

# Protecting critical undersea infrastructure under hybrid threats: A public-source governance framework for surveillance, attribution, redundancy, and continuity in the Nordic–Baltic region

Karim Hardy

[karim.hardy@minesparis.psl.eu](mailto:karim.hardy@minesparis.psl.eu)

 <https://orcid.org/0000-0003-2603-4551>

Mines Paris – PSL, Center for Research on Risks and Crises (CRC), 1 rue Claude Daunesse,  
06904 Sophia Antipolis, France

## Abstract

*Critical undersea infrastructure links digital communication, energy supply, economic activity, military mobility, and alliance coordination. Under hybrid-threat conditions, disruptions create not only physical damage but also uncertainty over cause, responsibility, and appropriate response. This study examines how public-source evidence can be used to compare security and defence governance for protecting undersea infrastructure. A structured corpus of forty-three public sources on the Nordic–Baltic region and connected European Union/North Atlantic Treaty Organization (EU/NATO) policy spaces was converted into 101 coded documentary governance observations and twelve contextual incidents or policy milestones. Coding distinguished surveillance, attribution, redundancy, and continuity of service while recording broader governance categories, actor type, scope, coordination interfaces and uncertainty. Descriptive frequencies, cross-tabulations, heatmaps, and a temporal comparison were produced through a reproducible Python workflow. Public-source visibility is uneven. Resilience planning, a cross-cutting mechanism, surveillance, and international coordination are documented more frequently than attribution and redundancy. Government, NATO, and EU actors dominate the public record; private operators and military organisations appear more selectively as primary actors. The Baltic Sea is the most visible subspace, and more than half the observations contain partial, verification-required, or disputed information. The four-function framework shows that undersea infrastructure protection is a layered security and defence governance problem rather than a purely technical or naval task. Public evidence can reveal institutional posture, coordination, and continuity priorities without disclosing operationally sensitive details. The framework is intended for comparative application elsewhere, but findings concern the Nordic–Baltic case.*

## Keywords:

critical undersea infrastructure, hybrid threats, maritime security, resilience governance, security and defence

### Article info

Received: 18 June 2026

Revised: 8 August 2026

Accepted: 31 August 2026

Available online: 28 October 2026

Citation: Hardy, K. (2026) 'Protecting critical undersea infrastructure under hybrid threats: a public-source governance framework for surveillance, attribution, redundancy, and continuity in the Nordic–Baltic region', *Security and Defence Quarterly*, 56(4). doi: [10.35467/sdq/235852](https://doi.org/10.35467/sdq/235852).



© 2026 K. Hardy. Published by War Studies University, Poland.

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).

## Introduction

Critical undersea infrastructure (CUI) is a strategic security and defence concern because submarine cables, power interconnectors, pipelines, and offshore energy systems underpin digital communication, energy markets, public administration, defence mobility, and alliance coordination. Local damage can propagate through interdependent civilian, commercial, and military networks; protection, therefore, concerns essential functions as well as physical assets ([Bueger and Liebetrau, 2021](#); [Gasztold and Akrap, 2022](#); [Sellevåg, 2022](#)).

Hybrid-threat conditions have intensified this problem. Undersea disruptions may be natural, unintentional, or intentional: earthquakes, submarine landslides, and other natural hazards coexist with fishing, anchoring, negligence, criminal activity, coercion, and sabotage ([Govella, 2025](#); [Watson, 2025](#)). Natural hazards form part of the wider CUI risk environment but are not coded in the present corpus, which concentrates on human-caused disruptions where attribution, responsibility, and strategic ambiguity are governance concerns. Public authorities must respond before cause and intent are settled, requiring them to maintain services, coordinate investigations, communicate uncertainty, and avoid premature escalation ([Ionita, 2023](#); [North Atlantic Treaty Organization \[NATO\], 2022](#)).

This study develops a public-source method that may be transferable across maritime regions, but its empirical application is deliberately bounded to the Nordic–Baltic maritime space and its connected European Union and North Atlantic Treaty Organization (EU/NATO) policy settings. It therefore distinguishes between a region-specific evidence base and a comparative methodological contribution.

