



Deterring Hybrid Warfare: NATO Approaches to Russian Sabotage

Anca Ioana Anescu

*Scholar Alumna, George C. Marshall European Center for Security Studies,
<https://www.marshallcenter.org>*

Abstract: This article presents a comparative analysis of how the concept of deterrence is understood and applied, with particular emphasis on its role in hybrid warfare, by the Russian Federation (action before reaction, coercive escalation), as opposed to NATO's approach, centered on the prevention of aggression through credible deterrence and a posture of collective resilience. Building on this comparison, the article further examines NATO's deterrence strategies against Russian hybrid warfare, focusing on sabotage as a key asymmetric tool rooted in Soviet-era covert practices and revived in recent years amid escalating gray-zone threats, particularly following the invasion of Ukraine and the targeting of NATO strategic infrastructure.

Applying an integrated methodology combining historical analysis, theoretical frameworks, case studies of recent incidents (2022–2025), theoretical modeling, and policy evaluation, the study argues that effectively countering sabotage within the hybrid domain can be achieved only through integrated deterrence. Such an approach should encompass proactive strategic anticipation based on historical patterns and precedents, enhanced intelligence-sharing, infrastructure resilience, and the operationalization of the principle of whole-of-society defense. Ultimately, the article argues that NATO and its allies must shift from a reactive posture to an anticipatory posture of defense and deterrence, aligning strategic foresight with adaptive defense capabilities.

Keywords: Deterrence, hybrid threats, conventional warfare, irregular warfare, sabotage.

Deterrence – A Historical and Theoretical Overview

Deterrence is defined in two primary contexts: (1) the act of preventing a particular act or behavior from occurring, such as the deterrence of crime, and (2) in politics, the policy of developing substantial military power to prevent other countries from attacking one's own country.¹

In 16th-century Salzburg, peasants rose against oppressive taxes and limited rights, rebelling against the wealthy prince-archbishops and attempting to seize the city. When they could not break through the walls of Hohensalzburg Fortress, they laid siege in hopes of starving the defenders into surrender. As supplies were short and only one bull remained, the city resorted to a clever deception: they paraded the brown-spotted bull along the fortress walls, then washed and painted it white the next day, and black the day after, making it appear as though they had many healthy animals. Fooled into thinking the city still had plenty of food, the besiegers gave up and withdrew. The deception proved so effective that it evolved into a local legend – a timeless narrative about deterrence and psychological warfare.²

This legend shows that the concept of *deterrence* has deep historical roots, existing informally long before it was formally defined. Early forms of deterrence can be seen in practices such as feudal alliances (through marriages and oaths of loyalty), the construction of castles and fortifications, the display of military capabilities through parades or tournaments, and the public punishment of criminals. In early forms of economic sanctions, nations would refuse to trade with aggressors in order to deter hostile actions.

Furthermore, deterrence is a fundamental aspect of human behavior and socialization that begins in early childhood. From a young age, individuals learn to avoid certain actions because of the threat of consequences, such as punishment or pain. Parents, for example, teach children not to engage in dangerous or inappropriate behavior through warnings, sanctions, or punishments. Therefore, deterrence is a universal and instinctive human act that people understand from an early age and use in everyday life, both for self-protection and to influence others' actions, regardless of the socio-cultural context to which they belong. This universality explains why deterrence is applied in contexts ranging from basic personal interactions to institutional security policies.

The concept of *deterrence*, etymologically linked to the Latin *terrere* ("to frighten"), refers to a rational strategy that uses the threat of punishment and the emotional response it triggers to prevent undesirable or hostile actions. In addition to the interpersonal aspect, deterrence has also existed in relationships among various forms of social and political organization, from tribes to states and supranational entities. It became a formalized and theorized strategy in the

¹ Lawrence Freedman, *Deterrence* (Cambridge, MA: Polity Press, 2004).

² "'Salzburger Bierfleisch' and the Legend of the Bull Washers," *Salzburg.info*, www.salzburg.info/en/magazin/art-culture/salzburger-bierfleisch-and-the-legend-of-the-bull-washers_a_445970.

works of scholars such as Thomas Schelling (1960; 1966) and Herman Kahn (1962), particularly in security in the Cold War era (1947–1991),³ due to the nuclear arms race. In particular, deterrence theory focused on the relationship between the United States and the Soviet Union under the menace and logic of mutually assured destruction.

Later, after the fall of the communist system in Europe and in the post-Cold War era (1990s–2000s), deterrence theory was adapted to address non-nuclear and non-state threats, such as terrorism and cyberattacks. Today, deterrence is a key component of cyber defense, law enforcement, and counterterrorism, as it has expanded into digital, hybrid, and asymmetric warfare contexts.

In the security domain, deterrence means preventing or discouraging an adversary from taking an action—usually an aggressive one or one intended to cause strategic damage, loss of life, and/or injuries—by threatening serious consequences.⁴ It often involves the threat of retaliation (instilling fear of consequences) or demonstrating the capability to inflict extremely serious damage, thereby reducing the expected benefit of such actions. In essence, deterrence means convincing an adversary that the risks and losses of its action are likely to exceed the benefits. A widely used definition of deterrence is the manipulation of an adversary's cost-benefit calculation regarding a given action. By diminishing anticipated advantages or increasing prospective costs (or both), one can convince the adversary to refrain from taking that action.⁵

Deterrence has two main forms. The first is *deterrence by denial*. Glenn H. Snyder defined it as deterrence achieved by the capability to deny the other party any gains from the move to be deterred.⁶ Michael J. Mazarr shows that deterrence by denial relies on a capability to deny that is equivalent to the capability to defend, and is thus effective in preventing an action by convincing a potential aggressor that the action is infeasible or unlikely to succeed, so that the aggressor cannot objectively hope to achieve its objectives.⁷ The second is *deterrence by punishment*, which threatens severe penalties (such as nuclear escalation or severe economic sanctions) in response to a hostile act.⁸ The focus of

³ Paul Kecskemeti, *Strategic Surrender: The Politics of Victory and Defeat* (Stanford, CA: Stanford University Press, 1958), 245–253.

⁴ Fiveable Content Team, “Deterrence,” *Fiveable: International Relations*, last updated August 2025, <https://fiveable.me/key-terms/introduction-international-relations/deterrence>.

⁵ Freedman, *Deterrence*.

⁶ Dmitry Adamsky, “Deterrence à la Ruse: Its Uniqueness, Sources and Implications,” in *NL ARMS Netherlands Annual Review of Military Studies 2020*, ed. Frans Osinga and Tim Sweijts (The Hague: T.M.C. Asser Press, 2021), 161–175, https://doi.org/10.1007/978-94-6265-419-8_9.

⁷ Michael J. Mazarr, “Understanding Deterrence,” *Perspective* no. 295 (Santa Monica, CA: RAND Corporation, 2018), https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf.

⁸ Mazarr, “Understanding Deterrence.”

deterrence by punishment is not the direct defense of the contested assets, but rather the threat of broader punishment that would raise the cost of an attack.

Deterrence Defined – Russia and NATO

A state's military strategy is shaped by how it understands and applies the concept of deterrence. A brief comparative view of how NATO and Russia understand deterrence can help explain the defensive or offensive posture these actors adopt in their military strategy. Deterrence can be applied not only in conventional warfare but also in response to hybrid threats and irregular warfare.

Deterrence is a concept deeply rooted in the defensive strategies of states and defensive alliances such as NATO. NATO sees deterrence and defense as core tasks and is committed to protecting the freedom and security of all Allies against all threats from all directions. The Alliance discourages aggression by maintaining a credible deterrence and defense posture that blends nuclear, conventional, and missile defense capabilities, complemented by space and cyber capabilities.⁹ In sharp contrast, Russia's deterrence strategy can be summed up as follows: *action before reaction*. Dmitry Adamsky's *Deterrence à la Russe* offers a comprehensive analysis of Russia's distinctive approach to deterrence, emphasizing its significant differences from Western paradigms.¹⁰

How Russia Deters – The Prominent Role of Sabotage

In Russian strategic discourse, the term for deterrence is *sderzhivanie*, literally meaning "restraining," "keeping out," or "holding back." It represents a multi-layered strategic doctrine in military and geopolitical thinking.¹¹ Unlike the Western term, which emphasizes fear, the Russian term lacks psychological implications and focuses more on the strategic imposition of costs.¹²

The Ministry of Defence's military-encyclopedia dictionary defines *strategicheskoe sderzhivanie* ("strategic deterrence") as a coordinated system of military and non-military measures aimed at stabilizing the military-political situation to deter all types of threats using all available state tools.¹³ Understood through a Western lens, *sderzhivanie* aligns closely with hybrid warfare, cross-

⁹ "Deterrence and Defence," NATO, December 10, 2025, www.nato.int/cps/en/natohq/topics_133127.htm.

