Sand in the gears: Sabotage in world politics

Joshua Rovner, Rory Cormac and Lennart Maschmeyer

20 October 2025

Contents

Abstract

Sabotage is ubiquitous but little understood in international relations. Sabotage, especially in terms of attacks on infrastructure and property, has increased in recent years and has taken a more central role in national security discourse across Europe. Unfortunately, scholarship is underdeveloped and fragmented across disciplinary silos, leading to conceptual confusion about the nature and scope of sabotage as a form of statecraft. This article seeks to provide conceptual clarity, and in doing so, lay the foundations to better understand and respond to such activity. It does so first by synthesizing ideas from disjointed literatures on conflict, intelligence, terrorism, public administration, and cybersecurity, before distilling key characteristics of sabotage and offering a novel definition. The article finds that sabotage is the weaponization of friction to degrade the performance of systems from within. Sabotage has a strategic logic distinct from related concepts of covert action and subversion: corrosively turning friction into advantage. This logic limits its impact as stand-alone tool but makes it particularly well-placed to enhance and enable other policy instruments. By placing sabotage on the research agenda and theoretically advancing scholarship on 'secret statecraft' more widely, this article has significant implications for understanding and responding to contemporary security challenges.

Keywords

cybersecurity, friction, intelligence, sabotage, strategy

Introduction

In September 2024, thousands of handheld pagers used by Hezbollah suddenly exploded. This audacious and sophisticated attack killed at least twelve people and injured thousands. With their primary mode of communication compromised, Hezbollah operatives switched to walkie-talkies. Those walkie-talkies exploded the following day in the vicinity of crowds who had gathered for the funerals of those killed by the pager attacks. Thirty-nine more died. There seems little question that Israel was responsible. The nature of this activity and its purposes, however, were not immediately clear. Some speculated this was a 'monumental cyber-attack'[1], ushering a new era in cyber-warfare.[2] Others immediately saw it in the context of Israel's long-standing approach

[1] Thomas Newdick Rogoway Tyler, 'Hezbollah's Exploding Pagers Could be as Monumental a Cyber-Espionage Operation as Stuxnet', *The War Zone* (17 September 2024), available at: <https://www.twz.com/news-features/hezbollahs-exploding-pagers-could-be-as-monumental-a-cyber-espionage-operation-as-stuxnet>, accessed 30 September 2024.

[2] Noureen Akhtar, 'Pagers Explosions Across Lebanon: Cyber Warfare's New Lethal Frontier', *Modern Diplomacy* (17 September 2024), available at: <https://moderndiplomacy.eu/2024/09/17/pagers-explosions-across-lebanon-cyber-warfares-new-lethal-frontier/>, accessed 30 September 2024.

to targeted killing.[3] Others, still, suggested that attacking Hezbollah's communications was an alternative to military invasion, deterring Hezbollah and its allies to avoid a larger war.[4] Conversely, legal analysts questioned whether this was an act of war in breach of international law.[5]

These ideas were plausible but incorrect. The pager attack was a classic act of sabotage: a deliberate effort to inject and weaponize friction into adversary systems, undermining their efficiency and morale. The individual explosions were small, but their combined effects devastated Hezbollah communications, sowed confusion, and induced paranoia.[6] Operatives were incapacitated and trust in communications plummeted. As it turned out, these effects helped facilitate Israel's ensuing invasion.[7]

The initial public response reflects deeper confusion about the scope, role, and nature of sabotage. This confusion is mirrored in the scholarly literature where sabotage remains ill-defined and often mythologized. This lack of conceptual clarity presents a significant challenge to international relations scholars, given the urgent need to put sabotage in theoretical and historical context. The pager operation was merely one in a spate of recent attacks. Security officials across Europe issued warnings following suspicious incidents in 2024, including fires in London and Lithuania, explosions at defence plants in Pennsylvania and Wales, and a string of plots to disrupt railways. German intelligence warned publicly that Russian sabotage had almost caused a plane crash. In September 2024, the head of Norwegian intelligence stated that 'We see acts of sabotage happening in Europe now'.[8] This pattern continued into 2025, with mul-

[3] Chris Livesay, 'Israel Had a Long, Partially Unclaimed History of Assassinations and Secret Operations Before the Exploding Pagers', *CBS News* (28 September 2004), available at: { www.cbsnews.com/news/israel-secret-operations-history-exploding-pagers-hezbollah/>, accessed 30 September 2024.

[4] Robert Satloff, 'How Exploding Pagers Can Lead to Calm Along Israel-Lebanon Border', The Washington Institute for Near East Policy (22 September 2024), available at: <https://www.washingtoninstitute.org/policy-analysis/how-exploding-pagers-can-lead-calm-along-israel-lebanon-border>, accessed 30 September 2024.

[5] Brian Finucane, 'Law of War Questions Raised by Exploding Pagers in Lebanon', *Just Security* (18 September 2024), available at: <https://www.justsecurity.org/100193/law-war-exploding-pagers-lebanon/>, accessed 30 September 2024.

[6] Maya Gebeily et al., 'How Israel's Bulky Pager Followed Hezbollah', *Reuters* (16 October 2024), available at: <www.reuters.com/graphics/ISRAEL-PALESTINIANS/HEZBOLLAH-PAGERS/mopawkkwjpa/>, accessed 14 October 2025.

[7] Close observers of the region anticipated the looming military problem that the pager attacks caused the Hezbollah soon after the operation was revealed. Vipratap Vikram Singh and Emile Hokayem, 'Pager Attack Increases Pressure on Hizbullah', International Institute for Strategic Studies (18 September 2024), available at: <https://www.iiss.org/online-analysis/online-analysis/2024/09/pager-attack-increases-pressure-on-hizbullah/>, accessed 29 August 2025.

[8] 'Vladimir Putin's Spies Are Plotting Global Chaos', *The Economist* (13 October 2024), available at: <www.economist.com/international/2024/10/13/vladimir-putins-spies-are-plotting-global-chaos>, accessed 31 October 2024.

tiple accusations of sabotage of underwear cables in the Baltic Sea.[9] In May, Poland closed the Russian consulate in Krakow after uncovering evidence proving Russian intelligence services were behind a huge fire that destroyed a shopping centre in the Polish capital.[10] Such activities, and their fallout, are only expected to increase.[11]

One prominent scholar put it bluntly: 'whereas previously special operations supported foreign policy, today special operations *are* [Russian] foreign policy'.[12] If Russia is responsible for many of these, what is the point? Is it an exercise in nihilism, sowing chaos for its own sake? Does Russia believe that sabotage will increase disillusionment with the so-called liberal international order? Or does it have more specific goals in mind, like increasing the costs of supporting Ukraine and slowing the delivery of military supplies?[13] The wide range of targets provides evidence for all of these interpretations. Indeed, sabotage has formed part of the conflict both before and following Russia's full-scale invasion in 2022, spanning fires in arms depots and explosions on bridges to short term cyber-attacks on energy infrastructure and longer-term destruction of undersea gas pipelines. In May 2024, a huge blaze destroyed a factory of the arms manufacturer Diehl (producer of the 'Iris-T' air defence system Germany delivered to Ukraine) in Berlin.[14]

As the pager attack demonstrates, Russia is not solely responsible for the surge in sabotage. Other states and non-state groups have become involved. In July 2024, for instance, a coordinated series of fires immobilized large sections of the French high-speed rail network on the eve of the Olympic Games. The French arson was quickly linked to the far left.[15]

The growing prominence of sabotage and ongoing discussions – both within and beyond academia – highlight a problem. Observers use the word sabotage to describe a wide variety of actions. There are many ways to disrupt machines and physical

[9] Richard Milne, 'Baltic Sea Data Cable Damaged in Latest Case of Potential Sabotage', *Financial Time* (28 January 2025), available at: <https://www.ft.com/content/b8765ad0-3e72-41b8-9915-da86b25de033>, accessed 31 January 2025.

[10] Shaun Walker, 'Poland to Close Russian Consulate in Krakow Over Warsaw Fire', *Guardian* (12 May 2025), available at: <https://www.theguardian.com/world/2025/may/12/poland-to-close-russian-consulate-krakow-warsaw-shopping-centre-fire>, accessed 30 May 2025.

[11] Matthew Redhead, 'Old Wine, New Bottles? The Challenge of State Threats', *RUSI Research Paper* (January 2025), available at: <https://www.socace-research.org.uk/publications/soc-ace-rp32-state-threats>, accessed 31 January 2025.

[12] Sergey Radchenko quoted in Redhead, 'Old Wine, New Bottles?'

[13] For discussion, see Daniela Richterova, Elena Grossfeld, Magda Long and Patrick Bury, 'Russian sabotage in the gig-economy era', *RUSI Journal,* 169:5 (2024), pp. 10–21.

[14] Bojan Pancevski, 'Russian Saboteurs Behind Arson Attack at German Factory', *Wall Street Journal* (23 June 2024), available at: <www.wsj.com/world/europe/russian-saboteurs-behind-arson-attackat-german-factory-c13b4ece>, accessed 30 September 2024.

[15] Sudip Kar-Gupta and Gabriel Stargardter, 'France Suspects Far-Left Groups Were Behind Rail Sabotage, Minister Says', *Reuters* (29 July 2024), available at: <https://www.reuters.com/world/europe/france-leaning-towards-far-left-suspects-behind-rail-sabotage-minister-says-2024-07-29/>, accessed 30 September 2024.

infrastructure, for instance, from manipulating supply chains to arson and the use of explosives. Attacks on information systems may similarly range from cutting cables to offensive cyberspace operations. Sabotage is sometimes assumed to be inherently violent, but also used to describe bureaucratic sabotage, policy sabotage, electoral sabotage or ideological sabotage. Meanwhile, some campaigns are conspicuous while others are meant to be invisible. All of this creates a puzzle about the parameters of sabotage and its place in the wider security landscape.

