EVRO–ATLANTSKI SVET SLOVENIJE
EURO–ATLANTIC COUNCIL OF SLOVENIA
Kardeljeva ploščad 5, 1000 Ljubljana, Slovenija, t. +386 (0)1 5805 327, e-mail: info@euroatlantic.org, www.euroatlantic.org

* * * Euro-Atlantic Bulletin * * *

* * * Evro-atlantski Bilten * * *

Publisher/Izdajatelj: EACS / EASS **Vol. 6 No. 4, 2025**

Editor/Urednik: prof. dr. Iztok Prezelj **October 7, 2025**

ISSN 2712-5270

http://www.euroatlantic.org/bilten/

Lessons from History about Russian Sabotage

Kevin Riehle[1]

Abstract

Historical information about Soviet sabotage planning is instructive in analyzing Russian sabotage operations today. The Soviet KGB was responsible during the Cold War for preparing target packages on critical infrastructure sites and planning operations against them to be executed during periods of increased political tension preceding war, in what Soviet planners called the "special period". Sabotage operations, which are executed during the "special period", are planned and executed differently from disinformation operations, which are executed routinely across the peacetime-wartime spectrum. The prevalence of Russian-sponsored sabotage operations in Europe since 2023 is an indication that Russian intelligence services have returned to Soviet-era planning and thresholds for executing sabotage operations.[2]

Keywords sabotage, Russian intelligence services, critical infrastructure, reconnaissance, recruitment

[1] Kevin Riehle, Lecturer in Intelligence and International Security at Brunel University London.
[2] Note: The views expressed in this paper are the author's own and are not necessarily those of the EACS.

Kardeljeva ploščad 5, 1000 Ljubljana, Slovenija, t. +386 (0)1 5805 327, e-mail: info@euroatlantic.org, www.euroatlantic.org

Introduction

There is much discussion about Russian sabotage operations taking place in Europe. The operations are often described as novel and are assigned vague labels such as "hybrid warfare" or "grey zone warfare" (Edwards and Seidenstein, 2025; Richterova et al, 2024a; Jones, 2025; de Buchet, 2025). Authors herald a "new era" in Russian sabotage, highlighted especially by the use of computer networks (Richterova et al, 2024b).

In reality, these operations are not new but are deeply ingrained in Soviet and now Russian covert action planning. They are intended to weaken adversaries' will and capability to fight wars, and in some cases, to exacerbate existing political contradictions and exploit divisive relationships between states.

Two distinct types of Russian covert activities are prominent today: physical sabotage and disinformation operations. During the Soviet era, the latter were known as "active measures" [активные мероприятия], and in the post-Soviet era they are referred to as "measures of support" [мероприятия содействия]. The Soviet Union, and now Russia, conducted disinformation operations across the peacetime-wartime spectrum. They are designed, as Yevgeniy Primakov described in 1992, "so that the policies of Russia, our state, proceed better and more efficiently" (Primakov, 2014, p. 213).

Physical sabotage actions are different. In the Soviet system, they were known as "special actions" [спецакции]. They were managed by a different and more covert element of the KGB, known in the 1960s as Department V, subordinate to Directorate S, which also ran KGB illegals operations. Department V was responsible for collecting intelligence on potential sabotage targets and planning operations against them. It conceived of a range of operations to recruit sabotage operators in adversarial countries and destroy targets on command. However, few operations were ever executed. They were filed away to be brought out in what Soviet planners called the "special period" [особый период], which meant the period of increased tension just before the initiation of full hostilities, when Soviet intelligence and military capabilities were placed on a higher level of readiness (Mitrokhin, 2002, p. 291).

The fact that Russia has been conducting "special actions," both physical and computer-based, in Ukraine since 2014 is an indicator that Russia has reached and surpassed the "special period" there. The increased incidence of such activities in Europe since the beginning of Russia's full-scale invasion of Ukraine means Russian decision makers believe Russia is in the "special period" in relation to NATO. Consequently, studying the history of Soviet era preparations to conduct "special actions" provides a useful foundation for understanding Russian operations today.