¹⁰ Adamsky, "Deterrence à la Ruse: Its Uniqueness, Sources and Implications."

¹¹ Samuel Charap, "Strategic Sderzhivanie: Understanding Contemporary Russian Approaches to 'Deterrence,'" *Security Insights* No. 62 (Garmisch-Partenkirchen: George C. Marshall European Center for Security Studies, September 2020), www.marshallcenter.org/en/publications/security-insights/strategic-sderzhivanie-understanding-contemporary-russian-approaches-deterrence-0.

¹² Charap, "Strategic Sderzhivanie."

¹³ "Sderzhivanie Strategicheskoe," Military-Encyclopedia Dictionary Online, n.d., accessed January 23, 2026, <https://1564.slovaronline.com/10093-сдерживание-стратегическое>. – in Russian

domain coercion, and nuclear brinkmanship.¹⁴ For Russia, security means maintaining constant pressure on adversaries, including NATO and the United States.

In addition to *sderzhivanie*, the concept of *ustrashenie*—translated as “intimidation”—is central to Russia’s doctrine. It includes nuclear signaling, overt military displays, disinformation, and psychological operations designed to confuse and demoralize opponents.¹⁵ This logic was evident in Russia’s military build-up on Ukraine’s borders in 2021–2022, which was used to coerce Western concessions and deter a severe response without direct warfare.

Sabotage, whether physical or cyber, is one of the most significant deterrence tools in Russia’s hybrid arsenal. The U.S. Department of Defense defines sabotage as a deliberate, covert action intended to damage, disrupt, or obstruct critical infrastructure and resources in pursuit of strategic objectives.¹⁶ It fits within both *sderzhivanie* (restraint) and *ustrashenie* (intimidation), aligning with Russia’s emphasis on ambiguity and strategic shaping.¹⁷ As an asymmetric tool, it is cost-effective, deniable, and strategically ambiguous – blurring the lines between peace and war.¹⁸ Russian sabotage is targeted and strategic, reflecting continuity with Soviet-era practices documented in Cold War archives.¹⁹ The KGB and GRU developed extensive plans for covert sabotage operations against Western critical infrastructure intended to drive wedges within NATO, demoralize the Allied states, disrupt supply chains, and instill political doubt. The targets were chosen for their symbolic and strategic value and included energy infrastructure such as power plants, oil pipelines, and refineries; transportation networks such as bridges, tunnels, ports, and highways; and telecommunications systems, including telephone hubs and radar stations. Key economic and military sites were marked for sabotage, such as the ports of Rotterdam and Antwerp, which supported the Vietnam War effort, as well as chemical plants and storage

¹⁴ Charap, “Strategic Sderzhivanie.”

¹⁵ Michael Kofman and Anya Loukianova Fink, “Escalation Management and Nuclear Employment in Russian Military Strategy,” *War on the Rocks*, June 23, 2020, <https://warontherocks.com/2020/06/escalation-management-and-nuclear-employment-in-russian-military-strategy/>.

¹⁶ “Exploring the Role of Covert Operations and Sabotage in Modern Military Strategies,” *Ops Defender*, May 8, 2024, <https://opsdefender.com/covert-operations-and-sabotage>.

¹⁷ Keir Giles, *Russia’s ‘New’ Tools for Confronting the West: Continuity and Innovation in Moscow’s Exercise of Power* (London: Chatham House, 2016), www.chathamhouse.org/sites/default/files/publications/2016-03-russia-new-tools-giles.pdf.

¹⁸ Valery Gerasimov, “The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations,” *Military Review* (January–February 2016): 23-29, https://www.armyupress.army.mil/Portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf.

¹⁹ Daniela Richterova, “The Long Shadow of Soviet Sabotage Doctrine?” *War on the Rocks*, August 19, 2024, <https://warontherocks.com/2024/08/the-long-shadow-of-soviet-sabotage-doctrine/>.

facilities in West Germany. Western special forces were also surveyed. Propaganda hubs such as Radio Free Europe in Munich were prime targets because of the ideological threat they posed to the Soviet bloc.²⁰

This continuity is confirmed by the Gerasimov Doctrine, which stresses the strategic importance of non-military tools. Sabotage supports this hybrid warfare mindset, remaining below NATO's Article 5 threshold. According to *Recorded Future*, arson and improvised explosives, as well as cover identities, recruited agents, targets, and timing (amid Western support for Ukraine), are all signature tactics echoing Soviet doctrine. Russian sabotage activities rely on techniques that ensure plausible deniability. Intelligence networks recruit agents who can execute these operations without creating direct links to the Russian state. Recent incidents emphasize the growing role of proxy actors, particularly foreign nationals and criminal networks recruited by Russian intelligence to conduct sabotage. Arrests across Europe have revealed the use of Balkan operatives, Belarusian couriers, and local informants to execute attacks, while Moscow could not be clearly held responsible.²¹

Reflecting Russian strategies from Cold War operations, Europe has faced a surge in such acts since the invasion of Ukraine in 2022 – arguably the most severe wave experienced by the West since the Second World War. Although officials are increasingly convinced that many of these attacks are orchestrated by the Kremlin, deniability remains a trademark of such operations. Intelligence agencies, Western governments, and NATO leaders have publicly condemned Russia and have confirmed that arrested saboteurs in countries like Poland, Germany, Romania, the United Kingdom, and the Czech Republic had links to Russian intelligence services. They have also warned about the threat posed by Russia-directed saboteurs operating on their territories, although these acts are often carried out by non-Russian nationals to provide the Kremlin with deniability. EU and NATO countries that adopted a flexible position toward Russia or remained neutral (Hungary, Turkey, Austria, Switzerland) do not appear on the 2022–2025 sabotage map, which could be another clue for attribution.²²

Russia's current sabotage tactics can be categorized into three groups: *economic* sabotage (targeting infrastructure essential to economic stability), *military* sabotage (disrupting arms production, transportation, and military readiness through attacks on weapons factories or logistics hubs), and *political destabilization* (amplifying socio-political divisions and instilling fear within local populations by creating a persistent threat of sabotage).²³ The U.S. Helsinki Commission report (2024) shows that about 150 instances of sabotage (seemingly random incidents) and other hybrid actions are believed to have been carried out

²⁰ Richterova, "The Long Shadow of Soviet Sabotage Doctrine?"

²¹ Insikt Group, "Russian Sabotage Activities Escalate Amid Fraught Tensions," Research Report, *Recorded Future*, November 14, 2024, <https://assets.recordedfuture.com/insikt-report-pdfs/2024/ta-ru-2024-1114.pdf>.

²² Insikt Group, "Russian Sabotage Activities Escalate Amid Fraught Tensions."

²³ Insikt Group, "Russian Sabotage Activities Escalate Amid Fraught Tensions."

by Russia against NATO member states most supportive of Ukraine in order to achieve several goals: deterring support for the attacked state, testing NATO's unity and resilience, including NATO's Article 4 and 5 commitments, interfering in national elections in various forms, exposing and damaging critical infrastructure, and conducting cognitive warfare through disinformation and fake news to create panic and erode trust in governments and alliances.²⁴ Tactics have included disrupting military logistics, arson, cyberattacks, damage to critical energy infrastructure, and support for proxy groups. Modern operations target power grids, transport, and public infrastructure, much as Soviet-era practices did.

