SABOTAGE OF SUBMARINE CRITICAL INFRASTRUCTURE (CABLES AND PIPELINES) IN THE BALTIC SEA, 2023–2025: THE ATTRIBUTION PROBLEM AND LEGAL GREY-ZONE GAPS

Mpho Khumalo

University of South Africa
Pretoria, Republic of South Africa
E-mail: mpho.khumalo@mylife.unisa.ac.za

Review Scientific Article

Received: 22.03.2026. Approved: 05.04.2026.

DOI: https://doi.org/10.65932/military-studies-2026-1-6
UDC: 327.88:351.86(261.24)"2023/2025"

Abstract: Between October 2023 and early 2025 the Baltic Sea experienced a sequence of damaging incidents to submarine telecommunications cables and energy pipelines, from the Balticconnector gas pipeline and adjacent data cables to the C-Lion1, Estlink 2, and related cable breaks, most of them attributed in public debate to anchor-dragging by vessels linked to a sanctioned shadow fleet. This review synthesises the peer-reviewed literature published between 2019 and 2026 on three questions raised by these events: why the infrastructure is so vulnerable, why responsibility is so hard to attribute, and why international law struggles to prevent or sanction such acts beyond the territorial sea. A semi-systematic, thematic review method was applied across Scopus, Web of Science, and Crossref, supplemented by primary legal instruments and European Union and NATO documents, yielding forty-seven sources synthesised into four domains: the threat landscape, the attribution problem, the legal grey-zone gaps, and the emerging response. The review's contribution is an integrative attribution–accountability gap framework that joins three literatures usually kept apart, the maritime-infrastructure-security, the grey-zone and attribution, and the law-of-the-sea literatures, and traces a four-link chain from detection to attribution to legal characterisation to response, showing that Baltic subsea sabotage occupies a doubly permissive space in which an act is simultaneously hard to attribute and hard to sanction. The synthesis finds that physical vulnerability is structural and growing, that deniability is the deliberate design feature of grey-zone action rather than an incidental difficulty, that the United Nations Convention on the Law of the Sea protects the laying of cables and pipelines far better than it protects them from intentional harm, and that the institutional response is real but immature. The review concludes that closing the accountability gap depends less on new technology than on strengthened coastal-state jurisdiction, evidentiary cooperation, and a resilience-by-design posture, and it identifies the absence of an agreed legal threshold for sabotage below the use of force as the field's central unresolved problem.

Keywords: *submarine cables, subsea pipelines, critical maritime infrastructure, grey-zone, attribution, UNCLOS, Baltic Sea security.*

INTRODUCTION

The seabed is the unseen floor of modern life. Roughly the entire intercontinental internet, the bulk of cross-border financial messaging, and a growing share of European energy move through cables and pipelines laid on or beneath it, and almost none of that

Military Studies: Journal for Strategy, Technology and Defence Sciences, Year 2026, Volume: 4, Issue: 1, Serial number: 5, p. 87 – 101.

infrastructure was designed to survive deliberate attack. For most of its history this exposure did not matter much, because the cost of reaching the seabed deterred all but states and the few states able to reach it had little reason to cut the lines they also depended upon. The Baltic Sea between October 2023 and early 2025 showed how thoroughly that calculus has changed. A run of incidents, beginning with simultaneous damage to the Balticconnector pipeline and nearby communications cables and continuing through the severing of the C-Lion1 and Estlink 2 connections and several other cables, demonstrated that subsea infrastructure can now be damaged repeatedly, cheaply, and with a degree of deniability that leaves victim states unsure whether they have suffered an accident, a provocation, or an act of war (Ringbom, 2025; Neal, 2026).

These events did not arrive without warning. The destruction of the Nord Stream pipelines in September 2022 had already exposed how a single covert act against subsea energy infrastructure could inflict strategic damage while resisting confident attribution (Sun, 2025; Gülcan & Erginer, 2023), and the academic security-politics literature had been arguing for some years that the hidden, distributed, and jurisdictionally awkward character of submarine cables made them an ideal target for coercion below the threshold of war (Bueger & Liebetrau, 2021). What the Baltic incident wave added was repetition and pattern, turning a shocking anomaly into a recognisable mode of pressure and forcing the questions this review addresses out of the seminar room and into the operations centres of coastal states.

The difficulty is that the evidence and analysis needed to understand the phenomenon are dispersed across three scholarly communities that rarely cite one another. The maritime-infrastructure-security literature explains the physical and strategic vulnerability of cables and pipelines and the governance of their protection; the security-studies literature on grey-zone conflict and the attribution problem explains why responsibility for such acts is so hard to establish and why that difficulty is exploited deliberately; and the international-law literature explains why the United Nations Convention on the Law of the Sea and the law of state responsibility offer such thin protection against intentional damage in the exclusive economic zone and on the high seas. A reader who consults only one of the three sees only a third of the problem.

This review is organised around four questions that span the three communities. The first asks what makes Baltic submarine cables and pipelines so vulnerable, and what the 2023–2025 incident wave reveals about the threat. The second asks why attribution of subsea sabotage is so difficult, and how grey-zone and deniability dynamics exploit that difficulty. The third asks what gaps in the law of the sea and in the law of state responsibility impede prevention, response, and accountability beyond the territorial sea. The fourth asks what governance, detection, resilience, and deterrence responses are emerging, and how adequate they are.

The contribution of this review is integrative rather than empirical. It proposes an attribution–accountability gap framework that connects the three literatures and traces a four-link causal chain, from detection of an incident, to technical and political attribution of responsibility, to the legal characterisation of the act, to the available response and accountability, showing that each link can fail and that Baltic subsea sabotage exploits the failure of several at once. The framework's claim is that the infrastructure sits in a doubly permissive space, technically hard to attribute and legally hard to sanction, and that this conjunction, not either difficulty alone, is what makes the seabed an attractive arena for grey-zone coercion. The framework is offered as an organising instrument for a fragmented field, which is the proper ambition of a review, and not as a new empirical finding.

