Contemporary Sabotage Operations

27 FEBRUARY 2023

Malte Koppermann



Bitte Title und Subtitle hinzufügen

Introduction

To advance and defend their national interests, states make use of the comprehensive toolkit of influence. On the one hand, traditional tools of influence include imposing sanctions, military exercises, or public diplomacy. On the other hand, states may opt to employ non-traditional measures of influence that are widely regarded as illegitimate in order to enhance traditional measures of influence (Hoffman, 2018). One such measure is

sabotage. This essay argues that contemporary state-led sabotage mirrors Cold War-era sabotage doctrines. The persistence of sabotage operations since the end of World War Two demonstrates the centrality of this tool in the repertoire of statecraft to advance and protect national interests. Despite changes in the narratives that justify covert action and the means of conducting sabotage, the key objective of defending national interests has remained constant.

The prevalence and significance of sabotage operations is reflected in contemporary media reporting, where Russian sabotage plots against the West have made repeated headlines. While Russian drones, bombs, and missiles continue to cause destruction across Ukraine, Russia is waging a non-lethal war against NATO. From weaponising migration to jamming the GPS signals vital to civilian aviation, Russia seeks to undermine and effectively halt Europe's support for Ukraine. Additionally, mysterious fires at arms manufacturing plants and severed or damaged undersea data cables in the Baltic Sea have been attributed to the Kremlin (Helsinki Commission, 2024). This shows that sabotage is a frequently used covert action tool. Despite Russian sabotage being on the rise, it is not unique to Russia but has been employed by the United States (U.S.) as well.

During the Cold War, sabotage was embedded in the ideological struggle between the capitalist United States and the communist Soviet Union. Both superpowers have employed covert action to frustrate the policies, economies and military capabilities of their systemic opponent and their respective allies. At the same time, they attempted to uphold plausible deniability for their actions to avoid a direct military confrontation. Although both refrained from ever conducting such operations directly on each other's territories, they were frequently carried out on the soil of their respective allies. Since the collapse of the Soviet Union, ideological motivations have made way for pragmatic considerations of national security. Transcending this shift in narratives is their persistent reliance on proxies to execute sabotage operations. Whether Operation Mongoose in the 1960s or hiring of saboteurs through social media, intelligence services would commit significant effort in order to evade direct attribution. At the same time, state-led sabotage adapts to technological advancements. Sophisticated cyber-enabled sabotage has given states the opportunity to disrupt critical infrastructure and military facilities remotely, achieving greater plausible deniability.

The critical examination of the extent to which contemporary state-led sabotage mirrors the Cold War-era sabotage doctrine reveals a significant continuation of its role in the pursuit of long-term strategic objectives. Due to the brevity of this essay, the analysis and comparison of state-led sabotage operations in light of Cold War-era sabotage doctrines is restricted to the United States and the Soviet Union, later the Russian Federation.

Cold War-era sabotage doctrines

Rovner (2023) defines sabotage as "the weaponization of friction." Here, friction is understood as all negative effects on the routine performance of organisations, including computer errors or mechanical defects. Sabotage, then, seeks to exploit and exacerbate these frictions in order to make them unbearable for the organisation. In the military-political complex, targets for sabotage are military assets and facilities, information systems, communication networks or intelligence agencies. It must be borne in mind that sabotage generally does not focus on short-term results. Rather, it "gradually increases friction in the service of long-term objectives" (Rovner, 2023). The U.S. Department of Defense defines sabotage in military terms as "an act or acts with intent to injure, interfere with, or obstruct the national defense of a country by willfully injuring or destroying [...] any national defense or war materiel, premises, or utilities, to include human and natural resources" (2010, p. 209). Although this essay employs both definitions, it is restricted to those operations that cause or intend to cause physical harm to life and property.

In the immediate aftermath of the Second World War, the Cold War quickly began to divide the world into the Eastern and Western blocs. As for the Soviet Union, Donnelly claimed that the USSR would use "any and every political tool" (1980, p. 35) in order to destroy global capitalism. According to documents shared between the Soviet KGB and East German and Czechoslovak intelligence agencies, Soviet sabotage pursued three objectives. It would aim to frustrate the Western bloc's pursuit of policies the Kremlin viewed as hostile, firstly, in the domestic context and, secondly, in the context of NATO. Thirdly, sabotage operations would try to downgrade the West's economic basis and military capabilities. Importantly, the intensity and severity of these operations would depend on the level of escalation with the West (Richterova, 2024). A special focus would be on sabotaging key military logistics hubs, airfields, and reserve forces in times of war (Sherfrey, 1987). Another key characteristic of the Soviet sabotage doctrine to amplify the fallout of sabotage activities by accompanying them with "active measures." In order to maximise the disruptive potential of kinetic operations, information warfare tactics, such as propaganda and disinformation, would seek to escalate the fallout of sabotage (Richterova, 2024). This highlights that sabotage does not appear in a vacuum. Instead, it is embedded in wider covert action or "active measures."