Kardeljeva ploščad 5, 1000 Ljubljana, Slovenija, t. +386 (0)1 5805 327, e-mail: info@euroatlantic.org, www.euroatlantic.org

Historical Soviet Operations

A number of sources shed light on Soviet-era covert sabotage planning. Most prominent among them are the materials that KGB officer Vasiliy Mitrokhin collected and that were exfiltrated from Russia with his defection in 1992. Professor Christopher Andrew compiled some of those materials into two large volumes: The Sword and the Shield and The World was Going Our Way (Andrew and Mitrokhin, 1999; Andrew and Mitrokhin, 2006). However, despite their over 1,300 pages, those books cannot fully capture the crates of papers that Mitrokhin turned over, which are now stored at Cambridge University and are available to researchers, with some restrictions.

Mitrokhin's materials list intelligence illegals who were involved across the planning cycle, from collecting targeting data to recruiting an agent network to executing an operation. Several illegals have discussed their own role in sabotage operations. Walter Krivitsky, who defected in 1937, described plans in the 1930s to recruit low-level, untrained agents to conduct sabotage operations against critical industries and infrastructure facilities in wartime (UK Security Service). A KGB illegal who defected in Canada in 1971, Mihal Mihalcin, provided information about his tasking to collect infrastructure targeting information ("Moscow Spy School's Rule"). Sabotage operations were also managed from Soviet embassies, as revealed by Oleg Lyalin, a KGB officer who defected in 1971. Oleg Kalugin, who published a book about his time as a KGB officer in the United States in the 1960s and 1970s, also discussed embassy-based sabotage-related collection and planning (Kalugin, 2009, pp. 147-148).

Due to the timeframe of these sources regarding KGB sabotage operations, most available details date from the 1960s. The picture becomes less clear from the 1970s onward; Lyalin's defection is likely a factor to the lack of information.

All Soviet-era sources unanimously agree that physical sabotage operations were reserved for the "special period," unlike "active measures," which were executed frequently. Those sources all paint a similar picture, which closely resembles sabotage operations that have been attributed to Russia since 2014. Consequently, studying these cases can offer valuable lessons about how Russia operates today.

Recruiting local agents

Early in the operational planning process, KGB rezidenturas were tasked with locating and recruiting support agents. Local, often untrained agents have always played a role in Soviet and Russian "special actions." Walter Krivitsky described three levels of Soviet agents in the 1930s: first, workers selected and transported to the Soviet Union for special sabotage training. They were instructed to remain quiet during peacetime and keep working in their jobs in key industries until activated. The second

Kardeljeva ploščad 5, 1000 Ljubljana, Slovenija, t. +386 (0)1 5805 327, e-mail: info@euroatlantic.org, www.euroatlantic.org

type consisted of untrained sabotage agents who could cause disruptions wherever they worked, such as by producing faulty products or intentionally slowing the production line. The third type was mass sabotage that could be conducted when activated during wartime. Krivitsky distinguished physical diversionary activity from what he called "decomposition" work, which involved covertly spreading pro-Soviet and anti-capitalist information. Physical and informational operations were handled differently from each other (UK Security Service, pp. 65-69).

KGB-planned "special actions" in the 1960s also involved recruiting sabotage operatives who were ready to proceed when ordered. In 1963, the KGB rezidentura in Baghdad, Iraq, was tasked with developing operation KHISAR targeting a gas-burning power plant located in Baghdad. A local KGB agent codenamed SLESAR ("mechanic") was tasked with finding suitable agents to make up an "intelligence sabotage group" [разведывательно-диверсионная группа; RDG] to execute the operation when ordered (Mitrokhin, Papers, no. 417).

Similarly, in 1964, the KGB recruited an Armenian electrician codenamed KOES in Syria and instructed him to recruit other pro-Soviet Armenians and Kurds for an RDG targeting the Syrian oil infrastructure (Mitrokhin, Papers, no. 51). In 1966, a KGB illegal codenamed GRACHEV was in Norway collecting intelligence on potential landing sites for sabotage teams and storage sites for equipment. He was tasked with spotting and assessing Norwegians in the vicinity of the landing sites that could be recruited to support operations (Mitrokhin, Papers, no. 365).