The article proceeds as follows. The next section positions the review and states its

method. A results section presents the thematic synthesis and the framework. Four analytical sections then develop the domains in turn, treating the threat landscape, the attribution problem, the legal grey-zone gaps, and the emerging response. A conclusion answers the four questions, states the review's limitations, and identifies what the field still needs to resolve.

LITERATURE REVIEW AND METHODOLOGY

Literature Review

The maritime-infrastructure-security literature is the first of the three the review draws together, and it has matured quickly under the pressure of events. Its agenda was set by the argument that the global submarine cable network is a form of hidden infrastructure whose very invisibility shapes the politics of its protection (Bueger & Liebetrau, 2021), and it has since produced a conceptual programme for critical maritime infrastructure protection that asks what, precisely, is to be protected and by whom (Bueger & Liebetrau, 2023), together with proposals for coordinating that protection across the maritime-security, cybersecurity, and counter-piracy domains (Liebetrau & Bueger, 2024). Onto this governance core a rapidly expanding applied literature has been grafted: comparative analysis of cable risk and resilience from the physical seabed up to geopolitics (Cannon et al., 2026), regional studies of the security gap in cable protection (Cannon, 2025; Davenport, 2025), assessment of the novel threat posed by uncrewed undersea vehicles (Rossiter, 2025), and engineering studies of how anchors and dropped objects actually damage subsea pipelines (Zhou et al., 2025; Zeng et al., 2025).

The second literature concerns grey-zone conflict and the attribution problem, and it supplies the strategic logic that the infrastructure literature describes only at its edges. Historical and conceptual treatments locate grey-zone action in a long tradition of coercion below the threshold of war while cautioning against the analytical looseness of the hybrid-warfare label (Hughes, 2020; Libiseller, 2023; Janičatová & Mlejnková, 2021), and a distinct body of work theorises the deniability that is the technique's defining feature, asking when plausible deniability works and why states neither confirm nor deny responsibility for covert acts (Poznansky, 2020; Brown & Fazal, 2021; Pischedda & Cheon, 2023). Sabotage has lately been brought back into the centre of this discussion as a deliberate instrument of statecraft rather than a marginal nuisance (Rovner et al., 2025; Lindsay, 2025), and the deterrence side has been examined through the difficulty of deterring sub-conventional and below-threshold interference (Halas, 2022; Bergaust & Sellevåg, 2024).

The third literature is the law of the sea and of state responsibility, and it is where the protection deficit is most precisely diagnosed. Several recent studies address the Baltic and Nord Stream incidents directly, analysing the law-of-the-sea issues raised by suspected attacks on submarine infrastructure (Ringbom, 2025), coastal-state jurisdiction over acts against transiting pipelines in the exclusive economic zone and on the continental shelf (Sun, 2025), and the conventional jurisdictional approaches available to protect cables and pipelines together with their limits (Lott, 2025). A broader body treats the underlying regime, including the coastal-state obligation not to impede pipelines on the continental shelf (Kamiński & Szewczyk, 2022), the protection of cables under investment law (Yang, 2021), and the use of grey-zone lawfare around passage and operational rights (McLaughlin, 2024), while the attribution side is supplied by the international-law scholarship on due diligence as a secondary rule and on the patchwork of protective obligations that govern responsibility for harm (Mackenzie-Gray Scott, 2021; Coco & de Souza Dias, 2021).

The gap this review addresses is the absence of any synthesis that joins the three. Each community analyses one face of the

problem with sophistication, yet the phenomenon of Baltic subsea sabotage is constituted precisely by their intersection, in which a physically vulnerable target is struck by a deniable act that the law cannot easily characterise or sanction. The attribution–accountability gap framework introduced here is the device by which the three faces are brought into a single view.

Research Methodology

This article is a semi-systematic, thematic literature review rather than a meta-analysis or a fully protocolised systematic review, and the choice follows from the subject: the relevant evidence spans engineering studies, security-studies theory, doctrinal legal analysis, and primary legal instruments, a heterogeneity that makes quantitative pooling impossible and thematic synthesis appropriate. The search drew on Scopus, Web of Science, and Crossref, supplemented by targeted retrieval of primary legal instruments and of European Union and NATO documents. Search terms combined an infrastructure set, including submarine cable, subsea pipeline, critical maritime infrastructure, and seabed warfare, with a security-and-law set, including grey zone, hybrid threat, attribution, sabotage, UNCLOS, state responsibility, and Baltic Sea, joined by Boolean operators, and the reference lists of the most central sources were hand-searched for further leads.

Inclusion criteria were peer-reviewed journal articles published between 2019 and 2026, written in English, and addressing at least one of the four domains; primary legal instruments and intergovernmental documents were admitted separately as primary sources of the legal and institutional context, with treaties cited at their year of adoption as an explicit exception to the recency rule. Exclusion criteria removed non-peer-reviewed commentary, think-tank and grey-literature reports, and non-indexed or predatory outlets, except where an intergovernmental document was itself the object of analysis. Screening prioritised Scopus-indexed venues, and of the forty-seven sources retained, thirty-nine are peer-reviewed articles in Scopus-indexed journals and the remaining eight are primary legal instruments and European Union or NATO documents. Table 1 records the criteria and counts. I want to be candid that the search was not exhaustive in the PRISMA sense, without dual independent screening or formal risk-of-bias appraisal, so the review should be read as a structured narrative synthesis.

Parameter	**Specification**
Databases	Scopus, Web of Science, Crossref (+ UNCLOS, ILC, EU, NATO documents)
Period	2019–2026 (treaties/legal instruments cited at adoption year)
Language	English
Source types	Peer-reviewed articles; primary legal instruments; EU/NATO documents
Synthesis	Thematic synthesis into four domains; attribution–accountability gap framework
Sources retained	47 total; 39 in Scopus-indexed journals

Table 1. Search and selection summary for the semi-systematic review.

Synthesis proceeded by coding each source to one or more of four domains that emerged inductively and were then used to organise the material: the threat landscape, the attribution problem, the legal grey-zone gaps, and the emerging response. Within and across these domains the analysis traced the four-link chain, detection, attribution, legal characterisation, and response, that constitutes the framework, asking at each link what

the literature shows can go wrong and how the Baltic incidents illustrate it. The incidents themselves are treated as the documented empirical backdrop discussed by the legal and security sources rather than as objects of independent fact-finding, since this is a review of the scholarship and not an investigation of the events.

RESEARCH RESULTS

The thematic synthesis produced four domains and one organising framework. The domains are uneven in their evidentiary maturity, and that unevenness is itself a result worth stating before the framework is presented. The legal domain is the best developed for the Baltic specifically, because several 2024–2025 articles analyse the incidents and the Nord Stream precedent directly (Ringbom, 2025; Sun, 2025; Lott, 2025). The attribution domain is supported by a mature theoretical literature on deniability that predates the incidents but maps onto them precisely (Poznansky, 2020; Brown & Fazal, 2021). The threat-landscape domain is broad but globally rather than Baltic-focused, drawing heavily on cable-security studies from other regions (Cannon, 2025; Davenport, 2025). The response domain is the most provisional, because the institutions are new and the peer-reviewed evaluation of them is only beginning (Liebetrau & Bueger, 2024; Becker, 2025).

The framework that organises these domains is the four-link attribution–accountability chain set out in Table 2. Each link is a point at which the conversion of a seabed incident into accountability can fail: detection may be late or ambiguous; attribution may be technically or politically unattainable; legal characterisation may fall into a gap between accident, tort, and armed attack; and response may be foreclosed by jurisdictional limits even when responsibility is morally clear. The central result of the synthesis is that Baltic subsea sabotage does not exploit a single weak link but the compounding of several, so that an act can be detected yet unattributable, or attributed yet uncharacterisable, or characterised yet unsanctionable, and the attacker needs only one link to hold to escape accountability while the defender needs all four.

Link	Failure mode	Representative evidence
1. Detection	Late, ambiguous, or accident-indistinguishable damage signatures	Gülcan & Erginer (2023); Liang et al. (2024); Qi et al. (2026)
2. Attribution	Deniability by design; proxy/shadow-fleet vessels; evidentiary thresholds	Poznansky (2020); Brown & Fazal (2021); Rovner et al. (2025)
3. Legal characterisation	No agreed threshold between accident, tort, and use of force	Ringbom (2025); Lott (2025); McLaughlin (2024)
4. Response / accountability	Jurisdiction thin beyond territorial sea; weak enforcement	Sun (2025); Kamiński & Szewczyk (2022); Becker (2025)

Table 2. The attribution–accountability gap framework: four links from incident to accountability, the failure mode at each, and representative evidence.

A second result, cutting across the four links, concerns the role of the shadow fleet and the anchor as the signature method of the Baltic wave. The recurrence of damage caused by vessels dragging anchors across cable and pipeline corridors, rather than by sophisticated covert means, is consequential precisely because it sits at the boundary of every link: an anchor drag is hard to distinguish from negligence at detection, supplies

built-in deniability at attribution, resists characterisation as an armed attack at the legal link, and is committed by flag-of-convenience vessels that complicate enforcement at the response link (Ringbom, 2025; Lott, 2025; Zhou et al., 2025). The crudeness of the method is not a sign of limited capability; it is the optimisation of the method to the gaps the framework identifies, and the analytical sections develop that argument.

THE THREAT LANDSCAPE: PHYSICAL VULNERABILITY AND THE BALTIC INCIDENT WAVE

The first domain establishes that the vulnerability is structural rather than incidental. Submarine cables and pipelines are laid, by physical necessity, in long, thin, fixed, and mapped corridors, and they cannot be hardened along their length or moved when threatened, so the protection problem is qualitatively different from that of a discrete installation (Bueger & Liebetrau, 2021). The infrastructure-security literature has formalised this into a programme of critical maritime infrastructure protection that begins by asking what is even meant by protecting a distributed, partly private, partly hidden network whose ownership and jurisdiction change along its route (Bueger & Liebetrau, 2023). The applied studies then quantify the exposure: cable-risk mapping that integrates seabed bathymetry with geopolitics to rank corridors by vulnerability (Cannon et al., 2026), regional analyses of the security gap between the value of cables and the means available to protect them (Cannon, 2025; Davenport, 2025), and assessments of an emerging threat vector in the form of uncrewed undersea vehicles able to reach and manipulate the seabed at low cost (Rossiter, 2025).

The engineering literature supplies the mechanism by which the abstract vulnerability becomes a severed line. Numerical studies of subsea pipelines subjected to anchor impact and dragging show how readily a dragged anchor concentrates damaging force on a pipeline, and how the damage scales with anchor mass and drag geometry (Zhou et al., 2025), while reliability modelling that treats dropped-object impact and corrosion as competing failure processes quantifies how external mechanical insult interacts with the slow degradation of an ageing asset (Zeng et al., 2025; Yazdi et al., 2022). For cables the insult need not even be large, since a comparatively light anchor can shear a communications cable, and the same studies that map cable risk emphasise that the energy required to cause strategically significant damage is trivial relative to the value destroyed (Cannon et al., 2026). The physical asymmetry between the cost of attack and the cost of consequence is the material foundation of the whole problem.

That asymmetry is amplified by interdependence. The resilience literature shows that energy and telecommunications infrastructures are coupled, so that damage to one cascades into the other and a localised seabed incident can propagate into disproportionate systemic effect (Alkhaleel, 2024; Tong et al., 2025). The Baltic is a particularly concentrated instance of this coupling, with electricity interconnectors, gas pipelines, and data cables sharing a small, shallow, and heavily trafficked sea, so that the same corridor may carry several critical functions and a single anchor may sever more than one (Becker, 2025). The Nord Stream destruction and the situational-awareness gaps it exposed had already demonstrated that the maritime picture over such corridors was far thinner than the value passing through them warranted (Gülcan & Erginer, 2023), and the Baltic incident wave of 2023–2025 confirmed that the corridors remained, in practice, undefended along most of their length (Ringbom, 2025).