The distribution and forms of these acts are wide-ranging. To name only some examples: in Germany, critical railway communication cables were severed in October 2022, halting trains across northern regions. In 2024, the Diehl Metal factory, involved in producing IRIS-T air defense systems, was set ablaze, and a Russian-linked plot to assassinate the Rheinmetall CEO was disrupted. A DHL freight hub in Leipzig was targeted with an incendiary parcel sent via Lithuania, as part of a broader transnational sabotage network. Poland has faced repeated incidents, including an arson plot against a paint factory in January 2024, a massive fire at Warsaw's main shopping center in May, and multiple foreign nationals have been arrested for sabotage. In Romania, a Colombian national trained by Russian operatives was caught preparing attacks on infrastructure in Bragadiru in July 2024, and the country faced over 85,000 cyberattacks and coordinated disinformation during its presidential election. In the United Kingdom, a DHL facility in Birmingham was set on fire by a parcel believed to have been a dry run for larger-scale sabotage, echoing a similar case in Germany. The Baltic region also saw disruption, with submarine cables between Finland and Estonia damaged in late 2024 in an incident suspected to have been caused by Russia's shadow fleet, and Eastlink 2, a major power link, disabled by a dragging anchor. A plot to set fire to a bus depot in Prague was thwarted by Czech intelligence in June 2024, Lithuania's IKEA warehouse was damaged by a suspicious fire in May, and Belgium experienced an explosion at a military equipment warehouse in Antwerp in 2023.²⁵ Although some target countries are still investigating the causes or identifying the perpetrators, Poland, Germany, the Czech Republic, Denmark, the United Kingdom, and Romania have already arrested individuals linked to these attacks. However, operations often originate through proxy actors or Russian networks based in third countries such as Belarus, Serbia, or even

²⁴ U.S. Commission on Security and Cooperation in Europe, *Spotlight on the Shadow War* (Washington, DC: U.S. Commission on Security and Cooperation in Europe, 2024), <https://www.csce.gov/wp-content/uploads/2024/12/Spotlight-on-the-Shadow-War-Website.pdf>.

²⁵ U.S. Commission on Security and Cooperation in Europe, *Spotlight on the Shadow War*.

Latin America.²⁶ Furthermore, these governments have publicly held Russia responsible, expressing varying degrees of confidence in their conclusions.²⁷

Given the ongoing geopolitical tensions, particularly the prolonged war of attrition and the stalemate in peace negotiations, incidents of sabotage are likely to increase, underscoring the urgent need for effective deterrence, prevention, and containment.²⁸ The scale and sophistication of covert operations are expected to grow in what appears to be a troubling revival of Cold War practices under current hybrid conditions.²⁹ Without solid countermeasures, these covert actions could undermine national security and NATO's support for Ukraine. To address the evolving threat landscape, European nations must enhance intelligence sharing, strengthen infrastructure security, and closely monitor potential targets for signs of escalation.³⁰

Understanding the sabotage strategy used during the Cold War helps us, to some extent, predict future instances of sabotage and counter them through deterrence, prevention, and containment.

²⁶ "NATO Says Russian Hybrid Attack Intensify on Members' Territories," *Reuters*, May 2, 2024, www.reuters.com/world/europe/nato-says-russian-hybrid-attack-intensify-members-territories-2024-05-02/; "Fake News from Russian, Belarusian Services Spiked during Floods in Poland, Minister Says," *Reuters*, September 25, 2024, www.reuters.com/world/europe/fake-news-russian-belarusian-services-spiked-during-floods-poland-minister-says-2024-09-25/; "From Russia to Serbia: How RT Spreads the Kremlin's Propaganda in the Balkans despite EU Sanctions," *Reporters Without Borders (RSF)*, September 30, 2024, <https://rsf.org/en/russia-serbia-how-rt-spreads-kremlin-s-propaganda-balkans-despite-eu-sanctions>.

²⁷ "Terrorist Group Responsible for Arson Attacks across Europe Taken to Court," Eurojust – European Union Agency for Criminal Justice Cooperation, 27 January 2026, <https://www.eurojust.europa.eu/news/terrorist-group-responsible-arson-attacks-across-europe-taken-court>; James C. Reynolds, "Russia Could Be Behind Cyber Attacks on British Businesses like M&S, NATO General Warns," *Independent*, December 4, 2025, www.independent.co.uk/news/world/europe/russia-cyber-attack-marks-and-spencer-nato-b2877844.html; Simon Lewis, "US Warns of Russian Effort to Tilt 2024 Elections in Europe against Ukraine," *Reuters*, January 18, 2024, www.reuters.com/world/us-warns-russian-effort-tilt-2024-elections-europe-against-ukraine-2024-01-18/; "Russian Hybrid Operations Very Concerning, Say Romania, Poland and Latvia," *Reuters*, June 11, 2024, www.reuters.com/world/europe/russian-hybrid-operations-very-concerning-say-romania-poland-latvia-2024-06-11/.

²⁸ "Countering Hybrid Threats," NATO, updated January 29, 2026, https://www.nato.int/cps/en/natohq/topics_156338.htm; Insikt Group, "Russian Sabotage Activities Escalate Amid Fraught Tensions."

²⁹ Eitvydas Bajarūnas, "The Hybrid Threat Imperative: Deterring Russia Before It Is Too Late," *Comprehensive Report* (Washington, D.C.: Center for European Policy Analysis, 2025), <https://cepa.org/comprehensive-reports/the-hybrid-threat-imperative-deterring-russia-before-it-is-too-late/>.

³⁰ Filip Bryjka, "NATO Members on Guard Against Russian Sabotage," *The Polish Institute of International Affairs (PISM), Bulletin No. 112 (2420)*, July 29, 2024, <https://pism.pl/publications/nato-members-on-guard-against-russian-sabotage>.

Western/NATO Approaches to Deterrence and Combating Sabotage

Western notions of deterrence focus on denial, punishment, and resilience. *Deterrence à la Russe* exploits societal fear, strategic infrastructural weaknesses, deniable attribution, and, maybe most importantly, its adversaries' self-deterrence – the hesitation to act out of fear of escalation.³¹

NATO has shifted from a reactive posture to a more proactive and integrated approach to deterrence and defense against aggression. A key element of this transformation is the adoption of the *Deterrence and Defense of the Euro-Atlantic Area* (DDA) concept, which marks a major shift from the post-Cold War NATO deterrence posture centered on crisis management. The DDA modernizes NATO's strategic planning to address the challenges of the 21st century, especially those posed by a more aggressive Russia.³² Covington emphasizes that this new approach to deterrence reflects NATO's understanding that it cannot wait until a crisis emerges. Instead, to be effective, deterrence should be integrated into everyday Alliance activities, even in peacetime, through a constant demonstration of military readiness and cross-domain cohesion that displays measures and capabilities and denies adversaries any window of strategic opportunity.³³

One of the DDA's key features is the coordinated employment of land, air, maritime, cyber, and space capabilities. It enhances NATO's ability to respond to complex hybrid threats that go beyond traditional battlefield frontiers. Furthermore, the DDA strengthens NATO's political and military unity by reinforcing the link between strategic planning and political decision-making. Covington notes that the DDA facilitates quicker, more coordinated reactions in times of peace, crisis, and war. This is crucial not only for deterring aggression but also for managing escalation and maintaining control over any possible conflict. The DDA's effectiveness was demonstrated through NATO's response to Russia's invasion of Ukraine in 2022.³⁴ It provided the basis for the Alliance's rapid deployment of troops to its eastern flank, thereby preventing Russian attempts to extend the conflict beyond Ukraine's borders.

According to Covington, this rapid and coordinated response tested the DDA as an instrument of crisis management as much as of war deterrence.³⁵ By showing Moscow that the Alliance is neither weak nor irresolute, NATO effectively raised the costs of further aggression.³⁶ Overall, the DDA is both a conceptual and an operational pillar of NATO's renewed and critical strategic adaptation to

³¹ Adamsky, "Deterrence à la Ruse: Its Uniqueness, Sources and Implications."

³² Stephen R. Covington, "NATO's Concept for Deterrence and Defence of the Euro-Atlantic Area (DDA)," Belfer Center for Science and International Affairs, Harvard Kennedy School, August 2, 2023, www.belfercenter.org/publication/natos-concept-deterrence-and-defence-euro-atlantic-area-dda.

³³ Covington, "NATO's Concept for Deterrence and Defence of the Euro-Atlantic Area."

³⁴ NATO, "Deterrence and Defence."

³⁵ Covington, "NATO's Concept for Deterrence and Defence of the Euro-Atlantic Area."