Sometimes, the specific actions that would be taken depended on the agents that could be recruited. In 1970, the KGB developed a plan, codenamed TAYFUN, to sabotage a satellite communications ground station, codenamed KOSMOS, in the city of Katahagi, north of Tokyo, Japan. Depending on the types of agents the KGB could recruit, the methods of a sabotage attack could include shooting at the antennas, blowing up the water supply, shooting through the windows into the computer room or food supply, or blowing them up with explosives (Mitrokhin, Papers, nos. 511, 513).

During the Soviet era, sabotage agents were recruited based on their sympathy for communism. Today, the ideological driver is different: alignment with the belief that Russia is the protector of traditional values and a strong power. This ideological driver can be seen in the recruitment of Dylan Earl, who led a Russian-sponsored operation to damage a warehouse in east London that contained Starlink satellite equipment destined for Ukraine. Earl was reportedly sympathetic to Russia, which got him noticed in Moscow (Barnes, 2025). A recruited agent in Greece claimed a similar motivation when he was arrested in April 2025. The agent, a 59-year-old house painter who had immigrated from the former Soviet Union, operated for at least six months photographing the port of Alexandroupolis and nearby military installations, especially shipments bound for Ukraine. Greek police claimed that the agent was doing it "to help the 'motherland'" (Papadopoulos, 2025). Russian agent recruiters seek

Kardeljeva ploščad 5, 1000 Ljubljana, Slovenija, t. +386 (0)1 5805 327, e-mail: info@euroatlantic.org, www.euroatlantic.org

potential agents who express pro-Russian political views and regularly press that ideology to encourage agents.

Conducting Reconnaissance

The KGB conducted detailed reconnaissance of sabotage targets, collecting every aspect of security, movement, vulnerabilities, and strong points that were necessary to plan an operation. Soviet GRU defector Vladimir Rezun (pen name Viktor Suvorov) emphasized the importance of targeting an adversary's critical infrastructure, calling it the adversary's "nervous system (Suvorov, 1987, pp. 6-7). Targeting communications, energy generation facilities, oil pipelines, water distribution, and transportation systems required detailed intelligence collection to ensure that a sabotage attack would have the desired disruptive effect.

For example, in planning for sabotaging object KOSMOS near Tokyo the KGB collected intelligence about the personnel who worked there, security measures, electricity inputs, telephone communications, weak points, communications antenna configurations, which rooms contained computer equipment and which were used for food storage, along with information about the local neighborhood and routes of approach to the facility (Mitrokhin, Papers, no. 511).

Another contingency plan in Japan, codenamed VULKAN, identified the locations of beaches on the east coast of Honshu Island suitable for landing sabotage troops, along with small nearby villages and the distances and routes of travel between them, the amount of road traffic, and descriptions of the topography. The KGB determined that the region was a popular tourist destination, and no special permits were required to visit there. The operational package included descriptions of communication lines, electrical generation plants, airfields, oil storage facilities, and industrial plants to be targeted (Mitrokhin, Papers, no. 317). Two other sabotage plans for Japan, codenamed VOLNA-1 and VOLNA-2, envisioned blowing up water distribution pipelines that supplied water to portions of the Tokyo metropolitan area (Mitrokhin, Papers, no. 513). The attacks were to be conducted during the "special period" and would involve either a KGB agent-illegal or a KGB staff officer, depending on the agent network available at the time (Mitrokhin, Papers, no. 511). They were both intended to cause panic in the local population.

KGB illegal Mihal Mihalcin, who operated in Canada in the mid-to-late 1960s, was trained to reconnoiter military installations and infrastructure facilities, such as waterworks and pipelines. He was to note their construction materials, power sources, security measures, and personnel, particularly the names of senior officers or directors, for whom he was instructed to look for exploitable vulnerabilities ("Moscow Spy School's Rule"). Similarly, a KGB illegal codenamed PAKO was in the Middle East from 1962 to 1968 to collect intelligence on oil pipelines leading from Saudi Arabia

Kardeljeva ploščad 5, 1000 Ljubljana, Slovenija, t. +386 (0)1 5805 327, e-mail: info@euroatlantic.org, www.euroatlantic.org

and Iraq to Lebanese Mediterranean ports. He was tasked to collect details of difficult to access portions of the pipeline routes, such as where they crossed ravines, gullies, and cliffs (Mitrokhin, Papers, nos. 429, 430).