A specific maritime phenomenon ties these vulnerabilities to a method: the so-called shadow fleet of ageing, opaquely owned, and often inadequately insured tankers that proliferated to move sanctioned oil and that has become the vehicle of choice for anchor-dragging incidents. Such vessels are

attractive instruments precisely because their flag, ownership, and insurance are deliberately obscured, so that a ship found to have dragged its anchor across a corridor offers little upward inference about sponsorship, and because their presence in Baltic shipping lanes is unremarkable until the moment damage occurs (Rossiter, 2025; Becker, 2025). The detection literature treats them as the central object of maritime-domain awareness, since the behaviours that betray a deliberate drag, loitering over a corridor, anomalous speed, and a track that deviates onto the cable route, are exactly the anomalies that vessel-tracking analytics are now trained to flag (Liang et al., 2024; Qi et al., 2026). The shadow fleet is thus not a peripheral detail but the operational embodiment of the threat landscape, converting structural vulnerability into repeatable incident.

The incident wave thus reads less as a series of accidents than as the exploitation of a known and documented exposure. Whether each specific event was deliberate is a question the legal sources treat with appropriate caution, since an anchor drag is genuinely ambiguous, but the pattern, repeated damage to high-value corridors by vessels behaving anomalously, is exactly what the threat-landscape literature had predicted would become attractive once the deterrent of difficulty fell away (Bueger & Liebetrau, 2021; Rossiter, 2025). The threat landscape, in short, is one in which the target is fixed and exposed, the method is cheap and ambiguous, and the consequence is systemic, and that combination is the precondition for everything the subsequent domains describe.

THE ATTRIBUTION PROBLEM: DENIABILITY, AMBIGUITY, AND THE GREY ZONE

The second domain explains why a detected incident so rarely becomes an attributed one. The security-studies literature is clear that grey-zone action is not a new category of conflict but the deliberate operation of coercion in the space below the threshold that would trigger a decisive response, and that ambiguity is its organising principle rather than a by-product (Hughes, 2020; Janičatová & Mlejnková, 2021). The hybrid-warfare label is criticised within that literature for analytical looseness, and the criticism matters here because it warns against treating every ambiguous seabed incident as proof of a coordinated campaign, a caution the legal sources echo (Libiseller, 2023). What the literature does establish firmly is that deniability is engineered: the actor chooses methods, proxies, and timing precisely so that responsibility cannot be fixed to the standard a forceful response would require.

The deniability scholarship gives this its sharpest form. Plausible deniability is theorised not as the actor's hope of escaping suspicion, which is usually futile, but as the manipulation of the gap between what is suspected and what can be proven to a political or legal standard (Poznansky, 2020). The finding that states routinely neither confirm nor deny responsibility for covert operations explains the otherwise puzzling behaviour around subsea incidents, in which a suspected sponsor stays silent and a victim cannot move from suspicion to attribution without evidence it does not possess (Brown & Fazal, 2021). The recent assessment of whether deniability actually works, drawing on unclaimed coercive acts in the Ukraine war, suggests that the technique succeeds less by convincing anyone of innocence than by denying the target the certainty needed to retaliate proportionately (Pischedda & Cheon, 2023). Applied to the Baltic, the implication is that the attacker's goal is not to be believed innocent but to keep the victim below the evidentiary threshold for a response.

Sabotage is the form of grey-zone action best suited to this purpose, and the literature has lately restored it to prominence. The argument that sabotage is a recurring instrument of statecraft, valuable precisely because it inflicts cost while supplying deniability, reframes the Baltic incidents as a contemporary

instance of a durable technique rather than as a novelty (Rovner et al., 2025), and the re-examination of landmark covert operations shows how sabotage has migrated from cyber means back toward physical effect when physical effect is harder to attribute (Lindsay, 2025). The shadow fleet completes the picture: by routing damage through flag-of-convenience vessels with opaque ownership, the sponsor inserts a layer of deniable agency between itself and the act, so that even a vessel caught dragging its anchor across a cable supplies only a weak inference about who, if anyone, directed it (Rovner et al., 2025; Ringbom, 2025).

The attribution problem therefore has technical, evidentiary, and political layers that compound. Technically, the seabed is poorly observed and an anchor drag leaves an ambiguous signature, a gap the maritime-domain-awareness literature is trying to close with automated anomaly detection from vessel-tracking data (Liang et al., 2024; Qi et al., 2026). Evidentially, even good tracking data establishes that a vessel was present and behaving oddly, not that it acted on instruction, which is the proposition a response would need to rest on. Politically, the victim faces the deniability calculus directly, weighing the cost of acting on incomplete attribution against the cost of letting the act pass. The international-law scholarship on due diligence offers a partial way through, by shifting some of the burden onto the state from whose vessels or territory the harm emanates, but it does so at the level of secondary rules whose application to deniable seabed acts remains contested (Mackenzie-Gray Scott, 2021; Coco & de Souza Dias, 2021). Attribution, in sum, fails not at one layer but across all three, which is why the framework treats it as the pivotal link.

LEGAL GREY-ZONE GAPS: UNCLOS, JURISDICTION, AND STATE RESPONSIBILITY

The third domain locates the gaps in the law itself, and the legal literature is unusually candid that they are real. The United Nations Convention on the Law of the Sea was built to guarantee the freedom to lay submarine cables and pipelines, not to protect them from those who would deliberately cut them, and its architecture reflects that origin (United Nations, 1982). On the high seas and in the exclusive economic zone the freedom to lay cables and pipelines is strongly protected, yet the Convention's provisions on breaking or injuring them, inherited in substance from the nineteenth-century cable-protection regime, impose obligations chiefly on the flag states of offending vessels and address the negligent cable-cutter far better than the state-sponsored saboteur (United Nations, 1982; Convention for the Protection of Submarine Telegraph Cables, 1884). The most direct recent analyses of the Baltic incidents conclude that the rules are not so much absent as mismatched, old rules confronting a new threat they were not designed to meet (Ringbom, 2025).

Jurisdiction is the crux. Because most of the damaged Baltic infrastructure lies in the exclusive economic zone or on the continental shelf rather than in the territorial sea, the coastal state's enforcement powers are sharply constrained, and the analyses of coastal-state jurisdiction over acts against transiting pipelines show how narrow the lawful options are between the strong protection the Convention gives to laying and the weak protection it gives against harm (Sun, 2025; Lott, 2025). The coastal state's own obligations compound the asymmetry, since it is required not to impede the laying or maintenance of pipelines on its continental shelf even as it lacks clear authority to act against a vessel that damages them (Kamiński & Szewczyk, 2022). Scholars have explored adjacent regimes to fill the gap, including the

protection of cables under international investment law (Yang, 2021), but these are partial and indirect, and the systematic treatment of conventional jurisdictional approaches concludes that each available basis, flag-state, coastal-state, and nationality jurisdiction, leaves a remainder that the deniable saboteur can occupy (Lott, 2025).

The law of state responsibility is the second legal layer, and it is where attribution and accountability formally meet. The codified secondary rules on attribution and state responsibility (International Law Commission, 2001), elaborated by the scholarship on due diligence, in principle allow a state to be held responsible for harm emanating from its territory or agents, including a failure to exercise due diligence over vessels it could control, and this is the doctrinal route most likely to bear weight against deniable seabed acts (Mackenzie-Gray Scott, 2021; Coco & de Souza Dias, 2021). Yet the route is demanding: it requires attribution to a sufficient legal standard, which the previous section showed is exactly what deniability denies, and it offers remedies that are slow and contested where the victim seeks deterrence rather than eventual reparation. The grey-zone use of the law itself, in which an actor exploits the rules on passage and operational rights to cloak hostile activity in legal form, adds a further twist that the lawfare literature has begun to map (McLaughlin, 2024).

The legal domain therefore confirms the framework's third link with precision. The act of cutting a Baltic cable or pipeline falls into a characterisation gap: it is plainly not a mere accident when the pattern is considered, yet it is difficult to characterise as an armed attack that would justify forceful response, and the categories between, internationally wrongful act, breach of due diligence, criminal damage under domestic law applied extraterritorially, fit awkwardly and carry weak enforcement (Ringbom, 2025; Sun, 2025; Lott, 2025). The absence of an agreed threshold for sabotage below the use of force is not a technicality; it is the legal expression of the same permissive space the strategic literature describes, and closing it is, on the evidence reviewed, the central unresolved problem of the field.

RESPONSES: GOVERNANCE, DETECTION, RESILIENCE, AND DETERRENCE

The fourth domain surveys what is being done, and the honest assessment is that the response is real, accelerating, and still immature. At the governance level the European Union has moved to strengthen the resilience of critical entities and network systems through its critical-entities-resilience and network-and-information-security legislation (European Union, 2022a; European Union, 2022b), and comparative analysis of how Baltic states have transposed that legislation shows both genuine progress and uneven implementation across the region (Becker, 2025). NATO has responded institutionally, raising the protection of undersea infrastructure to alliance priority and standing up coordinating bodies for it (NATO, 2023), and the EU and NATO have created a joint task force on the resilience of critical infrastructure that treats subsea assets as a shared concern (European Union & NATO, 2023). The maritime-security scholarship welcomes this turn while warning that coordination across the maritime, cyber, and energy domains remains the binding constraint, as the lessons drawn from piracy and cybersecurity governance suggest (Liebetrau & Bueger, 2024; Bueger & Liebetrau, 2023).

Detection is the technical front, and it is advancing fastest. Because the seabed cannot be watched directly along its length, surveillance concentrates on the vessels above it, and the maritime-domain-awareness literature has produced unsupervised and dual-modality methods for detecting anomalous vessel behaviour from automatic-identification-system data, precisely the loitering, deviation, and speed signatures that an anchor-dragging sabotage would produce (Liang et

al., 2024; Qi et al., 2026). The situational-awareness gap exposed by Nord Stream has narrowed as states fuse vessel-tracking, sensor, and patrol data over critical corridors (Gülcan & Erginer, 2023), and physical-protection frameworks developed for offshore installations such as wind farms offer transferable methods for prioritising scarce protective resources along cable and pipeline routes (Tecklenburg et al., 2025). Detection cannot by itself solve the attribution problem, since establishing presence is not establishing direction, but it raises the cost of deniability by making anomalous behaviour visible and recorded.

Resilience is the response that does not depend on solving attribution at all, and the reviewed evidence increasingly favours it. If a severed cable can be rerouted and a damaged pipeline bypassed quickly enough, the strategic value of cutting it falls, and the interdependence literature that diagnoses the cascade risk also points toward the redundancy, route diversity, and rapid-repair capacity that blunt it (Alkhaleel, 2024; Tong et al., 2025). For the Baltic specifically, resilience means denser interconnection so that no single corridor is decisive, pre-positioned repair capability so that downtime is short, and the treatment of subsea infrastructure as a system to be kept functioning under attack rather than as a set of assets to be perfectly defended (Becker, 2025; Bueger & Liebetrau, 2023). Resilience reframes the contest from prevention, which the legal and attribution gaps make unreliable, to endurance, which the defender can control.

Between detection and resilience sits the underrated link of evidentiary cooperation, which the synthesis suggests may matter more than any single technology. Because attribution fails at the political and evidentiary layers as much as the technical one, the value of a detection is realised only if Baltic states share vessel-tracking, sensor, and forensic data quickly enough to build a common picture before a suspect vessel leaves the region, and the comparative study of how the littoral states have implemented European resilience legislation finds that this cross-border coordination, rather than national capability alone, is the binding constraint (Becker, 2025; Liebetrau & Bueger, 2024). The experience of smaller states with thin maritime-security capacity shows how easily an incident in one jurisdiction becomes unprosecutable once the vessel and its evidence move into another (McCabe & Flynn, 2023). Strengthening the machinery for joint investigation, including agreed procedures for boarding, evidence preservation, and the exchange of intelligence, addresses the response link directly, and it does so without requiring the elusive agreement on a new legal threshold, which is why several analyses treat evidentiary cooperation as the most actionable near-term measure (Ringbom, 2025; Becker, 2025).