³⁶ Covington, "NATO's Concept for Deterrence and Defence of the Euro-Atlantic Area."

the realities of modern warfare and geopolitical rivalry. By embracing a proactive, cross-domain approach to deterrence, NATO has strengthened its commitment to collective defense and demonstrated its capacity to adapt to emerging security challenges.

Deterring Sabotage – A Particularly Challenging Task

NATO classifies sabotage as a hybrid threat, which may include tactics that often remain below the threshold of conventional conflict, complicating attribution and response, such as cyberattacks, disinformation, political interference, and covert operations.³⁷ Sabotage is one of the most complex and challenging tools of hybrid warfare. It is difficult to address through conventional deterrence, prevention, or containment, as it merges characteristics of conventional warfare and terrorism. Sabotage combines military, cyber, economic, and informational tactics employed covertly, below the threshold of open conflict.

The similarities between sabotage and conventional warfare are found in their targets and effects. Both often focus on strategic infrastructure—such as railways, fuel depots, and supply lines—which is critical to an adversary's operational capabilities and, when disrupted, can generate panic.³⁸ Regarding effects, like conventional warfare, sabotage can lead to significant casualties, including injuries and deaths among the civilian population, for example, when it takes the form of explosions or arson. In some cases, when incidents result in victims from third-party states, as seen in international incidents such as plane hijackings and explosions, sabotage may go beyond conventional warfare in its impact.³⁹

Sabotage can be deployed both as a standalone tool of hybrid warfare and in support of conventional operations. However, unlike conventional warfare, sabotage can be conducted by intelligence agencies, resistance groups, or mercenaries. It is rarely claimed and is difficult to attribute under plausible deniability.⁴⁰

Sabotage and terrorism both seek to influence political or military decision-making processes or the behavior of society by generating fear and uncertainty through destruction and violence. Their targets may include political, economic, and military assets; damage to them creates disorder, erodes public confidence,

³⁷ NATO, "Countering Hybrid Threats."

³⁸ Krzysztof Izak, "Terrorist and Sabotage Attacks on Selected Critical Infrastructure Systems – A Historical Perspective," *Terrorism – Studies, Analyses, Prevention*, Special Issue (2025): 71-111, <https://doi.org/10.4467/27204383TER.25.015.21518>.

³⁹ Witold Skomra and Karolina Wojtasik, "Critical Infrastructure as a Target for Hybrid Operations: Case Studies of Attacks Against the Facilities and Systems of CI," *Terrorism – Studies, Analyses, Prevention*, Special Issue (2025): 13-34, <https://doi.org/10.4467/27204383TER.25.013.21516>.

⁴⁰ Joshua Rovner, Rory Cormac, and Lennart Maschmeyer, "Sand in the Gears: Sabotage in World Politics," *European Journal of International Security*, First View (2025), <https://doi.org/10.1017/eis.2025.10025>.

and diminishes the adversary's operational capability through psychological effects such as fear and distrust. The main difference between the two is that terrorist acts usually target civilians, while acts of sabotage target infrastructure and physical or cyber networks, but rarely human beings directly. Yet some forms of sabotage, such as arson or power grid destruction, can have the same effects as terrorism.

Deterring sabotage is not only about preventing damage to strategic infrastructure but, more importantly, about protecting democratic institutions, economic stability, military readiness, and the political cohesion of the Alliance, while ensuring that NATO's commitment to collective defense is taken seriously amid constant, mounting hybrid threats. Deterring sabotage is therefore extremely important but also particularly challenging due to its asymmetrical nature. A credible deterrence strategy that clearly conveys real consequences, improved attribution capabilities, and strong resilience can make sabotage much more costly and less appealing. NATO has clearly stated that significant hybrid attacks, including acts of sabotage, could lead to the invocation of Article 5, the collective defense clause.⁴¹ This is intended to discourage adversaries by reinforcing the Alliance's commitment to collective defense. Since sabotage is increasingly seen as a central tactic in hybrid warfare, particularly in light of Russia's hostile activities in the Euro-Atlantic area, NATO's approach to it is part of its broader strategy for resilience, deterrence, and defense against irregular warfare.⁴² NATO has publicly denounced Russia's operations as a widening campaign of hostile activities across the Euro-Atlantic space. It has outlined actions to be taken, including enhanced intelligence-sharing, reinforced protection of critical and undersea infrastructure, increased cyber defense, and stricter controls on Russian intelligence personnel operating within member states.⁴³ In response to numerous sabotage incidents, NATO and Western governments have increasingly adopted more assertive countermeasures.⁴⁴ Several NATO members have established task forces to monitor and protect vital infrastructure.⁴⁵ New national security strategies are being adopted, and legal frameworks are being revised and adapted to the new security environment.⁴⁶ In parallel, law enforce-

⁴¹ NATO, "Deterrence and Defence."

⁴² NATO, "Deterrence and Defence."

⁴³ "Statement by the North Atlantic Council on Recent Russian Hybrid Activities," NATO, May 2, 2024, <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/05/02/statement-by-the-north-atlantic-council-on-recent-russian-hybrid-activities>.

⁴⁴ "Resilience, Civil Preparedness and Article 3," NATO, updated November 13, 2024, <https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3>.

⁴⁵ "NATO's Maritime Activities," NATO, updated March 10, 2025, www.nato.int/en/what-we-do/operations-and-missions/natos-maritime-activities.

⁴⁶ "Critical Infrastructure Resilience at EU Level," European Commission, January 13, 2026, https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en.

ment agencies coordinate closely with foreign partners to investigate and prevent suspected sabotage plots.⁴⁷ Ongoing efforts also aim to increase societal resilience by strengthening public vigilance and awareness.⁴⁸

Because of the strategic ambiguity of sabotage, deterrence must be part of a comprehensive hybrid deterrence strategy that integrates tools from the diplomatic, informational, military, economic, counterterrorism, and legal spheres.⁴⁹ Integrated deterrence against hybrid threats, including sabotage, needs to combine military readiness, legal attribution, social resilience, and strategic anticipation. Mitigating hybrid threats requires resilience-building in both civilian and military sectors, public-private partnerships to protect critical infrastructure, proactive steps to counter disinformation and contain its psychological and political impact,⁵⁰ and strategic communication to control public panic, strengthen national unity, and demonstrate determination.⁵¹ Unified messaging, timely attribution, and cross-border coordination increase deterrent effects.⁵²

A Deterrence Toolbox for NATO and the West

The West is limited in its non-military response options, aside from the extensive economic and diplomatic sanctions against Moscow, which would become even less damaging to Russia if the United States agreed to lift them. Yet NATO's measures for addressing sabotage cover a broad spectrum of tactics. These include political signaling to show unity and determination⁵³; preserving military readiness through joint operations and training exercises that demonstrate robust defense; operational deployments to secure vulnerable infrastructure⁵⁴; crisis-management drills that simulate sabotage scenarios in order to test and effectively enhance response strategies; frequent evaluations and updates of security protocols to protect critical infrastructure against cyber sabotage; cyber-forensic efforts to identify and expose perpetrators⁵⁵; reinforcing vulnerable in-

⁴⁷ "Polish Army to Help Power Grid Protect Key Infrastructure," *Reuters*, December 3, 2025, www.reuters.com/business/aerospace-defense/polish-army-help-power-grid-protect-key-infrastructure-2025-12-03.

⁴⁸ House of Commons, Defence Committee, "Oral Evidence: Defence in the Grey Zone, HC 50," UK Parliament Committees, April 23, 2024, <https://committees.parliament.uk/oralevidence/14668/html>.

⁴⁹ "Hybrid Threats: Hybrid Threats as a Concept," European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), accessed January 24, 2026, www.hybridcoe.fi/hybrid-threats/.

⁵⁰ "Deterrence and Resilience," Hybrid CoE, Thematic reports and other publications (2023/2024), <https://www.hybridcoe.fi/deterrence-and-resilience/>.

⁵¹ "NATO's Approach to Counter Information Threats," NATO, updated February 3, 2025, https://www.nato.int/cps/en/natohq/topics_219728.htm.

⁵² NATO, "Countering Hybrid Threats."

⁵³ NATO, "Countering Hybrid Threats."

⁵⁴ NATO, "Countering Hybrid Threats."

⁵⁵ NATO, "NATO's Approach to Counter Information Threats."

frastructure.⁵⁶ Strategic communications to counter disinformation campaigns⁵⁷ and public awareness initiatives are also critical, as they educate both the private and public sectors about sabotage risks and encourage the reporting of suspicious activities, which is crucial for early detection.

