SECURITY & DEFENCE QUARTERLY

Hybrid coercion and maritime deterrence in the Baltic Sea: Critical undersea infrastructure and narrative contestation

Achille Castrogiovanni

Achilles.Castrogiovanni@research.sunderland.ac.uk

https://orcid.org/0009-0009-6953-3757

Independent Researcher; PhD in Political Sciences and International Studies, University of Sunderland, UK

Abstract

This article examines how maritime hybrid coercion in the Baltic Sea is framed, interpreted, and deterred across North Atlantic Treaty Organization (NATO), European Union (EU), and regional policy documents as well as selected Russian official narratives. It asks how recent public sources conceptualise critical undersea infrastructure incidents, shadow-fleet activity, and maritime ambiguity, and what their comparison reveals about deterrence, attribution, and escalation. The study employs qualitative comparative document analysis and structured close reading of three source clusters: analytical assessments of the Baltic maritime security, NATO, EU, and regional policy outputs, and Russian official doctrines and statements. The analysis is organised around four indicators: coercive mechanisms, deterrence mechanisms, escalation dynamics, and narrative frames. This design allows the article to distinguish evidence of events, evidence of policy adaptation, and evidence of public legitimation or counter-framing. The findings show that the Baltic maritime hybrid coercion operates through the interaction of material disruption, legal and attributional ambiguity, and narrative contestation. Critical undersea infrastructure incidents and shadow-fleet dynamics should be analysed together because both exploit commercial opacity, uncertain intervention powers, and contested public attribution. The article finds that effective deterrence depends not only on naval capability but also on resilience, surveillance, attribution, rapid repair, regulatory adaptation, and credible strategic communication. The Baltic case shows that maritime hybrid coercion operates through infrastructure disruption, legal and attributional ambiguity, and narrative contestation. NATO, EU, and regional actors are adapting through surveillance, resilience, regulation, and legal coordination, but deterrence by punishment remains limited by attribution problems, unclear intervention authority, and escalation risks.

Keywords:

Baltic Sea, hybrid warfare, critical undersea infrastructure, maritime deterrence, grey-zone coercion

Article info
Received: 1 April 2026
Revised: 7 May 2026
Accepted: 7 May 2026
Available online: 00 June 2026

Citation: Castrogiovanni A. (2026) 'Hybrid coercion and maritime deterrence in the Baltic Sea: Critical undersea infrastructure and narrative contestation', *Security and Defence Quarterly*, 54(2), pp. 73–90. doi: 10.35467/sdq/221580.

Introduction

Since Russia's war in Ukraine in February 2022, the Baltic Sea has re-emerged as a focal theatre for European security, not only because of its role in conventional reinforcement and sea lines of communication but also because of the region's exposure to ambiguous, deniable, and operationally disruptive activities directed at maritime infrastructure (Lawrence *et al.*, 2025; Praks, 2024). The International Centre for Defence and Security (ICDS) policy paper on hybrid and high-end warfare in the Baltic Sea region explicitly frames this dual challenge. Indeed, North Atlantic Treaty Organization (NATO) already faces "undeclared hybrid warfare" in the Baltic Sea region while simultaneously needing a credible capability to deter and, if necessary, fight in a complex, high-end maritime theatre (Lawrence *et al.,* 2025).

Two recent developments have significantly altered the strategic geometry of the region. Firstly, the accession of Finland in 2023 and Sweden in 2024 to NATO has strengthened the Allied posture and changed NATO's regional planning assumptions, including maritime responsibilities in peacetime and crisis (Lawrence *et al.,* 2025; North Atlantic Treaty Organization [NATO], 2024a). Secondly, a sequence of incidents affecting undersea cables and power links has drawn attention to the security of critical undersea infrastructure (CUI) and the limitations of the existing deterrence concepts for sub-threshold aggression (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2024; Lawrence *et al.*, 2025; Praks, 2024). The ICDS paper documents, *inter alia*, the Estlink-2 and related data-cable incidents associated with the vessel Eagle S, subsequent Finnish investigative actions, and the launch of NATO's multi-domain activity "Baltic Sentry" in January 2025 (Lawrence *et al.*, 2025; NATO, 2025).

Although this analysis focuses on the Baltic Sea, the challenge is inherently global. Subsea cables and pipelines underpin modern connectivity, energy security, and military communications across regions ranging from the North Atlantic and Mediterranean to the Indo-Pacific (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2025; UK Parliament Joint Committee on the National Security Strategy, 2025). The Baltic's recent pattern of ambiguous disruption, intensified surveillance, and regulatory innovation is therefore best understood as an early case study of a wider contest over the security of CUI. The EU's 2025 Action Plan on Cable Security, alongside NATO and initiatives of Joint Expeditionary Force (JEF) aimed at enhancing monitoring and resilience, is likely to inform comparable approaches in other maritime theatres where state competition, sanctions-evasion shipping, and grey-zone coercion intersect (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2025; Joint Expeditionary Force, 2025; NATO, 2025; van Soest *et al.*, 2025).

In parallel, open-source and official assessments identify sanctions-evasion shipping, often described as the Russian "shadow fleet," as a distinct source of Baltic maritime risk. Opaque ownership, weak insurance, flag changes, and manipulation of automatic identification system (AIS) do not prove sabotage in any individual case, but they widen the operational ambiguity within which unsafe interactions, sanctions enforcement, and coercive signalling can overlap (Brown, 2025; Childs, 2025; European Parliamentary Research Service, 2024).

Meanwhile, Henrik Praks's Hybrid CoE Working Paper 32, Russia's Hybrid Threat Tactics against the Baltic Sea Region: From Disinformation to Sabotage, provides a broader regional baseline. It demonstrates how Russia's hybrid toolbox has become more aggressive and varied, ranging from disinformation, cyber operations, and sabotage to

instrumentalised migration and threats to energy and communications infrastructure (Praks, 2024, pp. 5, 9–23). At the same time, it emphasises that societies and institutions in the Baltic Sea have shown notable resilience and have limited the effectiveness of many influence operations (Praks, 2024, pp. 5, 22–23).

Rather than offering a general survey of Baltic security developments, this article addresses a more specific problem. It asks: how do NATO, EU, and regionally oriented policy documents, when read alongside selected Russian official narratives, frame maritime hybrid coercion in the Baltic Sea, and what does this comparison reveal about deterrence and escalation? The relevant gap in the literature lies not in the existence of a conflict continuum as such, but in the limited integration of three elements often treated separately: maritime infrastructure vulnerability, deterrence credibility, and competing official narratives of legality, blame, and escalation.

The article argues that the Baltic maritime hybrid coercion operates through a three-part mechanism: the disruption or endangerment of critical infrastructure and shipping; the exploitation of legal and attributional ambiguity; and the narrative competition over whether episodes are framed as accidents, lawful enforcement, coercion, or aggression. The contribution is therefore deliberately bounded. Rather than offering an exhaustive account of all NATO and EU responses or Russian messaging, the article analyses selected authoritative public sources to show how policy adaptation, deterrence dilemmas, and narrative contestation interact in the maritime theatre.