Between 1959 and 1965, the KGB collected intelligence on high-voltage electricity transmission lines that ran from Kelsterbach near Frankfurt am Main, Germany, to Rheinhof near the French border. A KGB agent codenamed KHIOS was tasked with obtaining a job at an electrical substation in Rheinhof in 1959, which allowed him to observe transmission lines crossing the Rhine River near Worms and near the village of Rohrhof. KHIOS provided technical details of the lines along that stretch and selected large-scale hiding sites. He reported precise locational information for emergency and fire services, transformers, and high-voltage towers. He collected details of the power demands in various locations and the transmission lines that served those locations. His information was required to plan operations against transmission lines and allowed the KGB to assess the impact of the sabotage on the local population (Mitrokhin, Papers, no. 255).

Oil pipelines were particularly attractive targets. The illegal KOES in Syria was tasked with collecting information about oil pumping stations near Palmyra and Homs, Syria. The ultimate objective was to use KOES as a sabotage agent to perform "special actions" against the oil distribution infrastructure, including sabotaging the electrical pump motors, thereby disrupting the flow of oil toward Syrian Mediterranean ports (Mitrokhin, Papers, no. 51).

In 1968, KGB headquarters sent an operational cable to all residencies titled "Recommendations for Creating the Necessary Conditions on the Territory of a Potential Adversary for Special Group [RDG] Operations in an Emergency" (Andrew and Mitrokhin, 1999, p. 375). Rezidenturas received specific instructions for what information to obtain for each target: the role of the target in peacetime and wartime, supported by documents, photographs, video films, maps, and diagrams detailing the target location, avenues of approach, work schedule, security, personnel, and neighboring facilities. A target file included the identities of agents recruited to support an operation, the necessary equipment, and the locations of dead drops and storage sites (Andrew and Mitrokhin, 1999, p. 636).

In 1971, Oleg Lyalin revealed the KGB's planning for operations in London, Washington, Paris, Bonn, Rome, and other Western capitals, as well as in cities in Canada. Lyalin reported that a Department V officer had been assigned to London since 1960 to develop sabotage operations targeting public utilities, railways, government and military communications, government offices, civil defense organizations, and emergency food supplies. Operations to sabotage those targets were to be "mounted in periods of great tension and in wartime" and "during the period of crisis preceding the outbreak of conventional war," or in other words, during the "special period" ("Defection of KGB Officer"). He reported operational plans already in place when he defected to flood the London Underground and blow up an early warning station at Fylingdale, North Yorkshire. Lyalin revealed

Kardeljeva ploščad 5, 1000 Ljubljana, Slovenija, t. +386 (0)1 5805 327, e-mail: info@euroatlantic.org, www.euroatlantic.org

that he was responsible for recruiting UK-based agents, some of whom he had already supplied with radios, to support future operations ("Defection of KGB Officer"). Lyalin's defection alarmed the KGB's Department V, and operational planning ground to a near standstill (Andrew and Mitrokhin, 1999, pp. 382-383). Few such operation plans are known from Lyalin's defection to the end of the Cold War.

There are echoes of Russian surveillance of critical infrastructure targets today. Dylan Earl conducted surveillance of the warehouse in East London before conducting an arson attack, and he recruited a group of sub-agents to conduct surveillance of two other businesses in London in preparation for further arson attacks (Counter Terrorism Policing, 2025).

Similarly, in 2023, the Polish counterintelligence service arrested fifteen people under suspicion of collecting information for future sabotage actions. A Belarusian agent was arrested in Gdansk in March, and he admitted to having been recruited to conduct reconnaissance of port facilities on the Baltic coast of Poland ("Służby wojskowe zatrzymały szpiega," 2023). Others, including Ukrainian refugees, were arrested after they were recruited to emplace cameras along Polish rail lines and trackers on rail cars carrying military equipment to Ukraine ("Российские спецслужбы," 2023). Another arrestee, Russian professional ice hockey player Maksim Sergeyev, was accused of identifying critical infrastructure facilities in the Silesia region of southwestern Poland ("Poland arrests Russian," 2023). These low-level, untrained agents resemble those that Krivitsky described in 1940, although their recruitment was based on either affinity for Russia or simply the need for money.

