



Research Article

Where Institutions Intersect: Analyzing Governance Seams in Hybrid Attacks on Critical Maritime Infrastructure

Deniz Kocak

*Helmut Schmidt University / University of the Federal Armed Forces Hamburg,
<https://www.hsu-hh.de/en/startpage>*

Abstract: Hybrid attacks on critical infrastructure pose significant coordination problems for the European Union, NATO, and their member states. This article examines which governance seams come into play in attacks on maritime infrastructure in the Baltic Sea region and how the actors involved respond institutionally. The analytical basis for this article is provided by the hybrid threat model developed by Giannopoulos, Smith, and Theocharidou, which systematizes actors, domains, tools, and escalation phases of hybrid activities. Methodologically, the study follows a case-study approach using congruence analysis, following Blatter and Haverland. The data are drawn from ten coded documentary and analytical sources, including EU Council recommendations, official government statements, NATO documents on underwater infrastructure, and UN Security Council records. The analysis supports all four theoretically derived assumptions: governance seams become salient at the intersections of civil and military responsibilities, national and supranational levels, political rhetoric and operational capacity, and public accountability and intelligence confidentiality. The documented institutional responses primarily address operational aspects without resolving the underlying structural problems. The results indicate that these governance seams are structural in nature and can mutually reinforce each other.

Keywords: hybrid threats, governance interfaces, critical infrastructure, resilience, security policy, gray zone conflict.

Introduction

Hybrid threats against critical infrastructure pose significant coordination problems for the European Union and NATO. The sabotage of the Nord Stream pipelines in September 2022, the damage to the Balticconnector gas pipeline in October 2023, and the alleged severing of undersea cables by the cargo ship Yi Peng 3 in November 2024 illustrate that maritime infrastructure in the Baltic Sea region has repeatedly been the target of attacks, the perpetrators of which have not always been conclusively identified.¹ These incidents raise the question of why institutional responses remain fragmented despite recognizable threat patterns.

Hybrid activities deliberately exploit ambiguity to make attribution difficult and undermine the legitimacy of robust countermeasures.² Fjäder and Schalin further emphasize that legal and institutional deficits characterize the space between war and peace and create organizational gray areas.³ What is missing, however, is a theory-driven, systematic examination of the extent to which documented incidents expose the governance seams that analytical models can derive and whether institutional responses address them.

Governance seams are understood as structural interfaces in the institutional framework where different areas of responsibility intersect and coordination problems can arise in specific incidents. These interfaces emerge along several analytically distinct dimensions: vertically, between national and supranational levels of authority; horizontally, between sectoral domains such as civil protection and military defense; functionally, between political decision-making and operational implementation; and epistemically, between requirements for public transparency and constraints of intelligence confidentiality. Unlike boundaries of responsibility, which denote legal and formal demarcations, or institutional dividing lines, which describe organizational distinctions, governance seams refer specifically to those junctures where coordination failures become likely under conditions of ambiguity or crisis.

¹ Christian Fjäder and Johan Schalin, *Building Resilience to Hybrid Threats: Best Practices in the Nordics*, Hybrid CoE Working Paper 31 (Helsinki: European Centre of Excellence for Countering Hybrid Threats, 2024), 5, <https://www.hybridcoe.fi/wp-content/uploads/2024/05/20240527-Hybrid-CoE-Working-Paper-31-Building-resilience-to-hybrid-threats-WEB.pdf>; Charlie Edwards and Nate Seidenstein, *The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure* (London: International Institute for Strategic Studies, August 2025), <https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure/>, 8-10.

² Armin Krishnan, "Fifth Generation Warfare, Hybrid Warfare, and Gray Zone Conflict: A Comparison," *Journal of Strategic Security* 15, no. 4 (2022): 14-31, 22-23, <https://doi.org/10.5038/1944-0472.15.4.2013>; Chiara Libiseller, "'Hybrid Warfare' as an Academic Fashion," *Journal of Strategic Studies* 46, no. 4 (2023): 858-880, 867, <https://doi.org/10.1080/01402390.2023.2177987>.

³ Fjäder and Schalin, *Building Resilience to Hybrid Threats*, 6.

The article closes the identified research gap by analyzing specific incidents in the Baltic Sea region using the hybrid threat model of Giannopoulos, Smith, and Theocharidou⁴ and examining the suitability of the institutional responses of the European Union, NATO, and affected member states. An institutional response is considered appropriate if it (a) addresses the specific governance seam, (b) creates legally secure options for action, and (c) improves coordination among the actors involved. The analysis uses a case study approach and congruence analysis, following Blatter and Haverland, to assess the extent to which empirical observations align with theoretically derived assumptions.⁵

The underlying theoretical assumption is that governance seams become particularly consequential where boundaries of responsibility intersect. The analysis will therefore examine which specific governance seams can be identified empirically. The article thus combines conceptual insights from the research literature with an empirical investigation of governance seams that arise at interfaces between national and supranational, civil and military, and sectoral responsibilities.

The article is structured as follows: First, the state of the art discusses the relevant literature on hybrid threats and governance challenges. Next, it presents the theoretical framework, introducing the hybrid threat model as an analytical basis. The methodology section explains the case-study approach and data sources. The analysis then examines the empirical findings, and the conclusion summarizes the results and discusses their implications for critical infrastructure governance.

State of the Art: Hybrid Threats and Governance Challenges

The question of which governance seams become apparent in hybrid attacks on critical infrastructure touches on several strands of research on conceptualizing hybrid threats, the challenges of state responses, and the buildup of resilience. The following discussion organizes the relevant literature according to an analytical principle: it first distinguishes between works that conceptualize the phenomenon of hybrid threats, then those that identify specific obstacles to response, and finally those that analyze institutional counterstrategies and concepts of resilience.

The Gray Zone as an Analytical Category

Research on hybrid threats and gray zone conflicts has done a great deal to clarify the terminology in recent years. There is broad consensus that the gray zone refers to a space for action that lies below the threshold of open warfare and in

⁴ Georgios Giannopoulos, Hanna Smith, and Maranthi Theocharidou, *The Landscape of Hybrid Threats: A Conceptual Model*, EUR 30585 EN (Luxembourg: Publications Office of the European Union, 2021), 11, <https://doi.org/10.2760/44985>.

⁵ Joachim Blatter and Markus Haverland, *Designing Case Studies: Explanatory Approaches in Small-N Research* (Basingstoke: Palgrave Macmillan, 2014).

which actors pursue political goals through a combination of military and non-military means.⁶ However, Edwards and Seidenstein criticize the fact that, in European contexts, the term often functions as a bureaucratic shield that tends to obscure rather than clarify responsibilities and to hinder rather than promote decisive action.⁷ Hybrid threats are understood in the literature as the coordinated use of diverse means below clear attribution thresholds, aimed at exploiting systemic vulnerabilities and cumulatively undermining the target's ability to act.⁸ The literature largely agrees that ambiguity should be understood not as a side effect but as a core strategic element of hybrid attacks. Several scholars⁹ converge on the view that this ambiguity serves multiple strategic functions: it complicates the legitimization of countermeasures, slows collective decision-making, and deprives targeted states of the political and legal justification for robust responses.

Structural Barriers to Response: Attribution, Responsibility, and Threshold Issues

Another aspect concerns the obstacles that hinder government responses to hybrid threats. Fjäder and Schalin identify the interaction between the concealment and difficult detection of hybrid activities and legal and institutional deficits in the gray zone.¹⁰ Added to this is conceptual inconsistency, which makes joint situation assessments difficult. These findings align with Rusinaitė's observation that fragmentation due to departmental silos prevents early, integrated planning.¹¹

Edwards and Seidenstein¹² point out that legal deficits, attribution uncertainty, and political reluctance hinder a consistent response and discourage public attribution. In addition, outdated, underinvested, and highly interconnected

⁶ Andrew Mumford and Pascal Carlucci, "Hybrid Warfare: The Continuation of Ambiguity by Other Means," *European Journal of International Security* 8, no. 2 (2023): 192-206, <https://doi.org/10.1017/eis.2022.19>.

⁷ Edwards and Seidenstein, *The Scale of Russian Sabotage Operations*, 4-5.

⁸ Viktorija Rusinaitė, *Turning Strategy into Praxis: Lessons in Hybrid Threat Deterrence*, Hybrid CoE Paper 25 (Helsinki: European Centre of Excellence for Countering Hybrid Threats, August 2025), 20 pp., 8-9, <https://www.hybridcoe.fi/wp-content/uploads/2025/08/Hybrid-CoE-Paper-25-Turning-strategy-into-praxis-web.pdf>.

⁹ Niklas Nilsson et al., "Security Challenges in the Grey Zone: Hybrid Threats and Hybrid Warfare," in *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*, ed. Mikael Weissmann et al. (London: I. B. Tauris, 2021), 1-18, 2-3, <https://doi.org/10.5040/9781788317795.0005>; Krishnan, "Fifth Generation Warfare, Hybrid Warfare, and Gray Zone Conflict," 22-23; Libiseller, "'Hybrid Warfare' as an Academic Fashion," 867.

¹⁰ Fjäder and Schalin, *Building Resilience to Hybrid Threats*, 6, 8f.

¹¹ Rusinaitė, *Turning Strategy into Praxis: Lessons in Hybrid Threat Deterrence*, 11-12.

¹² Edwards and Seidenstein, *The Scale of Russian Sabotage Operations*, 5, 12-13.

infrastructure increases systemic vulnerability, with cascading effects across borders.¹³ The literature thus identifies a structural dilemma: the deliberate blurring of the boundaries between war and peace obscures responsibilities and decision-making processes, while democratic systems are limited in their response options by constitutional constraints.¹⁴ Kähkö ¹⁵ also warns against a passive status quo logic among Western actors, who see gray zone activities primarily as something that others engage in, while they themselves can only react and protect themselves.

Resilience as an Institutional Response

Given the obstacles to response described above, resilience has become a guiding concept for dealing with hybrid threats. Bourbeau understands resilience as a process of exemplary adaptations aimed at preserving, slightly modifying, or fundamentally transforming a reference object.¹⁶ In terms of security policy, de Coning describes resilience as the ability of society to ward off, cope with, and recover from hybrid attacks without losing fundamental values, social cohesion, and collective identity.¹⁷ Jungwirth and colleagues¹⁸ further develop this perspective and regard resilience as a systemic capacity to ward off hybrid threats through coordinated protection, adaptation, and recovery capabilities across all social subsystems, with explicit consideration given to interdependencies.

However, the literature makes it clear that resilience alone is not sufficient and is associated with considerable implementation challenges. Rusinaitė ¹⁹ argues that a one-sided focus on resilience can appear weak to the outside world and undermine deterrence. De Coning emphasizes that the fundamental unpredictability of social systems complicates linear crisis planning and renders classic top-down control models largely ineffective in hybrid situations.²⁰ At the operational level, the heterogeneity of national regulations, the high proportion of critical infrastructure in private hands, and investment backlogs also hinder the

¹³ Ondřej Filipec, "Multilevel Analysis of the 2021 Poland-Belarus Border Crisis in the Context of Hybrid Threats," *Central European Journal of Politics* 8, no. 1 (2022): 1-18, 12, https://doi.org/10.24132/cejop_2022_1.

¹⁴ Nilsson et al., "Security Challenges in the Grey Zone," 2.

¹⁵ Ilmari Kähkö, "The Evolution of Hybrid Warfare: Implications for Strategy and the Military Profession," *Parameters* 51, no. 3 (2021): 116-127, 118-119, <https://doi.org/10.5540/0031-1723.3084>.

¹⁶ Philippe Bourbeau, *On Resilience: Genealogy, Logics, and World Politics* (Cambridge: Cambridge University Press, 2018), 13.

¹⁷ Cedric de Coning, *Strengthening the Resilience and Adaptive Capacity of Societies at Risk from Hybrid Threats*, Hybrid CoE Working Paper 9 (Helsinki: European Centre of Excellence for Countering Hybrid Threats, 2021), 17.

¹⁸ Rainer Jungwirth et al., *Hybrid Threats: A Comprehensive Resilience Ecosystem — Executive Summary*, EUR 31104 EN (Luxembourg: Publications Office of the European Union, 2023), <https://doi.org/10.2760/37899>, 5.

¹⁹ Rusinaitė, *Turning Strategy into Praxis: Lessons in Hybrid Threat Deterrence*, 15-16.

²⁰ de Coning, *Strengthening the Resilience and Adaptive Capacity*, 15-16.

achievement of a uniform level of resilience.²¹ Angstrom and Ljungkvist add that the privatization and fragmentation of critical services complicate government control and lead to a diffusion of responsibility.²² Effective strategies therefore require a combination of denial through hardening and cost imposition through sanctions.²³

Institutional Countermeasures

Research documents a variety of institutional responses to hybrid threats. Nilsson and colleagues outline the establishment of specialized institutions such as the NATO StratCom Centre of Excellence in Riga and the European Centre of Excellence for Countering Hybrid Threats in Helsinki.²⁴ Edwards and Seidenstein point to maritime initiatives such as Baltic Sentry and NorthSeal, as well as legal measures such as the British National Security Act.²⁵

At the national level, different approaches can be observed, but they all share common coordination problems. Sweden, for example, has been pursuing a decentralized model since 2014, in which every authority and, ultimately, every citizen is expected to be constantly prepared to avert hybrid attacks.²⁶ This decentralization is a response to the realization that hybrid threats affect different levels simultaneously and would overwhelm a purely centralized command center.²⁷ The Nordic countries as a whole have established specialized agencies for psychological defense and screening mechanisms for foreign direct investment.²⁸ However, such national efforts reach their limits when hybrid attacks affect cross-border infrastructure. To close these coordination gaps, Jungwirth and colleagues propose a hybrid toolbox at the EU level that bundles operational, diplomatic, legal, and military instruments and makes them readily available.²⁹

Research Gap and Positioning of the Article

The above discussion has revealed that, although conceptual foundations and significant obstacles to response have been identified in the literature, there is no systematic empirical investigation of specific governance seams. This article

²¹ Edwards and Seidenstein, *The Scale of Russian Sabotage Operations*, 7-8.

²² Jan Angstrom and Kristin Ljungkvist, "Unpacking the Varying Strategic Logics of Total Defence," *Journal of Strategic Studies* 47, no. 4 (2024): 498-522, 21, <https://doi.org/10.1080/01402390.2023.2260958>.

²³ Rusinaitė, *Turning Strategy into Praxis: Lessons in Hybrid Threat Deterrence*, 9-10.

²⁴ Nilsson et al., "Security Challenges in the Grey Zone," 6.

²⁵ Edwards and Seidenstein, *The Scale of Russian Sabotage Operations*, 10-12.

²⁶ Angstrom and Ljungkvist, "Unpacking the Varying Strategic Logics of Total Defence," 19.

²⁷ Angstrom and Ljungkvist, "Unpacking the Varying Strategic Logics of Total Defence," 11.

²⁸ Fjäder and Schalin, *Building Resilience to Hybrid Threats*, 12-13, 15-17.

²⁹ Jungwirth et al., *Hybrid Threats: A Comprehensive Resilience Ecosystem*, 10.

addresses this gap by examining specific incidents in the Baltic Sea region using the hybrid threat model developed by Giannopoulos, Smith, and Theocharidou and assessing the suitability of the corresponding institutional responses. This analytical approach is operationalized in the following theoretical section using the hybrid threat model.

Theoretical Framework

The analysis of hybrid threats to critical infrastructure requires a conceptual framework that captures the heterogeneity of the actor landscape and maps institutional response patterns. The analytical basis is provided by the hybrid threat model developed by Giannopoulos, Smith, and Theocharidou,³⁰ which identifies four pillars: actors and their strategic goals, domains as targets of attack, tools of influence, and phases of escalation.

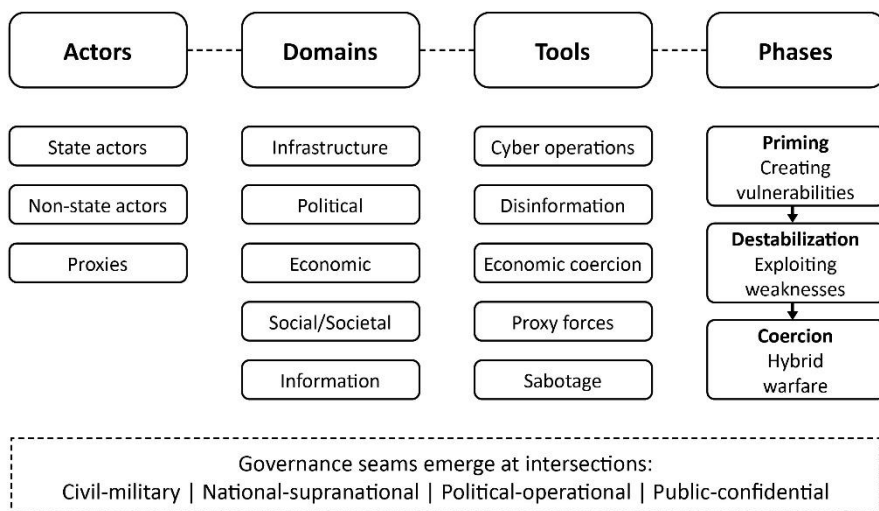


Figure 1: Hybrid Threat Model (adapted from Giannopoulos et al., 2021).

This model is suitable for investigating the governance seams defined at the outset for two main reasons. First, it enables the systematic identification of vulnerabilities that arise at the interfaces between different areas of responsibility. The model identifies typical points of attack in democratic societies, such as the interfaces between civil and military responsibilities or between different legal

³⁰ Giannopoulos, Smith, and Theocharidou, *The Landscape of Hybrid Threats*, 11.

frameworks.³¹ Maritime infrastructure such as submarine cables and pipelines falls into this category, as it crosses national borders and is subject to different levels of regulation.

Second, the model provides an analytical approach to the phases of hybrid operations. The distinction between priming, destabilization, and coercion through hybrid warfare illustrates that visible attacks usually follow long-term preparatory phases.³² For governance analysis, this means that institutional responses must be tailored not only to acute incidents but also to preceding activities. The priming phase aims to create or exploit vulnerabilities without crossing the threshold of detectability.³³

The infrastructure sector holds a significant position in the model. It is described as a mega-domain that encompasses multiple sectors and can therefore be divided into subdomains.³⁴ Attacks can target the degradation of services, the destruction of key components, increases in operating costs, or the creation of unilateral dependencies. This categorization thus allows for the precise classification of specific incidents in the Baltic Sea region.

Theoretically supported assumptions can be derived from the hybrid threat model and tested through congruence analysis. These assumptions are subjected to a systematic congruence test in the analysis section. The hybrid threat model describes democratic societies as vulnerable at the interfaces between different areas of responsibility.³⁵ For the purposes of this study, these interfaces can be operationalized along four core dimensions of institutional differentiation: civil and military responsibilities, national and supranational levels, political rhetoric and operational capacity, and public and confidential information flows. This operationalization gives rise to the following assumptions:

Assumption 1 (A1): Attacks on cross-border maritime infrastructure reveal coordination problems at the governance seam between civil and military responsibilities. Civil infrastructure of strategic importance triggers both civil protection mechanisms and military response capabilities, whose interaction is hampered by institutional divisions.

Assumption 2 (A2): Incidents affecting multiple national jurisdictions or international waters highlight governance seams at the interface between national and supranational responsibilities. The legal framework, in particular the UN Convention on the Law of the Sea, limits the scope for intervention by coastal states in exclusive economic zones and creates enforcement deficits.

Assumption 3 (A3): In the case of hybrid attacks whose attribution remains legally uncertain, the governance seam between political rhetoric and operational capacity becomes salient (for brevity, below this is often referred to as

³¹ Giannopoulos, Smith, and Theocharidou, *The Landscape of Hybrid Threats*, 10-11.

³² Giannopoulos, Smith, and Theocharidou, *The Landscape of Hybrid Threats*, 36-41.

³³ Giannopoulos, Smith, and Theocharidou, *The Landscape of Hybrid Threats*, 37.

³⁴ Giannopoulos, Smith, and Theocharidou, *The Landscape of Hybrid Threats*, 27-28.

³⁵ Giannopoulos, Smith, and Theocharidou, *The Landscape of Hybrid Threats*, 10-11.

“attribution uncertainty”). Political condemnations are made without legally certain attribution, which limits the legitimacy of countermeasures.

Assumption 4 (A4): The exchange of information in hybrid incidents is hampered by the governance seam between public accountability and intelligence confidentiality. Operational requirements for secrecy conflict with the democratic legitimacy of countermeasures.

Beyond individual assumptions, the hybrid threat model suggests these governance seams do not occur in isolation and can reinforce one another in specific incidents.³⁶ For example, attribution uncertainty (A3) can complicate public communication (A4), while jurisdictional fragmentation (A2) can further complicate civil-military coordination (A1).

However, the model also has limitations that warrant acknowledgment. It was developed primarily as a descriptive framework for EU institutions and may therefore emphasize European governance structures over alternative analytical perspectives. Moreover, the model’s focus on institutional interfaces may underestimate the role of informal coordination mechanisms, individual agency, and adaptive practices that can mitigate governance seams in practice. The model also does not provide criteria for weighting the relative importance of different governance seams or predicting which seams will prove most consequential in specific incidents. Despite these limitations, the model provides analytical utility in identifying potential coordination problems.

The congruence analysis examines the extent to which these expectations are empirically supported. The responsiveness of European institutions depends on how well these governance seams can be bridged through coordinated mechanisms. The hybrid threat model makes it possible to identify the attack vectors and assess the adequacy of institutional responses.³⁷ For the empirical analysis, this means that specific incidents in the Baltic Sea region are examined along the four pillars of the model. Identifying the actors involved, the domains attacked, the tools used, and the respective phase enables a structured assessment of the governance seams that became apparent and the institutional countermeasures.

Methodology

This research follows a case study-based approach that aims to identify causal mechanisms and generate theory-based findings. According to Gerring,³⁸ case studies enable researchers to prioritize internal validity and to trace causal relationships within a small number of cases. The gain in knowledge lies less in the breadth of generalization than in the depth of understanding of specific causal

³⁶ Giannopoulos, Smith, and Theocharidou, *The Landscape of Hybrid Threats*, 14.

³⁷ Giannopoulos, Smith, and Theocharidou, *The Landscape of Hybrid Threats*.

³⁸ John Gerring, *Case Study Research: Principles and Practices* (Cambridge: Cambridge University Press, 2007), 37-38.

relationships. This methodological orientation aligns with the research question: which governance seams become apparent in hybrid attacks on Baltic Sea infrastructure, and how do European institutions respond to them? The present case study makes it possible to capture precisely these interactions, which would not be possible in the same way through a quantitative cross-sectoral analysis.

The analytical method used is congruence analysis, as described by Blatter and Haverland.³⁹ This method examines the extent to which empirical observations correspond to theoretically derived assumptions. In contrast to covariance-based designs, the focus is not on variation across many cases but on comparing theory and empirical evidence within selected cases.⁴⁰ One advantage of congruence analysis is that it enables a theory-driven structuring of the empirical material without reducing the multidimensionality of the phenomena under investigation. The hybrid threat model provides the theoretical assumptions regarding the domains, tools, and phases of hybrid activities.⁴¹ Congruence analysis allows the empirical findings to be assessed for their fit with these theoretical categories and identifies governance seams at the interfaces between different areas of responsibility.

Case selection is based on theoretical relevance. The focus is on incidents and institutional responses in the Baltic Sea region that affect critical infrastructure such as submarine cables and pipelines. The study period covers 2021–2025, thus encompassing a phase of increased hybrid activities in Europe as well as institutional adaptation processes at the European level.

The analysis is based on ten coded sources of various types (see Table 1). These include policy documents from the European Union and NATO, official statements from national governments and infrastructure operators, analyses from the Hybrid Centre of Excellence, and record from meetings of the UN Security Council.

The selection of sources follows the principle of triangulation in order to capture different institutional perspectives on the same events. The heterogeneity of the source types enables a multi-perspective analysis of events and institutional reactions. A structured coding table was developed for the evaluation. For each source, the table records the observed activity, the domains affected according to the categorization by Giannopoulos, Smith, and Theocharidou,⁴² the tools used or implied, the phase in the hybrid activity spectrum, and the attribution status. Table 1 summarizes the key coding results. Visible governance seams form a core analytical category and are coded along the dimensions of civil-military, national-international, political-operational, and public-secret. These cate-

³⁹ Blatter and Haverland, *Designing Case Studies: Explanatory Approaches in Small-N Research*.

⁴⁰ Blatter and Haverland, *Designing Case Studies: Explanatory Approaches in Small-N Research*, 144–145.

⁴¹ Giannopoulos, Smith, and Theocharidou, *The Landscape of Hybrid Threats*, 11.

⁴² Giannopoulos, Smith, and Theocharidou, *The Landscape of Hybrid Threats*, 27–28.

Table 1. Overview of Coded Sources with Assignment to Theoretical Assumptions (A1–A4).

No.	Source	Document Type	Date	Assumptions
1	EU Council 2022	EU Council Recommendation	Dec. 8, 2022	A1, A2, A3, A4
2	Fingrid EstLink2	Company statement	Dec. 25, 2024	A2
3	Finland GovCom 2023	Government press release	Oct. 10, 2023	A1, A2, A4
4	Giannopoulos et al. 2021	JRC research report	2021	(Theory)
5	Kalm 2024	policy analysis	May 29, 2024	A2, A3, A4
6	NATO CUIIN 2024	NATO press release	May 23, 2024	A1, A2
7	Praks 2024	policy analysis	2024	A1, A2, A3
8	Sari 2025	policy analysis	2025	A2, A3
9	Savitz 2024	policy analysis	2024	A1, A3
10	UNSC 15243	UN Security Council	March 27, 2023	A2, A3, A4

A1: Governance seam between civil and military responsibilities

A2: Governance seam between national and supranational responsibilities

A3: Governance seam between political rhetoric and operational capacity

A4: Governance seam between public accountability and intelligence confidentiality

gories are derived directly from the theoretical framework and operationalize the concept of governance seams.

The data quality is subject to several limitations. First, intelligence findings and operational details are not accessible for reasons of confidentiality. The analysis is therefore based on publicly available sources and is necessarily limited by this perspective. Second, distortions arising from the institutional positioning of the sources cannot be ruled out, which is why the statements of various actors are systematically compared. The results therefore do not claim to provide conclusive causal explanations but aim to identify recurring patterns in critical infrastructure governance.

Analysis

The aim of this section is to use the coded sources to empirically verify the governance seams defined at the outset. The analysis follows the logic of congruence analysis by systematically comparing the four theoretically derived assumptions (A1 to A4) with the empirical findings. The evaluation of the ten sources

makes it possible to identify recurring patterns in institutional responses and those areas in which questions of responsibility manifest themselves as coordination problems.

Empirical Findings: Incidents and Affected Domains

The coded sources document a series of incidents affecting the maritime infrastructure in the Baltic Sea region. In September 2022, underwater explosions destroyed three of the four Nord Stream pipelines in the exclusive economic zones of Sweden and Denmark. In March 2023, the UN Security Council reported that preliminary information from European authorities pointed to an act of sabotage with the possible involvement of a state actor.⁴³ One year later, on October 8, 2023, a leak was detected in the Balticconnector gas pipeline. The Finnish government announced that the damage had been localized in Finland's exclusive economic zone.⁴⁴ According to expert estimates, the damage could not have been caused by normal gas transmission operations. At the same time, disruptions to telecommunications cables were detected.⁴⁵ In November 2024, the Chinese cargo ship *Yi Peng 3* left the Russian port of Ust-Luga and, presumably by dragging its anchor, severed two submarine cables in Swedish and Danish waters over a distance of about 100 miles.⁴⁶

Analysis of the domains affected reveals a consistent pattern. All incidents primarily concern the infrastructure domain, with energy and communications infrastructure appearing to be particularly vulnerable targets. These infrastructures are described as a mega-domain in the hybrid threat model.⁴⁷ The incidents also regularly involve other domains: the political domain is engaged through government statements, the legal domain through investigations in several jurisdictions, and the diplomatic domain through international consultations. The

⁴³ United Nations, "Security Council Rejects Draft Resolution Establishing Commission to Investigate Sabotage of Nord Stream Pipeline," 9295th Meeting, SC/15243, UN Meetings Coverage and Press Releases, March 27, 2023, accessed December 16, 2025, <https://press.un.org/en/2023/sc15243.doc.htm>.