More explicitly, this article locates its contribution at the junction of four debates, rather than within a single generic account of hybrid warfare. Firstly, hybrid-warfare scholarship explains the combination of conventional, irregular, informational, and coercive instruments while also warning against using "hybrid warfare" as an all-purpose label for Russian conduct (Hoffman, 2007; Monaghan, 2015; Renz and Smith, 2016). Secondly, grey-zone and extended-deterrence literature clarifies why below-threshold activity exploits ambiguity, calibrated risk, and the reluctance of defenders to escalate (Lanoszka, 2016; Mazarr, 2015). Thirdly, recent submarine-infrastructure scholarship shows that cables and pipelines are not merely technical background systems but strategic assets whose protection involves geography, ownership, repair capacity, public–private governance, and legal authority (Bashfield, 2025; Bueger and Liebetrau, 2021; Govella, 2025). Finally, the current law-of-the-sea scholarship on submarine cables and pipelines has sharpened the problem of jurisdiction and enforcement, particularly where suspected damage occurs outside territorial waters or involves commercially ambiguous vessels (Lott, 2025; Ringbom, 2025). The added value of this article is to connect these debates through the Baltic case. It shows that maritime hybrid coercion becomes strategically significant when infrastructure vulnerability, sanctions-evasion shipping, legal ambiguity, deterrence by denial, and official narrative contestation interact within the same maritime theatre.

Hybrid warfare, grey zones, maritime deterrence, and narrative contestation: literature and analytical framework

Conceptually, the argument lies at the intersection of three bodies of literature: debates on "hybrid warfare," scholarship on grey-zone competition and coercion below the threshold of armed conflict, and work on maritime deterrence and critical infrastructure protection. Hoffman's (2007, 2009) early formulation of hybrid warfare emphasised adversaries that combine conventional capabilities, irregular tactics, terrorism, and

criminality within the same battlespace to generate synergistic effects against stronger opponents. A recent work by Ploumis (2022) likewise argues that hybrid strategies combine asymmetric, conventional, and irregular methods to secure strategic advantage while complicating an adversary's response. In this reading, hybridity refers to the simultaneous use of multiple modes of violence rather than to any specific domain or geography. Later applications to Russia's interventions in Georgia and Ukraine extended the concept to include broader informational and political tools.

More precisely, Renz and Smith's (2016) work on Russian hybrid warfare cautions against an overly expansive use of the term. They argue that "hybrid warfare" often has been transformed from a specific military-strategic concept into a quasi-theory of Russian foreign policy, and that such inflation risks analytical confusion and unhelpful threat inflation. Monaghan (2015) likewise argues that the "war" in Russian conceptions of "hybrid warfare" must be taken seriously: Russian thinking on conflict remains firmly anchored in war, strategy, and state survival, rather than in a supposedly novel and all-encompassing repertoire of ambiguous tools. From this perspective, hybrid methods are best understood as one component of a broader Russian theory of conflict, which treats peace and war as existing along a continuous spectrum.

Parallel work on disinformation and "active measures" situates contemporary Russian practices in a longer history of political warfare. Rid's (2020) study of active measures documents how disinformation campaigns, forgeries, and covert influence operations have long been used to exploit social cleavages and erode trust in institutions. Although the technological environment has changed, the underlying logic of manipulating perceptions, sowing doubt over attribution, and constraining adversary decision-making is consistent. Hybrid CoE analysis of Russian tactics in the Baltic Sea region suggests that these methods are combined with sabotage, intelligence activity, and economic leverage to exploit vulnerabilities in energy and communications infrastructure (Praks, 2024, pp. 9–21). This pattern aligns with the established grey-zone literature that frames competitive activity below the threshold of armed attack as a deliberate strategy to exploit legal and political seams (Lanoszka, 2016; Mazarr, 2015).

A second strand of scholarship focuses on grey-zone competition and coercion below the threshold of armed conflict. Much of this literature highlights the centrality of political objectives, legal ambiguity, and calibrated risk-taking in shaping state behaviour. It emphasises the use of limited, reversible, and often deniable measures designed to secure strategic advantage without triggering a large-scale military response (Iskandarov and Gawliczek, 2020; Lanoszka, 2016; Mazarr, 2015). Within this context, hybrid warfare can be conceptualised as an operational modality within the grey zone, rather than as a synonym for it: grey-zone competition denotes the broader competitive environment, whereas hybrid warfare refers to specific combinations of instruments employed within that environment.

Finally, debates on deterrence and defence have begun to address the maritime dimension of hybrid conflict more explicitly. Deterrence theory has traditionally focused on conventional and nuclear forces, and on signalling costs and risks to a clearly identified adversary. Hybrid activity directed against CUI, however, raises distinct challenges: attribution may be slow or contested, damage may be reversible yet cumulatively significant, and the boundary between criminality, commercial risk, and national security is often blurred. NATO's concept of countering hybrid threats, as articulated in the Warsaw Summit communiqué and the subsequent policy documents, reflects this shift by recognising that hybrid action against Allies could, under certain circumstances, lead to a decision to invoke Article 5, while still placing primary responsibility for responding to such activity on the targeted state (NATO, 2016, 2024b).

Recent scholarship on CUI sharpens this maritime dimension of deterrence. Bueger and Liebetrau (2021) conceptualise submarine cables as hidden infrastructure whose security politics connect technical systems, private ownership, and state security agendas. Bashfield's (2025) argument on seabed lines of communication similarly reframes cables, pipelines, and seabed systems as maritime routes and assets that require defence planning, not merely commercial risk management. Govella's (2025) work on undersea cables, geoeconomics, and security adds that contemporary cable risk is shaped not only by physical vulnerability but also by securitisation, investment choices, regulatory decisions, and a whole life-cycle approach to resilience, including licensing, maintenance, protection, and repair. Legal scholarship reaches a parallel conclusion from a different angle. Lott (2025) shows that conventional jurisdictional approaches give coastal states more limited authority over cross-border submarine cables and pipelines than over some other offshore structures, while Ringbom's (2025) analysis of suspected Baltic attacks demonstrates how new security problems are being channelled through older law-of-the-sea categories. This article builds on those debates by treating legal authority, resilience, and strategic communication as components of deterrence rather than as separate technical, legal or diplomatic issues.