In October 2022, Ukrainian authorities arrested Anton Mysyk, who was similarly tasked with emplacing cameras along rail lines near Odesa, Ukraine, to collect the movements of military equipment and weapons (Romanenko, 2023). Mysyk's tasking appears to have gone further than just collection to executing attacks: police found explosives and ammunition when Mysyk was arrested (Ukraine Supreme Court, 2025).

Russian hydrographic research ships, such as the Yantar, have been observed on multiple occasions reconnoitering undersea communications cables. Russian ships have loitered over undersea cables off the coast of the United States and in the North Atlantic Ocean, including near the UK and Ireland (Barker, 2025). Computers are also important tools for surveilling potential sabotage targets and for spotting, assessing, and communicating with agents. Russian-sponsored computer-based surveillance of critical infrastructure is reported regularly (UK National Cyber Security Centre, 2024; Swai, 2025; US Federal Bureau of Investigation, 2025). Although these incidents are often labeled "attacks," they are in fact modern equivalents of surveillance in preparation for sabotage attacks like the KGB planned routinely during the Cold War. Because many critical infrastructure facilities have an internet-facing presence, computer networks allow remote access to targets, thereby avoiding the need for in-person surveillance in some instances.

Kardeljeva ploščad 5, 1000 Ljubljana, Slovenija, t. +386 (0)1 5805 327, e-mail: info@euroatlantic.org, www.euroatlantic.org

Computer networks also help to identify people sympathetic to Russia using social media watering holes, many of which are created by Russian intelligence services for that very purpose. Such a method was seen in the London arson attack, when a Russian service, likely the GU posing as the Wagner Group, identified Dylan Earl from his participation in pro-Russian social media platforms (Counter Terrorism Policing, 2025). The GU had already pinpointed the warehouse containing satellite communications equipment before contacting an agent. How the service knew what was in the warehouse is unclear—that was likely determined through previous reconnaissance. Although Earl could be identified online, the facility was not accessible via a computer network and required an agent on-site to execute the operation.

Technical collection, whether conducted by hydrographic vessels or computer networks, combined with human collection on the shoreline or inside facilities, provides Russia with an accurate picture of the targeted locations, like undersea communications cables and other critical infrastructure targets. These reconnaissance missions represent a collaborative relationship between Russian human and technical intelligence collection platforms (Sanger and Schmitt, 2015). While Russian services can approach some critical infrastructure systems via computer networks, they cannot do so for all of them. Russian services undoubtedly continue to seek insiders in infrastructure facilities to provide precise targeting data, even if some of the data can be collected online. Computers do not alter the purpose of surveillance or recruiting agents.

Political and Military Purposes

Lyalin reported that the objective of sabotage operations included the "demoralization of the civilian population and the complete disruption of the political and economic life of the country" ("Defection of KGB Officer"). The destruction of water distribution systems in Japan had such an objective. Consequently, most operations were planned to be executed in the "special period," when the environment was already tense and the risk of political backlash was less of a concern.

Other operations had both political and military purposes and were planned for peacetime to damage political adversaries or distract attention from Soviet aggression. Lyalin noted a proposal that the London KGB rezidentura submitted to headquarters for an operation to contaminate Holy Loch, Scotland, where US nuclear submarines were ported, with radioactive material and to blame US Naval forces. Such an operation was intended to turn the UK population against the United States ("Defection of KGB Officer"). The operation would have required the approval of the Central Committee of the Communist Party of the Soviet Union, which was never obtained.

Kardeljeva ploščad 5, 1000 Ljubljana, Slovenija, t. +386 (0)1 5805 327, e-mail: info@euroatlantic.org, www.euroatlantic.org

The KGB rezidentura in Athens proposed a physical sabotage operation, codenamed YAYTSO ("egg"), with a political purpose in 1969. The operation envisioned an explosion in a building owned by the Turkish government located near the Turkish consulate in Thessaloniki. The bombing would be blamed on nationalist Greeks who had emigrated from Turkey and who criticized the Turkish government. The explosion was not intended to cause heavy damage, but to further aggravate already tense Greek-Turkish relations, resulting in complications for NATO, to which both countries belonged (Mitrokhin, Papers, p. 408; Andrew and Mitrokhin, 1999, nos. 394-396).