⁴⁴ Finnish Government, "Location of Leak in Balticconnector Gas Pipeline Identified in Finland's Economic Zone," press release, Ministry of Economic Affairs and Employment, Prime Minister's Office, October 10, 2023, accessed December 16, 2025, <https://valtioneuvosto.fi/en/-/10616/location-of-leak-in-balticconnector-gas-pipeline-identified-in-finland-s-economic-zone>.

⁴⁵ Henrik Praks, *Russia's Hybrid Threat Tactics against the Baltic Sea Region: From Disinformation to Sabotage*, Hybrid CoE Working Paper 32 (Helsinki: European Centre of Excellence for Countering Hybrid Threats, May 2024), 21, www.hybridcoe.fi/wp-content/uploads/2024/05/20240530-Hybrid-CoE-Working-Paper-32-Russias-hybrid-threat-tactics-WEB.pdf.

⁴⁶ Aurel Sari, *Protecting Maritime Infrastructure from Hybrid Threats: Legal Options*, Hybrid CoE Research Report 14 (Helsinki: European Centre of Excellence for Countering Hybrid Threats, March 2025), 27-29, www.hybridcoe.fi/wp-content/uploads/2025/03/20250306-Hybrid-CoE-Research-Report-14-web.pdf.

⁴⁷ Giannopoulos, Smith, and Theocharidou, *The Landscape of Hybrid Threats*, 27-28.

European Union Council Recommendation of December 2022 illustrates this interdependence.⁴⁸ In addition to infrastructure damage, the sources also document upstream activities.

The so-called Airiston Helmi case concerns the systematic acquisition of real estate by Russian citizens on strategically significant Finnish islands near Turku between 2007 and 2018. The acquired properties were located in close proximity to major shipping routes and military facilities. Finnish authorities launched an investigation in 2018 after indications of suspicious activity emerged, including extensive construction work and unusual visitor patterns.⁴⁹ This case illustrates the priming phase of hybrid operations as defined by the model proposed by Giannopoulos, Smith, and Theocharidou, since the aim was not immediate destabilization but rather the establishment of long-term access and options for action. Such activities aim to create vulnerabilities or map existing weaknesses without crossing the threshold of detection. The case thus differs categorically from infrastructure attacks, yet demonstrates that hybrid threats do not begin with visible damage but are often preceded by years of preparatory actions.⁵⁰

Congruence Test: Theoretical Assumptions

In the following, the four theoretically derived assumptions are compared with the empirical findings. The structure follows the approach recommended by Blatter and Haverland,⁵¹ in which theoretical assumptions are explicitly compared with observed patterns. The aim is to examine whether and how governance seams cause coordination problems in specific incidents.

On the Governance Seam between Civil and Military Responsibilities (A1)

The first assumption postulated that attacks on cross-border maritime infrastructure create coordination problems due to the governance seam between civil and military responsibilities. The empirical findings support this assumption.

The EU Council Recommendation⁵² of December 2022 explicitly emphasizes that cooperation between the European Union and NATO must fully respect the competences set out in the treaties. This wording refers to the governance seam itself, making clear that cooperation should take place only while maintaining existing institutional divisions. The governance seam therefore remains, even though the need for coordination is recognized. The practical dimension of this governance seam became apparent during the Balticconnector investigations:

⁴⁸ Council of the European Union, *Council Recommendation of 8 December 2022 on a Union-wide Coordinated Approach to Strengthen the Resilience of Critical Infrastructure*, 2023/C 20/01 (Brussels: European Union, 2023), para. 3, para. 37, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj%3AJOC_2023_020_R_0001.

⁴⁹ Praks, *Russia's Hybrid Threat Tactics against the Baltic Sea Region*, 21-22.

⁵⁰ Giannopoulos, Smith, and Theocharidou, *The Landscape of Hybrid Threats*, 31-32.

⁵¹ Blatter and Haverland, *Designing Case Studies: Explanatory Approaches in Small-N Research*, 165-167.

⁵² Council of the European Union, *Council Recommendation*, 2023/C 20/01, para. 37.

the Finnish Border Guard, as a paramilitary organization, supported the civilian investigative authority, while the Estonian Navy was also involved.⁵³ NATO responded to the series of incidents by increasing naval patrols and establishing a Maritime Center for Security of Critical Undersea Infrastructure.⁵⁴ Military resources were thus used to protect civilian infrastructure without the boundaries of responsibility being conclusively clarified. The involvement of multiple authorities in the EstLink 2 incident in December 2024 also showed overlap between civil and security interests in investigating the cable damage.⁵⁵ The governance seam as a structural feature persists, with coordination problems arising on a situational basis. Within the documented incidents, congruence is high, though the representativeness of these patterns for other infrastructure types or regions remains to be established.

On the Governance Seam between National and Supranational Responsibilities (A2)

The second assumption was that incidents occurring in multiple national jurisdictions or international waters would cause coordination problems due to the governance seam between national and supranational responsibilities. This expectation has also been strongly supported by the empirical evidence. The EU Council Recommendation explicitly addresses infrastructure outside the territory of Member States.⁵⁶ The UN Convention on the Law of the Sea significantly restricts the rights of coastal states to intervene in exclusive economic zones, resulting in an enforcement deficit.⁵⁷ This deficit forms the structural basis of the governance seam. The coordination problems become apparent in specific incidents.

In the Balticconnector investigations, it first had to be clarified whether Finnish or Estonian authorities were responsible, as the incident affected different exclusive economic zones.⁵⁸ The EstLink 2 incident also illustrates this dimension: the power transmission connection links Finland and Estonia, meaning that the cross-border infrastructure required coordination between the authorities of both countries and the grid operators Fingrid and Elering.⁵⁹ The UN Security

⁵³ Finnish Government, "Location of Leak in Balticconnector Gas Pipeline."

⁵⁴ NATO, "NATO Holds First Meeting of Critical Undersea Infrastructure Network," May 23, 2024, accessed December 16, 2025, <https://www.nato.int/en/news-and-events/articles/news/2024/05/23/nato-holds-first-meeting-of-critical-undersea-infrastructure-network>.

⁵⁵ Fingrid, "Fault in the EstLink 2 Electricity Transmission Connection Between Finland and Estonia Located in the Submarine Cable," press release, December 26, 2024, accessed December 16, 2025, <https://www.fingrid.fi/en/news/news/2024/fault-in-the-estlink-2-electricity-transmission-connection-between-finland-and-estonia-located-in-the-submarine-cable/>.