Conceptual confusion has important implications. It risks misunderstandings of so-called grey zone activity by overemphasizing novelty, impact, and secrecy, which in turn complicates policy and legal responses. For example, the UK's *National Security Act 2023* created a new criminal offence of 'sabotage', but applies it only to attacks conducted by, on behalf of, or in the interests of a foreign state. Finding evidence that meets this 'foreign condition' is likely to prove difficult, given the murky details of unexpected fires, suspicious malfunctions, and sundry breakdowns.

In seeking to put sabotage firmly on the research agenda, this article addresses the following questions. First, what is sabotage and what differentiates it from adjacent activities and concepts? Second, what is its distinct strategic logic and how does it work? Third, what can it achieve and what are its limitations?

In doing so, it not only seeks to set the research agenda but also to use sabotage as a vehicle to advance theoretically the literature on covert action and so-called secret or 'grey' statecraft. We make three arguments. First, sabotage is the weaponization of friction to degrade the performance of a target's system from within. Second, sabotage has a strategic logic distinct from related concepts of covert action (which hinges on non-acknowledgement or plausible deniability) and subversion (which hinges on manipulating behaviour). In short, its logic hinges on turning friction into advantage. Third, given this distinct logic, sabotage is limited as a stand-alone tool, but rather works to enhance and enable other policy instruments. Although other tools of 'secret statecraft' also act as force-multipliers, sabotage's distinct logic makes it particularly well-placed to do so: degrading performance creates space for other policy tools.

We advance these arguments by surveying multiple literatures on sabotage and highlighting several unsolved challenges. We then use a process of qualitative meta-synthesis to distil core characteristics of sabotage, before testing these against related concepts of covert action and subversion. This helps determine the parameters of sabotage and refine our definition. Finally, we examine the strategic utility across a range of purposes: deterrence and counterproliferation, counterterrorism and counterinsurgency, diplomacy and war. The conclusion discusses new directions for research on sabotage and international security.

Sabotage: Current understandings and challenges

Multiple scholarly disciplines have addressed the issue of sabotage but have tended to do so within disciplinary silos, thereby creating competing understandings and conceptual confusion.

Military historians have devoted considerable attention to memorable case studies. Lawrence of Arabia's efforts against Ottoman infrastructure dominated understandings of sabotage in the First World War and created an enduring legacy.[16] Historians have also focused on Special Operations Executive activity in the Second World War. Tasked by Churchill with 'setting Europe ablaze', it planted explosives deep behind enemy lines – hidden in everything from bottles to horse droppings – to disrupt railroads, military depots, bridges, etc.[17] British and American operatives organized resistance in Nazi occupied Europe, training locals in sabotage techniques. Most famous of all was the allied sabotage against Nazi Germany's nuclear programme.[18]

However dramatic, such stories warp our understanding of sabotage. They suggest that small numbers of daring and committed operatives can produce extraordinary results, even changing the course of war. In focusing on weapons, techniques, and operations, the phenomenon of sabotage is often left undefined or taken for granted.[19] Moreover, studies imply that sabotage involves explosive attacks on infrastructure, thereby often reducing it to a narrow military tactic, with little attention to underlying strategic questions or recognition of its existence beyond the conventional military domain.[20]

Intelligence scholarship has expanded the study of sabotage in peacetime and has contributed important work on the use and limits of secrecy. Studies of covert operations are particularly relevant to students of sabotage, given that secrecy prevails in both domains.[21] Influenced by the US 1948 National Security Council Directive 10/2,

[16] For early discussion, see Irving Howe, 'T. E. Lawrence: The problem of heroism', *The Hudson Review*, 15:3 (1962), pp. 333–64. For a more recent account of how the war was supposedly shaped by adventurers like Lawrence see Scott Anderson, *Lawrence in Arabia: War, Deceit, Imperial Folly and the Making of the Modern Middle East* (London: Atlantic Books, 2014).

[17] See, for example, Giles Milton, *Churchill's Ministry of Ungentlemanly Warfare: The Mavericks who Plotted Hitler's Defeat* (London: John Murray, 2015). For a highly impressive tonic, see Halik Kochanski, *Resistance: The Underground War in Europe, 1939–45* (London: Penguin, 2022).

[18] See Damien Lewis, *Hunting the Nazi Bomb: The Secret Mission to Sabotage Hitler's Deadliest Weapon* (London: Quercus, 2016); Neal Bascomb, *The Winter Fortress: The Epic Mission to Sabotage Hitler's Atomic Bomb* (New York: Bloomsbury, 2016).

[19] See, for example, an influential account of the Special Operations Executive: Mark Seaman (ed.), *Special Operations Executive: A New Instrument of War* (Abingdon: Routledge, 2006).

[20] For an exception see Kochanski, *Resistance*. See also James Kiras, *Special Operations and Strategy: From World War II to the War on Terrorism* (Abingdon: Routledge, 2004).

[21] See for example recent works by leading scholars such as Loch Johnson, *The Third Option: Covert Action and American Foreign Policy* (Oxford: Oxford University Press, 2022), and Rhodri Jeffrey's-Jones, *A Question of Standing: The History of the CIA* (Oxford: Oxford University Press, 2022). See also a recent article by a new generation of scholars using the Cold War as the key refer-

which specified sabotage within a list of 'clandestine activities',[22] scholars have since typically presented sabotage as an option within the covert action toolkit, alongside propaganda, illicit financing of foreign groups, secret paramilitary support, assassinations, coup-plotting, and so forth. Indeed, Loch Johnson, perhaps the most influential scholar of such activities, describes sabotage as a 'form' of covert action, recognizing its economic role and its place often in the broader context of paramilitary attacks.[23]

This is important, and sabotage – notably in the form of physically attacking infrastructure (described by Johnson as classic sabotage) – can undoubtedly be a form of covert action when conducted in a plausibly deniable or unacknowledged manner. However, this is not always the case, and interpreting it solely through the prism of covert action or intelligence studies leads to a limitation and a misunderstanding. Like military history, such scholarship is limited by its tendency to take definitions of sabotage as implicit or for granted and struggles to interrogate assumptions of 'success'.[24] It risks overemphasizing the kinetic or paramilitary dimension of sabotage, at the expense of, for example, cyber-attacks or sabotage's intangible psychological effects. This, in turn, creates some conceptual confusion about the relationship between sabotage and other 'forms' of covert action, risking the conflation of means with ends. For example, it struggles to explain famous examples of historical 'administrative' or 'bureaucratic sabotage' conducted by US and UK agencies, which conflate subversion and/or propaganda with sabotage[25]; and, separately, why analysts have described pro-

---

ence point against which to compare today's Russian sabotage: Richterova et al., 'Russian sabotage'. Elsewhere, and building on work by pioneering intelligence historians, International Relations scholars are increasingly examining the role of covert action as state intervention. See Austin Carson, 'Facing off and saving face: covert intervention and escalation management in the Korean War', *International Organization*, 70:1 (2016), pp. 103–131; Rory Cormac and Richard J. Aldrich, 'Grey is the new black: Covert action and implausible deniability', *International Affairs*, 94:3 (2018), pp. 477–94; Rory Cormac, *How to Stage a Coup and Ten Other Lessons from the World of Secret Statecraft* (Atlantic, 2022); and Lindsey O'Rourke, *Covert Regime Change: America's Secret Cold War* (Ithaca, NY: Cornell University Press, 2018).

[22] NSC 10/2, 'National Security Council Directive on Office of Special Projects' (18 June 1948), available at: <https://history.state.gov/historicaldocuments/frus1945-50Intel/d292>, accessed 30 September 2024.

[23] Johnson, *The Third Option*, p. 33 and chapter 1.

[24] For discussion, see Rory Cormac, Calder Walton, and Damien Van Puyvelde, 'What constitutes successful covert action? Evaluating unacknowledged interventionism in foreign affairs', *Review of International Studies,* 48:1 (2022), pp. 111–28.

[25] See, for example, the American Office of Strategic Services, 'Simple Sabotage Field Manual,' 1944, which famously outlines how to disrupt meetings and otherwise cause bureaucratic headaches, available at: <https://www.cia.gov/static/5c875f3ec660e092cf893f60b4a288df/SimpleSabotage.pdf>. Likewise, the British Special Operations Executive undertook so-called administrative sabotage by, for example, forging Nazi ration cards. Lee Richards, *The Black Art: British Clandestine Psychological Warfare Against the Third Reich* (London: psywar.org, 2010), pp. 11 and 65–80.

paganda as ideological sabotage.[26] In this sense, sabotage is a strategic method that can be implemented by a variety of means traditionally associated with covert action.

A welcome recent exception lies in Richterova et al., which defines sabotage as: 'a classic form of kinetic covert warfare, [it] is designed to hit the enemy in a deniable, undetectable way: to weaken, sow chaos, heighten uncertainty or "weaponise friction" in times of crisis and escalation'.[27] This is helpful, but again explicitly limits sabotage to a 'kinetic' and 'warfare' context in which deniability and undetectability are central. The wider study of secrecy in international relations has developed hugely in recent years,[28] and defining sabotage as inherently deniable and undetectable does not recognize the more nuanced dimensions of exposure and attribution elsewhere.