The Nordic–Baltic maritime space is a strategically significant setting because dense cross-border connectivity, private ownership, energy interdependence, total-defence traditions, and overlapping national, Nordic, EU, and NATO responsibilities coexist. National strategies in Finland, Norway, and Sweden increasingly connect infrastructure resilience, hostile-state activity, and whole-of-society preparedness ([Government of Finland, 2022, 2024](#); [Government of Norway, 2023, 2024](#); [Government Offices of Sweden, 2024](#); [Nordic Defence Cooperation \[NORDEFCO\], 2024](#)). The region concentrates governance problems found wherever strategic infrastructure crosses borders, sectors, and public–private authority.

Since 2022, the Nord Stream, Balticconnector, data-cable, and Estlink 2 incidents have generated investigations, restoration measures, and policy responses without always producing immediate or uncontested attribution ([Associated Press, 2024, 2025a](#); [Reuters, 2023, 2025b](#); [Swedish Prosecution Authority, 2024](#)). NATO created a coordination cell and Baltic Sentry, while the EU adopted cable-specific recommendations and an action plan ([European Commission, 2024](#); [European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2025](#); [NATO, 2023a, 2025](#)). The field is emerging, but public debate remains incident-driven.

The existing research establishes the strategic importance of undersea systems and the need for resilience, monitoring, and cross-sector coordination. It is less systematic about how distinct governance functions are distributed across the public record. Incident narratives can show what happened; they do not by themselves compare how institutions organise surveillance, attribution, backup capacity, and service continuity. Nor do they consistently distinguish public visibility from actual capability. This creates a methodological

gap: security researchers need a reproducible way to study an operationally sensitive domain without either remaining at a general rhetorical level or disclosing details that could increase vulnerability.

The present study therefore asks the following question: How can public-source evidence be used to compare security and defence governance functions for CUI protection under hybrid-threat conditions? Three subsidiary questions address function visibility, actor distribution, and the wider lessons of the Nordic–Baltic case. The study contributes a four-function framework, a reproducible public-source coding procedure, and a region-bounded empirical comparison with wider methodological relevance for defence policy, resilience planning, and civil–military/public–private coordination. The following sections develop the framework, method, results, discussion, limitations, and conclusions.

## **Critical undersea infrastructure protection as security and defence governance**

### **Critical undersea infrastructure and security interdependence**

Critical undersea infrastructure is difficult to govern because its strategic value is produced by interdependence. A cable, pipeline, or electricity link is not important only as an asset; it is important because services, institutions, and users depend on it. Undersea systems also operate within broader networks, so the consequences of disruption depend on substitution possibilities, repair capacity, market balancing, and cross-border assistance. Research on submarine cables has shown how infrastructure can remain politically hidden until disruption makes its strategic role visible ([Bueger and Liebetrau, 2021](#)). Later work on critical maritime infrastructure similarly emphasises that protection involves multiple sectors, authorities, and threat environments rather than a single maritime-security instrument ([Bueger and Liebetrau, 2023](#)).

System-of-systems research treats resilience as an interaction among functions, processes, assets, and stakeholders rather than asset hardening alone ([Godzimirski, 2022](#); [Sellevåg, 2022](#)). The relevant unit is the governance arrangement that identifies priority functions, allocates responsibility, and preserves essential services. Economic and societal resilience thus become parts of comprehensive defence ([Constantinescu, 2023](#); [Gasztold and Akrap, 2022](#)).

### **Hybrid threats, ambiguity, and attribution**

Hybrid threats exploit the space between routine competition and overt armed conflict. They combine political, informational, economic, cyber, intelligence, and military instruments while preserving uncertainty about sponsorship, intent, or threshold. In the maritime environment, the same physical outcome may initially be consistent with accident, poor seamanship, criminal conduct, or hostile action. The governance challenge is therefore sequential: authorities must detect an event, protect evidence, coordinate legal and intelligence processes, maintain services, and communicate without allowing uncertainty to become paralysis. NATO's strategic, resilience, and summit documents place critical infrastructure within deterrence and defence because disruption can impose strategic costs below the threshold of conventional attack ([NATO, 2022](#), [2023b](#), [2024a](#), [2024b](#)).

Attribution is central but constrained. Legal proof, intelligence confidence, political judgement, and public communication operate according to different standards. The discontinued Swedish Nord Stream investigation and continuing reporting around Balticconnector and later cable damage show that incidents can remain strategically salient even when legal responsibility is unresolved or jurisdictionally fragmented ([Reuters, 2023, 2025b](#); [Swedish Prosecution Authority, 2024](#)). This study therefore codes attribution separately from threat framing, and records uncertainty rather than treating every disruption as sabotage.