⁵⁶ Council of the European Union, *Council Recommendation*, 2023/C 20/01, para. 3.

⁵⁷ Sari, *Protecting Maritime Infrastructure from Hybrid Threats*, 27-32.

⁵⁸ Finnish Government, "Location of Leak in Balticconnector Gas Pipeline."

⁵⁹ Fingrid, "Fault in the EstLink 2 Electricity Transmission Connection."

Council meeting in March 2023 highlights this governance seam particularly clearly: the Russian draft resolution to establish an international commission of inquiry failed due to twelve abstentions, while parallel national investigations were underway in Denmark, Germany, and Sweden.⁶⁰ This process reveals the conflict between the international demand for clarification and the primacy of national investigations. The governance seam creates concrete coordination problems in the form of conflicting investigative claims. For the examined incidents, congruence is high. Whether these coordination challenges reflect enduring structural features or context-specific circumstances warrants further investigation.

On the Governance Seam between Political Rhetoric and Operational Capacity (A3)

The third assumption was that the deliberate ambiguity of hybrid attacks triggers a coordination problem at the governance seam between political rhetoric and operational capacity, manifesting as a sequence of condemnation and sanctioning. The empirical findings clearly support this assumption.

The EU Council Recommendation is a non-binding political instrument that proposes concrete operational measures.⁶¹ The discrepancy between political rhetoric and actual options for action is particularly evident in attribution. The European Council strongly condemned the Nord Stream sabotage and announced a unified and determined response.⁶² At the same time, no public attribution to a specific actor was made. This restraint reflects the operational difficulty of attributing hybrid activities with legal certainty. Savitz describes how, in cases of infrastructure damage, it is often difficult to provide evidence and how attackers can invoke plausible deniability.⁶³ In the Balticconnector incident, however, experts largely agree that the prolonged anchor dragging could not have been accidental.⁶⁴ Nevertheless, no legally conclusive attribution to a state actor had been made by the time this analysis was completed. The governance seam between the political will to act and the legally secure capacity to act thus creates ongoing coordination problems. Congruence is high for the incidents under review, though the extent to which classified processes may mitigate the publicly visible gap cannot be assessed.

⁶⁰ United Nations, "Security Council Rejects Draft Resolution," SC/15243.

⁶¹ Council of the European Union, *Council Recommendation*, 2023/C 20/01, para. 2.

⁶² Council of the European Union, *Council Recommendation*, 2023/C 20/01, para. 4.

⁶³ Scott Savitz, *Uncrewed Maritime Vessels: Shaping Naval Power in Hybrid Threat Operations*, Hybrid CoE Working Paper 34 (Helsinki: European Centre of Excellence for Countering Hybrid Threats, 2024), 15, www.hybridcoe.fi/wp-content/uploads/2024/10/20241007-Hybrid-CoE-Working-Paper-34-Uncrewed-maritime-vessels-WEB.pdf.

⁶⁴ Praks, *Russia's Hybrid Threat Tactics against the Baltic Sea Region*, 21, footnote 60.

On the Governance Seam between Public Accountability and Intelligence Confidentiality (A4)

The fourth assumption postulated that information sharing in hybrid incidents is hampered by the governance seam between public accountability and intelligence confidentiality. This governance seam creates coordination problems arising from the tension between transparency requirements and secrecy interests.

An EU Council Recommendation stresses that no Member State is required to share information that could be detrimental to its national security interests.⁶⁵ At the same time, it calls for increased information sharing. This inconsistency highlights the governance seam.

In the Yi Peng 3 case, China conducted investigations aboard the ship behind closed doors.⁶⁶ In the Nord Stream investigations, neither Sweden nor Denmark publicly announced any suspects before Sweden closed its investigation.⁶⁷ This secrecy may have operational reasons, but it makes public accountability difficult and undermines the legitimacy of applying certain countermeasures.

After the Balticconnector incident, the Finnish authorities were in close contact with allies and partners.⁶⁸ At the same time, details concerning the status of the investigation and potential suspects were not communicated publicly. The information provided on the EstLink 2 incident was also limited to stating that the authorities were investigating the sequence of events, without revealing any details about suspicions or progress in the investigation.⁶⁹ These parallel flows of information show how the governance seam creates concrete coordination problems between confidential and public channels. The coordination problem manifests itself in the difficulty of establishing democratic legitimacy for countermeasures when secrecy prevents public disclosure of evidence. Political decision-makers face the dilemma of either acting without public justification or refraining from action until public disclosure is possible. Congruence is high within the scope of this analysis, though distinguishing hybrid-specific governance deficits from challenges inherent in any sensitive investigation requires comparative research.

Summary of the Congruence Test

The congruence test supports all four assumptions for the examined incidents. The findings demonstrate the analytical utility of the framework for cross-border maritime infrastructure, though generalization to other infrastructure types or

⁶⁵ Council of the European Union, *Council Recommendation*, 2023/C 20/01, para. 2.

⁶⁶ Sari, *Protecting Maritime Infrastructure from Hybrid Threats*, 29.

⁶⁷ Helga Kalm, "NATO's Path to Securing Undersea Infrastructure in the Baltic Sea," Carnegie Endowment for International Peace, May 29, 2024, accessed December 16, 2025, <https://carnegieendowment.org/research/2024/05/nato-baltic-sea-security-nord-stream-balticconnector>.

⁶⁸ Finnish Government, "Location of Leak in Balticconnector Gas Pipeline."

⁶⁹ Fingrid, "Fault in the EstLink 2 Electricity Transmission Connection."

geographical contexts requires additional empirical investigation. It is noteworthy that the governance seams do not occur in isolation but reinforce each other: attribution uncertainty (A3) hinders public communication (A4), while jurisdictional fragmentation (A2) further complicates civil-military coordination (A1). This interdependence of governance seams was theoretically expected and has been empirically supported.

The documented institutional responses can be divided into three categories. First, new coordination structures were created: in May 2024, NATO established the Critical Undersea Infrastructure Network and a Maritime Centre within NATO Maritime Command.⁷⁰ Industry, including energy operators, was integrated into these structures. Second, the affected states intensified their cooperation in investigations and increased maritime surveillance. Finland and Estonia strengthened their regulatory cooperation immediately after the Balticconnector incident.⁷¹ Third, legal frameworks have been adapted: the EU Council Recommendation refers to the Critical Entities Resilience (CER) Directive, the Network and Information Security (NIS2) Directive, and the Digital Operational Resilience Act (DORA) as tools to strengthen resilience.⁷² These three instruments address different governance interfaces. The CER Directive requires Member States to identify critical infrastructure and develop national resilience strategies, thereby establishing uniform minimum standards for physical security. The NIS2 Directive extends cybersecurity regulations to additional sectors and introduces stricter reporting requirements. It thereby formalizes the information exchange between private operators and government agencies. DORA focuses on the digital resilience of the financial sector. However, all three instruments operate within existing jurisdictional boundaries and do not fundamentally alter the structural governance interfaces themselves.