A few other measures, which are already being implemented by some countries but require greater effort, or need to be put into practice both at the national level and as a coordinated strategy among the allies, include:

- *Forecasting and Anticipating Sabotage Trends*

Effective deterrence against Russian sabotage requires strategic anticipation based on patterns, precedents, and foresight. Because sabotage is opportunistic, covert, and deniable, it is difficult to foresee, particularly when it is carried out by proxies. However, recognizing and classifying consistent patterns in Russian hybrid activity is a good starting point for predicting potential targets and weak points and, consequently, for establishing deterrent and defensive measures.⁵⁸

Intelligence-driven threat diagnosis and prognosis are essential. This involves mapping potential future targets for sabotage, such as energy infrastructure, military transport nodes, communications systems, and cyber systems.⁵⁹ The geographic focus will likely include Eastern Europe, the Baltic states, western Russia, occupied Ukrainian territories, and NATO civilian infrastructure.⁶⁰ Based on the findings from recent incidents, future sabotage could involve tactics such as cyberattacks on infrastructure in the Nordic and Baltic regions, covert attacks on NATO rail networks and logistics hubs, energy disruptions, hybrid activities involving Russian private military contractors in the Balkans, and false-flag incidents that could provoke overreaction.⁶¹

Key measures include incorporating lessons learned into threat modeling,⁶² investing in predictive intelligence, hardening targets with redundant systems,

⁵⁶ NATO, "NATO's Approach to Counter Information Threats."

⁵⁷ "NATO 2022 Strategic Concept Adopted by Heads of State and Government at the NATO Summit in Madrid," NATO, June 29, 2022, <https://www.act.nato.int/wp-content/uploads/2023/05/290622-strategic-concept.pdf>.

⁵⁸ Hanna Mäkinen, "Russia's Hybrid Warfare in Europe," *Baltic Rim Economies*, no. 1 (January 2026): 141, https://www.centrumbalticum.org/files/7113/BRE_1_2026.pdf.

⁵⁹ Helmi Pillai, "Protecting Europe's Critical Infrastructure from Russian Hybrid Threats," Policy Brief, Centre for European Reform, April 25, 2023, www.cer.eu/publications/archive/policy-brief/2023/protecting-europes-critical-infrastructure-russian-hybrid.

⁶⁰ Anna Maria Dyner, "Preparing for Russian Hybrid Activities Against NATO and EU Countries," The Polish Institute of International Affairs (PISM), Bulletin No. 183 (2100), November 25, 2022, <https://www.pism.pl/publications/preparing-for-russian-hybrid-activities-against-natoand-eu-countries>.

⁶¹ Seth G. Jones, "Russia's Shadow War Against the West," CSIS Briefs, Center for Strategic and International Studies, March 18, 2025, <https://www.csis.org/analysis/russias-shadow-war-against-west>.

⁶² Pillai, "Protecting Europe's Critical Infrastructure from Russian Hybrid Threats."

upgrading physical security, enabling real-time detection of suspicious activities, and strengthening public-private partnerships, especially in the energy, transport, and cyber sectors.

- *Attribution*

Unlike conventional warfare or terrorism, sabotage is frequently concealed through operations carried out under false flags or by non-state actors.⁶³ Therefore, deterrence relies heavily on the credible attribution of past events, followed by legal and economic consequences, as well as effective early warning and national and international cooperation. Official public attribution of sabotage can also serve as a deterrent, as states demonstrate their ability to detect, investigate, and respond to covert operations, and it can trigger diplomatic or collective responses against the hostile actor.

- *Preparedness and Readiness*

NATO's deterrence tactics also include high levels of military readiness and presence, particularly in Eastern Europe through its Enhanced Forward Presence initiative. Special operations forces and intelligence units are deployed to monitor and secure high-risk sites.⁶⁴

To improve preparedness and training, it is essential to conduct regular drills that simulate sabotage and cyberattack scenarios, participate in multilateral NATO exercises that practice joint infrastructure defense, and establish cross-sector coordination and interagency task forces. Training exercises and joint operations reassure allies, but they also serve as a deterrent against state-sponsored acts of sabotage.

- *Resilience*

NATO encourages member states to improve national resilience, recognizing that the first line of defense against sabotage is at the national level. The Alliance has developed resilience baselines across key sectors, encourages regular stress testing, and provides guidelines for civil preparedness.

Comprehensive deterrence involves building resilience and ensuring a rapid response to raise the costs for adversaries. Estonia and Israel provide instructive examples.⁶⁵ Estonia has institutionalized rapid attribution and robust public-private cyber resilience programs, hosts NATO's CCDCOE in Tallinn, and has hardened infrastructure and credible deterrence signals.⁶⁶ Israel emphasizes preemptive intelligence, infrastructure hardening, swift retaliation, and real-

⁶³ Alex P. Schmid, "Defining Terrorism," ICCT Report, International Centre for Counter-Terrorism, March 2023, <https://icct.nl/publication/defining-terrorism>.

⁶⁴ "Strengthening NATO's Eastern Flank," NATO, October 23, 2025, www.nato.int/cps/en/natohq/topics_136388.htm.

⁶⁵ Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014).

⁶⁶ Alexander Klimburg, ed., *National Cyber Security Framework Manual* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2012), <https://ccdcoe.org/library/publications/national-cyber-security-framework-manual>.

time response.⁶⁷ The Baltic states have diversified energy sources, strengthened cooperation, and benefited from NATO and EU military support.⁶⁸ Resilience and swift recovery rely on specialized crisis teams (mobile repair and cyber forensics), public-private partnerships in preparedness and information sharing, and the creation of redundant supply chains and backup systems, such as alternative power and communication channels.⁶⁹

- *Legal Response*

Legal and institutional measures support these operational efforts. Hybrid threats call for changes to legal systems, particularly with regard to acts of sabotage that mirror terrorist tactics – they must be clearly outlawed. Enhanced counterterrorism legislation should be extended to covert acts of sabotage, with targeted heavy sanctions and faster investigative procedures to ensure deterrence through prompt punishment.⁷⁰ Many NATO countries have reinforced counterintelligence capabilities and enacted or updated legislation targeting sabotage, espionage, and covert influence operations. Improved coordination between military police and civilian law enforcement further strengthens domestic security frameworks.⁷¹

- *Cybersecurity*

Cybersecurity plays a critical role in sabotage deterrence. Cyberattacks are now widely recognized as potential triggers for Article 5, NATO's collective defense clause. The Alliance has established a Cyber Rapid Reaction Team and collaborates with both the European Union and private-sector actors to enhance cyber resilience across its members. Hybrid threats, which combine cyber operations, disinformation, and physical sabotage, are addressed through the NATO Hybrid Threats Centre of Excellence in Finland, which supports the development of tailored strategies and best practices.⁷² Additionally, many NATO countries invest significantly in cybersecurity initiatives to protect critical infrastructure from cyber sabotage, conducting regular assessments and updating security protocols.

⁶⁷ Alon Ben-Meir, "Israel's Pre-Emptive Strategy and Peace," *AlonBen-Meir.com*, February 11, 1989, accessed January 24, 2026, <https://alonben-meir.com/writing/israels-pre-emptive-strategy-and-peace/>.

⁶⁸ "NATO Launches 'Baltic Sentry' to Increase Critical Infrastructure Security," *News Release*, NATO, January 14, 2025, www.nato.int/en/news-and-events/articles/news/2025/01/14/nato-launches-baltic-sentry-to-increase-critical-infrastructure-security.

⁶⁹ "The NATO Cooperative Cyber Defence Centre of Excellence Is a Multinational and Interdisciplinary Cyber Defence Hub," NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), accessed January 24, 2026, <https://www.ccdcoe.org>.

⁷⁰ NATO, "Countering terrorism," What We Do, updated August 6, 2025, www.nato.int/en/what-we-do/deterrence-and-defence/countering-terrorism.

⁷¹ European Centre of Excellence for Countering Hybrid Threats, *Annual Report 2023*.

⁷² European Centre of Excellence for Countering Hybrid Threats, *Annual Report 2022*.