Sabotage is also relevant to literature on cyber operations, much of which similarly emphasizes their military and extraordinary nature. The first wave of theorizing conceived of cyber operations primarily as a means of war.[29] Many ascribed extraordinary strategic potential to cyber-attacks, expecting them to herald a revolution in the nature of conflict itself.[30] Some scholars, however, identified the relevance of cyber operations for sabotage early on. Thomas Rid argued in 2013 that cyber operations primarily conduct three types of activity: espionage, sabotage, and subversion.[31] He suggests a narrow conception of sabotage as weakening or disabling military or economic systems, however, that excludes much of the activity described above. As a result, the impact is limited, and there is no need to articulate the range of outcomes it can achieve under different circumstances.[32] More recent scholarship on cyber conflict has shifted from a focus on warfare to low intensity conflict. An influential book acknowledges the suitability of cyber operations for sabotage yet treats them as different because cyber

[26] As understood by the Soviets during the Cold War. See Kenneth Pridham, 'The Soviet view of current disagreements between the United States and Western Europe', *International Affairs*, 59:1 (1982), pp. 17–31.

[27] Richterova et al., 'Russian sabotage', p. 10.

[28] For a review see Allison Carnegie, 'Secrecy in international relations and foreign policy', *Annual Review of Political Science,* 24 (2021), pp. 213–233.

[29] John Arquilla and David Ronfeldt, 'Cyberwar is coming!', *Comparative Strategy* 12:2 (1993), pp. 141–65; Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* (New York: Thunder's Mouth Press, 1995); Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (eds.), *Cyberpower and National Security* (Washington, D.C.: National Defense University Press, 2009); William J. Lynn III, 'Defending a new domain: the Pentagon's cyberstrategy', *Foreign Affairs*, 89:5 (2010), pp. 97–108; Jordan Branch, 'What's in a name? Metaphors and cybersecurity', *International Organization,* 75:1 (2021), pp. 1–32.

[30] Schwartau, *Information Warfare*; Ralf Bendrath, 'The cyberwar debate: Perception and politics in US critical infrastructure protection', *Information Security: An International Journal,* 7 (2001), pp. 80–103; Dima Adamsky and Kjell Inge Bjerga, 'Introduction to the information-technology revolution in military affairs', *The Journal of Strategic Studies,* 33:4 (2010), pp. 463–68; and Lucas Kello, 'The meaning of the cyber revolution: perils to theory and statecraft', *International Security* 38:2 (2013), pp. 7–40.

[31] Thomas Rid, *Cyber War Will Not Take Place* (Oxford: Oxford University Press, 2013).

[32] Rid, *Cyber War*, p. 57.

operations are capable of vastly more strategic impact than sabotage.[33] Consequently, the authors argue that cyber operations exist in a new category of power, and again conflate a range of distinct activities – i.e. espionage, sabotage, subversion – under the umbrella term. In short, the relevance of cyber operations as means of sabotage is underdeveloped, and consequently, the scope of activities involved and their strategic potential are unclear.

Sabotage spans scholarship far beyond the fields of military history, covert action, and cyber studies. Once again, other disciplinary approaches and their definitions focus narrowly on specific types of sabotage related to different domains. Sabotage is listed as one form of 'bureaucratic spoiling' by public administration scholars interested in organizational efficiency.[34] Others similarly define 'policy sabotage' as 'the deliberate effort to hinder the implementation of a policy enacted by the opposition party'.[35] These terms give little sense of the types, usage, and deliberate coordination of sabotage recognizable to, say, military historians. They do, however, explicitly recognize that 'sabotage is multifarious and not limited to violent actions' (although defining it as 'to be engaged in negative work' is perhaps too broad[36]), and emphasize that 'administrative sabotage is defined by intent' over means: an agency 'deliberately seeks to kill or nullify a statutory program in whole or part, that Congress has charged the agency with administering'.[37] While the centrality of intent could apply beyond administrative and legal scholarship, the nullification of Congressional programmes is, again, limited to a specific domain.

Industrial sabotage was originally seen as an anarcho-syndicalist tool to bolster workers' pay and conditions,[38] with classic definitions including 'the rule-breaking which takes the form of conscious action or inaction directed towards the mutilation or destruction of the work environment...' (from 1971) and 'the clogging of the machine of capitalist industry by the use of certain forms of action, not necessarily violent and not necessarily destructive...' (from 1920).[39] Meanwhile, terrorism and political

[33] Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace* (New York: Oxford University Press, 2022), p. 58.

[34] Frederik Trettin and Julian Junk, 'Spoilers from within: bureaucratic spoiling in United Nations Peace Operations', *Journal of International Organizations Studies,* 5:1 (2014), pp. 13–27; see also A. Brecht, 'Bureaucratic sabotage', *The ANNALS of the American Academy of Political and Social Science*, 189:1 (1937), pp. 48–57.

[35] Alexander V. Hirsch and Jonathan P. Kastellec, 'A theory of policy sabotage', *Journal of Theoretical Politics,* 34:2 (2022), pp. 191–218.

[36] John Brehm and Scott Gates, *Working, Shirking, and Sabotage: Bureaucratic Response to a Democratic Public* (Ann Arbor: University of Michigan Press, 1997), p. 28.

[37] David L. Noll, 'Administrative sabotage', *Michigan Law Review,* 120 (2022), pp. 753–824, at p.763. Noll argues it is the intent to kill or nullify a programme that differentiates sabotage from slacking or shirking.

[38] The classic text is Emile Pouget, *Sabotage*, translated from the French and introduced by Arturo Giovannitti (Chicago: Charles H. Kerr, 1913).

[39] For discussion, see, Geoff Brown, *Sabotage* (Nottingham, UK: Spokesman Books, 1977), p. xi. He adopted the latter.

violence scholars debate 'ecotage', defined as 'a variety of criminal acts (e.g. vandalism, arson, and threats) undertaken in the name of protecting nature'.[40] Expansive definitions of terrorism used by law enforcement agencies encompass environmentally motivated sabotage, yet critics point to a fundamental conceptual difference between violence against people (terrorism) and against property (sabotage).[41] Despite focusing on a siloed domain and limiting sabotage to physical violence, discussions of ecotage and ecoterrorism do highlight the political nature of the definition, raising important questions about labelling and power dynamics.

Fault lines within existing (and implicit) definitions include the levels of organization or coordination, intent versus means, and the roles of violence, criminality, target (people versus property), secrecy, and directness. We are left with a conceptual muddle. Observers define many different activities as sabotage, but it is not immediately clear what they have in common. At the same time, observers have described other activities, which look to us like sabotage, as something different, again eroding conceptual clarity and leading to scholars talking across each other.

Conceptualizing sabotage

To help overcome this problem and build a concept of sabotage that is useful to historians, social scientists, and policymakers, this section identifies common characteristics of sabotage activity from antiquity to the present. It does so using a method of qualitative meta-synthesis to systematically review and analyse studies across multiple disciplines to identify common themes, patterns, and concepts. We adopt an interpretative process, developed from social sciences but innovative in strategic studies, to code and refine similarities across a wide range of cases emanating from diverse fields, from military history to cybersecurity, industrial relations to terrorism studies.[42] This

[40] Travis Wagner, 'Reframing ecotage as ecoterrorism: news and the discourse of fear', *Environmental Communication,* 2:1 (2008), pp. 25–39; Alexandra Plows, Derek Wall, and Brian Doherty, 'Covert repertoires: ecotage in the UK', *Social Movement Studies,* 3:2 (2008), pp. 199–219.

[41] For discussion, see Sean Fleming, 'Searching for ecoterrorism: the crucial case of the Unabomber', *American Political Science Review,* 118:4 (2024), pp. 1986–99. See also Ben Farrer and Graig R. Klein, 'How radical environmental sabotage impacts US elections', *Terrorism and Political Violence,* 34:2 (2019), pp. 218–239. They point to 'Forceful and Violent Environment Sabotage (FVES)' defined 'as deliberate acts of property damage, aimed at preventing harm to the natural environment'.

[42] We first defined our leading research question – what is sabotage and how does it work? – before setting criteria for inclusion to develop our conceptualization. These included cases defined or described in academic literature as 'sabotage', using a deliberately inclusive approach spanning cases from military history to management studies, and from Ancient Greece to contemporary Russia; and cases defined or described as sabotage-adjacent e.g. 'ecotage'. Second, we developed inductive coding schemes to systematically determine patterns across diverse cases. We asked whether these cases commonly included violence; about the nature of the target; about the intent of the saboteur; about the methods of operation; and about secrecy. Third, we evaluated the comprehensiveness of the search scope by examining cases not defined or described as sabotage within the academic literature but where the emerging themes or

allows us to derive a novel and substantive definition and develop new conceptual insights.[43] Three common characteristics of sabotage stand out.