In parallel with this predominantly NATO- and EU-centred body of scholarship, Russian strategic documents conceptualise the same competitive space in markedly different terms. The 2023 Foreign Policy Concept represents Russia as a "state-civilisation" engaged in defending a multipolar, law-based international order against the "neo-colonial" policies of the United States and other "unfriendly states," while foregrounding sovereignty, non-interference, and the principle of the so-called indivisible security (Ministry of Foreign Affairs of the Russian Federation, 2023). The concept, together with the related presidential decrees, explicitly reserves the right to respond to "unfriendly acts," including sanctions and hostile information campaigns, through a combination of symmetrical and asymmetrical measures (President of the Russian Federation, 2023). The Information Security Doctrine, originally adopted in 2000 and revised in 2016, identifies the principal threats in the information sphere as foreign political and psychological influence, and emphasises Russia's prerogative to safeguard its information sovereignty and critical infrastructure. Regarding the 2000 doctrine, this article relies on the official Russian text and uses an archival unofficial English translation solely as an aid to translation; for the 2016 doctrine, it refers to both the official Russian text and the official English version (Russian Federation, 2000a, 2000b, 2016a, 2016b). In doctrinal terms, instruments that NATO commonly characterises as elements of hybrid warfare are thus represented in Russian official discourse as defensive countermeasures to Western pressure.

Official narratives occupy a distinct place within this framework. They are not treated here as transparent evidence of underlying intentions but as forms of public strategic communication: efforts to allocate blame, legitimise one's own conduct, portray the adversary as escalatory or unlawful, and shape the thresholds at which audiences interpret an event as an accident, enforcement action, coercion, or attack (Praks, 2024; Rid, 2020). In the Baltic maritime context, where attribution is contested, and many incidents involve ostensibly civilian vessels or dual-use infrastructure, such narratives matter directly for deterrence. They shape whether surveillance, boarding, sanctions enforcement, cable protection, and military presence are presented as prudent defensive measures or as provocative escalatory acts (Ministry of Foreign Affairs of the Russian Federation, 2023, 2025; NATO, 2024b).

Building on the above-mentioned literature, this article adopts an analytical framework centred on the interaction of three dimensions: hybrid coercion, maritime deterrence, and narrative contestation. Here, hybrid coercion refers to repeated below-threshold actions that exploit infrastructural vulnerability, commercial opacity, and legal ambiguity in order

to impose costs and test responses. Maritime deterrence refers to the combination of denial, resilience, surveillance, intervention authority, and punishment through which states seek to reduce both feasibility and attractiveness of such actions. Narrative contestation refers to the public struggle over attribution, legality, and responsibility for escalation.

This framework yields three analytical expectations. Firstly, if the Baltic incidents form part of a broader pattern of coercion, then they should appear across sources as more than isolated accidents and should be linked to cumulative effects on readiness, cost, and decision time. Secondly, if maritime deterrence differs from conventional deterrence, sources should emphasise resilience, attribution, and regulation alongside naval power. Thirdly, if narratives matter, Western and Russian official texts should do more than merely describe events differently; they should assign legitimacy and responsibility for escalation in systematically opposed ways. The value of the Baltic case, therefore, lies less in claiming that hybrid-continuum thinking is novel than in specifying how infrastructural vulnerability, deterrence credibility, and narrative competition interact in a maritime theatre.

The analytical payoff of this positioning is therefore specific. The article does not add another generic case of hybrid warfare; it specifies a maritime-infrastructure mechanism. In that mechanism, a single episode may operate at several levels at once: as physical disruption, commercial-shipping problem, legal-threshold test, deterrence signal, and narrative opportunity. This is the contribution carried into the empirical sections below.

Methodology and source selection

This study employs qualitative comparative document analysis and structured close reading of a purposively selected corpus of publicly available materials. Rather than relying on two reports alone, the empirical base is organised into three source clusters: (1) analytical diagnoses of the Baltic maritime environment; (2) NATO, EU, and JEF/UK-related official policy outputs; and (3) Russian official doctrines and statements that frame the same developments from Moscow's perspective. The first cluster includes the ICDS paper and the Hybrid CoE working paper, supplemented by additional analytical and policy-oriented assessments (Aitken, 2025; Brown, 2025; Childs, 2025; European Parliamentary Research Service, 2024; UK Parliament Joint Committee on the National Security Strategy, 2025; van Soest *et al.*, 2025). The second cluster includes NATO's Warsaw Summit communiqué, NATO materials on countering hybrid threats and Baltic Sentry, the European Commission's cable security and mandatory ship-reporting initiatives, and JEF/UK statements. The third cluster includes the 2023 Foreign Policy Concept, the presidential decree approving it, the 2000 and 2016 Information Security Doctrines in their official Russian versions, together with the official English 2016 publication and an archival unofficial English translation of the 2000 text, the Russian Foreign Ministry's statement on sanctions, and Russian official or UN-reported positions on Nord Stream and related Baltic incidents (Russian Federation, 2000a, 2000b, 2016a, 2016b).

The methodological assumption underpinning the design is that public documents can reveal how actors frame, classify, and respond to maritime incidents, even when they cannot reveal classified attribution or internal decision-making. The unit of analysis is therefore not the individual incident alone but the recurring relationship between incident type, policy response, and official narrative. The study consequently examines how incidents are made strategically meaningful through policy adaptation, legal classification, and public communication.

For analytical transparency, the source clusters were not treated as interchangeable: analytical studies were used primarily to identify recurring patterns of vulnerability and escalation risk; Western official documents to capture declared policy responses and legal-operational adaptation; and Russian official texts to analyse public legitimation, blame allocation, and counter-framing. The corpus is purposively bounded rather than exhaustive. These sources were selected because they are authoritative, contemporaneous, and directly relevant to the three elements under examination: maritime hybrid coercion, deterrence responses, and official narrative framing. The aim is therefore analytical leverage rather than statistical representativeness. The Baltic case is particularly suitable because it combines repeated CUI incidents, shadow-fleet enforcement challenges, recent NATO adaptation, and explicit Russian counter-framing within a compact regional theatre.

The rationale for source selection follows from this design. Analytical reports were included where they offered detailed assessment of operational patterns and infrastructure vulnerabilities; NATO, EU, JEF, and UK materials were included where they recorded declared policy adaptation; and Russian official texts were included where they provided public counter-framing on sovereignty, sanctions, information security, and escalation. This source hierarchy allows the article to distinguish between evidence of events, evidence of policy response, and evidence of narrative positioning.

The close reading proceeded on the basis of four coding indicators. Firstly, coercive mechanism: references to sabotage, deniable interference, commercial opacity, AIS manipulation, cost imposition, or probing behaviour. Secondly, deterrence mechanism: references to denial, resilience, surveillance, legal intervention, punishment, or war-fighting capability. Thirdly, escalation dynamic: references to reaction time, crisis instability, miscalculation, threshold ambiguity, or high-end conflict. Fourthly, narrative frame: language assigning blame, legality, legitimacy, victimhood, or provocation. Inferences are drawn where these indicators recur across more than one source cluster, or where divergence between clusters is itself analytically significant. Here, a proposition is treated as strongly supported only where it is corroborated across at least two source clusters, preferably including one official source; where support is more limited, the text presents the point as an interpretation or plausible inference rather than as an established fact.

Operationally, the coding process proceeded in three steps. Firstly, each source was read for explicit references to CUI damage, shadow-fleet activity, surveillance, sanctions enforcement, legal thresholds, and escalation language. Secondly, those references were assigned to the above-mentioned four indicators. Thirdly, claims were compared across source clusters in order to separate strongly supported findings from more cautious interpretive inferences. A pattern of coercion is therefore inferred only if several features recur together, including repeated infrastructure or shipping-related pressure, ambiguity over responsibility, observable policy costs, and a contested narrative over legality or blame.

This research design imposes clear limits on the claims that can be advanced. Official narratives are treated as evidence of public framing and legitimation, rather than as transparent windows into actual intentions or covert decision-making. Likewise, document analysis cannot independently attribute specific incidents or establish causal responsibility for any individual episode. What it can do is identify recurring interpretive patterns, map the policy logic of competing actors, and show how material incidents, deterrence debates, and narrative contestation are linked in the public record. This also requires recognition of source asymmetries: analytical reports may offer richer operational details than official communiqués, whereas official documents are treated as authoritative evidence of policy position rather than as neutral proof of underlying events.

The category of pattern is used cautiously. It does not mean that every cable or pipeline incident is attributed to Russia, nor that each episode is directed from a single operational centre. It means that the public record shows repeated opportunities for coercive leverage produced by the same structural conditions: exposed infrastructure, opaque commercial shipping, slow attribution, uncertain intervention powers, and adversarial framing.

For this reason, the article distinguishes explicitly between isolated incidents and evidence of a coercive pattern. An incident is treated as isolated if the available public record supports only a discrete technical failure, accident, criminal episode, or unresolved investigation, and where there is no demonstrable recurrence, no connection to a wider vessel or infrastructure-security problem, no significant policy adaptation, and no sustained official narrative contestation. By contrast, the article treats an episode as contributing to a pattern only if several criteria appear together: recurrence across comparable maritime or infrastructure targets; operational ambiguity, such as disputed attribution, opaque ownership, AIS irregularities, or dual-use vessel activity; strategic effect, including repair costs, disruption, surveillance requirements, or regulatory mobilisation; and narrative exploitation, meaning official or semi-official efforts to frame the episode as accident, provocation, lawful commerce, sanctions abuse, or aggression. The threshold is therefore cumulative rather than attributional: the article does not need to prove central direction for each episode, but it also avoids treating every Baltic maritime incident as part of a single coordinated campaign.

Findings: the maritime hybrid problem in the Baltic

Taken together, the corpus indicates that the Baltic maritime coercion problem is not adequately addressed by treating cable-cutting incidents and sanctions evasion as analytically separate developments. Instead, the broader pattern consists of the exploitation of ambiguity across the intersecting domains of infrastructure protection, commercial shipping, law enforcement, and deterrence. The sections that follow examine this pattern through the lenses of CUI interference, shadow-fleet dynamics, and the selected NATO, EU, and regional responses that have developed in response.

CUI interference as a campaign logic

Recent Baltic CUI incidents are strategically significant not merely as technical failures but because they impose immediate economic and security costs while complicating attribution (Lawrence *et al.*, 2025; Praks, 2024, pp. 21–23; van Soest *et al.*, 2025). From the perspective of hybrid coercion, interference with CUI offers three principal advantages to an aggressor. Firstly, it preserves plausible deniability: maritime "accidents" and complex forensic environments delay formal attribution and create scope for competing narratives. Secondly, it generates an asymmetric cost exchange, whereby relatively low-cost interference can produce expensive repairs, insurance repercussions, and political pressure. Finally, it enables operational reconnaissance through action, as each episode tests detection capabilities, legal authorities, and mechanisms of multinational coordination.

The Hybrid CoE working paper anticipates this logic in its taxonomy of Russian hybrid activities, identifying threats to energy and communications infrastructure, alongside sabotage, intelligence activity, and coercive information operations, as central components of Russia's broader hybrid repertoire in the region (Praks, 2024, pp. 14–21). Read together, the two studies suggest that CUI interference may plausibly be interpreted as a recurring pattern of coercion in the public record rather than as a series of isolated acts of vandalism. Repeated and ambiguous incidents may serve to probe Alliance seams, accustom publics

to heightened levels of risk, and signal that further escalatory options remain available. At the same time, the available open-source material does not warrant attributing every incident to a single centrally directed campaign.

This distinction is important for the evidentiary handling of recent Baltic examples. The Estlink-2 and associated data-cable damage linked in the public record to the vessel Eagle S is treated here as a stronger illustrative case because it combines damage to electricity and communications infrastructure, Finnish investigative action, immediate regional concern, JEF activation, and NATO's subsequent Baltic Sentry activity (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2024; Joint Expeditionary Force, 2025; NATO, 2025; Police of Finland, 2024; UK Government, 2025). The evidentiary significance of the case lies not in proving, on public sources alone, a centrally directed Russian operation, but in showing how a maritime incident can generate precisely the combination of material disruption, attributional uncertainty, regulatory response, and narrative contestation that makes CUI interference strategically consequential. By contrast, a one-off cable fault or maritime accident with no recurrence, no suspicious vessel behaviour, no wider policy response, and no official counter-framing would not meet the article's threshold for inclusion in a coercive pattern.

Accordingly, Section 4.1 applies the methodological threshold set out above rather than redefining it. The point is not to infer covert intent from each episode, but to show when recurring cost, response-testing, shadow-fleet opacity, and competing official narratives make a maritime incident strategically consequential.

"Shadow-fleet" dynamics and regulatory counter-pressure

Shadow-fleet dynamics constitute a second layer of maritime hybrid coercion because they occupy the intersection of sanctions evasion, maritime safety, environmental risk, and national security (Brown, 2025; Childs, 2025; European Parliamentary Research Service, 2024; Lawrence *et al.*, 2025). Opaque ownership structures, inadequate insurance, frequent flag changes, and irregular AIS behaviour do not in themselves establish sabotage in any individual case, but they do increase the operational ambiguity within which deniable interference may occur. For NATO and EU actors, the challenge lies in the fact that the same platforms may appear simultaneously as commercial vessels, targets of sanctions enforcement, and potential vectors of coercive signalling.

Russian officials, for their part, reject the label of "shadow fleet" and portray recent EU and NATO measures as forms of illegitimate economic warfare. Statements by the Foreign Ministry characterise successive EU sanctions packages as "illegal unilateral coercive measures" and present efforts to restrict Russian-linked tankers as politically motivated attempts to undermine lawful trade and maritime commerce (Ministry of Foreign Affairs of the Russian Federation, 2025). Within the broader official framing set out in Russia's 2023 Foreign Policy Concept, enhanced Allied surveillance and sanctions-enforcement activity can thus be represented as further evidence of Western pressure rather than as defensive maritime security measures (Ministry of Foreign Affairs of the Russian Federation, 2023, 2025).

NATO and regional operational adaptation

Selected NATO, EU, and regionally led responses indicate that Baltic governments and institutions are beginning to adapt, albeit unevenly, to this maritime hybrid environment.

NATO's "Baltic Sentry" activity, announced in January 2025, is presented as a measure intended to strengthen the protection of critical infrastructure and enhance Allies' capacity to detect and respond to destabilising acts directed against undersea cables and pipelines (NATO, 2025). In parallel, the UK-led Joint Expeditionary Force (2025) has activated "Nordic Warden," an AI-enabled threat-tracking system that uses vessel data, including AIS, to assess risks to undersea infrastructure and monitor the shadow fleet (UK Government, 2025).

The ICDS paper emphasises the need for coordination across these lines of effort while also underscoring structural constraints, notably the difficulty of sustaining a dense and persistent maritime presence across the Baltic as a whole, and the political and legal controversy surrounding the stopping and inspection of suspect vessels beyond territorial waters (Lawrence *et al.*, 2025). These constraints reinforce the importance of integrating regulatory, intelligence, and operational instruments rather than relying on naval presence alone.

A sharper assessment of sufficiency should distinguish between visibility, enforceability, and resilience. On visibility, Baltic Sentry is a meaningful improvement because NATO presents it as combining frigates, maritime patrol aircraft, naval drones, and national surveillance assets in order to improve the protection of CUI and the Alliance's ability to respond to destabilising acts. On risk identification, Nordic Warden adds value because the UK Government (2025) describes it as an AI-enabled system using AIS and other data to assess the risk posed by vessels, issue warnings to JEF participants and NATO Allies, and monitor twenty-two areas of interest. These measures are nevertheless not fully sufficient on their own: they improve detection, warning and political signalling, but they do not by themselves guarantee continuous physical protection of all cables and pipelines, nor do they automatically resolve the legal and political problem of stopping, boarding or diverting a suspect vessel before damage occurs. The EU Action Plan on Cable Security reinforces this judgement by treating cable security as a full resilience cycle of prevention, detection, response, repair, and deterrence, rather than as a matter of military presence alone (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2025; NATO, 2025; UK Government, 2025).

Deterrence in the hybrid maritime domain: denial, punishment, and the attribution trap

The deterrence problem becomes more clearly defined once such incidents are conceptualised as recurrent acts of coercive probing rather than as isolated anomalies. The central issue is not simply whether an adversary can inflict physical damage on infrastructure, but whether the targeted states can attribute, disrupt, and publicly classify the act with sufficient speed and authority to deter recurrence. This helps to explain why denial, resilience, and legal authority assume greater salience in this context than in conventional force-on-force models of deterrence.

Why concepts of conventional deterrence do not transfer cleanly?

Many concepts of deterrence, derived from the Cold War nuclear and conventional experience, do not transfer neatly to the hybrid maritime domain (Lawrence *et al.*, 2025; NATO, 2016; UK Parliament Joint Committee on the National Security Strategy, 2025).

Incidents at sea may resemble criminal acts, regulatory breaches, or safety failures more closely than overt hostile military operations; the actors involved may be private entities, state-linked agents operating with partial deniability, or some combination thereof. The resulting policy dilemma follows directly from this ambiguity: effective prevention and response require enhanced intervention capacity, including the ability to stop, inspect, and, where necessary, divert suspect vessels, yet such intervention itself entails legal, political, and escalatory risks, particularly in international waters.

Deterrence by denial: resilience and surveillance

Against this backdrop, deterrence by denial acquires a distinctive maritime-infrastructure dimension. The ICDS paper treats resilience, hardening, and redundancy in energy and communication networks as functionally integral to deterrence by denial, insofar as they increase the level of effort required for an attacker to generate meaningful effects (Lawrence *et al.*, 2025). Rapid repair capacity and planned rerouting options further reduce the anticipated benefits of sabotage. Similarly, enhanced surveillance and maritime domain awareness, supported by sensors, patrols, and data-fusion systems, such as "Baltic Sentry" and "Nordic Warden," increase the likelihood that suspicious activity will be detected and disrupted, even if not every element of CUI is monitored physically at all times.

These findings accord with the Hybrid CoE's assessment that states in the Baltic Sea region have reduced their vulnerability by lessening their dependence on Russian energy leverage, strengthening alliances, and investing in societal resilience (Praks, 2024, pp. 22–23). On this account, Russia's capacity for influence is constrained by its increasingly "toxic reputation" and by heightened public awareness of disinformation and coercive economic practices. Nonetheless, the paper cautions that Moscow will continue to test boundaries and may adopt more escalatory tactics as opportunities arise (Praks, 2024, p. 23).

Deterrence by punishment: weak credibility without attribution

Deterrence by punishment is limited by a distinct constraint: attribution. The ICDS paper identifies attribution as the principal impediment to credible punishment-based deterrence in the CUI context (Lawrence *et al.*, 2025). Even where political leaders and commentators suspect Russian responsibility for particular incidents, official investigations have often failed to yield public attributions that are sufficiently robust in legal and political terms. In the absence of a clearly identified perpetrator, the threat of punishment lacks credibility; where attribution is established, the calibration of a proportionate response that avoids unintended escalation becomes politically and strategically contested.

From hybrid to high-end conflict: escalation pathways and Baltic warfighting requirements

The link between hybrid activity and high-end conflict in this article is analytical rather than deterministic. The claim is not that cable-related incidents mechanically lead to war, but that repeated maritime coercion can affect readiness, heighten mistrust, and create pathways to escalation within a theatre already central to NATO reinforcement and Russian signalling. The Baltic case is particularly instructive because hybrid incidents, regulatory adaptation, and conventional planning are unfolding within the

same operational space. The argument, therefore, concerns cumulative strategic effect, rather than the treatment of each discrete maritime incident as a direct precursor to war.

Hybrid as prelude, not prediction

Recent analyses caution that repeated, deniable interference can generate escalation risks even in the absence of any intention to trigger major war. By increasing uncertainty and imposing recurrent costs, maritime hybrid coercion incentivises countermeasures that combine law enforcement, regulatory action, and naval posture, thereby creating the potential for friction and signalling spirals. In a dense operational environment, such as the Baltic Sea, attribution disputes, uncertain legal thresholds, and the dual-use commercial activity associated with sanctions evasion can further heighten the risk of miscalculation (Brown, 2025; Childs, 2025; van Soest *et al.*, 2025).

Recent policy and think-tank assessments likewise judge deliberate large-scale conflict in the Baltic to be unlikely in the near term while still identifying plausible pathways to accidental or inadvertent escalation driven by unsafe interactions at sea, damage to CUI, degraded readiness, and crisis miscalculation (Brown, 2025; UK Parliament Joint Committee on the National Security Strategy, 2025; van Soest *et al.*, 2025).