## Civil–military and public–private governance

The actors who own, monitor, regulate, investigate, and defend CUI are not identical. Operators hold technical knowledge and repair resources; governments hold legal and diplomatic authority; armed forces and coast guards contribute maritime awareness, deterrence, and protective presence. NATO adds alliance security and military integration, while the EU supplies maritime-security, market, cyber, transport, and resilience instruments ([European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2023](#); [European Commission and NATO, 2023](#); [European Maritime Safety Agency, 2024](#); [Monaghan \*et al.\*, 2023](#)).

National and regional strategies place CUI protection within comprehensive-security and total-defence thinking. Denmark, Estonia, Finland, Germany, Latvia, Lithuania, Norway, and Sweden increasingly connect national security with civil preparedness, infrastructure resilience, cyber risk, and hostile-state activity ([Federal Government of Germany, 2023](#); [Ministry of Defence of Denmark, 2023](#); [Ministry of Defence of Latvia, 2023](#); [Ministry of National Defence of Lithuania, 2021](#); [Riigikogu and Government of Estonia, 2023](#); [Security Committee of Finland, 2025](#)). Work on Latvia's strategic defence documents also shows an increasing but uneven role of private sector in critical infrastructure, cybersecurity, and continuity ([Juberte Krūmiņa, 2024](#)). Industry facing analyses identify divergent public–private risk models, fragmented regulation, and policy instability around long-lived infrastructure projects ([Channer, 2024](#)). The [International Cable Protection Committee \(n.d.\)](#) recommends operator consultation, cross-agency coordination, and a single governmental point of contact for installation, repair, and protection.

Technology can expand surveillance options, as [Pajak \(2025\)](#) shows for artificial intelligence (AI)-driven naval drones, but its value still depends on mandates, information sharing, evidence handling, operator coordination, and escalation management. This study therefore focuses on the governance functions and interfaces revealed in public documents.

## Four-function analytical framework

The framework distinguishes four functions that are analytically separate but operationally interdependent. Surveillance is the detection and monitoring of risks and disruptions through maritime domain awareness, patrols, sensors, information sharing, and related measures. Attribution is the establishment or communication of cause, responsibility, or plausible culpability through investigation, forensics, intelligence, legal action, and political judgement. Redundancy is the availability of alternative capacity, reserve systems, repair resources, or substitute routes that reduce dependence on a single element.

Continuity of service is the maintenance or restoration of essential functions through rerouting, balancing, emergency procedures, repair, and organisational recovery.

The four functions were selected because they represent distinct governance problem domains: awareness of disruption, establishment of cause and responsibility, availability of alternative capacity, and preservation or restoration of essential service. Their selection is conceptual rather than frequency-based. Resilience planning is treated as a cross-cutting governance mechanism because it can enable all four functions rather than constitute a separate functional outcome. Coordination, information sharing, deterrence, crisis response, and legal action are likewise treated as mechanisms or interfaces that enable, connect, or shape the four core functions. Supplementary Table S2 summarises the category-type mapping used in the analysis.

The distinction matters because resilience can otherwise become an undifferentiated label. Surveillance without attribution may improve awareness while leaving accountability and response uncertain. Attribution without redundancy may identify responsibility but fail to preserve service. Redundancy may exist technically, yet without continuity arrangements it may remain difficult to mobilize. Continuity without adequate surveillance may remain reactive. The four functions are connected through civil–military, public–private, and international interfaces, but each raises a different question of governance and produces different types of public evidence. Table 1 summarises their definitions, public-source indicators, and security significance.

The framework measures public-source governance visibility, not hidden capability. That distinction is both methodological and substantive. Public documents signal priorities, justify spending, communicate deterrence, define expectations, and support democratic accountability, but they also omit classified, commercially sensitive, or operationally risky details. Visibility is therefore a partial indicator of institutional posture. It is valuable when interpreted as evidence about how the problem is constructed and coordinated publicly, not as a complete inventory of what can be done by states and operators.