The weaponization of friction

Intentions are crucial: sabotage weaponizes friction. Friction refers to ordinary sources of organizational inefficiency, such as technical difficulties and workplace disputes. These prosaic problems affect all organizations, but they are usually manageable. Sabotage seeks to aggravate friction to cause a meaningful decline or disruption in productivity and morale. Done well, sabotage operations not only target an adversary's physical and communications infrastructure, but also its *esprit de corps*. And these effects may radiate outwards: policymakers may have to shift resources in an effort to repair the damage, frustrated bureaucrats lose morale, and wider public confidence is undermined.[44]

Put more abstractly, sabotage thus interferes with the normal functioning of complex systems. Sabotage may target any type of bureaucracy, such as industrial facilities, research institutes, government bureaus, international organizations, intelligence agencies, or military headquarters.[45] It can directly interfere in organizational processes to inject friction, using a range of techniques such as those described in the famous Office of Strategic Service's field manual, including 'misfiling essential documents' and applying 'all regulations to the last letter'.[46] Sabotage can also target the underlying infrastructure that the functioning of an organization or society depends upon –

---

patterns applied, such as cyber-attacks, to ensure reliability and counter the bias of the initial 'sabotage' search and then repeated the coding process and analysis. Fourth, we constructed a working definition, testing it against cases and related concepts to make it as concise and analytically useful as possible.

[43] For discussion of the method, see Stefanie Habersang and Markus Reihlen, 'Advancing qualitative-meta studies: current practices and reflective guidelines for synthesizing qualitative research', *Organizational Research Methods* (2024), available at: <https://doi.org/10.1177/10944281241240>, accessed 30 September 2024.

[44] This section builds on Joshua Rovner, 'Theory of sabotage', *Etudes Françaises de Renseignement et de Cyber,* 1:1 (2023), pp. 139–153. Rovner defined sabotage as the weaponization of friction and speculated about the possible targets of sabotage operations. This article goes further by analysing a wider range of cases from a wider range of disciplinary perspectives, describing the other fundamental characteristics of sabotage, and by exploring the value of sabotage as an enabling tool.

[45] Clausewitz famously described the pernicious effects of friction on armies. He did not, however, theorize on the deliberate use of friction against rival forces, treating it instead as a wartime inevitability. Carl von Clausewitz, *On War*, eds. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), pp. 119–121. John Boyd later treated friction as a variable that might be manipulated, rather than a constant. John R. Boyd, *A Discourse on Winning and Losing*, ed. Grant T. Hammond (Montgomery, AL: Air University Press, 2018). For an excellent discussion of these duelling perspectives, see Olivia Garard, 'Reconsidering Clausewitz on friction', *War on the Rocks* (23 January 2023), available at: <https://warontherocks.com/2023/01/reconsidering-clausewitz-on-friction/#:~:text=Per%20Clausewitz%2C%20friction%20concerns%20how,atmosphere%20that%20hampers%20activity%20there, accessed 30 September 2024.

[46] OSS, 'Simple Sabotage Field Manual'.

for example cutting the power in an industrial facility. Because a growing range of both organizational processes and infrastructure is computerized, cyber operations are capable of a growing scope of sabotage.

Finally, friction affects the public and private sector, rendering both vulnerable to sabotage. All these targets are also subject to physical and psychological harm. Indeed, the immediate physical consequences of sabotage may be less important than secondary psychological effects of weaponized friction, as colleagues start to question each other's competence and loyalty. Sabotage thus not only targets friction within systems but also amongst people within those systems by targeting trust (hence moving beyond certain terrorism definitions limiting sabotage to attacks on property to incorporate wider understandings from public administration scholarship). Indeed, public administration scholars have long recognized the importance of trust in navigating friction.[47] Sabotage exploits this linkage. Throughout history, saboteurs have undermined the target's trust in their infrastructure. Lawrence of Arabia attacked Ottoman confidence in its railway system. The Soviets accompanied Cold War sabotage plans with propaganda campaigns designed to amplify any kinetic effects to spread further confusion and paralysis. One GRU defector, in the early 1970s, told of a plan to sow panic about the presence of nuclear submarines by contaminating Holy Loch, on the east coast of Scotland, with radioactive material.[48] Similar psychological effects exist today. Fears of electoral sabotage in the United States may be more important than hypothetical operations against election machines, for example, if they exacerbate the loss of faith in government institutions.

Working from the inside–out – physically or digitally

Most forms of political power work from the outside in. Diplomacy can put external pressure on a government to act according to one's interest. Threats of using force can further facilitate coercion. Warfare in turn projects power by deploying one's material capabilities against and within enemy territory.

Sabotage, in contrast, works from the inside–out. It is intrusive, quietly burrowing into a target organization to weaponize friction. Historically, saboteurs required human agents who were willing to put themselves at risk while infiltrating enemy organizations, or (para)military units conducting stealthy operations within adversary territory. Their deployment in enemy territory and organizations means these agents can be captured or killed, and the more daring the activity involved, the higher these risks become.

Modern sabotage can reduce this risk because of increasingly long and complex global supply chains. Rather than operating within enemy territory, supply chains can be compromised and machinery sabotaged from neutral or friendly territory. Implanting faulty hardware from a distance can cause machines to fail. Hiding bombs

[47] Samuel A. Colbert and John T. McDonough, 'The politics of trust and organizational empowerment', *Public Administration Quarterly,* 10:2 (1986), pp.171–188.

[48] MI5, GOLDFINCH report, July 1972, FCO168/4860, The National Archives, UK.

in machine parts delivered to a facility can damage or destroy it. Finally, cyber operations offer a way to conduct sabotage across borders as well, adding to the range of available means to induce friction. Computer systems can be sabotaged remotely using a range of social engineering or hacking techniques, i.e. exploiting vulnerabilities in people, hardware, and software.[49] Irrespective of how one gains access to enemy systems, the effects are produced from within. Hackers stealthily gain control of systems to disrupt or disable them as desired.

While the rise of cyber operations offers new opportunities for sabotage, it also introduces added challenges – especially when more violent means are required to achieve the desired degree of friction. Perhaps somewhat counterintuitively, given the widespread fear of catastrophic cyber-attacks[50], traditional means retain an edge in these cases. Reporting on the Hezbollah case discussed at the outset illustrated pervasive dread of catastrophic cyber sabotage. Yet reality showed the opposite. Hezbollah's fear of cyber-attacks and espionage motivated it to turn to an obsolete communications technology. This choice in turn provided an opportunity for traditional sabotage with explosives as supply chains were fragmented and suppliers scarce. According to detailed public reporting, Israel ingeniously exploited this opportunity. In short, when damage and destruction are the aim, traditional sabotage likely remains the more potent threat.[51] Israel's choice in favour of plastic explosives over cyber means in 2021's sabotage of Iran's Natanz nuclear enrichment facility provides further evidence of this realization amongst states.[52] It is all the more pertinent given Natanz was the target of the first cyber-physical sabotage operation, Stuxnet.

Novel opportunities provided by cyber means promise to expand the strategic impact of sabotage in two ways. First, attackers can combine traditional and cyber sabotage operations to strike deep and wide. Success will require significant preparation

---

[49] Jon Erickson, *Hacking: The Art of Exploitation* (San Francisco: No Starch Press, 2003); Kevin D. Mitnick, *The Art of Deception: Controlling the Human Element of Security* (Indianapolis, IN: Wiley, 2003); and Susan Young and Dave Aitel, *The Hacker's Handbook: The Strategy behind Breaking into and Defending Networks* (Boca Raton: CRC Press, 2004).

[50] ABC News, 'CIA director warns of "Cyber-Pearl Harbor,"' *ABC News* (11 February 2011), available at: <https://abcnews.go.com/News/cia-director-leon-panetta-warns-cyber-pearl-harbor/story?id=12888905>, accessed 30 September 2024; Miguel Alberto Gomez and Eula Bianca Villar, 'Fear, uncertainty, and dread: cognitive heuristics and cyber threats', *Politics and Governance,* 6:2 (2018), pp. 61–72; Keith Alexander, 'Cyber warfare in Ukraine poses a threat to the global system', *Financial Times* (15 February 2022), available at: <https://www.ft.com/content/8e1e8176-2279-4596-9c0f-98629b4db5a6>, accessed 30 September 2024; and Ryan Shandler, Michael L. Gross, and Daphna Canetti, 'Cyberattacks, psychological distress, and military escalation: an internal meta-analysis,' *Journal of Global Security Studies,* 8:1 (2023), pp. 1–19.

[51] Nicole Perlroth, *This is How They Tell Me the World Ends: The Cyberweapons Arms Race* (New York: Bloomsbury Publishing, 2021).

[52] Jake Wallis Simons, 'EXCLUSIVE: Mossad Recruited Top Iranian Scientists to Blow up Key Nuclear Facility', *The Jewish Chronicle* (2 December 2021), available at: <https://www.thejc.com/news/world/exclusive-mossad-recruited-top-iranian-scientists-to-blow-up-key-nuclear-facility-1.523163>, accessed 30 September 2024.

time, coordination, and organizational capacity. Second, attackers can also combine traditional and cyber means within individual operations. Russia's so-called use of local 'gig workers' for sabotage operations provides a key example.[53] The 'cyber' component is the digitally networked command and control infrastructure, facilitating recruitment and coordination of local agents. Conversely, human agents can offer a way to compromise highly secured computer systems lacking technical vulnerabilities in order to sabotage them via cyber means.

Similarly, advances in lethal autonomous weapons systems offer new opportunities to assassinate targets within adversary territory remotely, without human agents involved. Instead of deploying field agents or soldiers into harm's way, weapons systems can be assembled in safe houses within adversary territory from individually inconspicuous parts. Yet just like with cyber operations, there are new challenges as well. Because autonomous weapon systems depend on artificial intelligence, for example, and because artificial intelligence is prone to unpredictable and unexplainable behaviour, relying on such systems introduces new causes of failure.[54]

Clandestine intrusions: Visible outcomes

Tactical success requires a commitment to operational secrecy. Sabotage campaigns rely on their targets' ignorance because successful intrusions require that defenders remain unaware. Targeted organizations may be concerned about sabotage in general, but – when sabotage is successful – they do not discover specific operations until it is too late. Keeping defenders in the dark is a prerequisite for generating meaningful effects, because revelation may allow them to take pre-emptive actions (e.g. changes to operations procedures and communications protocols) before the effects of sabotage accumulate. Conventional military attacks can succeed, by contrast, by overwhelming the defender. In these cases, the enemy knows it is under attack but simply cannot stop it.