Deterrence is the hardest response, because it runs directly into the attribution and legal gaps the framework identifies. The sub-conventional-deterrence literature shows how difficult it is to deter acts that are designed to stay below the threshold of a forceful response, since the deniability that protects the attacker also denies the defender the justification to punish (Halas, 2022; Bergaust & Sellevåg, 2024). Recent assessments of NATO's posture in the Baltic argue for rebalancing toward exactly this problem, treating below-threshold interference with infrastructure as a core rather than a peripheral mission and accepting that deterrence here will rest more on denial and resilience than on the threat of retaliation (Gioe et al., 2025; Duenow, 2025). The smaller coastal states, whose maritime-security capacity is often thin, face this most acutely, and the study of one such state's struggle to govern its subsea infrastructure shows how far institutional capacity lags the threat (McCabe & Flynn, 2023). The response domain, taken together, suggests a realistic strategy that concedes the difficulty of prevention and deterrence and invests instead in detection that raises the cost of deniability and resilience that lowers the value of success.

CONCLUSION

The Baltic seabed has become a theatre in which the strengths of the modern interconnected economy are turned into vulnerabilities, and the 2023–2025 incident wave made plain that the lines on the seabed can be cut faster than the law, the institutions, or the analysis can keep up. This review set out to assemble the dispersed evidence into one account and to answer four questions about why this is so.

On the first question, the threat landscape is structurally permissive: the infrastructure is fixed, exposed, and interdependent, the method of attack is cheap and ambiguous, and the consequence is systemic, a combination the maritime-infrastructure-security literature had anticipated and the incident wave confirmed (Bueger & Liebetrau, 2021; Cannon et al., 2026; Ringbom, 2025). On the second, attribution fails not at a single layer but across the technical, evidentiary, and political layers at once, because deniability is the engineered core of grey-zone action rather than an incidental difficulty, and the shadow fleet supplies a ready layer of deniable agency (Poznansky, 2020; Brown & Fazal, 2021; Rovner et al., 2025).

On the third question, the law of the sea protects the laying of cables and pipelines far better than it protects them from intentional harm, coastal-state jurisdiction is thin in the exclusive economic zone and on the continental shelf where most of the damage occurs, and the law of state responsibility offers a doctrinally available but practically demanding route that founders on the same attribution problem; the absence of an agreed threshold for sabotage below the use of force is the central legal gap (Ringbom, 2025; Sun, 2025; Lott, 2025). On the fourth, the response is real but immature, with European Union and NATO governance advancing, detection improving fastest, resilience emerging as the most controllable lever, and deterrence remaining the hardest because it collides directly with the attribution and legal gaps (Becker, 2025; Liebetrau & Bueger, 2024; Gioe et al., 2025).

The principal contribution of this review is the attribution–accountability gap framework that connects the maritime-infrastructure-security, the grey-zone and attribution, and the law-of-the-sea literatures and traces the four-link chain from detection to attribution to legal characterisation to response. The framework's value is integrative: it shows that Baltic subsea sabotage succeeds not by defeating any single defence but by exploiting the compounding of weak links, so that the attacker needs only one to hold while the defender needs all four, and it thereby explains why crude methods such as anchor-dragging are not a sign of limited capability but an optimisation to the gaps. That is the legitimate ambition of a review, to give a fragmented field an organising structure, and it is the one pursued here.

The review's limitations are real and bound its claims. The threat-landscape evidence is drawn substantially from cable-security studies of other regions and applied imperfectly to the Baltic; the response domain rests on institutions too new for mature peer-reviewed evaluation; the method was a structured narrative synthesis rather than a protocolised systematic review, without dual screening or formal bias appraisal; and the review deliberately refrains from independent fact-finding about the incidents, relying instead on the legal and security scholarship that analyses them, so its account of any specific event is only as firm as those sources. These boundaries point to what the field most needs next: an agreed legal threshold distinguishing sabotage from accident and from armed attack; empirical study of whether strengthened detection actually raises the cost of deniability; and comparative evaluation of which resilience investments most reduce the strategic value of an attack. Until that work is done, the safest reading is that closing the accountability gap depends less on new technology than on strengthened coastal-state jurisdiction, deeper evidentiary

cooperation among the Baltic states, and a resilience-by-design posture that makes the seabed less worth attacking in the first place.

BIBLIOGRAPHY

Alkhaleel, B. A. (2024). Machine learning applications in the resilience of interdependent critical infrastructure systems—A systematic literature review. *International Journal of Critical Infrastructure Protection, 44*, 100646. https://doi.org/10.1016/j.ijcip.2023.100646

Becker, M. (2025). Transposing EU-legislation on critical infrastructure protection: Legal implementation performance in the Baltic Sea region. *International Journal of Critical Infrastructure Protection, 50*, 100781. https://doi.org/10.1016/j.ijcip.2025.100781

Bergaust, J. C., & Sellevåg, S. R. (2024). Improved conceptualising of hybrid interference below the threshold of armed conflict. *European Security, 33*(2), 169–195. https://doi.org/10.1080/09662839.2023.2267478

Brown, J. M., & Fazal, T. M. (2021). #SorryNotSorry: Why states neither confirm nor deny responsibility for cyber operations. *European Journal of International Security, 6*(4), 401–417. https://doi.org/10.1017/eis.2021.18

Bueger, C., & Liebetrau, T. (2021). Protecting hidden infrastructure: The security politics of the global submarine data cable network. *Contemporary Security Policy, 42*(3), 391–413. https://doi.org/10.1080/13523260.2021.1907129

Bueger, C., & Liebetrau, T. (2023). Critical maritime infrastructure protection: What's the trouble? *Marine Policy, 155*, 105772. https://doi.org/10.1016/j.marpol.2023.105772

Cannon, B. J. (2025). Undersea cable security in the Indo-Pacific: Enhancing the Quad's collaborative approach. *Marine Policy, 171*, 106415. https://doi.org/10.1016/j.marpol.2024.106415

Cannon, B. J., Matsuo, K., & Matsuda, M. (2026). Mapping undersea cable risk from bathymetry to geopolitics: Evidence-based rankings and tailored resilience strategies. *Marine Policy, 186*, 107012. https://doi.org/10.1016/j.marpol.2025.107012

Coco, A., & de Souza Dias, T. (2021). 'Cyber due diligence': A patchwork of protective obligations in international law. *European Journal of International Law, 32*(3), 771–806. https://doi.org/10.1093/ejil/chab056

Convention for the Protection of Submarine Telegraph Cables. (1884). Paris, 14 March 1884.