- *Integrating Counterterrorism Strategies*

Sabotage shares some characteristics with terrorism, including small clandestine teams as actors, symbolic infrastructure as targets, improvised explosives as tools, and arson, cyber breaches, and insider threats as methods of operation. Effective deterrence and prevention of sabotage resembling counterterrorism operations (CTS) require a multi-layered strategy that blends intelligence, civil-military coordination, infrastructure redundancy and physical security, legal enforcement, and rapid-response capabilities.⁷³

Methods usually used to reduce risks of terrorist acts could also be adopted to counter sabotage threats, particularly those involving low-tech yet high-impact tactics such as arson. Because of its simplicity, deniability, and potentially catastrophic effects, arson has become a favored method of sabotage.⁷⁴ It requires few resources and no advanced technology, and rarely leaves behind forensic evidence; as a result, clear attribution is challenging and risky. Fires can cause mass panic and even human casualties, damaging vital infrastructure far beyond the initial target and disrupting services.⁷⁵

Common arson targets include military depots, transportation hubs (to paralyze logistics), energy infrastructure (to cause blackouts or fuel shortages), and industrial facilities (to halt production and inflict economic loss). Arson is often used in hybrid warfare along with cyberattacks or disinformation campaigns, thereby increasing the psychological and operational damage.

Particular steps are required to counter arson sabotage. Early-warning fire detection systems—including smoke and heat sensors coupled with CCTV—can drastically reduce response times. While surveillance tools such as drones and thermal cameras help identify suspicious activity in sensitive areas, physical security measures, including fencing and controlled access, help deter unauthorized entry. Especially where state monitoring is limited, involving local staff and residents through community watch programs provides an additional layer of vigilance.⁷⁶ While strong legal enforcement and the prosecution of arsonists dis-

⁷³ United Nations Office of Counter-Terrorism and Counter-Terrorism Committee Executive Directorate, *The Protection of Critical Infrastructure Against Terrorist Attacks: Compendium of Good Practices* (New York: United Nations, 2018), www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021_Jan/compendium_of_good_practices_eng.pdf.

⁷⁴ Robert Arthur Baird, "Pyro-Terrorism – The Threat of Arson-Induced Forest Fires as a Future Terrorist Weapon of Mass Destruction," *Studies in Conflict & Terrorism* 29, no. 5 (2006): 415-428, <https://doi.org/10.1080/10576100600698477>.

⁷⁵ Organization for Security and Co-operation in Europe (OSCE), *Project PROTECT – Technical Guide on Physical Security Considerations for Protecting Critical Infrastructure from Terrorist Attacks* (Vienna: OSCE Secretariat, Transnational Threats Department, October 2025), https://www.osce.org/sites/default/files/f/documents/e/6/597756_0.pdf.

⁷⁶ "Enhancing Community Safety Against Incendiary Fires: Prevention and Awareness," Approved Group International (community patrols and vigilance), August 13, 2024,

courage future incidents, emergency preparedness—including fire drills and rapid-deployment teams—helps contain damage.⁷⁷

- *Physical Security of Strategic Infrastructures*

A strategic priority of NATO has become the protection of critical infrastructure – energy grids and pipelines, undersea cables, transport and communications networks, and military facilities. Accordingly, the Alliance promotes intelligence sharing among Allies and partners to detect sabotage attempts early; joint exercises to simulate hybrid and sabotage scenarios and improve response capabilities; enhanced maritime domain awareness, especially in the North and Baltic Seas; and coordination with private-sector stakeholders in energy and telecommunications.⁷⁸ Other measures include the thorough implementation of security protocols, the use of motion sensors, CCTV cameras, and thermal surveillance, the fortification of vulnerable sites with barriers and fences, and drone patrols and satellite remote monitoring of vital areas. Access controls and personnel vetting should also be widely applied.⁷⁹ Concurrently, cyber defenses—especially for Supervisory Control and Data Acquisition (SCADA) systems and industrial control systems (ICS)—must be strengthened to prevent the disabling of alarm or fire-suppression systems before a physical attack.⁸⁰

In February 2023, NATO established the Critical Undersea Infrastructure Coordination Cell to coordinate efforts among Allies and improve the resilience of key maritime infrastructure.⁸¹ Additionally, the proposed EU-NATO Task Force on Resilience of Critical Infrastructure aims to institutionalize knowledge sharing and coordination in this domain.⁸²

<https://approvedgroupinternational.com/enhancing-community-safety-against-incendiary-fires-prevention-and-awareness/>.

⁷⁷ National Protective Security Authority (UK), “Fire as an Act of Sabotage Guidance: Countering the Threat of Sabotage Operations to UK Interests and National Security,” last updated September 25, 2024, www.npsa.gov.uk/national-security-act/countering-threat-sabotage-operations-uk-interests-national-security/fire-act-sabotage-guidance.

⁷⁸ NATO, “Resilience, Civil Preparedness and Article 3.”

⁷⁹ “NATO Allies Join Forces to Enhance the Security of Critical Undersea Infrastructure,” News, NATO, December 10, 2024, www.nato.int/en/news-and-events/articles/news/2024/12/10/nato-allies-join-forces-to-enhance-the-security-of-critical-undersea-infrastructure.

⁸⁰ Joshua Taylor, “Effectiveness of SCADA System Security Used Within Critical Infrastructure,” *ArXiv*, December 18, 2020, <https://arxiv.org/abs/2012.11375>.

⁸¹ “NATO Stands Up Undersea Infrastructure Coordination Cell,” News, NATO, February 15, 2023, https://www.nato.int/cps/en/natohq/news_211919.htm.

⁸² See Table 1: “European Institutions Relevant for Protecting CUI” in Sean Monaghan et al., “NATO’s Role in Protecting Critical Undersea Infrastructure,” *CSIS Brief*, December 19, 2023, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-12/231219_Monaghan_NATO_CUI.pdf.

- *Public Awareness and Civil Preparedness*

Public awareness campaigns aimed at educating both the public and private sectors about the risks of sabotage and the importance of reporting suspicious activities are crucial for early detection. Some NATO states, such as Sweden and Finland, have adopted a “Total Defense” approach, actively involving the population in national resilience planning and crisis response.⁸³

- *Whistleblower Policies*

Community engagement and local intelligence become the first lines of defense against sabotage. Building local confidence, encouraging tip-offs, and training communities to report suspicious activity allow authorities to develop a network of human intelligence capable of spotting early signs of sabotage plots. This is especially important in rural or industrial zones with vulnerable critical infrastructure, where authorities have only a limited presence. Creating confidential mechanisms for employees to report concerns without fear of retaliation may also help promote vigilance.

- *Enhanced Defense Cooperation and Counterintelligence Operations*

An important pillar of deterrence strategy is enhanced intelligence and defense cooperation. NATO has significantly improved real-time intelligence sharing—focusing on foreign intelligence services and proxy actors, as well as on internal threats posed by hostile insiders—and on operational planning among member states to detect, assess, and prevent sabotage. Sharing situational awareness allows for quick responses and coordinated preventive measures.⁸⁴ Strategic partnerships and collaborations with non-NATO partners and international organizations contribute to the sharing of best practices to deter sabotage and to ensure collective security. NATO and its allies can establish a credible deterrence architecture and counter contemporary sabotage threats through proactive anticipation, intelligence sharing, infrastructure protection, and the fostering of societal resilience.⁸⁵

- *Enhancing the Rapid Response Capacity*

Counter-sabotage planning should include specialized quick-reaction teams trained in firefighting, damage assessment, and crisis management. These teams

⁸³ “Total Defence,” Government Offices of Sweden, accessed January 25, 2026, <https://www.government.se/government-policy/total-defence>.

⁸⁴ NATO, “Resilience, Civil Preparedness and Article 3.”

⁸⁵ Filip Bryjka and Tomasz Zając, “EU and NATO Countries Strengthen the Protection of Critical Infrastructure,” Bulletin No. 79 (2198), PISM, June 22, 2023, www.pism.pl/publications/eu-and-nato-countries-strengthen-the-protection-of-critical-infrastructure.

should work closely with law enforcement and private security operators to ensure a swift, coordinated response. Fire drills, emergency evacuation plans, and real-time simulations help increase resilience and preparedness.⁸⁶

Conclusion

Deterrence strategies must adapt to the complexities of hybrid warfare, particularly in the face of asymmetric threats in the grey zone, such as sabotage. NATO's strategic evolution toward a proactive, integrated deterrence approach, exemplified by the DDA concept, underscores the need for a multidomain operational framework to respond effectively to these threats.