The need for clandestine intrusion is a characteristic shared with espionage. However, sabotage and espionage are distinct. Both rely on deception to enter enemy networks, but spies seek to remain hidden to keep collecting information. Espionage facilitates sabotage by providing vital information about adversary vulnerabilities as well as best practices for gaining entry and maximizing effect. As a result, spies are temperamentally averse to exploiting their presence to disrupt enemy operations. Sabotage risks this kind of compromise. That said, because sabotage often requires long lead times, agents may have ample opportunities to steal secrets in the course of their preparatory work. In this sense, sabotage can enable espionage if the goal is to learn more about how adversaries behave under stress. Sabotage might also create new oppor-

[53] Richterova, et al., 'Russian sabotage'.

[54] Paul Scharre, 'A Million Mistakes a Second', *Foreign Policy* (12 September 2018), available at: <https://foreignpolicy.com/2018/09/12/a-million-mistakes-a-second-future-of-war/>, accessed 30 September 2024.

tunities to recruit human sources, because increasing friction can alienate disgruntled bureaucrats. In these senses, sabotage and espionage are mutually reinforcing. In other cases, however, they work at cross-purposes. Because sabotage heightens the risk of discovery, agents have good reasons to lay low. And if the discovery of sabotage causes counterintelligence services to become more vigilant and ruthless, agents may stop collecting altogether.

It is important here to distinguish 'clandestine' from 'covert'. The conceptual difference is familiar to students of intelligence but may not be for IR generalists. Clandestine operations are *secret*; adversaries cannot see evidence of anything amiss. Covert operations are *deniable*; adversaries may well see the problem, but they cannot necessarily determine who is responsible. As with espionage, sabotage campaigns rely on clandestine intrusions.

Following the clandestine intrusion, sabotage becomes distinct from espionage in another core manner: unlike espionage, it generates visible outcomes. It exists in the realm of policy execution and, like covert action, often exploits uncertainty and ambiguity regarding sponsorship. Indeed, sabotage efforts are often (but not always) covert, concealing the perpetrator's identity if not the act itself. Saboteurs can then exploit the victim's resulting uncertainty, weaponizing friction further. Even after targets realize that something is wrong, they often remain uncertain about the cause. The search for an explanation might help them find answers. On the other hand, it might compound the problem by triggering security measures that lead to paranoia, accusations, and internal recriminations. Lingering doubt about the *real* source of trouble may be just as consequential as the actual physical effect of sabotage. This is one reason why sabotage can cheaply impose long-term costs. By playing on the psychology of targets and exploiting the unsettling sense that their machines have been compromised, a small investment can yield outsize results.

Consequently, determining the line between foreign sabotage and internal dysfunction is often difficult. The upshot is uncertainty about the cause and the perpetrator. More than two centuries ago, a petty criminal, deludedly thinking he had the full backing of the American envoy in Paris and the Continental Congress in Philadelphia, sabotaged British naval shipyards during the American War of Independence. Panicked British officers were convinced that the gang of saboteurs was far bigger, and better directed, than was actually the case.[55] Leaders also point to external sabotage to divert attention from internal infrastructure failures. When an Indian train derailed in 2016, killing 151 people, the railway minister later alluded to sabotage before having to insist that he was not looking for scapegoats, while the prime minister spoke of 'conspiracy'

[55] See Ralph Thompson, 'Dockyard Incendiarist: the tale of "John the Painter"', *The National Archives, UK* (15 March 2023), available at: <https://blog.nationalarchives.gov.uk/dockyard-incendiarist-the-tale-of-john-the-painter/>, accessed 14 October 2025.

directed by Pakistan. Investigators ultimately did not file a charge sheet after forensic reports ruled out the fractured track being caused by explosives.[56]

At the other end of the spectrum, saboteurs may *want* to be discovered. Here, sabotage follows similar logics to so-called implausibly deniable covert actions. They include seeking to signal the state's ability to penetrate adversary security protocols, to signal credible resolve while mitigating the broader diplomatic consequences,[57] or to generate ambiguity in the grey zone between exposure and acknowledgement.[58] In a particularly outlandish example, in February 2025 Benjamin Netanyahu presented Donald Trump with a golden pager during a visit to the United States supposedly representing a turning point in Israel's war with Hezbollah.[59] Exposure does not always mean failure. At the same time, it is essential not to give too much credit to saboteurs by assuming that all exposed operations were carefully calibrated, rather than caused by poor tradecraft.[60]

In some cases, saboteurs seek to leave no trace. In others, they find it useful to imply their role.[61] Curiouser still is the notion that victims of sabotage might find it useful to *allow* their adversaries to retain a modicum of deniability. Doing so might buy time to quietly rebuild defences without tipping off the saboteur, while simultaneously gaining valuable intelligence about their methods. Public attribution also risks creating public pressure for leaders to act, even if they would rather not.[62]

This section has drawn on multiple cases and definitions across multiple literatures to distil core common characteristics of sabotage. They include (a) the weaponization of friction to enable a political or military goal, and (b) a clandestine means of undermining adversary institutions from within, but one which has visible effects, and which has the potential for generating further uncertainty and friction.

---

[56] Suhasini Haidar and Somesh Jha, 'Distinguish Between Sabotage, Accidents', *The Hindu* (9 February 2017), available at: <www.thehindu.com/news/national/%E2%80%98Distinguish-between-sabotage-accidents%E2%80%99/article17264184.ece>, accessed 31 October 2024; Vijaita Singh, 'NIA won't file Chargesheet in Kanpur Derailment Case', *The Hindu* (21 October 2018), available at: <www.thehindu.com/news/national/nia-wont-file-chargesheet-in-kanpur-derailment-case/article25280396.ece>, accessed 31 October 2024.

[57] Austin Carson and Keren Yarhi-Milo, 'Covert communication: the intelligibility and credibility of signaling in Secret', *Security Studies*, 26:1 (2016), pp. 124–156.

[58] Cormac and Aldrich, *Grey is the New Black*, pp. 477–494.

[59] Anon., 'Netanyahu Gifts Trump a Golden Pager During US Visit', *BBC News* (7 February 2025), available at: <https://www.bbc.co.uk/news/videos/cg7zp1dgmxmo>, accessed 28 February 2025.

[60] For a similar argument on Russia and assassination, see Kevin Riehle, 'Ignorance, indifference, or incompetence: why are Russian covert actions so easily unmasked?', *Intelligence and National Security*, 39:5 (2024), pp. 864–878.

[61] For a related argument, see Brendan Rittenhouse Green and Austin Long, 'Conceal or reveal? Managing clandestine military capabilities in peacetime competition', *International Security,* 44:3 (2020), pp. 48–83.

[62] Florian J. Egloff and Max Smeets, 'Publicly attributing cyber attacks: a framework', *Journal of Strategic Studies,* 46:3 (2023), pp. 502–533.

Sabotage as a distinct phenomenon

Our initial conceptualization of sabotage raises questions about its relationship to related concepts of covert action and subversion. Addressing these – and explicitly differentiating sabotage – is vital to provide conceptual clarity; add nuance to discussions of secret statecraft and theoretically advance the literature on covert action by differentiating logics of secrecy from action; and justify the need to place sabotage on the research agenda. (See Table 1).

Table 1.

Key Attributes of the Dark Arts

As alluded to earlier, sabotage and covert action overlap but are conceptually distinct, and the differences matter. Covert action involves influencing political, economic, or military conditions abroad where the essential characteristic is that the responsible party disclaims responsibility. As Title 50 of the US Code puts it, covert action occurs 'where it is intended that the role of the United States will not be apparent or acknowledged publicly'. This can be pursued using a range of activities, from unattributable propaganda to targeted killings.

Given its secretive characteristics, it is unsurprising that sabotage is subject to similar limitations and trade-offs described in the recent wave of literature on covert action in international relations. We do not claim otherwise. Sabotage, like covert action, is designed to shape outcomes and is an enabler or force multiplier of other policy levers.[63] Like covert action, and as discussed above, it can follow similar logics of (im)plausible deniability, and also like covert action, secrecy is both a boon and a bane because it limits the extent of the damage sabotage can achieve. Existing literature identifies a trade-off between secrecy and scale in covert operations at large limiting their strategic impact.[64] Operations large enough to make a difference strategically face a high risk of being discovered and neutralized before producing an effect, while those small enough to stay hidden are likely to fall short of producing a strategically relevant impact. More recent work on subversion, which shares the reliance on infiltration of systems from within that is typical of many sabotage operations, identifies two additional trade-offs: speed and unreliability.[65] Specifically, Lennart Maschmeyer discovered a trilemma between speed, intensity, and volatility in subversion operations that we argue is shared by sabotage operations as well.[66]

[63] See, for example, David V. Gioe, 'Cyber operations and useful fools: the approach of Russian hybrid intelligence', *Intelligence and National Security*, 33:7 (2018), pp. 954–973.

[64] Gregory F. Treverton, *Covert Action: The Limits of Intervention in the Postwar World* (London: I.B. Tauris, 1987); and O'Rourke, *Covert Regime Change*.

[65] Melissa M. Lee, *Crippling Leviathan: How Foreign Subversion Weakens the State* (Ithaca, NY: Cornell University Press, 2020); and Lennart Maschmeyer, 'The subversive trilemma: why cyber operations fall short of expectations', *International Security,* 46:2 (2021), pp. 51–90. Lee highlights the principal-agent trade-offs involved in the use of non-state armed groups as subversive proxies. Maschmeyer emphasizes the technical trade-offs involved in the use of malicious code.

[66] Maschmeyer, 'The Subversive Trilemma'.

Yet sabotage is conceptually distinct. Covert action is fundamentally characterized by the perpetrator's non-acknowledgement of its interfering role; it does not describe the strategic logic of the act itself. Sabotage focuses on that logic: to degrade a target's performance by weaponizing friction inside a system.[67] This end can be pursued by various means, including those traditionally seen as sabotage (arson, cable cutting, etc.), as well as propaganda, covert political influence, economic activity, cyber-attacks, assassination, and so on. Unlike covert action, the interferer's role can be denied or acknowledged; instead, the defining feature of sabotage is the use of various means to weaponize friction to degrade performance.

Revealing this strategic logic of sabotage helps distinguish between covert – or 'grey' – activity that may use the same means but for other ends. For example, disinformation can subversively manipulate a specific foreign policy outcome and/or degrade an information ecosystem.

There are clear similarities between sabotage and subversion. Subversion also exploits target systems from within, and sometimes seeks to undermine them. However, it does so through manipulation. Subversion is an indirect means of interfering in adversary affairs by exploiting vulnerabilities in institutions, societies, and, today, also computer systems to infiltrate and manipulate them.[68] Melissa Lee defines subversion as the empowerment of proxy groups to undermine rival states from within, and, critically, to encourage civilians to question their loyalties.[69] As Jill Kastner and William Wohlforth put it, subversion uses 'domestic interference to undermine or manipulate a rival'.[70]

Sabotage is different. Whereas subversion manipulates behaviour, sabotage degrades performance. Sabotage is disruptive and destructive, seeking to throw sand in the gears of the machine, whereas subversion is generative, seeking to alter what the machine produces or even change the machine altogether. Subversion manipulates targets towards behaving in a way the subverter wants to produce a distinct outcome. It turns people and institutions into unwitting agents pursuing the subverter's interests. Sabotage does not change the behaviour of targets, but rather subtracts capability by degrading their performance. It is degenerative. Our distinction challenges other works on subversion which rely on broader definitions.[71]

---

[67] It targets both social and technical systems, namely institutions and organizations, as well as infrastructure and industrial machinery.

[68] Paul W. Blackstock, *The Strategy of Subversion: Manipulating the Politics of Other Nations* (Chicago: Quadrangle Books, 1964), p. 50; and Lennart Maschmeyer, *Subversion: From Covert Operations to Cyber Conflict* (New York: Oxford University Press, 2024), chapter 1.

[69] Lee, *Crippling Leviathan*, pp. 8–10.

[70] Jill Kastner and William C. Wohlforth, 'A measure short of war', *Foreign Affairs,* 100:4 (2021), pp. 118–131, at p. 119. For a longer treatment, see Kastner and Wohlforth, *A Measure Short of War: A Brief History of Great Power Subversion* (New York: Oxford University Press, 2024).

[71] Andreas Krieg, *Subversion: The Strategic Weaponization of Narratives* (Washington, DC: Georgetown University Press, 2023), p. 2.

This core difference matters because it shapes the range of ends that sabotage and subversion can serve. Subversion attempts to manipulate people and institutions in order to produce specific opinions, behaviours, and policies. Sabotage attempts to degrade organizational performance, information systems, and facilities. This distinction allows us to code the logic of different activities. Disinformation, for example, is sabotage if it degrades the information ecosystem but subversive if it generatively influences opinion. Similarly, electoral interference is sabotage if it degrades electoral processes but subversive if it generatively manipulates electoral outcomes. This conceptual clarity helps differentiate between distinct logics usually unhelpfully conflated under the generic banner of covert action. Real-world intelligence contests, of course, often involve elements of both sabotage and subversion. This is especially the case in protracted campaigns amongst rivals, which are likely to include a mix of activities.

Having compared our conceptualization of sabotage to related concepts of covert action and subversion, we propose that sabotage is the weaponization of friction to degrade the performance of systems from within. This inherently relies on clandestine intrusion but deliberately leaves open levels of acknowledgement and violence.

Sabotage in strategy

Having defined and conceptualized sabotage, we now address its strategic use and utility. We do so by returning to the diverse case studies and, through a process of systematic comparison, assess effectiveness, limitations, and contextual factors. Below we show how and why sabotage offers utility as an enabler in adversarial diplomacy, counterproliferation efforts, counterterrorism and counterinsurgency, deterrence, and conventional war.

Despite the limitations briefly discussed above and familiar to scholars of covert action, sabotage can enable and enhance other operations. We argue that given its distinct strategic logic – degrading performance rather than generating outcomes – its enabling function is more pronounced compared to other tools of secret statecraft. Sabotage degrades, creating space for other tools. By 'enable' we mean laying groundwork for operations using different policy tools. By 'enhance' we mean adding to the overall effect of broader campaigns. Our analysis of multiple existing literatures revealed that cases of sabotage span the entire spectrum of war, peace, and the so-called grey zones in between. Here, we distil them into five broad, if fuzzy-edged, categories whereby policymakers use sabotage in support of broader objectives, along with historical illustration to offer insight into the conditions under which sabotage acts as an enabler and enhancer – and how things go wrong.

Adversarial diplomacy

Sabotage operations can enhance adversarial diplomacy, defined as efforts to isolate and pressure rival states. 'Wedge strategies' designed to pry adversary coalitions apart are a good example. Recent research has focused on the role of accommodation in drawing a rival's allies away from its orbit.[72] Yet states can also use sabotage to raise costs, adding coercive pressure to accommodation strategies. Sabotage may be ideal for this purpose: it creates enough friction to make alliance membership a headache, but not so much that it provokes a direct conflict. Its deniability helps diplomats gently wrest allies apart, without inadvertently forcing them to fight for their own public credibility. Overt violence, by contrast, would be more likely to drive adversaries together.

Wedges have intrigued strategic theorists going back to antiquity. Sun Tzu's *Art of War* (5$^{\text{th}}$ cen. BCE) describes the value of attacking enemy alliances, though it does not provide specific recommendations for how to do so.[73] Sabotage might help. States may weaponize friction against their enemy's allies not only to reduce the enemy's capabilities but also to remind foreign patrons about the costs of their support, all the while using deniability to control the risk of escalation. Allegations of Russian sabotage may fit this pattern. In 2011, Russia allegedly destroyed an ammunition depot in Bulgaria with artillery destined for Georgia. In 2014, it targeted a Czech warehouse with military materials destined for Ukraine, and Western officials suspect Russia's hand in a series of fires in Europe and the United States following their expressions of support for Ukraine in the ongoing war.[74]

Sabotage may also improve the effectiveness of economic sanctions by preventing targets from evading them. Sanctions impose costs and imply relief as a reward for compliance. Targets of sanctions are incentivized to evade these costs by finding alternative suppliers for imports and new export markets to continue trading in secret. Sabotage can help disrupt these activities by targeting and imposing costs on the third parties (states and firms) involved. For example, the CIA allegedly sabotaged Leyland buses en route from the UK to Cuba in contravention of an economic blockade against Havana, potentially even including the sinking of a ship carrying 42 buses in 1964.[75]

Although this logic is straightforward, sabotage is ultimately of limited value for adversarial diplomacy. The problem, derived from our first trade-off above, is that the demands of deniability are inversely proportional to the cost on adversaries. Because sabotage operations need to be small enough to remain ostensibly covert, they cannot impose sufficient costs to coerce the victim towards changing course. This is likely why

[72] Timothy W. Crawford, *The Power to Divide: Wedge Strategies in Great Power Competition* (Ithaca, NY: Cornell University Press, 2021).

[73] Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (Oxford: Oxford University Press, 1971), p. 78.

[74] Richterova et al., 'Russian Sabotage'.

[75] William Blum, *Killing Hope: US Military and CIA Interventions since World War II* (London: Zed Books, 2003), p.18.

they have been ineffectual at reducing Western support for Ukraine. At most, sabotage operations work slowly and cumulatively, reminding their targets about the costs of noncompliance. Again, the war in Ukraine is instructive. The costs of sabotage pale in comparison with the human and material toll of the war itself.

Counterproliferation

Sabotage is famously associated with counterproliferation. Alleged sabotage against Iraq and Iran targeted their nascent nuclear weapons programmes. Israel reportedly sabotaged the supply chain feeding Iraq's nuclear effort in the 1970s, planting explosives on a reactor core bound for Iraq while sitting in a French port.[76] More recently, the Stuxnet virus targeted Iran's nuclear programme by sabotaging uranium centrifuges at its enrichment facility at Natanz.[77]

Sabotage seems tailor made for counterproliferation. Aspiring nuclear powers require money, expertise, fissile material, and highly specialized components, many of which need to be sourced from witting and unwitting international suppliers.[78] The existence of multiple supply networks creates opportunities for intrusion by saboteurs. They create bottlenecks, which may be vulnerable to attack, as in the case of Iraq the 1970s. The expansion of cyberspace creates other sabotage opportunities, as in the case of Iran in the 2000s. Making a nuclear weapon is hard for newcomers. Sabotage makes it harder.