Another sabotage operation with a political intent was conceived in 1968 to distract Western attention from the Soviet invasion of Czechoslovakia. The plan, codenamed ZVENO ("link"), envisioned sabotaging the Central European oil pipeline near Bodensee/Lake Constance, which forms part of the border between Germany, Switzerland, and Austria. A KGB illegal based in Switzerland, Gennadiy Mikhailovich Alekseyev (YAKOV), along with a Vienna KGB rezidentura agent, reconnoitered the target and devised a detailed operational plan. The KGB purchased explosives and intended to blame the explosion on Italian extremists. However, the KGB ultimately abandoned the operation as too politically risky (Andrew and Mitrokhin, 1999, nos. 375-376, 638). Alekseyev was arrested in Switzerland for obtaining a false identity (Office of the Attorney General, 1975).

The KGB never executed such large-scale, politically oriented physical sabotage operations. Today, some analysts claim that Russian sabotage operations since 2014 are intended for the political purpose of destabilizing Europe (Edwards and Seidenstein, 2025). However, the small-scale sabotage operations that Russia has conducted since 2023 do not reach the grandiose level of Soviet-era planned operations. Today's Russian operations appear more likely to be related to the war in Ukraine and often target Ukraine-related supplies, such as in the UK, Germany, Poland, and Greece. They are directed more toward disrupting the flow of weapons to Russia's wartime enemy than exacerbating political crises in Europe.

Some Policy Recommendations

1. Recognize Russia's perception of the situation in Europe

Russia's execution of physical sabotage activities is an indicator of Russian decision makers' view of the situation in Europe as having progressed to the "special period," as it was defined during the Cold War. As NATO planners prepare for future Russian actions, they must recognize that Russia will be less restrained and less concerned about the consequences or potential counteractions. Combined with Russia's designation of NATO countries and nearly all European countries as "unfriendly," sabotage operations will be designed to reduce adversaries' will and capability to fight against Russia, which Russian leaders believe is inevitable.

Kardeljeva ploščad 5, 1000 Ljubljana, Slovenija, t. +386 (0)1 5805 327, e-mail: info@euroatlantic.org, www.euroatlantic.org

2. Analyze Operations Through Russia's Lens

NATO planners need to analyze Russian preparations for sabotage operations as a comprehensive whole, rather than in artificially separated pieces. Computer-based operations and physical operations are the same in Russia's military planning, and taken together they form a unified manifestation of Russian operational planning. Reconnaissance conducted via a recruited agent on the ground and via a computer network serves the same purpose; thus, organizationally dividing them in our security systems creates unnecessary and counterproductive seams (Riehle, 2025).

On the other hand, disinformation operations and sabotage operations are different. They have different thresholds in Russian planning, with disinformation operations occurring routinely, in peacetime and wartime, to clear the path for Russian national security policies. Sabotage, on the other hand, is a wartime operation, conducted either in preparation for war or in war itself, as is occurring in Ukraine. Recognizing the difference between these operations enables NATO planners to concentrate resources effectively.

3. Monitoring Critical Infrastructure Sites

European security services need to monitor civilian critical infrastructure facilities for potential surveillance. Russian intelligence services will prepare target packages for civilian infrastructure, such as power generation, water distribution, transportation, and military command sites. Reconnaissance precedes an attack; thus, observations of reconnaissance, both physical and computer-based, are indicators that Russian services are preparing to attack a facility. Security services can expect increased reconnaissance around oil distribution infrastructure facilities, especially considering Ukraine's success in targeting Russia's oil network (Cleave, 2025).

Conclusion

Physical sabotage is not new in Russia. Numerous operations were planned during the Cold War, with support agents recruited, target packages compiled, and even, in some cases, equipment delivered. But the Soviet government never proceeded with them because the political leadership never determined that the political environment had reached the "special period."