The challenge of deterring sabotage—characterized by deniability and ambiguity—requires a comprehensive strategy that encompasses legal, economic, military, intelligence, and social dimensions. By reinforcing critical infrastructure, enhancing public awareness, and fostering international cooperation, nations can build a resilient deterrence posture that addresses immediate threats and provides long-term stability and security. History shows that the Russian pattern of deterrence is applied ceaselessly in both peace and war; therefore, we recognize that our defensive strategy must also be a constant, daily effort, regardless of developments in the security environment. Likewise, the lessons learned from historical and contemporary deterrence practices will be vital in shaping effective responses to the evolving landscape of hybrid threats.

Disclaimer

The opinions, findings, conclusions, and recommendations expressed in this publication are those of the author and do not necessarily reflect the official policy or position of the Partnership for Peace Consortium, its participating institutions, or any governmental or international organizations affiliated with its governance structure.

About the Author

Anca Anescu is a GCMC Scholar Alumna and a Romanian policy analyst with expertise in Eastern European geopolitics, specializing in irregular warfare and hybrid threats, with a particular interest in cognitive warfare and the weaponization of interdependencies. <https://orcid.org/0009-0009-1690-5692>

⁸⁶ Lars Fredholm and Anna-Lena Göransson, eds., *Emergency Response Management in Today's Complex Society* (Swedish Civil Contingencies Agency, 2010); Luca Galbusera et al., "Game-based Training in Critical Infrastructure Protection and Resilience," *International Journal of Disaster Risk Reduction* 78 (August 2022): 103109, <https://doi.org/10.1016/j.ijdrr.2022.103109>.

Bibliography

- “Salzburger Bierfleisch’ and the Legend of the Bull Washers,” *Salzburg.info*, https://www.salzburg.info/en/magazin/art-culture/salzburger-bierfleisch-and-the-legend-of-the-bull-washers_a_445970.
- “Countering Hybrid Threats,” NATO, updated January 29, 2026, www.nato.int/cps/en/natohq/topics_156338.htm.
- “Critical Infrastructure Resilience at EU Level,” European Commission, January 13, 2026, https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en.
- “Deterrence and Defence,” NATO, December 10, 2025, www.nato.int/cps/en/natohq/topics_133127.htm.
- “Deterrence and Resilience,” Hybrid CoE, Thematic reports and other publications (2023/2024), <https://www.hybridcoe.fi/deterrence-and-resilience/>.
- “*Enhancing Community Safety Against Incendiary Fires: Prevention and Awareness*,” Approved Group International (community patrols and vigilance), August 13, 2024, <https://approvedgroupinternational.com/enhancing-community-safety-against-incendiary-fires-prevention-and-awareness/>.
- “Exploring the Role of Covert Operations and Sabotage in Modern Military Strategies,” *Ops Defender*, May 8, 2024, <https://opsdefender.com/covert-operations-and-sabotage>.
- “Fake News from Russian, Belarusian Services Spiked during Floods in Poland, Minister Says,” *Reuters*, September 25, 2024, www.reuters.com/world/europe/fake-news-russian-belarusian-services-spiked-during-floods-poland-minister-says-2024-09-25/.
- “From Russia to Serbia: How RT Spreads the Kremlin’s Propaganda in the Balkans despite EU Sanctions,” Reporters Without Borders (RSF), September 30, 2024, <https://rsf.org/en/russia-serbia-how-rt-spreads-kremlin-s-propaganda-balkans-despite-eu-sanctions>.
- “Hybrid Threats: Hybrid Threats as a Concept,” European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), accessed January 24, 2026, <https://www.hybridcoe.fi/hybrid-threats/>.
- “NATO 2022 Strategic Concept Adopted by Heads of State and Government at the NATO Summit in Madrid,” NATO, June 29, 2022, <https://www.act.nato.int/wp-content/uploads/2023/05/290622-strategic-concept.pdf>.
- “NATO Allies Join Forces to Enhance the Security of Critical Undersea Infrastructure,” News, NATO, December 10, 2024, <https://www.nato.int/en/news-and-events/articles/news/2024/12/10/nato-allies-join-forces-to-enhance-the-security-of-critical-undersea-infrastructure>.

- "NATO Launches 'Baltic Sentry' to Increase Critical Infrastructure Security," *News Release*, NATO, January 14, 2025, <https://www.nato.int/en/news-and-events/articles/news/2025/01/14/nato-launches-baltic-sentry-to-increase-critical-infrastructure-security>.
- "NATO Says Russian Hybrid Attack Intensify on Members' Territories," *Reuters*, May 2, 2024, <https://www.reuters.com/world/europe/nato-says-russian-hybrid-attack-intensify-members-territories-2024-05-02/>.
- "NATO Stands Up Undersea Infrastructure Coordination Cell," *News*, NATO, February 15, 2023, https://www.nato.int/cps/en/natohq/news_211919.htm.
- "NATO's Approach to Counter Information Threats," NATO, updated February 3, 2025, https://www.nato.int/cps/en/natohq/topics_219728.htm.
- "NATO's Maritime Activities," NATO, updated March 10, 2025, www.nato.int/en/what-we-do/operations-and-missions/natos-maritime-activities.
- "Polish Army to Help Power Grid Protect Key Infrastructure," *Reuters*, December 3, 2025, <https://www.reuters.com/business/aerospace-defense/polish-army-help-power-grid-protect-key-infrastructure-2025-12-03>.
- "Resilience, Civil Preparedness and Article 3," NATO, updated November 13, 2024, <https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3>.
- "Russian Hybrid Operations Very Concerning, Say Romania, Poland and Latvia," *Reuters*, June 11, 2024, <https://www.reuters.com/world/europe/russian-hybrid-operations-very-concerning-say-romania-poland-latvia-2024-06-11/>.
- "Sderzhivanie Strategicheskoe," *Military-Encyclopedic Dictionary Online*, n.d., accessed January 23, 2026, <https://1564.slovaronline.com/10093-сдерживание-стратегическое>. – in Russian
- "Statement by the North Atlantic Council on Recent Russian Hybrid Activities," NATO, May 2, 2024, www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/05/02/statement-by-the-north-atlantic-council-on-recent-russian-hybrid-activities.
- "Strengthening NATO's Eastern Flank," NATO, October 23, 2025, www.nato.int/cps/en/natohq/topics_136388.htm.
- "Terrorist Group Responsible for Arson Attacks across Europe Taken to Court," Eurojust – European Union Agency for Criminal Justice Cooperation, 27 January 2026, <https://www.eurojust.europa.eu/news/terrorist-group-responsible-arson-attacks-across-europe-taken-court>.
- "The NATO Cooperative Cyber Defence Centre of Excellence Is a Multinational and Interdisciplinary Cyber Defence Hub," *NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)*, accessed January 24, 2026, <https://www.ccdcoe.org>.

"Total Defence," Government Offices of Sweden, accessed January 25, 2026, <https://www.government.se/government-policy/total-defence>.

Adamsky, Dmitry, "Deterrence à la Ruse: Its Uniqueness, Sources and Implications," in *NL ARMS Netherlands Annual Review of Military Studies 2020*, ed. Frans Osinga and Tim Sweijs (The Hague: T.M.C. Asser Press, 2021), 161-175, https://doi.org/10.1007/978-94-6265-419-8_9.

Baird, Robert Arthur, "Pyro-Terrorism – The Threat of Arson-Induced Forest Fires as a Future Terrorist Weapon of Mass Destruction," *Studies in Conflict & Terrorism* 29, no. 5 (2006): 415-428, <https://doi.org/10.1080/10576100600698477>.

Bajarūnas, Eitvydas, "The Hybrid Threat Imperative: Deterring Russia Before It Is Too Late," Comprehensive Report (Washington, D.C.: Center for European Policy Analysis, 2025), <https://cepa.org/comprehensive-reports/the-hybrid-threat-imperative-deterring-russia-before-it-is-too-late/>.

Ben-Meir, Alon, "Israel's Pre-Emptive Strategy and Peace," *AlonBen-Meir.com*, February 11, 1989, <https://alonben-meir.com/writing/israels-pre-emptive-strategy-and-peace/>.