Sabotage is also appealing for counterproliferation because of the bureaucratic complexity of emerging nuclear efforts. Most countries starting nuclear programmes have ultimately failed to build nuclear weapons. A key reason is the difficulty in sustaining long-term political support for scientific and engineering research. Successful programmes require a combination of sharp-elbowed bureaucrats and dogged researchers, working in concert for many years.[79] Maintaining this relationship is sometimes too much. Foreign saboteurs might exploit that reality by adding an extra dose of bureaucratic friction to a demanding scientific problem.

Yet sabotage is unlikely to succeed on its own, especially if emerging nuclear powers are committed to achieving a full fuel cycle and weapons capability. States are capable of replacing faulty parts and finding alternative suppliers. They are able to withstand setbacks as they accumulate the knowledge and physical capabilities required to make progress independently. Once they start enriching uranium, moreover, they can absorb

[76] Ian Black and Benny Morris, *Israel's Secret Wars: A History of Israel's Intelligence Services* (New York: Grove Weidenfeld, 1991), pp. 332–334; and Yossi Melman, 'Israeli nuclear engineer confirms: the Mossad sabotaged Iraqi nuclear equipment on French soil', *Haaretz* (13 June 2021).

[77] Kim Zetter, *Countdown to Zero: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown, 2014).

[78] Chaim Braun and Christopher F. Chyba, 'Proliferation rings: new challenges to the nuclear nonproliferation regime', *International Security,* 29:2 (2004), pp. 5–49.

[79] Jacques E.C. Hymans, *Achieving Nuclear Ambitions: Scientists, Politicians, and Proliferation* (Cambridge: Cambridge University Press, 2012).

sabotage while continuing to accumulate fissile material. In the Iran case, for example, the total production of enriched uranium actually increased during the Stuxnet virus's attack window.[80] Meaningful counterproliferation therefore requires more than sabotage: military action, sanctions, and diplomacy all play a part. A mixture of sanctions and diplomatic incentives culminated in the 2015 agreement to eliminate Iran's enriched uranium stockpile and limit future production. Sabotage at best enabled and enhanced the diplomatic effort if Iranian leaders feared that efforts to subvert the deal would be in vain.

Counterterrorism and counterinsurgency

Sabotage can bolster campaigns against armed non-state groups, causing them physical and psychological harm. Terrorist and insurgent groups suffer friction like anyone else, though their small size, relative to the state, could be conceived to limit the effects of sabotage and direct action is difficult because members have powerful incentives to remain hidden and vigilant. Yet their small size also reduces their margin for error. Friction within armed groups may significantly reduce their capacity for violence. Friction can come, for example, in the form of setting members against each other, a long-time tactic of British intelligence,[81] or targeting communications systems as Western intelligence did to confuse and disrupt Islamic State.[82] The recent operation against Hezbollah is a reminder that sabotage is possible. It also highlights sabotage as a method of disrupting coordination. Denying armed groups access to communications technologies forces them into face-to-face meetings, limiting the extent of their plans.[83]

The psychological consequences of sabotage on armed groups may be substantial, even if the physical effects are modest. Successful intrusions may affect group morale, an important levelling factor for militants with limited means. The shocking discovery of sabotage may lead to a destructive spiral of accusations and counteraccusations, as militants try to identify the saboteurs in their midst. A sense of group cohesion and unity of purpose are likely to suffer.[84]

---

[80] Jon R. Lindsay, 'Stuxnet and the limits of cyber warfare', *Security Studies,* 22:3 (2013), pp 365–404, at pp. 390–391.

[81] Rory Cormac, *Disrupt and Deny: Spies, Special Forces, and the Secret Pursuit of British Foreign Policy* (Oxford: Oxford University Press, 2018), p.238.

[82] Deborah Haynes, 'Into the Grey Zone', *Sky News* (8 February 2021), available at: <https://news.sky.com/story/into-the-grey-zone-the-offensive-cyber-used-to-confuse-islamic-state-militants-and-prevent-drone-attacks-12211740>, accessed 30 September 2024.

[83] Armed groups have used a variety of methods to communicate online while concealing their identities and locations. Undermining confidence in those methods is a potentially powerful way to inhibit their activities. Brian Fishman, 'Crossroads: counter-terrorism and the internet', *Texas National Security Review,* 2:2 (2019), pp. 82–100.

[84] Psychological operations against the Abu Nidal Organization targeted the paranoia of its leader. Timothy Naftali, *Blind Spot: The Secret History of American Counterterrorism* (New York: Basic Books, 2005), pp, 197–198.

Injecting friction can extend beyond the group itself to its patrons. An external supplier of money and guns can be a lifeline for a non-state group with few organic capabilities. Sabotaging financial networks might complicate efforts to pay the foot soldiers or acquire weapons, as the French attempted during the Algerian War by sabotaging West German arms dealers.[85] The more ambitious the armed group, the more resources it will require – and the larger the supporting organizational infrastructure that will become involved in its efforts.[86]

Where an insurgent group eschews terroristic violence and coercion in favour of winning 'hearts and minds', sabotage can play another role. Individuals have a range of choices when confronted with an armed insurgency. They can support counterinsurgency efforts, joining the state's security forces, or they can support the insurgency, joining the armed movement and putting their lives at risk. In between these poles lie ways that civilians can aid an insurgency – or work against it.[87] People are inclined to support a rebellion if they believe that organization is capable. States can use this calculus to their advantage, employing sabotage against insurgent organizations to make them look inept and doomed to fail. Successful sabotage operations throw a wrench the works of rebel groups, making them less able to do what they must to challenge a state: fundraising, recruiting, organizing, planning, and coordinating attacks. The less they can perform these tasks, and the more they descend into toxic infighting, the less likely civilians will be willing to move along the spectrum from neutrality to full support. Sabotage helps to defeat insurgent groups by embarrassing them.

Despite its potential, sabotage is unlikely to serve as a foundation of counterterrorism and counterinsurgency. Most armed groups succumb to intelligence and law enforcement – or collapse on their own – without need for sabotage.[88] Weaponizing friction may help against larger groups with more resources and a wider support network, but working successfully against these groups requires a combination of public diplomacy, international police work, cooperative intelligence efforts, and joint military operations. Sabotage may contribute to this broader campaign by both enhancing overall effectiveness and enabling other tools, but it will not be decisive.

---

[85] Mathilde Von Bülow, 'Myth or reality? The Red Hand and French covert action in Federal Germany during the Algerian War, 1956–61', *Intelligence and National Security,* 22:6 (2007), pp. 787–820.

[86] David Tucker, *Skirmishes from the Edge of Empire: The United States and International Terrorism* (Westport, CT: Praeger, 1997), p. 104. Tucker was Acting Director of Policy Planning for the Assistant Secretary of Defence for Special Operations/Low-Intensity Conflict.

[87] Roger D. Petersen, *Resistance and Rebellion: Lessons from Eastern Europe* (Cambridge: Cambridge University Press, 2001).

[88] Audrey Kurth Cronin, *How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns* (Princeton, NJ: Princeton University Press, 2009).

Deterrence

States tend to be more aggressive if they believe that they enjoy a clear technological advantage over their adversaries, allowing them to control events in crises and war.[89] Sabotage may help disabuse them of these ideas by degrading technical capabilities and undermining adversary confidence. Peacetime sabotage of military equipment and communications infrastructure can produce accumulating evidence of failures. It can also target supply chains, deceiving adversaries into using faulty hardware and software. Adversaries may lose confidence in their capabilities as a result. Well-timed information operations can further exacerbate these effects. They might inject fog onto hypothetical battlefields during military exercises, casting doubt on hopes that adversaries can rapidly seize control of the information environment in a future conflict. Poor exercise performance might cause leaders to jettison hopes of decisive victory.[90]

Saboteurs reinforce the message by designing operations that make it possible for the victim to identify the attacker, because doing so might cause them to reassess the technological balance. States that thought they enjoyed a technological advantage might reconsider. Demonstrating logics of implausible deniability, the attacker might disclaim responsibility in public, but the victim should have little doubt about the attackers' technological prowess.

Deterrence via sabotage, however, depends on other factors. Power parity means that slight differences in operational efficiency could mean a lot in the event of war. States with overwhelming numerical advantages, however, will be more willing to tolerate peacetime friction. They can succeed without exquisite precision and recover in the event of wartime mishaps. The utility of sabotage for deterrence, then, depends on tangible issues like force posture and the military balance, along with intangible factors like political determination and the will to persist.

Timing also matters. All things being equal, sabotage is more likely to succeed during peacetime than in a deep crisis or conflict. Friction accumulates slowly. In line with our trade-offs above, efforts to accelerate the effect through more expansive sabotage campaigns are more likely to be discovered. In addition, states in crises are likely to take pre-emptive steps to harden communications, create alternative and redundant networks, and test their physical capabilities in the expectation of combat. Saboteurs will have a difficult time achieving their goals against alert defenders.[91]

---

[89] Alexander L. George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice* (New York, NY: Columbia University Press, 1974); Seyom Brown, *The Illusion of Control: Force and Foreign Policy in the 21st century* (Washington, DC: Brookings Institution Press, 2003); and Janice Gross Stein, 'Bringing politics back in: The neglected explanation of the Oct. 7 surprise attack', *Texas National Security Review,* 7:4 (2024), pp. 73–93.

[90] Rovner, 'Theory of sabotage', pp. 141–142.