Today, Russia is executing large sabotage operations in Ukraine and small-scale sabotage in Europe using a spectrum of methods, from physical destruction to computer-based operations. Although Western powers often separate Russian physical and computer-based sabotage into distinct disciplines, that division creates unnecessary and counterproductive seams in Western understanding of Russian covert sabotage activities. Studying historical operations reveals elements of similar operations today, providing valuable insights regardless of the physical or virtual method used. They

Kardeljeva ploščad 5, 1000 Ljubljana, Slovenija, t. +386 (0)1 5805 327, e-mail: info@euroatlantic.org, www.euroatlantic.org

also indicate that Russia has moved closer to the "special period" in Europe than it ever did during the Soviet era.

References

Andrew, Christopher and Vasili Mitrokhin (1999). The Mitrokhin Archive and the Secret History of the KGB. New York: Basic Books.

Andrew, Christopher and Vasili Mitrokhin. (2006) The World Was Going Our Way: The KGB and the Battle for the Third World. New York: Basic Books.

Barker, Memphis. (2025, 29 January). "The Russian Spy Ship in Britain's Waters Preparing Ground for War," The Telegraph, https://www.telegraph.co.uk/news/2025/01/29/russian-spy-ship-british-waters-preparing-war/.

Barnes, Trevor. (2025, 8 July). "Revealed: How Moscow's Wagner Group recruited young British men online to plot London arson attack," The Standard, , https://www.standard.co.uk/news/crime/moscow-wagner-group-putin-arson-london-warehouse-ukraine-b1237045.html.

Cleave, Iona. (2025, 27 September). "Great Russian petrol crisis rattles Putin," The Telegraph, https://www.telegraph.co.uk/world-news/2025/09/27/russian-petrol-crisis-rattles-putin/.

Counter Terrorism Policing. (2025, 11 July). "Group convicted after Russian-ordered arson attack in London," https://www.counterterrorism.police.uk/group-convicted-after-russian-ordered-arson-attack-in-london/.

de Buchet, Ninon. (2025, 26 August). "Hybrid Threats and the Evolution of Russian Sabotage," E-International Relations, https://www.e-ir.info/2025/08/26/hybrid-threats-and-the-evolution-of-russian-sabotage/.

"Defection of KGB Officer," British intelligence summary shared with the FBI, in Oleg Lyalin FBI file, 105-216642 serial 7. Obtained via FOIA.

Edwards, Charlie and Nate Seidenstein. (2025, 19 August). "The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure," International Institute of Strategic Studies, https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure/.

Jones, Seth G. (2025, 18 March). "Russia's Shadow War Against the West," Center for Strategic and International Studies, https://www.csis.org/analysis/russias-shadow-war-against-west.

Kardeljeva ploščad 5, 1000 Ljubljana, Slovenija, t. +386 (0)1 5805 327, e-mail: info@euroatlantic.org, www.euroatlantic.org

Kalugin, Oleg (2009). Spymaster: My Thirty-Two Years in Intelligence and Espionage Against the West. New York: Basic Books.

Mitrokhin, Vasiliy (ed.). (2002). KGB Lexicon: The Soviet Intelligence Officer's Handbook. London: Frank Cass.

Mitrokhin, Vasiliy, The Papers of Vasiliy Mitrokhin, MITN 2/16/2, K16 Illegals, Churchill Archives Centre, Cambridge University.

"Moscow Spy School's Rule: Never Tell Your Wife." (1972, 11 September). The Toronto Star, 4.

Office of the Attorney General of the Canton of Bern. (1975). "Auszug aus dem Urteil des Kassationshofes vom 12. September 1975 i.S. Mürner gegen Schweiz, BGE 101 IV 306," https://www.servat.unibe.ch/dfr/bge/c4101306.html.

Papadopoulos, Yiannis. (2025, 2 May). "Espionage in Alexandroupoli: House painter turned spy," Ekathimerini, https://www.ekathimerini.com/news/1268429/espionage-in-alexandroupoli-house-painter-turned-spy/.

"Poland arrests Russian ice-hockey player on spying charges." (2023, 30 June). Reuters, https://www.reuters.com/world/europe/poland-arrests-russian-ice-hockey-player-spying-charges-2023-06-30/.