Bryjka, Filip, "NATO Members on Guard Against Russian Sabotage," *The Polish Institute of International Affairs (PISM), Bulletin* No. 112 (2420), July 29, 2024, <https://pism.pl/publications/nato-members-on-guard-against-russian-sabotage>.

Bryjka, Filip, and Tomasz Zajac, "EU and NATO Countries Strengthen the Protection of Critical Infrastructure," *Bulletin* No. 79 (2198), PISM, June 22, 2023, <https://www.pism.pl/publications/eu-and-nato-countries-strengthen-the-protection-of-critical-infrastructure>.

Charap, Samuel, "Strategic Sderzhivanie: Understanding Contemporary Russian Approaches to 'Deterrence'," *Security Insights* No. 62 (Garmisch-Partenkirchen: George C. Marshall European Center for Security Studies, September 2020), <https://www.marshallcenter.org/en/publications/security-insights/strategic-sderzhivanie-understanding-contemporary-russian-approaches-deterrence-0>.

Covington, Stephen R., "NATO's Concept for Deterrence and Defence of the Euro-Atlantic Area (DDA)," Belfer Center for Science and International Affairs, Harvard Kennedy School, August 2, 2023, www.belfercenter.org/publication/natos-concept-deterrence-and-defence-euro-atlantic-area-dda.

Dyner, Anna Maria, "Preparing for Russian Hybrid Activities Against NATO and EU Countries," *Bulletin* No. 183 (2100), Polish Institute of International Affairs, November 25, 2022, <https://www.pism.pl/publications/preparing-for-russian-hybrid-activities-against-natoand-eu-countries>.

European Centre of Excellence for Countering Hybrid Threats, *Annual Report 2023*.

European Centre of Excellence for Countering Hybrid Threats, *Annual Report 2022*.

- Fiveable Content Team, "Deterrence," *Fiveable: International Relations*, last updated August 2025, <https://fiveable.me/key-terms/introduction-international-relations/deterrence>.
- Fredholm, Lars, and Anna-Lena Göransson, eds., *Emergency Response Management in Today's Complex Society* (Swedish Civil Contingencies Agency, 2010).
- Freedman, Lawrence, *Deterrence* (Cambridge, MA: Polity Press, 2004).
- Galbusera, Luca, et al., "Game-based Training in Critical Infrastructure Protection and Resilience," *International Journal of Disaster Risk Reduction* 78 (August 2022): 103109, <https://doi.org/10.1016/j.ijdrr.2022.103109>.
- Gerasimov, Valery, "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," *Military Review* (January–February 2016): 23-29, www.armyupress.army.mil/Portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf.
- Giles, Keir, *Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power* (London: Chatham House, 2016), www.chathamhouse.org/sites/default/files/publications/2016-03-russia-new-tools-giles.pdf.
- House of Commons, Defence Committee, "Oral Evidence: Defence in the Grey Zone, HC 50," UK Parliament Committees, April 23, 2024, <https://committees.parliament.uk/oralevidence/14668/html>.
- Insikt Group, "Russian Sabotage Activities Escalate Amid Fraught Tensions," *Research Report, Recorded Future*, November 14, 2024, <https://assets.recordedfuture.com/insikt-report-pdfs/2024/ta-ru-2024-1114.pdf>.
- Izak, Krzysztof, "Terrorist and Sabotage Attacks on Selected Critical Infrastructure Systems – A Historical Perspective," *Terrorism – Studies, Analyses, Prevention*, Special Issue (2025): 71-111, <https://doi.org/10.4467/27204383TER.25.015.21518>.
- Jones, Seth G., "Russia's Shadow War Against the West," CSIS Briefs, Center for Strategic and International Studies, March 18, 2025, www.csis.org/analysis/russias-shadow-war-against-west.
- Kecskemeti, Paul, *Strategic Surrender: The Politics of Victory and Defeat* (Stanford, CA: Stanford University Press, 1958).
- Klimburg, Alexander, ed., *National Cyber Security Framework Manual* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2012), <https://ccdcoe.org/library/publications/national-cyber-security-framework-manual>.
- Kofman, Michael, and Anya Loukianova Fink, "Escalation Management and Nuclear Employment in Russian Military Strategy," *War on the Rocks*, June 23, 2020, <https://warontherocks.com/2020/06/escalation-management-and-nuclear-employment-in-russian-military-strategy/>.

- Lewis, Simon, "US Warns of Russian Effort to Tilt 2024 Elections in Europe against Ukraine," *Reuters*, January 18, 2024, <https://www.reuters.com/world/us-warns-russian-effort-tilt-2024-elections-europe-against-ukraine-2024-01-18/>.
- Mäkinen, Hanna, "Russia's Hybrid Warfare in Europe," *Baltic Rim Economies*, no. 1 (January 2026): 141, www.centrumbalticum.org/files/7113/BRE_1_2026.pdf.
- Mazarr, Michael J., "Understanding Deterrence," *Perspective* no. 295 (Santa Monica, CA: RAND Corporation, 2018), https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf.
- Monaghan, Sean, et al., "NATO's Role in Protecting Critical Undersea Infrastructure," *CSIS Brief*, December 19, 2023, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-12/231219_Monaghan_NATO_CUI.pdf.
- National Protective Security Authority (UK), "Fire as an Act of Sabotage Guidance: Countering the Threat of Sabotage Operations to UK Interests and National Security," last updated September 25, 2024, <https://www.npsa.gov.uk/national-security-act/countering-threat-sabotage-operations-uk-interests-national-security/fire-act-sabotage-guidance>.
- NATO, "Countering terrorism," What We Do, updated August 6, 2025, www.nato.int/en/what-we-do/deterrence-and-defence/countering-terrorism.
- Organization for Security and Co-operation in Europe (OSCE), *Project PROTECT – Technical Guide on Physical Security Considerations for Protecting Critical Infrastructure from Terrorist Attacks* (Vienna: OSCE Secretariat, Transnational Threats Department, October 2025), www.osce.org/sites/default/files/f/documents/e/6/597756_0.pdf.
- Pillai, Helmi, "Protecting Europe's Critical Infrastructure from Russian Hybrid Threats," *Policy Brief*, Centre for European Reform, April 25, 2023, www.cer.eu/publications/archive/policy-brief/2023/protecting-europes-critical-infrastructure-russian-hybrid.
- Reynolds, James C., "Russia Could Be Behind Cyber Attacks on British Businesses like M&S, NATO General Warns," *Independent*, December 4, 2025, www.independent.co.uk/news/world/europe/russia-cyber-attack-marks-and-spencer-nato-b2877844.html.
- Richterova, Daniela, "The Long Shadow of Soviet Sabotage Doctrine?" *War on the Rocks*, August 19, 2024, <https://warontherocks.com/2024/08/the-long-shadow-of-soviet-sabotage-doctrine/>.
- Rovner, Joshua, Rory Cormac, and Lennart Maschmeyer, "Sand in the Gears: Sabotage in World Politics," *European Journal of International Security*, first view (2025), <https://doi.org/10.1017/eis.2025.10025>.
- Schmid, Alex P., "Defining Terrorism," ICCT Report, International Centre for Counter-Terrorism, March 2023, <https://icct.nl/publication/defining-terrorism>.

Singer, Peter W., and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014).

Skomra, Witold, and Karolina Wojtasik, "Critical Infrastructure as a Target for Hybrid Operations: Case Studies of Attacks Against the Facilities and Systems of CI," *Terrorism – Studies, Analyses, Prevention*, Special Issue (2025): 13-34, <https://doi.org/10.4467/27204383TER.25.013.21516>.

Taylor, Joshua, "Effectiveness of SCADA System Security Used Within Critical Infrastructure," *ArXiv*, December 18, 2020, <https://arxiv.org/abs/2012.11375>.

U.S. Commission on Security and Cooperation in Europe, *Spotlight on the Shadow War* (Washington, DC: U.S. Commission on Security and Cooperation in Europe, 2024), www.csce.gov/wp-content/uploads/2024/12/Spotlight-on-the-Shadow-War-Website.pdf.

United Nations Office of Counter-Terrorism and Counter-Terrorism Committee Executive Directorate, *The Protection of Critical Infrastructure Against Terrorist Attacks: Compendium of Good Practices* (New York: United Nations, 2018), https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf.