Czechia and Bulgaria

Two separate explosions occurred at an ammunition depot in Vrbětice, Czechia, on October 16 and December 3, 2014, respectively. These explosions resulted in the deaths of two workers and the destruction of 150 tons of ammunition, which were very likely headed toward Ukraine.[33] Three more explosions took place at ammunition depots in Bulgaria in 2015, destroying weapons destined for Ukraine and Georgia. The same year, the owner of the weapons stored in the Czech and Bulgarian depots, Emilian Gebrev, his son, and his business associate were poisoned by an unknown substance. Notably, since 2015, more explosions have taken place at Gebrev's EMCO ammunition warehouses, with the most recent explosion happening in 2023.

According to the Czech government, operatives of GRU Unit 29155 were responsible for the explosions in Czechia. The Bulgarian government has also reported that Russia was involved in the explosion of the EMCO ammunition depots and the poisoning of Grebev. Open-source investigative journalists, including Bellingcat, have reported that at least six members of the sabotage subunit of GRU Unit 29155, as well as the commander of Unit 29155, General Andrey Averyanov, traveled to Czechia in the days leading up to the first explosion. According to Czech and Bulgarian governments, as well as open-source reporting, the GRU carried out sabotage operations in Czechia and Bulgaria to destroy weapons being transferred to Ukraine and Georgia.

The explosions at ammunition depots in Czechia and Bulgaria, linked to GRU Unit 29155, further demonstrate Russia's continuation of Soviet-era sabotage objectives and tactics. By targeting weapons shipments destined for Ukraine and Georgia, Russian intelligence disrupted its adversaries' military capabilities, mirroring Soviet-era objectives of covertly weakening opponents through sabotage. The involvement of GRU operatives and the use of poisonings to target individuals further align with Soviet sabotage objectives, showing continuity in strategy despite the modern context.

Shaposhnikov Family

The case of the Shaposhnikov family, likely GRU agents, provides insights into how the GRU uses agents in support of its operations. According to The Insider, the Shaposhnikovs were reportedly instrumental in aiding GRU agents with various missions across Europe at least since 2014, including

[33] Bulgarian arms manufacturer and trader EMCO disputed this narrative.

the aforementioned sabotage of ammunition depots in Bulgaria and Czechia.[34] Elena Shaposhnikova was reportedly directly employed by GRU's Unit 29155, and she "likely directed and supervised her husband's – and possibly their son's – activities in support of Russian state interests." The Insider further noted that the Shaposhnikov family engaged in various activities in support of GRU, including intelligence-gathering, logistical facilitation, providing safe havens, recruitment efforts, and aiding in securing physical access for GRU operatives conducting sabotage missions. Notably, the family reportedly used Villa Elena, a hotel in Greece, as a safe house for members of GRU Unit 29155.

The Shaposhnikovs' activities supporting the GRU mirror Suvorov's description of Spetsnaz agents: they provided secure hiding places, essential resources, intelligence, and operational security — critical elements that enabled GRU operatives to execute sabotage activities successfully. The case study further illustrates a continuation of the Soviet-era use of agent networks in modern-day operations.

Analysis of Potential Russian Sabotage Activities in June 2024

While Russia is not in a direct war with the West, Moscow perceives that in Ukraine, it is engaged in a proxy war with the West. [35] [36] [37] [38] [39] [40] [41] As a result, Moscow almost certainly engages in gray-zone activities, specifically sabotage, to weaken the West's military capabilities. This is particularly true given the West is arming and providing materiel to Ukraine. These operations are deliberately conducted below the threshold of war to avoid escalating the conflict into a direct Russia-NATO war. As such, identified plausible Russian sabotage activities so far have not resulted in significant damage to the critical infrastructure of the six countries. However, as tensions between the West and Russia are almost certainly to remain at a low point, Russian intelligence operations are very likely to engage in more effective sabotage operations, with the potential to result in significant disruptions in operations and destruction of critical infrastructure facilities.