On the other side of the Iron Curtain, on May 4, 1948, the U.S. Policy Planning Staff ushered in U.S.-led organised political warfare in order to pursue and protect national objectives using all means available. Ostensibly, it would serve as the answer to Soviet political warfare that had "become the most refined and effective of any in history" (Thorne & Patterson, 1996, p. 669). On the one hand, the realisation of this doctrine would rely on overt actions, meaning traditional statecraft such as diplomacy and economic

tools. On the other hand, the United States would also engage in covert operations. The National Security Council Directive on Covert Action specified that "propaganda; economic warfare; preventive direct action, including sabotage [...]" (NSC 10/2, 1948) were permissible in order to fight "International Communism." Crucially, these actions were to be conducted in a manner that offered the U.S. Government plausible deniability. This precaution was undertaken in order to avoid a direct military confrontation with the Soviet Union or its allies. The declassified 1976 Church Report found that the Central Intelligence Agency (CIA) had conducted 900 major covert action projects between 1961 and 1976 (Select Committee to Study Governmental Operations, 1976). However, the report did not specify how many of these were sabotage.

The analysis of both doctrines highlights that sabotage does not appear in a vacuum. Instead, it is embedded in a wider array of covert actions or "active measures." An analysis of sabotage operations must appreciate the clandestine context in which sabotage operations in tandem with other covert actions are executed. Looked at individually, any one covert action may have limited impact. However, as Rovner (2023) describes, sabotage is not a game-changer but a gradual exploitation of friction in service of long-term objectives. . Additionally, "when augmented with other coercive operations," (Reed, 2021, p. 22), it can have a strategic impact.

Same objective, different narrative

Although the narratives that legitimise sabotage have shifted, the objectives have remained unchanged. The key motivation behind sabotage is to frustrate the opponent's capabilities and resolve in order to defend and advance one's own national interests. The Cold War was characterised by a competition of ideologies. The capitalist United States was fighting communism while the communist Soviet Union wanted to dispose of the imperialist West. However, in the contemporary era, state-led sabotage has shifted from being embedded in a confrontation of ideological systems towards pragmatic considerations.

The United States have leveraged strategic sabotage to advance their foreign policy objectives since the Directive on Covert Action. During the Vietnam War, the two superpowers were in a proxy war against each other. While the United States supported the South Vietnamese regime in its fight against communism in Vietnam, the Soviet Union aided North Vietnam and the Viet Cong. In the 1950s and 1960s, the CIA actively conducted sabotage operations behind enemy lines in North Vietnam. Targets included "trains, buses, contaminating fuel and oil, organizing two hundred Vietnamese commandos trained by the CIA, and burying weapons in the cemeteries of Hanoi" (Weiner, 2007, p. 211). More than four decades later, the United States was at war with Iraq in 2003. Here, the CIA organised and led a group of Iraqi paramilitaries – the Scorpions – to conduct sabotage missions

around the start of the war (p. 492). The justifying narrative was no longer the fight against international communism but the alleged possession of weapons of mass destruction by the Iraqi regime and the global war on terrorism. The continued use of sabotage shows that it does not depend on ideological justifications. Instead, it is an available means in the toolkit of statecraft and warfare in order to disrupt governments and their policies that are seen as obstructive to United States strategic interests.

In 1968, Chairman of the KGB, Yuri Andropov, issued the order "On tasks of State security agencies in combating ideological sabotage by the adversary" (Andrew, 1999, p. 7). The Soviet Union became obsessed with combating domestic dissent and foreign policies it perceived as antagonistic to the regime. Even human rights were perceived as a weapon of the imperialist West to subvert Moscow. This "ideological subversion" by the West was to serve as a narrative to justify Soviet kinetic operations. This twentieth-century narrative has largely made way to more generic justifications under President Putin. In 2023, he issued a new foreign policy against the "hostile" West that was supposedly waging a hybrid war against the Russian Federation (Bloomberg, 2023).