Official Russian statements also counter-frame maritime incidents as evidence of Western escalation rather than Russian coercion. In the Nord Stream case, Moscow described the blasts as international terrorism, requested an independent Security Council investigation, alleged possible Western involvement and denied responsibility (Reuters, 2023; United Nations, 2023). Subsequent commentary on Baltic cable and pipeline incidents extends this logic by presenting NATO and EU responses, including the Baltic Sentry, as justificatory devices for sanctions and military measures. The narrative function is therefore less to clarify individual incidents than to reverse attribution and shift escalation responsibility onto the "collective West" (Ministry of Foreign Affairs of the Russian Federation, 2023, 2025).

Capability shortfalls and priorities for high-end Baltic maritime operations

A key contribution of the ICDS analysis lies in its explicit linkage between hybrid deterrence and conventional maritime posture. It argues that NATO must retain the capacity to deter Russia from transitioning from hybrid activity to conventional conflict by maintaining credible capabilities in sea control and sea denial, air and coastal defence, mine warfare, and joint operations in the Baltic theatre (Lawrence *et al.*, 2025). The paper identifies a number of priority investments, including improved maritime surveillance, particularly in the Gulf of Finland; enhanced air- and coastal-defence missile systems; modernised mine-laying platforms; upgraded surface fleets; and more robust intelligence, surveillance, and reconnaissance (ISR) and targeting architectures. Drawing on the lessons from Ukraine, it also highlights the potential of unmanned systems and long-range precision fires while cautioning against overreliance on unproven technologies at the expense of operational reliability (Lawrence *et al.*, 2025).

The present article contends that the strategic logic is straightforward: in the absence of credible conventional capability, hybrid interference may be perceived in Moscow as a relatively low-risk form of experimentation, thereby potentially emboldening escalation

or, at the very least, increasing the frequency and boldness of coercive probes. Conversely, a robust maritime and joint posture reinforces deterrence in the hybrid domain by signalling that escalation dominance does not rest with the aggressor.

Timing, initiative, and management of crisis

Furthermore, the ICDS paper introduces an important temporal dimension to deterrence. It argues that the decisive arena is often the pre-crisis period, during which hybrid actions, legal manoeuvring, and ostensibly routine maritime interactions gradually shape readiness, decision-making cultures, and political resolve (Lawrence *et al.*, 2025). By the time a crisis becomes visible, key trajectories may already have been set by prior choices, sunk costs, and entrenched narrative frames. This, in turn, underscores the importance of early and visible adjustments in maritime posture, regular exercises incorporating hybrid scenarios, and pre-negotiated crisis-management mechanisms.

From an Alliance perspective, this suggests that escalation management cannot be improvised in the midst of a crisis. Procedures for incident prevention, rapid deconfliction, and proportionate response, including in the maritime domain, must be continuously rehearsed alongside deterrence signalling. Otherwise, the very ambiguity that renders hybrid tactics attractive to the aggressor also heightens the risk that an incident escalates into a confrontation that neither side initially intended.

Discussion and policy implications: towards an integrated maritime deterrence architecture

The discussion turns on one central claim: the Baltic case refines the hybrid-warfare and grey-zone literature by showing how maritime coercion is channelled through infrastructure vulnerability, commercial opacity, legal ambiguity, and public narrative framing. This does not require treating every incident as evidence of an omnipotent or centrally directed hybrid campaign. Rather, the case supports a bounded interpretation: repeated exploitation of seams becomes strategically significant when it affects readiness, compresses decision time, and contests public legitimacy. The policy discussion therefore turns on four operational tests: whether current measures improve persistent visibility, shorten attribution and decision cycles, create lawful intervention options, and reduce coercive leverage through resilience, redundancy, and rapid repair.

A synthesis of these sources supports several policy implications for NATO, the EU, and regional groupings. Firstly, CUI security should be treated as a core element of deterrence rather than as an auxiliary resilience agenda. Investments in hardening, redundancy, and rapid repair capacity directly reduce the coercive leverage that may be derived from cable and pipeline interference, thereby strengthening deterrence by denial (Lawrence *et al.*, 2025; Praks, 2024, pp. 22–23). This is consistent with both the EU Action Plan on Cable Security and the UK parliamentary evidence, which treat resilience, repair capacity, and crisis preparedness as integral components of security rather than as merely technical afterthoughts (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2025; UK Parliament Joint Committee on the National Security Strategy, 2025).

Secondly, multinational surveillance and response mechanisms should be institutionalised, but their limits must be realistically acknowledged. The Baltic Sentry and Nordic Warden demonstrate adaptive operational responses that leverage data fusion and AI-assisted

risk assessment. However, the ICDS paper is sceptical about the feasibility of sustaining long-duration, high-density deployments without broader capacity growth and burden-sharing arrangements (Lawrence *et al.*, 2025; NATO, 2025; UK Government, 2025). Clear prioritisation of critical routes and assets, combined with flexible surge capacity, will be essential.

For this reason, the policy test is cumulative. Detection systems, resilience planning, and regulatory reporting only become a credible deterrence architecture if they are connected to pre-agreed legal thresholds, rapid national enforcement decisions, sustained maritime and aerial assets, industry cooperation, repair capacity, and escalation-management procedures. The main weakness is therefore not the absence of initiatives, but the risk that visibility, resilience, and enforceability develop at different speeds (NATO, 2025; UK Government, 2025; European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2025).

Thirdly, legal seams for intervention and enforcement should be narrowed. The Helsinki summit's decision to convene a group of legal experts in order to clarify international law tools for hybrid situations in the maritime domain signals recognition that existing frameworks are being stress-tested (Lawrence *et al.*, 2025). At the same time, the EU measures requiring insurance reporting for ships in Mandatory Ship Reporting Systems (MRS) areas illustrate how regulatory instruments can constrain grey-zone shipping behaviour and complement naval capacity (European Commission, 2025).

Fourthly, strategic communication should be calibrated. Public messaging needs to support deterrence and collective resolve, but it should avoid claims that cannot be substantiated without compromising intelligence sources or due-process standards. Credibility is strengthened when attribution, enforcement, and legal argumentation are aligned with publicly demonstrable evidence while escalation management benefits from language that is firm without being alarmist (UK Parliament Joint Committee on the National Security Strategy, 2025; van Soest *et al.*, 2025).

Additionally, escalation-management pathways for maritime incidents must be clarified and practised. If accidental or inadvertent escalation is a central risk vector, then incident-prevention protocols, communications channels, and decision-support tools should be tested in realistic exercises that include ambiguous CUI events and shadow-fleet activities.

Finally, hybrid deterrence should be explicitly linked to high-end readiness in force-development priorities and command arrangements. Investments in sea surveillance, air and coastal defence, mine warfare, ISR, and modular, resilient platforms serve dual purposes. They are simultaneously enablers of warfighting and signals of resolve in the hybrid domain. Command structures that integrate maritime, cyber, space, and information operations are better placed to control escalation dynamics and respond coherently across the hybrid–high-end continuum (Hoffman, 2007; Lawrence *et al.*, 2025; Renz and Smith, 2016).