Sabotage Assessment Criteria

Based on Spetsnaz's sabotage objectives and tactics, as well as information derived from documented Russian sabotage operations, we used the following criteria to assess plausible instances of Russian sabotage:

- The target is an important resource within a critical infrastructure sector
- Disruption or destruction of the target would undermine a country's military capabilities, economic strength, or political stability
- Rudimentary tools or tactics are employed to achieve a desired effect, such as arson, mechanical damage, or electrical overloads

[34] *https://theins[.]ru/politika/271203*
[35] *https://tass[.]ru/opinions/15309535*
[36] *https://poland[.]mid[.]ru/ru/press-centre/news/o_roli_zapada_v_konflikte_na_ukraine/*
[37] *https://tass[.]ru/politika/16862443*
[38] *https://iz[.]ru/1665428/2024-03-14/lavrov-ukazal-na-fakticheskoe-vedenie-zapada-voiny-protiv-rossii*
[39] *https://tass[.]ru/politika/20314217*
[40] *https://regnum[.]ru/news/3852320*
[41] *https://ria[.]ru/20230324/medvedev-1860259498.html*

- Absence of evidence that the incident was naturally occurring or the result of unintentional actions
- The suspected involvement of low-level criminals, disaffected members of society, anarchists, or domestic violent extremists, as Russian intelligence and special forces recruit these groups to support or conduct sabotage operations
- Using means and resources provided by external parties — such as financing, safe houses, intelligence, and equipment — particularly those connected to the GRU
- Statements made by current or former government and political officials after the incident occurred, including whether they are investigating the incident as sabotage

Per our **Methodology**, we identified 21 incidents of interest (**Appendix C**) in six European countries that border Russia in June 2024. We evaluated these incidents to identify three examples that plausibly could have been instances of Russian sabotage based on the above criteria.

Finland — Water Treatment Break-Ins

- In June 2024, Finnish authorities initiated investigations into several break-ins into water towers and water treatment facilities across the country. According to Finnish media, the first break-ins were reported in May 2024, and there were at least eleven break-in attempts between May and early August 2024. The affected water facilities were primarily located near Tampere and Helsinki, Finland's most populated regions. According to local reporting, the police have not commented on whether there are any connections between the incidents. These cases are plausible economic or political sabotage incidents aimed at disrupting operations at Finland's water treatment facilities, potentially contaminating Finland's water supplies and instilling fear among the Finnish population.[42]

Poland — Mesko Arms Factory Explosion

- On June 10, 2024, a blast occurred at the Mesko arms factory in the southeastern Polish city of Skarżysko-Kamienna, resulting in a fire and killing a 59-year-old worker. Notably, the Mesko arms factory produces ammunition that is supplied to Ukraine, including the Piorun man-portable air defense systems.[43] On the same day, Poland's Prime Minister Donald Tusk stated, "[T]here is no reason to believe that any external force was behind this dramatic event".[44] However, on June 11, 2024, former Minister of National Defense of Poland Janusz Onyszkiewicz stated that the incident "could be the work of the Russian intelligence agencies".[45] Similarly, General Stanisław Koziej, former head of Poland's Presidential National Security Bureau and Secretary of the National Security Council, stated that "the possibility of deliberate sabotage" has to be considered during the investigation into the explosion. Targeting the factory would very likely

[42] Oleg Kalugin, the former head of political intelligence in the KGB residency in Washington, has stated that a sabotage expert ''did everything from plotting ways to poison the Capital's water system to drawing up assassination plans for U.S. leaders'', indicating that Soviet forces had plans to target water treatment facilities in adversary states.
[43] *https://mil[.]in[.]ua/en/news/an-explosion-occurred-at-the-polish-defense-plant-mesko/#:~:text=In%202022%2C%20Ukraine%20signed%20a,was%20introduced%20to%20Ukrainian%20engineers.&text=Mesko%20serves%20as%20a%20technology,component%2C%20and%20technical%20support%20provider.*
[44] *https://kyivindependent[.]com/poland-says-no-external-force-behind-fatal-arms-plant-explosion/*
[45] *https://www.ukrinform[.]net/rubric-polytics/3873749-blast-at-mesko-ammo-plant-could-be-russian-sabotage-polands-exdefense-chief.html*

degrade the factory's production capabilities, supporting Russia's objective of disrupting Western military aid to Ukraine. Additionally, since the start of the war in Ukraine, the Russian government has made several claims threatening Western defense companies operating in Ukraine. The target is also similar to previous GRU sabotage operations targeting ammunition depots in Czechia and Bulgaria. Based on these details, this incident is a plausible military sabotage incident, even though initial reports stated the blast "may have been triggered by a malfunction in production equipment".