[91] Joshua Rovner, 'Sabotage and War in Cyberspace', *War on the Rocks* (19 July 2022), available at: <https://warontherocks.com/2022/07/sabotage-and-war-in-cyberspace/>, accessed 31 October 2024.

Conventional war

Finally, sabotage can enable conventional military operations. It can inject friction into command and control (C2) systems, making it harder for enemies to organize and coordinate their activities; into intelligence networks, making it harder for enemies to maintain battlespace awareness; and into the routines of large armed bureaucracies, making it harder to fight coherently. Combined, such sabotage would leave the adversary scrambling to improvise under the weight of accumulating friction.

This applies to attack as well as defence. Attackers may use sabotage for 'operational preparation of the battlefield'[92], quietly undermining enemy defensive preparations by throwing communications into disarray. Israel's sabotage against Hezbollah before the recent invasion provides a potential example. Suddenly lacking safe communications devices, wounded and isolated Hezbollah operatives struggled to organize a defence of southern Lebanon. There is some evidence that Second World War sabotage campaigns helped pin down German forces, reducing their presences in Normandy and easing the D-Day invasion in June 1944.[93]

Conversely, defenders can protect themselves by sabotaging enemy capabilities and undermining confidence – as illustrated by Mujahideen (covertly supported by Saudi Arabia) sabotage of fuel supplies to Soviet helicopters during the 1980s Afghanistan War causing helicopters to fall from the sky.[94]

Indeed, sabotage of production capabilities and storage facilities can hamper the enemy's ability to sustain the fight. Shortages in key supplies amongst military units can reduce their battlefield effectiveness and morale. Russia's alleged sabotage against military depots supplying Ukraine might have served this purpose. An ancillary benefit is that enemy leaders may feel compelled to redirect their military forces towards counter sabotage work, when they would be better served at the front. In other cases, sabotage may deny the enemy key technological breakthroughs. The famous sabotage against the Nazis' nuclear programme played a role in stopping it from acquiring the bomb. This might have prevented Adolf Hitler from gambling on escalation in the later stages of the war. Given Hitler's affinity for miracle weapons, this was not an abstract concern.[95]

The common thread in these propositions is the confrontation between pre-war expectations and wartime realities. No army can escape friction, but sabotage can make it worse. Indeed, the logic of wartime sabotage requires thinking about conflict as a contest of bureaucratic efficiency, not just a test of strength.

---

[92] Ben Buchanan and Fiona S. Cunningham, 'Preparing the cyber battlefield: assessing a novel escalation risk in a Sino-American crisis', *Texas National Security Review,* 3:4 (2020), pp. 54–81.

[93] Colin Beavan, *Operation Jedburgh: D-Day and America's First Shadow War* (New York, NY: Penguin, 2007), pp. 292–293.

[94] Prince Turki Alfaisal al Saud, *The Afghanistan File* (London: Arabian Publishing, 2021), pp. 55–7, 85.

[95] Alan Bullock, *Hitler: A Study in Tyranny*, abridged ed. (New York, NY: Harper & Row, 1971 [1952]), pp. 424–425.

Conclusion

Sabotage is a seductive option for the same reasons that limit its stand-alone impact. It promises to derail adversary plans and undermine their strength without the consequences of overt attribution. Working in secret, it weaponizes friction to throw sand in the gears of organizations and infrastructure from the inside. It operates on a destructive strategic logic to degrade performance. Ideally, it helps throw an adversary off balance or foil their action without the risk and costs of going to war. Crucially, however, in most cases its secret and insider approach bring uncertainty about outcomes and limit their scope. Sabotage is therefore most consequential when paired with other instruments, enabling and facilitating the use of other means to produce desired outcomes. It can support a range of policies, from adversarial diplomacy and economic statecraft to war, but it has limited value as a stand-alone tool.

Its degradation of performance means that its impact lies primarily as a force enabler: degradation creates time, space, and a more conducive atmosphere for other tools to be effective. This role especially highlights why technological change is unlikely to change sabotage's key characteristics and subsequent role in world politics. The post-Cold War era has undoubtedly witnessed extraordinary changes to information technologies. Yet recent events suggest that sabotaging these technologies via cyberspace often carries less punch than old-fashioned kinetic action. The fact that the recent string of sabotage operations against NATO members in Europe overwhelmingly involves traditional rather than cyber means underlines this division of labour. What better metaphor for this situation than commercial ships dragging their anchors to sever high-speed internet cables that establish the interconnected world making cyber operations possible in the first place?

Sabotage, by whatever means, is back. States are simultaneously enthused and alarmed by this trend; they have invested a lot of time and effort in developing sabotage operations for a range of purposes, while simultaneously sounding the alarm about their own vulnerability. American national security officials have expressed concerns about sabotage via cyberspace intrusions onto critical infrastructure, warning that in the event of a conflict, adversaries could cause enormous social and economic upheaval.[96] European intelligence officers have warned that physical attacks could have similar effects across the continent.[97] And most recently, Australian officials have become unusually willing to go public about the danger, assessing a rising threat of

[96] Patrick Tucker, 'Chinese Hacking Operations Have Entered a far more Dangerous Phase, US Warns', *Defense One* (1 February 2024), available at:<https://www.defenseone.com/technology/2024/02/chinese-hacking-operations-have-entered-far-more-dangerous-phase-us-warns/393843/>, accessed 31 October 2024.

[97] *Economist*, 'Vladimir Putin's spies'.

'high-impact sabotage' against high-profile targets.[98] Sabotage is a pressing global concern.

Policymaker fears, however, are sometimes exaggerated. It may be that the current wave of warnings about sabotage overstates the threat. Indeed, we find that sabotage is potentially useful, but only when it is coupled with other tools. Along the same lines, sabotage may be escalatory in some cases, but it might act as a release valve for political tension in others. Scholars are in the early stages of hypothesizing the conditions that make sabotage more or less useful – and more or less dangerous.

An evolving research agenda might tackle a host of other questions that connect history, secret statecraft, and international security. Did the growth of the modern administrative state encourage the rise of new forms of sabotage? If so, what were the results? Does the looming threat of sabotage tend to limit the peacetime expansion of military organizations, which were, after all, large armed bureaucracies that were particularly vulnerable to friction? Or did the fear of sabotage lead to the construction of parallel security services?

Similarly, we might compare the use of sabotage in peacetime and war. Although a great deal of the literature focuses on sabotage during conflict, it may be that it is more useful during periods of peace. The reason is that saboteurs struggle to remain hidden in the midst of wartime vigilance. Achieving peacetime intrusions may be easier in peacetime, when the watchers are prone to neglect. Yet even when the chances of discovery are low, states may consider the value of sabotage against the political and diplomatic risks. How have statesmen thought about this trade-off historically, if they have thought about it at all? How have the weighed the possible costs and benefits? And how have they measured success and failure?

Finally, how have the victims of sabotage reacted? Have targeted institutions suffered lasting damage from friction, or have been they learned to adapt and mitigate the effects? Were some victims better than others at recognizing the problem? Did they practice forms of surveillance which helped them spot sabotage operations in early days? Did organizational leaders sense a trade-off between strict security regime and organizational morale? If so, how did they manage that trade-off? And to what extent did bureaucrats urge policymakers to act against the foreign states who they suspected were responsible for weaponizing friction? Did sabotage lead to escalation? Alternatively, is there a risk of unwittingly overemphasizing the threat of sabotage and, in turn doing the adversary's job for them by creating more friction and paranoia, or wittingly overemphasize the threat to create scapegoats for internal conditions such as poor safety standards?

Such questions are clearly relevant to policy today, given the ongoing surge of sabotage in international politics. But they also have large theoretical implications for

[98] Matthew Knott, 'The Rest of the Decade will be Even Worse: ASIO boss Issues Dire Terror Threat Warning', *The Age* (19 February 2025), available at: <https://www.theage.com.au/politics/federal/the-rest-of-the-decade-will-be-even-worse-asio-boss-issues-dire-terror-threat-warning-20250219-p5ldak.html>, accessed 28 February 2025.

students of international security. This article provides a conceptual and historical basis for finding answers.

Acknowledgements

The authors would like to thank the editors at EJIS and the two anonymous reviewers for their excellent criticism and suggestions.

Joshua Rovner is an Associate Professor of International Relations at American University, where he researches intelligence, strategy, and international politics. His latest book is *Strategy and Grand Strategy* (Routledge, 2025).

Rory Cormac is a Professor of International Relations at the University of Nottingham. His research specializes in covert operations and secret statecraft, and he is the author of six books, including *Disrupt and Deny, Secret Royals*, and *How to Stage a Coup*. He has testified before UK and Australian parliamentary inquiries on subversion, disinformation, and electoral interference, and has shared his research findings with practitioners and policymakers across NATO and G7 states. His next book is *FAKERS: A Top-Secret Tale of Phantoms and Forgeries on the Disinformation Front Lines* (Oxford University Press, 2026).

Lennart Maschmeyer is an Assistant Professor in Cybersecurity Policy at the Jimmy and Rosalynn Carter School of Public Policy at the Georgia Institute of Technology. He is the author of *Subversion: From Covert Operations to Cyber Conflict* (Oxford University Press, 2024). His work has been published in *International Security*, the *Journal of Peace Research*, the *Journal of Strategic Studies*, and the *Journal of Information Technology and Politics*.

References

Joshua Rovner, Rory Cormac and Lennart Maschmeyer
Sand in the gears: Sabotage in world politics
20 October 2025

European Journal of International Security, First View, pp. 1–20. DOI: https://doi.org/10.1017/eis.2025.10025