Conclusions

In answer to the article's research question, the Baltic record indicates that maritime hybrid coercion is best analysed as the interaction of three processes: material interference with infrastructure and shipping; the exploitation of legal and attributional ambiguity; and narrative contestation over legitimacy, blame, and escalation. NATO, EU, and

regional responses reflect an emerging, although still uneven, adaptation to this environment through increased reliance on surveillance, resilience, and regulatory measures. However, punishment-based deterrence remains constrained by unresolved problems of attribution, intervention authority, and escalation risk.

The central implication for the Baltic security is that deterrence should be judged by the speed and coherence with which states can move from detection to classification, legal action, public explanation, and restoration of service. If any of these stages fails, the coercive value of ambiguity increases. If they are integrated, the expected gains from below-threshold interference decline.

The article, therefore, supports a narrower and more defensible claim than broad formulations of hybrid warfare sometimes allow. The Baltic evidence does not demonstrate an omnipotent or seamless Russian hybrid strategy, nor does it prove that a deliberate Russia–NATO war in the region is imminent. It does, however, show how repeated below-threshold activity can shape readiness, compress decision time, and complicate deterrence in a maritime theatre where commercial and military logics intersect.

Three future scenarios follow from this analysis. In the first, improved surveillance, repair capacity, and legal coordination reduce the benefits of maritime probing and push hostile activity towards less visible information or cyber channels. In the second, continued ambiguity around intervention powers leaves a persistent grey-zone space in which shadow-fleet activity and CUI incidents remain politically disruptive. In the third, a serious incident involving casualties, prolonged service disruption, or a contested boarding operation could accelerate escalation and force NATO, EU, and regional actors to define response thresholds under crisis pressure.

The study is limited by its reliance on public documents and a selection of official statements. It cannot adjudicate classified intelligence, establish responsibility for individual incidents, or exhaust the full range of NATO, EU, and Russian internal deliberations. Future research could extend the analysis through systematic event datasets, elite interviews, legal analysis of intervention authorities at sea, or comparative work across other theatres, such as the North Atlantic, Mediterranean, or Indo-Pacific. Even with those limits, the Baltic case already shows that infrastructure protection, strategic communication, and conventional readiness should be treated as mutually constitutive elements of maritime deterrence.

For policymakers, the most important finding is that maritime deterrence in the Baltic cannot be separated into technical infrastructure protection, legal enforcement, strategic communication, and conventional defence. These functions reinforce one another. A credible posture requires redundancy and repair to deny effects, surveillance, and attribution to reduce ambiguity, legal tools to enable proportionate intervention, and military readiness to prevent an adversary from treating hybrid pressure as strategically risk-free.

Funding

The author received no external funding for this research.

Disclosure Statement

No potential conflict of interest was reported by the author. The author read and agreed to the published version of the manuscript.

Data Availability Statement

This article draws exclusively from publicly available documents and publications; no new datasets were generated.

AI Use Disclosure

Artificial intelligence-assisted tools were used for document formatting. All substantive claims, interpretations, and source selections were reviewed and approved by the author, who is solely responsible for the content.

References

Aitken, J. (2025) *Undersea cables are vulnerable to sabotage, but this takes skill and specialist equipment*, RAND Corporation. Available at: https://www.rand.org/pubs/commentary/2025/07/undersea-cables-are-vulnerable-to-sabotage-but.html (Accessed: 23 December 2025).

Bashfield, S. (2025) 'Defending seabed lines of communication', *Australian Journal of Maritime & Ocean Affairs*, 17(4), pp. 557–569. doi: 10.1080/18366503.2024.2363607.

Brown, E. (2025) *The Baltic Sea at a boil: Connecting the shadow fleet and episodes of subsea infrastructure sabotage*, Carnegie Endowment for International Peace, 5 June. Available at: https://carnegieendowment.org/russia-eurasia/research/2025/06/baltic-russia-maritime-cable-sabotage (Accessed: 9 March 2026).

Bueger, C. and Liebetrau, T. (2021) 'Protecting hidden infrastructure: The security politics of the global submarine data cable network', *Contemporary Security Policy*, 42(3), pp. 391–413. doi: 10.1080/13523260.2021.1907129.

Childs, N. (2025) *Russia's "shadow fleet" and sanctions evasion: What is to be done?*, International Institute for Strategic Studies (Research Paper), 31 January. Available at: https://www.iiss.org/research-paper/2025/01/russias-shadow-fleet-and-sanctions-evasion/ (Accessed: 23 December 2025).

European Commission (2025) *New proposal to strengthen the EU mandatory ship reporting systems*, Directorate-General for Mobility and Transport, 19 February. Available at: https://transport.ec.europa.eu/news-events/news/new-proposal-strengthen-eu-mandatory-ship-reporting-systems-2025-02-19_en (Accessed: 9 March 2026).

European Commission and High Representative of the Union for Foreign Affairs and Security Policy (2024) *Joint statement by the European Commission and the high representative on the investigation into damaged electricity and data cables in the Baltic Sea*. Available at: https://ec.europa.eu/commission/presscorner/detail/en/statement_24_6582 (Accessed: 9 March 2026).

European Commission and High Representative of the Union for Foreign Affairs and Security Policy (2025) Joint communication to the European Parliament and the Council: EU action plan on cable security (JOIN). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025JC0009 (Accessed: 9 March 2026).

European Parliamentary Research Service (2024) *Russia's "shadow fleet": Bringing the threat to light*, Briefing, 14 November. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766242/EPRS_BRI(2024)766242_EN.pdf (Accessed: 23 December 2025).

Govella, K. (2025) 'Undersea cables, geoeconomics, and security in the Indo-Pacific: Risks and resilience', *Marine Policy*, 180, article 106809. doi: 10.1016/j.marpol.2025.106809.

Hoffman, F.G. (2007) *Conflict in the 21st century*: *The rise of hybrid wars*. Arlington, VA: Potomac Institute for Policy Studies.

Hoffman, F.G. (2009) 'Hybrid warfare and challenges', *Joint Force Quarterly*, 52(1), pp. 34–39.

Iskandarov, K. and Gawliczek, P. (2020) 'Hybrid warfare as an instrument of political leverage (with a special focus on the South Caucasus)', in Banasik, M., Gawliczek, P. and Rogozinska, A. (eds.) *The Russian Federation and international security*. Warsaw: Difin, pp. 117–136.

Joint Expeditionary Force (2025) *Public statement from the joint expeditionary force following the recent damage to the Estlink-2 cables*. Available at: https://jefnations.org/2025/01/06/public-statement-from-the-joint-expeditionary-force-following-the-recent-damage-to-the-estlink-2-cables/ (Accessed: 9 March 2026).

Lanoszka, A. (2016) 'Russian hybrid warfare and extended deterrence in Eastern Europe', *International Affairs*, 92(1), pp. 175–195. doi: 10.1111/1468-2346.12509.