Poland — Railroad Transshipment Terminal Fire

- On June 28, 2024, a fuel tank fire broke out on the premises of the Broad Gauge Metallurgy Line (LHS) transshipment terminal in Sławków, Poland, damaging four diesel tanks with a total capacity of 40,000 liters. LHS is the longest broad gauge line in Poland and the westernmost broad gauge line in Europe. Additionally, the line connects Poland to Ukrainian railways, serving as an important trade route for the two countries. In 2022, the operators of the LHS line signed a contract with the Polish Armed Forces to provide transportation services for their personnel and military equipment. This case is a plausible economic and military sabotage incident aimed at damaging the LHS line because of its importance to Poland's production capability, the Polish Armed Forces, and Ukraine's ability to connect to Poland.

The three examples above are the most plausible instances of Russian sabotage from our dataset of 21 incidents of interest (**Appendix C**). The above assessment criteria can be used to evaluate other incidents of interest as more information about them becomes publicly available. For example, on June 5, 2024, at 05:06 GMT+3, an explosion occurred at the fuel storage facility near Tallinn Port, burning "about 10 tons of heavy fuel oil". The Estonian government reported that the explosion occurred because an employee was working with fire ("*tuletöödest*") on the roof of the tank. However, Estonian officials did not provide any information on why the employee was working with fire on the roof of the tank that contained heavy fuel oil. More information is needed regarding this incident to be able to determine whether it was plausibly an example of Russian sabotage.

Mitigations

NATO and its member states should pursue the following actions to reduce physical vulnerabilities and mitigate the evolving threat from Russian sabotage:

- Use Recorded Future® Intelligence Cloud's Facility Risk feature to monitor notable events occurring in close proximity to critical infrastructure facilities.
- Use the Recorded Future Intelligence Cloud to track potential Russian sabotage events and monitor commonly used tactics.
- Enhance national and local counterintelligence, surveillance, and physical security monitoring measures around critical infrastructure, such as those identified in previously documented Russian sabotage operations.

- Increase cooperation and intelligence-sharing among European nations on Russian sabotage activities and collaborate on identifying transnational Russian agent networks.
- Monitor for signs of escalating Russian hybrid activities, such as sudden upticks in unexplained accidents or environmental incidents, and communicate risks to relevant businesses and industries.

Outlook

European governments' warnings about the threat of Russian sabotage very likely reflect a rising frequency of suspected sabotage incidents across Europe, particularly in countries bordering Russia. These incidents likely reflect a significant shift in the nature and scope of hybrid warfare tactics employed by Moscow against European countries. NATO countries' support for Ukraine in its active conflict with Russia — which the Kremlin has increasingly warned could put NATO at war with Russia — almost certainly underpins this shift. As tensions between the West and Russia are almost certainly to remain at a low point, Russian intelligence operations are very likely to engage further sabotage operations to destabilize NATO allies, degrade NATO's war-fighting capacity, disrupt NATO support to Ukraine (such as by targeting military assets NATO committed to providing to Ukraine), weaken the alliance's collective security by targeting critical infrastructure, overwhelm emergency services, and instill fear in local populations.

Critical infrastructure — such as energy grids, transportation networks, and military installations — will likely remain primary targets, with Russian sabotage operations potentially expanding into non-critical infrastructure to negatively affect an adversary's populations, including by instilling fear and panic. As relations between Russia and the West will almost certainly remain fraught, Russia is very likely to increase the destructiveness and lethality of its sabotage operations without crossing the threshold of war with NATO as discussed in the Gerasimov doctrine.[46] These physical attacks will likely complement Russian efforts in the cyber and influence operations realm in line with Russia's hybrid war doctrine.

Future Russian sabotage operations will likely adapt to new technologies and domestic political situations, with a growing emphasis on plausible deniability. For example, by recruiting or supporting low-level criminals, disaffected members of society, anarchists, or domestic violent extremists to conduct sabotage operations and communicating with them via anonymous communication mechanisms like Telegram. This will likely require Russia to establish more networks of local proxies (including European political extremist groups) and agents embedded within these countries or use its current networks more extensively — thereby complicating attribution and response efforts by Western governments.