Davenport, T. M. (2025). The protection of submarine cables in Southeast Asia: The security gap and challenges and opportunities for regional cooperation. *Marine Policy, 171*, 106435. https://doi.org/10.1016/j.marpol.2024.106435

Duenow, V. (2025). NATO's new members and the Baltic strategic balance. *Survival, 67*(1), 89–98. https://doi.org/10.1080/00396338.2025.2459021

European Union. (2022a). *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities*. Official Journal of the European Union, L 333, 164–198. https://eur-lex.europa.eu/eli/dir/2022/2557/oj

European Union. (2022b). *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. Official Journal of the European Union, L 333, 80–152. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

European Union, & NATO. (2023). *EU–NATO Task Force on the resilience of critical infrastructure: Final assessment report*. European Commission. https://commission.europa.eu/

Gioe, D. V., Miron, M., & Ozawa, M. (2025). Reassessing NATO's deterrence and defence posture in the Baltics: Rebalancing strategic priorities to counter Russian hybrid aggression. *Defense & Security Analysis, 41*(1), 145–165. https://doi.org/10.1080/14751798.2024.2424935

Gülcan, T. A., & Erginer, K. E. (2023). National and international maritime situational awareness model examples and the effects of North Stream pipelines sabotage. *International Journal of Critical Infrastructure Protection, 42*, 100624. https://doi.org/10.1016/j.ijcip.2023.100624

Halas, M. (2022). NATO's sub-conventional deterrence: The case of Russian violations of the Estonian airspace. *Contemporary Security Policy, 43*(2), 350–381. https://doi.org/10.1080/13523260.2022.2028464

Hughes, G. (2020). War in the grey zone: Historical reflections and contemporary implications. *Survival, 62*(3), 131–158. https://doi.org/10.1080/00396338.2020.1763618

International Cable Protection Committee. (n.d.). *The protection of submarine cables* [Industry resource]. ICPC. https://www.iscpc.org/

International Law Commission. (2001). *Articles on responsibility of states for internationally wrongful acts* (UNGA Res. 56/83, Annex). United Nations. https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf

Janičatová, S., & Mlejnková, P. (2021). The ambiguity of hybrid warfare: A qualitative content analysis of the United Kingdom's political–military discourse on Russia's hostile activities. *Contemporary Security Policy, 42*(3), 312–344. https://doi.org/10.1080/13523260.2021.1885921

Kamiński, T., & Szewczyk, R. (2022). The coastal state obligation not to impede the laying or maintenance of submarine pipelines on the continental shelf according to United Nations Convention on the Law of the Sea. *Marine Policy, 143*, 105086. https://doi.org/10.1016/j.marpol.2022.105086

Liang, M., Weng, L., Gao, R., Li, Y., & Du, L. (2024). Unsupervised maritime anomaly detection for intelligent situational awareness using AIS data. *Knowledge-Based Systems, 284*, 111313. https://doi.org/10.1016/j.knosys.2023.111313

Liebetrau, T., & Bueger, C. (2024). Advancing coordination in critical maritime infrastructure protection: Lessons from maritime piracy and cybersecurity. *International Journal of Critical Infrastructure Protection, 46*, 100683. https://doi.org/10.1016/j.ijcip.2024.100683

Lindsay, J. R. (2025). Stuxnet revisited: From cyber warfare to secret statecraft. *Journal of Strategic Studies, 48*(4), 834–873. https://doi.org/10.1080/01402390.2025.2481447

Lott, A. (2025). Conventional jurisdictional approaches to protecting submarine cables and pipelines. *International & Comparative Law Quarterly, 74*(S1), 63–84. https://doi.org/10.1017/s0020589325101164

Mackenzie-Gray Scott, R. (2021). Due diligence as a secondary rule of general international law. *Leiden Journal of International Law, 34*(2), 343–372. https://doi.org/10.1017/s0922156521000030

McCabe, R., & Flynn, B. (2023). Under the radar: Ireland, maritime security capacity, and the governance of subsea infrastructure. *European Security, 33*(2), 324–344. https://doi.org/10.1080/09662839.2023.2248001

McLaughlin, R. (2024). Different pacta or different servanda? Grey-zone lawfare and law of the sea-based passage and operational rights. *Ocean Development & International Law, 55*(3), 329–342. https://doi.org/10.1080/00908320.2024.2394615

NATO. (2023). *Vilnius Summit Communiqué*. North Atlantic Treaty Organization. https://www.nato.int/cps/en/natohq/official_texts_217320.htm

Neal, A. W. (2026). After Nord Stream: Four security dilemmas in critical maritime infrastructure protection. *International Affairs, 102*(1), 207–225. https://doi.org/10.1093/ia/iiaf229

Pischedda, C., & Cheon, A. (2023). Does plausible deniability work? Assessing the effectiveness of unclaimed coercive acts in the Ukraine war. *Contemporary Security Policy, 44*(3), 345–371. https://doi.org/10.1080/13523260.2023.2212464

Poznansky, M. (2020). Revisiting plausible deniability. *Journal of Strategic Studies, 45*(4), 511–533. https://doi.org/10.1080/01402390.2020.1734570