The suitability of these responses can be assessed using the criteria defined at the outset. With regard to addressing specific governance seams (a), the new NATO structures show operational improvements without, however, modifying the structural dividing lines themselves. With regard to legally secure options for action (b), the enforcement deficit in exclusive economic zones remains.⁷³ The Maritime Center has improved coordination among the actors involved (c), but fundamental questions of responsibility remain unresolved. Political condemnations are regularly issued without attribution, which limits their deterrent effect. NATO Secretary General Stoltenberg has stated that Russia is waging an intensifying hybrid campaign against the Allies.⁷⁴ However, attributing individual incidents to state actors remains legally uncertain. The governance seam between

⁷⁰ NATO, "NATO Holds First Meeting of Critical Undersea Infrastructure Network."

⁷¹ Finnish Government, "Location of Leak in Balticconnector Gas Pipeline."

⁷² Council of the European Union, *Council Recommendation*, 2023/C 20/01, para. 6-7.

⁷³ Sari, *Protecting Maritime Infrastructure from Hybrid Threats*, 27-32.

⁷⁴ NATO, "NATO Holds First Meeting of Critical Undersea Infrastructure Network."

political rhetoric and the legally secure capacity to act thus persists and continues to create coordination problems.

Discussion and Classification

The empirical findings support the theoretical assumption that governance seams exist at the interfaces between different areas of responsibility and become sources of coordination problems in hybrid incidents. In line with the hybrid threat model, the four identified governance seams run along established institutional dividing lines. These institutional dividing lines fulfill important functions in peacetime: they ensure the separation of powers, safeguard national sovereignty, and protect sensitive information. In the case of hybrid threats, however, these governance seams become salient in specific incidents and create practical coordination problems.

The phasing of the incidents paints a mixed picture. While the Airiston Helmi case, in which Russian citizens acquired real estate in strategically important areas, can clearly be classified as part of the priming phase,⁷⁵ the incidents involving infrastructure damage exhibit characteristics of the destabilization phase. Such incidents demonstrate vulnerabilities and test reactions without crossing the threshold into open confrontation.⁷⁶ The limited effect of the Balticconnector failure on gas supply security underscores the importance of resilience measures. Diversification via the LNG terminal in Inkoo (Ingå) had already reduced dependence on deliveries from Russia.⁷⁷ Uncertainty regarding attribution remains a consistent feature of all the cases examined. In none of the incidents was a final legal determination of the perpetrators made. This attribution deficit allows potential attackers to maintain plausible deniability. It complicates legally and politically secure countermeasures and thus perpetuates coordination problems at the governance seam between political will and operational capacity.

It should be noted that the cases examined concern cross-border maritime infrastructure. In purely national incidents or incidents involving other types of infrastructure, individual governance seams may be less relevant. The high degree of congruence therefore also reflects the theory-driven case selection. This methodological limitation implies that the findings demonstrate the applicability of the analytical framework to cross-border maritime infrastructure rather than establishing the universal prevalence of governance seams across all hybrid threat scenarios. Future research should include cases in which governance seams might be expected to be less pronounced in order to test the boundary conditions of the theoretical model.

⁷⁵ Giannopoulos, Smith, and Theocharidou, *The Landscape of Hybrid Threats*, 31-32.

⁷⁶ Praks, *Russia's Hybrid Threat Tactics against the Baltic Sea Region*, 23.

⁷⁷ Praks, *Russia's Hybrid Threat Tactics against the Baltic Sea Region*, 21-22.

Conclusion

This article examined governance seams in hybrid attacks on Baltic Sea maritime infrastructure. The congruence analysis supported all four assumptions with high empirical fit: coordination problems manifest at the civil-military interface (A1), the national-supranational interface (A2), in the gap between political rhetoric and operational capacity (A3), and the interface between public accountability and intelligence confidentiality (A4). These seams do not operate in isolation but reinforce each other. Attribution uncertainty (A3) complicates public communication (A4), while jurisdictional fragmentation (A2) impedes civil-military coordination (A1).

These findings can be systematized as follows: the identified governance seams run along institutional dividing lines that hybrid actors can exploit. First, they concern the interface between civil and military responsibilities; second, the interface between national and supranational levels; third, the relationship between political rhetoric and operational capacity; and fourth, the relationship between public accountability and intelligence confidentiality. The documented responses primarily address operational aspects without resolving the underlying structural problems. In particular, the attribution deficit enables potential attackers to maintain plausible deniability, as the analysis shows.

The article thus addresses a research gap arising from the predominantly abstract description of governance challenges by analyzing specific incidents through the lens of the hybrid threat model and examining the adequacy of institutional responses. The findings are subject to the limitations outlined in the methodology section with regard to geographical scope, attribution uncertainty, and access to sources. These limitations call for caution when making generalizations but do not detract from the structural patterns identified.

Future research could pursue several avenues. It would be worth examining whether the identified governance seams also occur in hybrid attacks on other types of infrastructure or in other geographical areas. Comparative assessments of how different analytical frameworks conceptualize hybrid threats could yield additional insights. While this study employed the model developed by Gianopoulos, Smith, and Theocharidou as a heuristic lens, alternative approaches such as the MCDC Countering Hybrid Warfare framework⁷⁸ may emphasize different institutional vulnerabilities and response mechanisms. Such a comparison would clarify which analytical tools prove most productive for specific governance contexts.

The Baltic Sea region shares certain characteristics with other maritime spaces subject to gray-zone activities. The South China Sea, where infrastructure

⁷⁸ Patrick J. Cullen and Erik Reichborn-Kjennerud, *Understanding Hybrid Warfare*, Multinational Capability Development Campaign (MCDC) project, 2017, accessed November 15, 2025, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf.

protection intersects with contested sovereignty claims, and the Eastern Mediterranean, where energy pipelines traverse multiple jurisdictional frameworks, present analogous coordination challenges. Investigating whether the governance seams identified here manifest similarly in these regions would test the broader applicability of the theoretical model and potentially reveal region-specific variations in institutional response patterns.

Furthermore, the question of how attribution processes can be accelerated and placed on a sound legal footing requires more in-depth investigation. Finally, an evaluation of the new coordination structures would be necessary to determine whether they actually shorten response times. The findings support critiques of purely resilience-based strategies already discussed in the literature. An effective strategy, therefore, requires a combination of hardening critical infrastructure and credible sanction mechanisms. The present study demonstrates that the identified governance seams are structural in nature and cannot be closed by individual institutional measures.