[46] *https://www.avnrf[.]ru/attachments/article/534/AVN-1(42)_maket_001-184.pdf*

Appendix A: Widely Read Online News Outlets

Analysts relied on several media landscape reports, including Reuters Institute for the Study of Journalism (RISJ), the BBC, and Media Landscapes. The following table provides a list of news outlets we searched during our research.

Country	Media Outlets
Estonia	Delfi Postimees ERR Õhtuleht Päästeamet
Finland	MTV Oy Yle Helsingin Sanomat Iltalehti Ilta-Sanomat
Latvia	VUGD Delfi.lv Leta.lv mixnews.lv La.LV Apollo
Lithuania	Lietuvos Rytas Delfi 15min Kauno Diena tv3.lt
Norway	VG Nett NRK News Dagbladet TV2 News
Poland	Gazeta Wyborcza Rzeczpospolita Polish News Agency (PAP) Onet.pl Interia

***Table 1**: Most popular news outlets in six countries we researched (Source: Recorded Future)*

Appendix B: CISA Critical Infrastructure Sectors

This report uses CISA's definition of critical infrastructure. CISA defines critical infrastructure as sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to a state that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. The following are sixteen critical infrastructure sectors identified by CISA:

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Services and Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Transportation Systems Sector
- Water and Wastewater Systems

Appendix C: Identified Incidents of Interest in Six European Countries

Estonia

	Location	Details [47]
1	Lööra	On June 3rd at 14:30 GMT+3, the alarm center received a report of a fire in an auxiliary building on the Ojasoo-Lööra road in the village of Lööra, Kose municipality. The first responders from Kose found a 15 x 30 meter gray PVC structure engulfed in flames. The fire was contained by 16:39 and fully extinguished by 21:01. The fire destroyed the PVC structure, along with the firewood and equipment inside. An investigation was initiated to determine the cause of the fire.
2	Tallinn	On June 5, 2024, a fuel tank exploded on Nõlva Street in North Tallinn (port area) at 05:06 GMT+3. The first responders arrived to find that the roof of a tank storing heavy fuel oil (marine fuel) had blown off. One worker, who was on the tank's roof at the time of the explosion, was injured. It is believed that the fire was likely caused by work being done on the roof, which ignited fuel vapors inside the tank. Fortunately, the tank was not full at the time, but it still contained around ten tons of heavy fuel oil. The quick response of the rescuers prevented further destruction of the tank. The exact cause of the explosion will be determined after further investigation.

***Table 2**: Incidents of interest in Estonia (Source: Recorded Future)*

Finland

	Location	Details
1	Turku, Tampere, Porvoo, and Sipoo	In June 2024, Finnish authorities began investigating unusual attempts to breach the water supply systems in Turku, Tampere, Porvoo, and Sipoo. According to Finnish media, the first break-ins were reported in May 2024, and there were at least eleven break-in attempts between May and early August 2024. The affected water facilities were primarily located near Tampere and Helsinki, Finland's most populated regions.
2	Joensuu	On June 28, 2024, a fire broke out at UPM's Joensuu plywood factory. The fire started in a dryer located in the factory hall and managed to spread to the roof structures. According to the rescue services, the initial blaze was quickly brought under control, resulting in only minor material damage.

[47] Analysts heavily relied on Google Translate to translate articles into English.

3	Santahamina	On June 26, 2024, Finnish Defence Forces reported that a fire broke out in the Santahamina garrison area. According to the Defense Forces, the fire occurred during an "operational activity" in the region, although the fire was far from buildings and did not cause personal or material damage. Finnish Defence Forces are investigating the cause of the fire.
4	Ruovesi	On June 23, 2024, a fire broke out in Ruovesi's municipal hall. According to the rescue service, the backup power source caught fire in the basement of the municipal hall. Because of the fire and the damage caused by it, employees of the municipal hall were asked to work remotely on June 24, 2024.
5	Lahti	On June 9, 2024, an industrial and storage hall in Lahti was completely destroyed by a large fire. Häme Police are investigating the incident as a case of arson.
6	Oulu	On June 5, 2024, the industrial hall of Encore Environmental Services caught fire in Oulu. According to Encore Environmental Services, the fire started in the recycling unit, which recycles cardboard, waste paper, data security papers, and household plastics. The cause of the fire is unknown.