Qi, Y., Yang, J., & Zhao, Y. (2026). Dual-modality vessel trajectory anomaly detection for maritime risk prevention based on automatic identification system data. *Reliability Engineering & System Safety, 276*, 112905. https://doi.org/10.1016/j.ress.2026.112905

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), 390–414. https://doi.org/10.1080/00908320.2025.2534621

Rossiter, A. (2025). Cable risk and resilience in the age of uncrewed undersea vehicles (UUVs). *Marine Policy, 171*, 106434. https://doi.org/10.1016/j.marpol.2024.106434

Rovner, J., Cormac, R., & Maschmeyer, L. (2025). Sand in the gears: Sabotage in world politics. *European Journal of International Security*, 1–20. Advance online publication. https://doi.org/10.1017/eis.2025.10025

Sun, Z. (2025). Coastal state jurisdiction over acts against transiting submarine pipelines in the exclusive economic zone and on the continental shelf—The case of the Nord Stream incidents. *Ocean Development & International Law, 56*(2), 125–147. https://doi.org/10.1080/00908320.2025.2457754

Tecklenburg, B., Stockbruegger, J., Niemi, A., & Sill Torres, F. (2025). Securing maritime infrastructures: A framework to evaluate physical protection measures for offshore wind farms. *Environment Systems and Decisions, 45*, 67. https://doi.org/10.1007/s10669-025-10055-w

Tong, W., Li, H. X., Nasirzadeh, F., Yao, F., & Ji, Y. (2025). Resilience of interdependent infrastructure networks: Review and future directions. *International Journal of Critical Infrastructure Protection, 51*, 100793. https://doi.org/10.1016/j.ijcip.2025.100793

United Nations. (1982). *United Nations Convention on the Law of the Sea*. 1833 UNTS 397. https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

Yang, W. (2021). Protecting submarine cables from physical damage under investment law. *Ocean Development & International Law, 52*(2), 93–112. https://doi.org/10.1080/00908320.2020.1869446

Yazdi, M., Khan, F., Abbassi, R., & Quddus, N. (2022). Resilience assessment of a subsea pipeline using dynamic Bayesian network. *Journal of Pipeline Science and Engineering, 2*(2), 100053. https://doi.org/10.1016/j.jpse.2022.100053

Zeng, W., Han, Y., Tian, X., & Zhao, J. (2025). Reliability modelling and assessment of subsea oil and gas pipelines considering competing failures caused by dropped object impact and corrosion degradation. *Applied Ocean Research, 164*, 104783. https://doi.org/10.1016/j.apor.2025.104783

Zhou, J., Wang, H., Yang, S., & Liu, Y. (2025). Numerical study on response of subsea pipeline subjected to anchor damage. *Ocean Engineering, 318*, 120179. https://doi.org/10.1016/j.oceaneng.2024.120179

SABOTAŽA PODMORSKE KRITIČNE INFRASTRUKTURE (KABLOVI I PLINOVODI) U BALTIČKOM MORU 2023–2025: PROBLEM ATRIBUCIJE I PRAVNE PRAZNINE DJELOVANJA U „SIVOJ ZONI“

Mpho Khumalo

Univerzitet Južne Afrike
Pretorija, Republika Južna Afrika
E-mail: mpho.khumalo@mylife.unisa.ac.za

Pregledni naučni članak

Primljeno: 22.03.2026. Odobreno: 05.04.2026.

DOI: https://doi.org/10.65932/military-studies-2026-1-6
UDK: 327.88:351.86(261.24)"2023/2025"

Sažetak: Između oktobra 2023. i početka 2025. godine Baltičko more pogodio je niz oštećenja podmorskih telekomunikacionih kablova i energetskih plinovoda, od plinovoda Balticconnector i obližnjih kablova do prekida na vodovima C-Lion1 i Estlink 2 i drugim kablovima, pri čemu se većina u javnoj raspravi pripisuje vučenju sidra plovila povezanih sa sankcionisanom „flotom u sjenci“. Ovaj pregledni rad sintetizuje recenziranu literaturu objavljenu između 2019. i 2026. godine o tri pitanja koja ti događaji otvaraju: zašto je ta infrastruktura toliko ranjiva, zašto je odgovornost tako teško pripisati i zašto međunarodno pravo teško sprečava ili sankcioniše takva djela izvan teritorijalnog mora. Primijenjena je polusistematska tematska metoda pregleda kroz baze Scopus, Web of Science i Crossref, uz primarne pravne instrumente i dokumente Evropske unije i NATO-a, čime je obuhvaćeno četrdeset sedam izvora sintetizovanih u četiri domena: prijetnja, problem atribucije, pravne praznine sive zone i odgovor koji se razvija. Doprinos rada jeste integrativni okvir praznine atribucije i odgovornosti koji povezuje tri literature koje se obično posmatraju odvojeno — literaturu o bezbjednosti pomorske infrastrukture, o sivoj zoni i atribuciji, te o pravu mora — i prati lanac od četiri karike, od detekcije preko atribucije i pravne kvalifikacije do odgovora, pokazujući da baltička podmorska sabotaža zauzima dvostruko dopušten prostor u kojem je djelo istovremeno teško pripisati i teško sankcionisati. Sinteza pokazuje da je fizička ranjivost strukturna i sve veća, da je poricivost namjerno svojstvo djelovanja u sivoj zoni, da Konvencija UN-a o pravu mora mnogo bolje štiti polaganje kablova i plinovoda nego njihovu zaštitu od namjernog oštećenja, i da je institucionalni odgovor stvaran ali nezreo. Zaključuje se da zatvaranje praznine odgovornosti manje zavisi od nove tehnologije, a više od ojačane jurisdikcije obalne države, dokazne saradnje i pristupa otpornosti po dizajnu, te se kao središnji neriješeni problem identifikuje odsustvo dogovorenog pravnog praga za sabotažu ispod upotrebe sile.

Ključne riječi: *podmorski kablovi, podmorski plinovodi, kritična pomorska infrastruktura, siva zona, atribucija, UNCLOS, bezbjednost Baltičkog mora.*