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

Dr. **Deniz Kocak** is a Research Associate at Helmut Schmidt University / University of the Federal Armed Forces Hamburg and Research Coordinator for the Interdisciplinary Research Focus Maritime Security (iFMS), specializing in security sector reform, maritime security, and Indo-Pacific security governance.
<https://orcid.org/0000-0002-3526-2962>

Bibliography

- Angstrom, Jan, and Kristin Ljungkvist. "Unpacking the Varying Strategic Logics of Total Defence." *Journal of Strategic Studies* 47, no. 4 (2024): 498–522. <https://doi.org/10.1080/01402390.2023.2260958>.
- Blatter, Joachim, and Markus Haverland. *Designing Case Studies: Explanatory Approaches in Small-N Research*. Basingstoke: Palgrave Macmillan, 2014.
- Bourbeau, Philippe. *On Resilience: Genealogy, Logics, and World Politics*. Cambridge: Cambridge University Press, 2018.
- Council of the European Union. *Council Recommendation of 8 December 2022 on a Union-wide Coordinated Approach to Strengthen the Resilience of Critical Infrastructure*, 2023/C 20/01. Brussels: European Union, 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj%3AJOC_2023_020_R_0001.
- Cullen, Patrick J., and Erik Reichborn-Kjennerud. *Understanding Hybrid Warfare*, Multinational Capability Development Campaign project, 2017. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf.
- de Coning, Cedric. *Strengthening the Resilience and Adaptive Capacity of Societies at Risk from Hybrid Threats*. Hybrid CoE Working Paper 9. Helsinki: European Centre of Excellence for Countering Hybrid Threats, 2021.
- Edwards, Charlie, and Nate Seidenstein. *The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure*. London: International Institute for Strategic Studies, August 2025. <https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure/>.
- Filipec, Ondřej. "Multilevel Analysis of the 2021 Poland-Belarus Border Crisis in the Context of Hybrid Threats." *Central European Journal of Politics* 8, no. 1 (2022): 1–18. https://doi.org/10.24132/cejop_2022_1.
- Fingrid. "Fault in the EstLink 2 Electricity Transmission Connection Between Finland and Estonia Located in the Submarine Cable." Press release, December 26, 2024. www.fingrid.fi/en/news/news/2024/fault-in-the-estlink-2-electricity-transmission-connection-between-finland-and-estonia-located-in-the-submarine-cable/.
- Finnish Government. "Location of Leak in Balticconnector Gas Pipeline Identified in Finland's Economic Zone." Press release, Ministry of Economic Affairs and Employment, Prime Minister's Office, October 10, 2023. <https://valtioneuvosto.fi/en/-/10616/location-of-leak-in-balticconnector-gas-pipeline-identified-in-finland-s-economic-zone>.

- Fjäder, Christian, and Johan Schalin. *Building Resilience to Hybrid Threats: Best Practices in the Nordics*. Hybrid CoE Working Paper 31. Helsinki: European Centre of Excellence for Countering Hybrid Threats, 2024. www.hybridcoe.fi/wp-content/uploads/2024/05/20240527-Hybrid-CoE-Working-Paper-31-Building-resilience-to-hybrid-threats-WEB.pdf.
- Gerring, John. *Case Study Research: Principles and Practices*. Cambridge: Cambridge University Press, 2007.
- Giannopoulos, Georgios, Hanna Smith, and Marianthi Theocharidou. *The Landscape of Hybrid Threats: A Conceptual Model*. EUR 30585 EN. Luxembourg: Publications Office of the European Union, 2021. <https://doi.org/10.2760/44985>.
- Jungwirth, Rainer, et al. *Hybrid Threats: A Comprehensive Resilience Ecosystem — Executive Summary*. EUR 31104 EN. Luxembourg: Publications Office of the European Union, 2023. <https://doi.org/10.2760/37899>.
- Käihkö, Ilmari. “The Evolution of Hybrid Warfare: Implications for Strategy and the Military Profession.” *Parameters* 51, no. 3 (2021): 116–127. <https://doi.org/10.55540/0031-1723.3084>.
- Kalm, Helga. “NATO’s Path to Securing Undersea Infrastructure in the Baltic Sea.” Carnegie Endowment for International Peace, May 29, 2024. <https://carnegieendowment.org/research/2024/05/nato-baltic-sea-security-nord-stream-balticconnector>.
- Krishnan, Armin. “Fifth Generation Warfare, Hybrid Warfare, and Gray Zone Conflict: A Comparison.” *Journal of Strategic Security* 15, no. 4 (2022): 14–31. <https://doi.org/10.5038/1944-0472.15.4.2013>.
- Libiseller, Chiara. “‘Hybrid Warfare’ as an Academic Fashion.” *Journal of Strategic Studies* 46, no. 4 (2023): 858–880. <https://doi.org/10.1080/01402390.2023.2177987>.
- Mumford, Andrew, and Pascal Carlucci. “Hybrid Warfare: The Continuation of Ambiguity by Other Means.” *European Journal of International Security* 8, no. 2 (2023): 192–206. <https://doi.org/10.1017/eis.2022.19>.
- NATO. “NATO Holds First Meeting of Critical Undersea Infrastructure Network.” May 23, 2024. www.nato.int/en/news-and-events/articles/news/2024/05/23/nato-holds-first-meeting-of-critical-undersea-infrastructure-network.
- Nilsson, Niklas, et al. “Security Challenges in the Grey Zone: Hybrid Threats and Hybrid Warfare.” In *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*, edited by Mikael Weissmann et al., 1–18. London: I. B. Tauris, 2021. <https://doi.org/10.5040/9781788317795.0005>.
- Praks, Henrik. *Russia’s Hybrid Threat Tactics against the Baltic Sea Region: From Disinformation to Sabotage*. Hybrid CoE Working Paper 32. Helsinki: European Centre of Excellence for Countering Hybrid Threats, May 2024. www.hybridcoe.fi/wp-content/uploads/2024/05/20240527-Hybrid-CoE-Working-Paper-32-Russia-Hybrid-Threat-Tactics-against-the-Baltic-Sea-Region-From-Disinformation-to-Sabotage-WEB.pdf.

[coe.fi/wp-content/uploads/2024/05/20240530-Hybrid-CoE-Working-Paper-32-Russias-hybrid-threat-tactics-WEB.pdf](https://www.hybridcoe.fi/wp-content/uploads/2024/05/20240530-Hybrid-CoE-Working-Paper-32-Russias-hybrid-threat-tactics-WEB.pdf).

Rusinaitė, Viktorija. *Turning Strategy into Praxis: Lessons in Hybrid Threat Deterrence*. Hybrid CoE Paper 25. Helsinki: European Centre of Excellence for Countering Hybrid Threats, August 2025. www.hybridcoe.fi/wp-content/uploads/2025/08/Hybrid-CoE-Paper-25-Turning-strategy-into-praxis-web.pdf.

Sari, Aurel. *Protecting Maritime Infrastructure from Hybrid Threats: Legal Options*. Hybrid CoE Research Report 14. Helsinki: European Centre of Excellence for Countering Hybrid Threats, March 2025. www.hybridcoe.fi/wp-content/uploads/2025/03/20250306-Hybrid-CoE-Research-Report-14-web.pdf.

Savitz, Scott. *Uncrewed Maritime Vessels: Shaping Naval Power in Hybrid Threat Operations*. Hybrid CoE Working Paper 34. Helsinki: European Centre of Excellence for Countering Hybrid Threats, 2024. <https://www.hybridcoe.fi/wp-content/uploads/2024/10/20241007-Hybrid-CoE-Working-Paper-34-Uncrewed-maritime-vessels-WEB.pdf>.

United Nations. "Security Council Rejects Draft Resolution Establishing Commission to Investigate Sabotage of Nord Stream Pipeline." 9295th Meeting, SC/15243, UN Meetings Coverage and Press Releases, March 27, 2023. <https://press.un.org/en/2023/sc15243.doc.htm>.