***Table 3**: Incidents of interest in Finland (Source: Recorded Future)*

Latvia

	Location	Details
1	Riga	On the morning of June 29, 2024, a fire broke out in the area of the Latvijas Finieris plant, located in the Bolderaja district of Riga. It was later confirmed that the fire did not originate at the plant or the nearby car service but on the premises of SIA Corvus Company, an enterprise specializing in hazardous waste disposal. Preliminary reports indicated that the fire posed a heightened risk, with barrels, waste, and oil burning, along with a two-story building containing office spaces and a garage.

***Table 4**: Incident of interest in Latvia (Source: Recorded Future)*

Lithuania

	Location	Details
1	Kaunas	On June 24, 2024, a fire was reported at the Kaunas Aviation Factory. According to firefighters, the blaze involved cut branches burning in a large open area. There was no threat to nearby buildings, as the fire was not close to them. The factory and the adjacent military airfield have been shut down since 2009.

***Table 5**: Incident of interest in Lithuania (Source: Recorded Future)*

Norway

	Location	Details
1	Between Asker and Drammen Lieråstunnel	On June 13, 2024, the fire service reported that an underground cable channel had caught fire. The incident caused delays on several train lines, including the Oslo S - Bergen line on the Bergen Railway and the Oslo S - Stavanger S line on the Sørlandsbanen.
2	Oslo	On June 6, 2024, Oslo police reported that five cars were set on fire in separate instances. According to Tore Barstad, head of the police force, "None of these fires started by themselves. Everything is considered deliberate and misguided actions". More car fires were reported on June 7, 2024. According to Oslo Police, since April 2024, at least sixteen cars have been set on fire. Local media reported that the police arrested a man in his twenties in connection with the car fires, though the details of the investigation remain unknown.

***Table 6**: Incidents of interest in Norway (Source: Recorded Future)*

Poland

	Location	Details
1	Skarżysko-Kamienna	On June 10, 2024, a blast occurred at the Mesko arms factory in the southeastern Polish city of Skarzysko-Kamienna, leading to a fire and the death of a 59-year-old worker. Local media reported that the explosion at the armaments factory killed one person and injured several others.
2	Żagań	On June 28, 2024, ten fire brigades were deployed to battle a fire at the military training ground in Żagań. Four Dromader firefighting aircraft were also sent to assist in controlling the blaze. Initially, the fire covered five hectares of land, but it later spread to seven hectares. The fire broke out after 14:00 GMT+2 during military exercises at the training ground.
3	Sławków	On June 28, 2024, a fuel tank fire broke out around 04:00 GMT+2 at

		the LHS transshipment terminal in Sławków. The fire involved four diesel tanks with a total capacity of 40,000 liters, though it is unclear how much oil was inside at the time. Several nearby trucks were also burned in the blaze. According to local reporting at the time, Minister of Internal Affairs and Administration Tomasz Siemoniak directed the Internal Security Agency and the police to take special precautions regarding the fire at the gas station in Sławków. LHS (the Broad Gauge Metallurgical Line) is the longest broad gauge railway in Poland and the westernmost such line in Europe, with a track gauge of 1520 mm. It runs from the Most station near Hrubieszów to Sławków.
4	Klonowo	On June 27, 2024, nearly one hundred firefighters were deployed to battle a fire in two wood processing production halls in the village of Klonowo, located in the Działdowo district, according to the fire department. Local law enforcement is currently investigating the cause of the fire.
5	Jelcz-Laskowice	On June 26, 2024, a huge fire struck at a historic palace in Jelcz-Laskowice. Smoke was visible from several kilometers away. Firefighters were ultimately able to bring the blaze under control, but the roof of the building collapsed. The owner intends to rebuild.
6	Sierpc	On June 24, 2024, a fire broke out in a grain warehouse near Sierpc, sending a cloud of black smoke over the area. The fire brigade responded to the scene, but approximately 500 tons of grain was burnt in the blaze.
7	Oświęcim	On June 21, 2024, a major fire broke out at the Synthos chemical plant in Oświęcim, with one person taken to the hospital. The blaze was quickly brought under control after 25 fire brigades were deployed on-site. An investigation was initiated to determine the cause of the fire.
8	Wroclaw	On June 16, 2024, a huge fire enveloped the historic Stolberg Palace in Wrocław. Firefighters fought the blaze all night, but the roof ultimately collapsed and the building was almost completely consumed. Plans for a replacement structure remain in flux.
9	Nowy Sącz	On June 16, 2024, a fire broke out in a historic church in Nowy Sącz, resulting in the destruction of the wooden presbytery. The wooden church, built in 1686, is a valuable monument. Since 1990, it has served as an auxiliary church after the new, larger Holy Cross Church was opened.