After the relative absence of sabotage post-Cold War, one may argue that the recent intensification of sabotage activities is a departure from the Soviet sabotage doctrine. Granted, since the full-scale invasion in Ukraine on February 24, 2022, there have been almost 150 Russian hybrid attacks on NATO territory, of which a third were sabotage operations targeting critical infrastructure (Helsinki Commission, 2024). However, as noted above, the intensity of sabotage operations was tied to the level of escalation (Richterova, 2024). As the war against Ukraine has continued and Western military, economic, and humanitarian aid has increased, so has Russian sabotage. Contrary to a departure from the Cold War, the intensification of sabotage activities represents the continuation of Soviet sabotage doctrine into the modern-day Russian Federation. What is more, contemporary sabotage mirrors its Cold War predecessor because it is accompanied by information warfare. The increase in sabotage activities has been coupled with a large-scale propaganda and disinformation campaign. By relying on the penetration of social media platforms in Western societies, the Kremlin has been adamant about sowing discord and skewing the discourse on the war in Ukraine. While the European Union has banned Russian government outlets RT, formerly Russia Today, and Sputnik (Council of the EU, 2022), Russia has made ingenious use of social media, botnets, and fake websites to distribute its narratives. As the Atlantic Council (2024) writes, although the Russian effort to justify the invasion of Ukraine has fallen short of expectations, Western societies have been highly responsive to the narrative that blames NATO for the war in Ukraine.

Hence, sabotage is about the protection of national interests at the expense of the policies and capabilities of "hostile" governments. The shift

in narratives from ideology to geostrategy notwithstanding, the objectives driving state-led sabotage have remained unchanged across decades.

Persistent use of proxies

In order to avoid direct military confrontation with one another or their allies, the United States and Soviet Union relied and continue to rely on proxies to conduct sabotage. Both superpowers used their intelligence services to train, equip and direct foreigners to conduct clandestine operations on their behalf. On the one hand, as for the United States during the Cold War, arguably the most prominent operation that included sabotage was Operation Mongoose, authorised by President Kennedy in 1961. One year before the Cuban missile crisis, President Kennedy was convicted to dispose of Cuba's communist leader, Fidel Castro. There were many options to achieve that goal. One such option would have been for the CIA to stage an attack on the U.S.-held Guantanamo Bay as a pretext to invade Cuba. However, the Kennedy Administration discarded that idea as an outright escalation that may have resulted in nuclear war (Weiner, 2007, pp. 192–193). The alternative was Operation Mongoose, the largest U.S. intelligence effort within a Communist state (Thorne et al., 1996, p. 666). Sabotage would play a crucial role in enhancing the efforts to recruit the local population for guerilla warfare. A concrete sabotage plot would have been to contaminate Cuban strategic assets such as petroleum, oil, and lubricants. Although the United States would have been able to "liberate" Cuba in an amphibious invasion by itself, it preferred relying on Cubans (Lansdale, 2004, pp. 540–541). This had two benefits. While it provided the United States with some deniability, it also prevented a direct military confrontation with Cuba, or worse, the Soviet Union.

On the other hand, the Russian Federation, as did the Soviet Union, relied on proxy forces for sabotage operations. During the Cold War, the Soviet Union hired "agent-executioners" or "agents-saboteurs" from abroad to conduct a variety of sabotage activities (Richterova, 2024). However, two factors led to the departure from that practice. First, Russia has lost much of its personnel under diplomatic cover in Europe. Whereas 1,500 Soviet officials had been expelled from Western states between 1946 and 1991, since the start of the Russian full-scale invasion of Ukraine in 2022, more than 700 diplomats have been asked to leave Europe and North America (Riehle, 2024, p. 1238). Second, recent developments in information communication technologies (ICT) have facilitated the hiring, handling, and payment of saboteurs. Taken together, Richterova et al. (2024) argue that Russia has taken notes from the gig economy in the outsourcing of sabotage operations. The ease of hiring saboteurs, the lack of direct connections to Russian intelligence services, and the anonymity in payments through cryptocurrencies at least partially offsets the sabotage potential lost through the expulsion of diplomats and agents under diplomatic cover. Richterova

et al.'s (2024) argument is being corroborated by recent acts of sabotage across Europe. For example, in 2024, Russia recruited around ten Estonian nationals via social media to conduct sabotage against government officials inside Estonia (Tucker, 2024).