Lawrence, T., Granholm, N., Ottosson, B. and Schvede, I. (2025) *Hybrid and high-end warfare in the Baltic Sea region: Safeguarding our maritime domain*, International Centre for Defence and Security, Tallinn. Available at: https://icds.ee/static/icds_policy_paper_hybrid_and_high-end_warfare_lawrence_granholm_ottosson_schvede_september_2025.pdf (Accessed: 23 December 2025).

Lott, A. (2025) 'Conventional jurisdictional approaches to protecting submarine cables and pipelines', *International & Comparative Law Quarterly*, 74(S1), pp. 63–84. doi: 10.1017/S0020589325101164.

Mazarr, M.J. (2015) *Mastering the gray zone: Understanding a changing era of conflict*. Carlisle, PA: Strategic Studies Institute, US Army War College. Available at: https://press.armywarcollege.edu/monographs/428/ (Accessed: 9 March 2026).

Ministry of Foreign Affairs of the Russian Federation (2023) *The concept of the foreign policy of the Russian Federation*. Available at: https://mid.ru/en/foreign_policy/fundamental_documents/1860586/ (Accessed: 23 December 2025).

Ministry of Foreign Affairs of the Russian Federation (2025) *Foreign Ministry spokeswoman Maria Zakharova's answer to a media question about the EU adopting 19th anti-Russia sanctions package*. Available at: https://mid.ru/en/foreign_policy/news/2055614/ (Accessed: 9 March 2026).

Monaghan, A. (2015) 'The "war" in Russia's "hybrid warfare"', *Parameters*, 45(4), pp. 65–74. doi: 10.55540/0031-1723.2987.

North Atlantic Treaty Organization (NATO) (2016) *Warsaw summit communiqué*, 9 July. Available at: https://www.nato.int/cps/en/natohq/official_texts_133169.htm (Accessed: 23 December 2025).

North Atlantic Treaty Organization (NATO) (2024a) *Enlargement and Article 10*. Available at: https://www.nato.int/en/what-we-do/partnerships-and-cooperation/enlargement-and-article-10 (Accessed: 7 March 2026).

North Atlantic Treaty Organization (NATO) (2024b) Countering hybrid threats. Available at: https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats (Accessed: 9 March 2026).

North Atlantic Treaty Organization (NATO) (2025) *NATO launches "Baltic Sentry" to increase critical infrastructure security*, 14 January. Available at: https://www.nato.int/en/news-and-events/articles/news/2025/01/14/nato-launches-baltic-sentry-to-increase-critical-infrastructure-security (Accessed: 9 March 2026).

Ploumis, M. (2022) 'Comprehending and countering hybrid warfare strategies by utilizing the principles of Sun Tzu', *Journal of Balkan and Near Eastern Studies*, 24(2), pp. 344–364. doi: 10.1080/19448953.2021.2006005.

Police of Finland (2024) *Police investigating incidents in the Gulf of Finland in cooperation with other authorities*, 26 December. Available at: https://poliisi.fi/en/-/police-investigating-incidents-in-the-gulf-of-finland-in-cooperation-with-other-authorities (Accessed: 7 May 2026).

Praks, H. (2024) 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. Available at: https://www.hybridcoe.fi/wp-content/uploads/2024/05/20240530-Hybrid-CoE-Working-Paper-32-Russias-hybrid-threat-tactics-WEB.pdf (Accessed: 23 December 2025).

President of the Russian Federation (2023) *Executive order approving Russia's foreign policy concept*. Available at: https://en.special.kremlin.ru/acts/news/70811 (Accessed: 9 March 2026).

Renz, B. and Smith, H. (2016) *Russia and hybrid warfare: Going beyond the label*, Aleksanteri Papers 1/2016. Helsinki: Kikimora Publications. Available at: https://helda.helsinki.fi/items/8ebfa5e9-2c55-42b9-aad2-d8e1aa3d7153 (Accessed: 9 March 2026).

Reuters (2023) *Russia wants U.N. Security Council to ask for Nord Stream blast inquiry*, 17 February. Available at: https://www.reuters.com/world/europe/russia-wants-un-security-council-ask-nordstream-blast-inquiry-2023-02-17/ (Accessed: 7 March 2026).

Rid, T. (2020) *Active measures*: *The secret history of disinformation and political warfare*. London: Profile Books.

Ringbom, H. (2025) 'New threats-old rules: Law of the sea issues raised by suspected attacks on submarine infrastructure in the Baltic Sea', *Ocean Development & International Law*, 56(3), pp. 390–414. doi: 10.1080/00908320.2025.2534621.

Russian Federation (2000a) *Доктрина информационной безопасности Российской Федерации* [*Doctrine of information security of the Russian Federation*], official Russian text. Available at: https://pravo.gov.ru/proxy/ips/?backlink=1&docbody=&nd=102161033&prevDoc=102025035 (Accessed: 16 March 2026).

Russian Federation (2000b) *Information security doctrine of the Russian Federation*, unofficial English translation (archival web reproduction). Available at: https://publicintelligence.net/ru-information-security-2000/ (Accessed: 16 March 2026).

Russian Federation (2016a) *Doctrine of information security of the Russian Federation*, official English version. Available at: https://www.scrf.gov.ru/security/information/DIB_engl/ (Accessed: 16 March 2026).

Russian Federation (2016b) Доктрина информационной безопасности Российской Федерации [*Doctrine of information security of the Russian Federation*], official Russian text, approved by Presidential Decree No. 646 of 5 December 2016. Available at: https://publication.pravo.gov.ru/document/view/0001201612060002 (Accessed: 16 March 2026).

UK Government (2025) *Joint expeditionary force activates UK-led reaction system to track threats to undersea infrastructure and monitor Russian shadow fleet*, 6 January. Available at: https://www.gov.uk/government/news/joint-expeditionary-force-activates-uk-led-reaction-system-to-track-threats-to-undersea-infrastructure-and-monitor-russian-shadow-fleet (Accessed: 9 March 2026).

UK Parliament Joint Committee on the National Security Strategy (2025) *Subsea telecommunications cables: Resilience and crisis preparedness*. London: House of Commons. Available at: https://publications.parliament.uk/pa/jt5901/jtselect/jtnatsec/723/report.html (Accessed: 23 December 2025).

United Nations (2023) *"Avoid speculation" about responsibility for 2022 Nord Stream pipeline explosions, speakers tell Security Council amid calls for transparent investigation* (SC/15206). Available at: https://press.un.org/en/2023/sc15206.doc.htm (Accessed: 7 March 2026).

Van Soest, H., Black, J., Fine, H. and Retter, L. (2025) Evolving threats to critical undersea infrastructure: Implications for European security and resilience. Santa Monica, CA: RAND Corporation, PE-A3800-1. doi: 10.7249/PEA3800-1.