***Table 7**: Incidents of interest in Poland (Source: Recorded Future)*

Appendix D: Historical Documented Sabotage Operations

The Conrad Case

In a report digitized in June 2007, Mitrokhin described the experience and activities of Conrad, also known as Gregor (real name Amman Joseph [Аммaн Езеф]), a KGB spy and "the head of military sabotage groups in Western Europe". Conrad was notable for establishing local sabotage networks comprised of Europeans willing to conduct operations within their countries, including Denmark, Poland, France, and Germany. According to Mitrokhin, Conrad was sent to Denmark in 1936 to carry out sabotage operations. These operations included the detonation of dynamite targeting two ships at the Port of Frederikshavn, the largest ferry harbor linking continental Europe to Scandinavia. For this operation, Conrad created a group of saboteurs, five individuals recruited earlier by Richard Jansen (Рихард Янсен), likely another Soviet intelligence officer.[48] One of the saboteurs was a steamboat engineer who supplied Conrad with dynamite. The operation ultimately failed due to poor planning and a lack of escape routes.

In 1938, Conrad made two attempts to sabotage the "Stefan Batory" ship, one of the best-known Polish vessels at the time. Neither attempt resulted in significant damage to the ship. Mitrokhin stated that during the first attempt, Conrad placed an incendiary device (a mix of cotton and paraffin)[49] in the ship's engine room and "calmly walked out of the ship". The second attempt also involved an effort to set the ship on fire, though Mitrokhin did not provide any additional information.

In 1952, Conrad was tasked with creating and heading sabotage units in West Germany, France, and Denmark. One of the objectives of these units was to carry out sabotage operations targeting US assets in the Kaiserslautern-Pirmasens area in Germany. Conrad was trained by Soviet intelligence to use various types of mines and create weapons and resource stashes in Western Germany. For his service to the Soviet Union, Conrad was awarded the Order of the Red Star in 1977. In 1981, at the age of 60, Conrad retired, likely in East Germany.

The Conrad case illustrates the Soviet Union's employment of operatives who recruit and train agents and direct them to conduct sabotage operations, allowing Russia to maintain plausible deniability. The Conrad Case also indicates that Soviet intelligence provided training on a need-to-know basis: Conrad was only trained on how to use mines in 1952, despite having conducted sabotage operations since at least 1936, according to Mitrokhin.

Russian Empire's Sabotage Efforts Against Germany

In his 1931 book, Drobov described several sabotage operations that were carried out in the early 1900s by officers of the Russian Empire or Soviet Union. While most of these operations were unsuccessful, they illustrate the types of activities Soviet/Russian intelligence agencies conducted to weaken their

[48] Mitrokhin does not provide any additional information on Jansen.
[49] Common ingredients in homemade exposive devices.

adversaries.[50] For example, Drobov stated that in January 1916, "the headquarters of the commander-in-chief of the Southwestern Front ordered a secret agent, a certain Fardi, to begin organizing a "revolutionary movement" in Türkiye, directed against the Germans who ruled there and the Young Turks who supported them". Ultimately, "Fardi" was unsuccessful, and the Stavka of the Supreme Commander, the supreme headquarters of the Russian Imperial Army in the field during World War I, severed ties with "Fardi". In another unsuccessful attempt, the Stavka attempted to organize "revolutionary committees" in Krupps factories in Alsace, which at the time was part of Germany, and carry out assassinations and explosions against government officials and buildings in the region. According to Drobov, the operation failed due to a lack of resources and talent.

[50] M A Drobov, *Малая война: партизанство и диверсии [Small War: Guerilla Warfare and Sabotage]*, 86.

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com