This demonstrates the persistent outsourcing of clandestine activities to gain (im)plausible deniability. Furthermore, those attacks were directly aimed at disrupting and degrading governments that pursued policies that were perceived as hostile to the United States or Russia. From a strategic standpoint, the two examples highlight that sabotage itself is no silver bullet. Rather, they are embedded in a wider context, intended to support traditional military action or the suppression of policies by adversarial governments.

The growing toolkit of sabotage

The exploitation of both new technologies and vulnerabilities showcases the continuation of advancing national interests by all means necessary. On the one hand, cyber- and cyber-enabled sabotage now constitute a central role in contemporary sabotage strategies. Unlike Cold War sabotage methods, cyber sabotage requires neither physical presence nor complex logistical and personnel arrangements. The contemporary interconnected world enables intelligence agencies to disrupt and even destroy critical infrastructure and military assets through offensive cyber means.

Regarding the United States, the most infamous example of cyber sabotage is the Stuxnet computer worm, targeting Iran's nuclear program. Although there is no concrete evidence of who exactly perpetrated the attack, the biggest beneficiaries of disrupted Iranian nuclear ambitions are the United States and Israel (Congressional Research Service, 2010, p. 5). The way the worm operated was through sabotaging the routine Siemens industrial control process technology that manages the speed of the motors (Farwell & Rohozinski, 2011, p. 25). This sabotage attack demonstrates how cyber capabilities can be used to generate a high impact without risking direct military confrontation with Iran. A high-risk alternative would have been an airstrike on nuclear enrichment facilities. Instead, the United States were able to protect their strategic objectives in the region while at the same time upholding plausible deniability.

As for the Russian Federation, cyber and cyber-enabled sabotage has been increasingly employed as part of the hybrid warfare campaign against the states providing aid to Ukraine. One example, the military intelligence (GRU) Unit 29155, is responsible for large-scale cyber sabotage operations, including the destruction of data and website defacements. U.S. authorities have observed more than 14,000 instances across 26 NATO and EU member states, where Unit 29155 has scanned domains for potential vulnerabilities (Cybersecurity & Infrastructure Security Agency, 2024). The number of successful cyber sabotage operations is not publicly available information.

As for another example, in late 2024, Polish authorities discovered a network of Russian and Belarussian-linked hackers. The group had been responsible for cyber sabotage activities against the Polish government, military, and economy (Antoniuk, 2024). Poland, one of the biggest military aid supporters to Ukraine, is a prime target for Russian subversive activities. As a member of NATO, Poland is not an attractive target for conventional attacks. In order to mediate the aggressive efforts to disrupt Polish support for Ukraine while staying below the threshold of war, Russia is using sabotage operations to frustrate Polish resolve. However, these attacks have hitherto not effectively undermined Polish determination in supporting Ukraine.

This example showcases that Russia will use any means at its disposal to stop policies it deems hostile towards its national interest. The same is true for the Stuxnet example. Taken together, the United States and Russia adapt their sabotage activities to technological advancements. In particular, cyber and cyber-enabled sabotage can be operated remotely. While United States saboteurs would have found it difficult to access Iranian nuclear enrichment facilities, Russia is facing increasing difficulty to keep its agents under diplomatic cover inside target countries. Where the recruitment of saboteurs fails, cyber sabotage offers a high-impact alternative that retains plausible deniability.

Concluding thoughts

State-led sabotage operations as a tool of statecraft have adapted to shifting political narratives, strategic considerations, and technological advancements. Irrespective of the time period, the core objective of this clandestine activity has remained consistent. It is used to advance and protect the national interest by frustrating, disrupting, and destroying the adversaries' military and economic policies and capabilities. Whereas Cold War-era sabotage was justified by ideological competition between the United States and the Soviet Union, contemporary efforts show a shift towards calculated strategic motivations. Despite this change, the reliance on proxies, upholding plausible deniability, and the incremental accumulation of short-term friction in the pursuit of long-term strategic objectives closely mirrors the Cold War-era sabotage doctrine. The recent intensification of sabotage by the Russian Federation underscores persistent use of sabotage in geopolitical competition. Since the operations must be understood in a wider context of political or hybrid warfare, there is a high probability of these attacks to continue.

Future research may benefit from investigating the actual impact of sabotage activities. Concretely, a comprehensive study of these operations has the potential to reveal their tactical, operational, and strategic value. Furthermore, it would be insightful to clearly distinguish between peace- and wartime sabotage, not only to analyse the impact but also.