Primakov, Yevgveniy (2014). "Разведка в современном мире," speech given to the Journalism Faculty, Moscow State University, 14 October 1992, in Primakov (ed.), Очерки истории российской внешней разведки [Essays on the History of Russian Foreign Intelligence], Vol. 6. Moscow: Mezhdunarodniye Otnosheniye.

Richterova, Daniela, Elena Grossfeld, Magda Long and Patrick Bury. (2024a, 17 September). "Russian Sabotage in the Gig-Economy Era," RUSI Journal, https://www.rusi.org/explore-our-research/publications/rusi-journal/russian-sabotage-gig-economy-era.

Richterova, Daniela, Elena Grossfeld, Magda Long, and Patrick Bury. (2024b, 4 November). "A New Era of Russ¬ian Sabotage." KCSI Insights, https://kcsi.uk/kcsi-insights/a-new-era-of-russian-sabotage.

Riehle, Kevin. (2025). Counterintelligence at its Core: Assessing and Preventing Foreign Espionage. Boulder, CO: Lynne Rienner Publishing.

Romanenko, Valentyna. (2023, 22 May). "Former Law Enforcement Officer Planning Explosions on Odesa Railway Given Life Sentence," Ukrainska Pravda, https://www.pravda.com.ua/eng/news/2023/05/22/7403347/.

Kardeljeva ploščad 5, 1000 Ljubljana, Slovenija, t. +386 (0)1 5805 327, e-mail: info@euroatlantic.org, www.euroatlantic.org

Sanger, David E. and Eric Schmitt. (2015, 25 October). "Russian Ships Near Data Cables Are Too Close for U.S. Comfort," New York Times, https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html.

"Służby wojskowe zatrzymały szpiega. Czego szukał w Polsce?." (2023, 27 March). Defense24, https://defence24.pl/polityka-obronna/sluzby-wojskowe-zatrzymaly-szpiega-czego-szukal-w-polsce.

Suvorov, Viktor. (1987). Spetsnaz: The Story of the Soviet SAS, London: Hamish Hamilton.

Swain, Gyana. (2025, 13 February). "Russian hacking group targets critical infrastructure in the US, the UK, and Canada," CSO, https://www.csoonline.com/article/3823955/russian-hacking-group-targets-critical-infrastructure-in-the-us-the-uk-and-canada.html.

UK National Cyber Security Centre. (2024, 1 May). "Heightened threat of state-aligned groups against western critical national infrastructure," https://www.ncsc.gov.uk/news/heightened-threat-of-state-aligned-groups.

UK Security Service, 'Information Obtained from General Krivitsky During His Visit to This Country, January–February 1940', The National Archives, Kew, London, KV 2/805, serial 55x.

Ukraine Supreme Court. (2025, 25 March). "Life imprisonment for high treason: Ukraine Supreme Court, Supreme Court upholds sentence to former security officer who passed data on Ukrainian Armed Forces to Russian special services," press release, https://court.gov.ua/eng/supreme/pres-centr/news/1779641/.

US Federal Bureau of Investigation. (2025, 20 August). "Russian Government Cyber Actors Targeting Networking Devices, Critical Infrastructure," Alert Number: I-082025-PSA, https://www.ic3.gov/PSA/2025/PSA250820.

"Российские спецслужбы вербовали в Польше украинских беженцев." (2023, 19 August). Ukrainskaya Pravda, https://www.pravda.com.ua/rus/news/2023/08/19/7416199/.

Kardeljeva ploščad 5, 1000 Ljubljana, Slovenija, t. +386 (0)1 5805 327, e-mail: info@euroatlantic.org, www.euroatlantic.org

EVRO-ATLANTSKI SVET SLOVENIJE
EURO-ATLANTIC COUNCIL OF SLOVENIA

Si želite izvedeti več o dejavnostih Evro-atlantskega sveta Slovenije? Vas zanima področje mednarodne varnosti? Pridružite se nam.

*Za več informacij obiščite našo spletno stran **www.euroatlantic.org** ali pošljite sporočilo na **info@euroatlantic.org**.*