Bibliography

Andrew, C. (1999). The sword and shield: The mitrokhin archive and the secret history of the KGB. New York, United States: Perseus Books Group.

Antoniuk, D. (2024, September 9). Poland dismantles cyber sabotage group linked to Russia, Belarus. Retrieved from https://therecord.media/poland-dismantles-cyber-sabotage-group-russia-belarus

Atlantic Council. (2024, November 26). Russia's evolving information war poses growing threat to the west. Retrieved from https://www.atlanticcouncil.org/blogs/ukrainealert/russias-evolving-information-war-poses-a-growing-threat-to-the-west/

Congressional Research Service. (2010, December 9). The stuxnet computer worm: Harbinger of an emerging warfare capability. Retrieved from https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-040.pdf

Council of the EU. (2022, March 2). EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik's broadcasting in the EU. Retrieved from https://www.consilium.europa.eu/en/press/press-releases/2022/03/02/eu-imposes-sanctions-on-state-owned-outlets-rtrussia-today-and-sputnik-s-broadcasting-in-the-eu/

Cybersecurity & Infrastructure Security Agency (2024, September 5). Russian military cyber actors target US and global critical infrastructure. Retrieved from https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a#:~:text=Since%20early%202022%2C%20the%20primary,European%20Union%20(EU)%20countries.

Donnelly, C. N. (1980). Operations in the enemy rear: Soviet doctrine and tactics. International Defense Review, 13(1), 35-41.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. Survival, 53(1), 23-40. DOI: https://doi.org/10.1080/00396338.2011.555586

Hoffman, F. G. (2018). Examining complex forms of conflict: Gray zone and hybrid challenges. PRISM, 7(4), 30-47.

Putin signs new Russia foreign policy against 'hostile' west (2023, March 31). Bloomberg. Retrieved from https://www.bloomberg.com/news/articles/2023-03-31/putin-signs-new-russia-foreign-policy-against-hostile-west

Reed, G. K. (2021). Assessing the effectiveness of strategic sabotage in supporting United States national security objectives (master's thesis). USMC Command and Staff College, Quantico, United States.

Richterova, D. (2024). The long shadow of Soviet sabotage doctrine? Retrieved from https://warontherocks.com/2024/08/the-long-shadow-of-soviet-sabotage-doctrine/

Richterova, D., Grossfeld, E., Long, M., & Bury, P. (2024). Russian sabotage in the gig-economy era. The RUSI Journal, 169(5), 10-21 DOI: 10.1080/03071847.2024.2401232

Riehle, K. P. (2024). Soviet and Russian diplomatic expulsions: How many and why? International Journal of Intelligence and CounterIntelligence, 37(4), 1238-1263. DOI: https://doi.org/10.1080/08850607.2023.2272216

Rovner, J. (2023). Theory of sabotage. Études françaises de renseignement et de cyber, 1(1), 139-153. doi: https://doi.org/10.3917/efrc.231.0139

Sherfrey, L. W. (1987). Operational employment of airborne forces: The Soviet approach and the implications for NATO (Monograph). Fort Leavenworth: School of Advanced Military Studies.

Thorne, C. T., & Patterson, D. S. (1996). Foreign relations of the United States: 1945-1950: Emergence of the intelligence establishment. Washington, D.C.: United States Government Printing Office.

Tucker, P. (2024, February 20). Russian hybrid operations on the rise in Estonia, Moldova: Similar Russian attempts to exploit ethnic divisions in democratic nations have preceded more aggressive action. Retrieved from https://www.defenseone.com/threats/2024/02/russian-hybrid-operations-rise-estonia-moldova/394318/

U.S. Department of Defense. (2019, November 8). Dictionary of military and associated terms. Retrieved from https://irp.fas.org/doddir/dod/jp1_02.pdf

U.S. Helsinki Commission. (2024). Spotlight on the shadow war: Inside Russia's attacks on NATO territory. Retrieved from https://www.csce.gov/publications/spotlight-on-the-shadow-war-inside-russias-attacks-on-nato-territory/

U.S. National Security Council. (1948, June 18). NSC 10/2. National security council directive on covert action. Retrieved from https://www.cia.gov/readingroom/docs/CIA-RDP80B01676R001100070002-3.pdf

Weiner, T. (2007). Legacy of ashes: The history of the CIA. New York, United States: The Doubleday Broadway Publishing Group.

DOI 10.69790/epis05.97220

EPIS