**Table 1. Four core governance functions for critical undersea infrastructure protection.**  
Note. CUI: critical undersea infrastructure.

| Core function         | Definition                                                                        | Typical public-source indicators                                                                              | Security and defence significance                                                           |
|-----------------------|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| Surveillance          | Detection, monitoring, and maritime awareness of CUI risk.                        | Patrols, monitoring initiatives, information-sharing systems, and alliance or national surveillance measures. | Enables warning and response; public visibility does not establish full capability.         |
| Attribution           | Establishing or communicating cause, responsibility, or suspected responsibility. | Investigations, official statements, legal proceedings, and calibrated attribution language.                  | Shapes accountability, deterrence, escalation, and the legitimacy of response.              |
| Redundancy            | Alternative capacity, backup systems, reserve routes, and repair resources.       | Alternative pathways, reserve capacity, repair capability, and resilience investments.                        | Reduces single-point dependence; details are often commercially or operationally sensitive. |
| Continuity of service | Maintaining or restoring essential functions after disruption.                    | Repair completion, rerouting, market balancing, emergency procedures, and cross-border assistance.            | Limits strategic effects and supports deterrence by denial.                                 |

## Methods

### Study design

The study uses structured public-source documentary analysis. Its purpose is to compare visible governance functions without reconstructing operational plans or technical vulnerabilities. The design treats documentary visibility as an empirical object: what institutions publicly identify, prioritise, coordinate, and report. This approach is appropriate for a field in which classified intelligence, commercial contingency plans, and detailed surveillance arrangements cannot be expected in open sources. It also responds to the need for transparent, reproducible security research that does not increase the vulnerability of the systems under study.

### Corpus and unit of analysis

The corpus contains forty-three public sources, 101 coded documentary governance observations, and twelve contextual incidents or policy milestones. It spans 2021–2026, with most observations from 2022 onward; selected 2021 entries provide doctrinal baselines and 2026 entries fall within the update window. The empirical scope includes the Baltic Sea, wider Nordic–Baltic region, the North Sea, and the High North when directly relevant, together with connected EU and NATO policy spaces. Sources include alliance, EU, national, operator, academic, think-tank, and selected reporting.

For analytical clarity, the revised presentation refers to “geographic or institutional scope” rather than “maritime area.” The scope variable distinguishes physical maritime spaces (Baltic Sea, North Sea, and High North), combined or multi-state regional frames (Baltic Sea–North Atlantic, Baltic Sea–North Sea, and Nordic–Baltic region), national frames (Finland and Norway), institutional policy spaces (EU and NATO/transatlantic), and global comparative frames. EU and NATO are therefore not treated as seas. Where a source explicitly linked more than one setting, a combined label was retained. Supplementary Table S1 provides the operational definitions.

A coded documentary governance observation is a discrete and traceable statement or passage in a public document that records a governance function, mechanism, actor configuration, coordination interface, or uncertainty condition. It is a documentary coding unit, not an in-person or field observation. For example, NATO’s public announcement of Baltic Sentry illustrates surveillance coding, whereas operator notices confirming restoration of C-Lion1 and Estlink 2 illustrate continuity-of-service coding (Cinia, 2025; Fingrid, 2025; NATO, 2025). A single policy document can contain several analytically distinct observations, while a high-profile incident may provide only contextual evidence. The source register preserves the link between each observation and its origin. Table 2 summarises the corpus components and their analytical roles.

### Inclusion and exclusion criteria

Sources were included when they provided traceable evidence relevant to CUI risk, surveillance, attribution, redundancy, continuity, coordination, or resilience. Official national, NATO, EU, regulatory, and operator materials were prioritised. Academic and think-tank sources were used to frame concepts and institutional roles. Selected public reporting was retained when official information remained incomplete or when a report documented a contextual incident, but such entries received lower or verification-required confidence

**Table 2. Corpus composition and analytical role.**

| Component                                 | Count | Analytical role                                                                                |
|-------------------------------------------|-------|------------------------------------------------------------------------------------------------|
| Public sources                            | 43    | Document the public-source corpus and preserve traceability.                                   |
| Coded documentary governance observations | 101   | Primary unit for comparing core functions, broader categories, actors, scopes, and interfaces. |
| Contextual incidents or milestones        | 12    | Situate the governance debate without making the study incident-driven.                        |
| Codebook entries                          | 31    | Define variables, values, coding rules, and uncertainty flags.                                 |

where appropriate. The corpus excludes unattributed claims that could not be traced to a stable source.

The analysis deliberately excludes precise cable routes, coordinates, access points, sensor locations, patrol patterns, repair vulnerabilities, and other details that could facilitate harm. It also avoids inferring classified capabilities from general statements. These exclusions limit operational description but do not prevent analysis of governance functions, institutional responsibilities, or public strategic communication.

## Coding procedure

The codebook records source identifier, year, geographic or institutional scope, country or actor, actor type, infrastructure type, threat type, governance category, governance mechanism, military role, civil–military interface, public–private interface, international coordination, legal or policy basis, evidence location, confidence, and uncertainty. “Governance category” is used when the field includes both the four core functions and broader cross-cutting mechanisms. Each observation retains a short evidentiary trace. Confidence categories reflect source status, specificity, and traceability; uncertainty flags distinguish settled public information from partial, verification-required, or disputed claims.

Coding was conducted by the author, and no independent inter-rater reliability statistic is claimed. Subjectivity was constrained by predefined values, source-level traceability, observation-level evidence, and explicit uncertainty coding. Ambiguous cases followed four decision rules: suspected sabotage did not count as attribution unless the source communicated cause, responsibility, or plausible culpability; redundancy required explicit alternative capacity, routes, reserves, or repair resources rather than generic resilience language; continuity required maintenance, rerouting, restoration, or recovery rather than backup capacity alone; and incomplete or disputed statements retained an uncertainty flag rather than being assigned the strongest category. Thus, restoration notices were treated as continuity evidence, while unresolved suspicion remained threat framing rather than attribution. These procedures support auditability but do not substitute for future independent recoding. Supplementary Table S3 summarises these coding decision rules.

For the coordination-interface matrix, “absent” means that the interface is not identified in the coded passage; “weak” indicates a general or limited mention with little role specificity; “moderate” indicates identifiable coordination or role sharing with some documentary detail; “strong” indicates explicit and structured coordination; and “unclear” indicates that the public source does not permit a defensible classification. These labels describe documentary visibility, not the actual quality of coordination. Supplementary Table S4 summarises the coordination-interface visibility levels.

## Analytical strategy

The Python-based workflow checked duplicate identifiers and missing required fields, calculated frequency distributions, produced cross-tabulations by geographic or institutional scope and actor type, generated heatmaps for governance categories and coordination interfaces, and plotted temporal visibility. The analysis is descriptive-comparative rather than causal or inferential. Counts indicate how often categories are represented in the coded public corpus; they do not estimate the prevalence or effectiveness of hidden operational practice. Interpretation therefore focuses on patterned visibility, institutional location, and documentary asymmetry.

## Reproducibility and research ethics

The anonymised replication package contains analytical dataset, codebook, source matrix, notebook, exported figures, and supplementary tables. The study uses public documentary sources only and involves no human participants or private personal data. The package excludes operationally sensitive details. This combination of transparency and restraint is central to the research design: reviewers can inspect how claims were produced without receiving information that could increase infrastructure vulnerability.

## Results

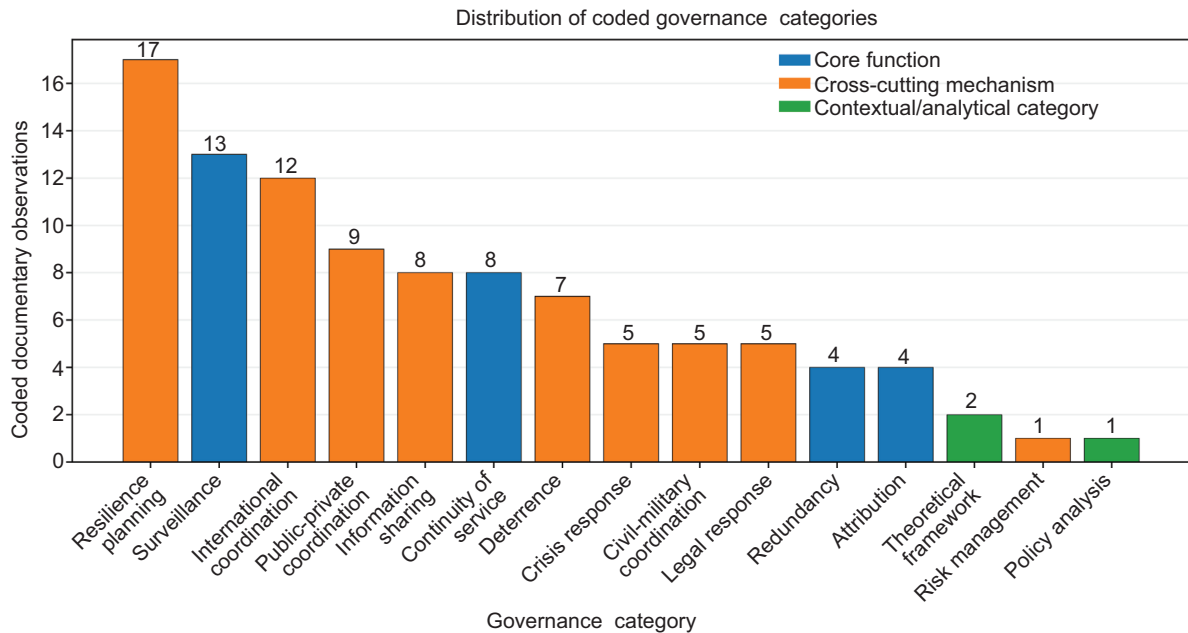
### Corpus overview and governance-category visibility

The 101 coded documentary governance observations form a governance record spanning four core functions and a broader set of cross-cutting mechanisms and contextual categories. Resilience planning is the most frequent cross-cutting mechanism, with seventeen observations, followed by surveillance with thirteen and international coordination with twelve observations. Public–private coordination appears in nine observations; information sharing and continuity of service each appear in eight observations; and deterrence appears in seven observations. Crisis response, civil–military coordination, and legal response each appear five observations. Among the four core functions, surveillance is most visible, followed by continuity of service, while attribution and redundancy each appear four observations. Theoretical framework, risk management, and policy analysis occur less frequently. Figure 1 presents the full distribution.

The distribution reveals an asymmetry in public documentation. Institutions frequently describe preparedness, monitoring, and cooperation, while attribution and backup capacity are less often made visible. This pattern cannot establish that attribution and redundancy are weak in practice. Attribution may remain legally or diplomatically constrained, and redundancy information may expose commercial dependencies or contingency design. The result is instead a finding about the public governance record: the core functions most closely associated with accountability and alternative capacity are among the least documented categories.

Threat framing reinforces the role of ambiguity. Hybrid threat is coded in fifty-two observations, sabotage in twenty-three, and suspected sabotage in thirteen observations, while accidental damage, coercion, cyber-physical disruption, and armed-conflict spillover appear less often. Hybrid-threat terminology therefore provides a dominant public frame, but a separate attribution variable prevents this frame from being treated as proof of responsibility.

Figure 1. Distribution of coded governance categories in the public-source dataset.



## Geographic and institutional-scope distribution

The Baltic Sea accounts for forty observations, followed by the wider Nordic–Baltic region with twenty-two and EU-level policy space with nineteen observations. The North Sea, NATO/transatlantic, and national and global entries are fewer, and the High North is represented only marginally. Figure 2 presents four core functions first, followed by cross-cutting and contextual categories. The Baltic Sea contains the widest spread, including surveillance, attribution, crisis response, legal response, and resilience planning. The Nordic–Baltic category is especially visible in international coordination, civil–military coordination, and resilience planning, while EU-level documents contribute strongly to continuity of service, information sharing, redundancy, and risk management.

This distribution reflects the corpus and period rather than the intrinsic importance of one sea area. Recent incidents and alliance responses made the Baltic Sea exceptionally visible. The EU and Nordic–Baltic entries broaden the record from specific disruptions to regulatory and regional arrangements. The empirical centre is therefore regional, but the governance architecture is multi-level.

## Actor types and governance categories

Government actors account for thirty-five observations, NATO for twenty-one and the EU for sixteen observations. Private operators appear as a primary actor in five observations and explicitly military organisations in three observations. Figure 3 presents the four core functions first and then the broader coded categories. The aggregates should not be interpreted as a marginal military role: NATO and government documents contain surveillance, deterrence, and civil–military elements, but actor type records the principal institutional author. The result is a layered field in which military relevance is frequently mediated through government and alliance structures.

Figure 2. Coded governance categories by geographic or institutional scope.

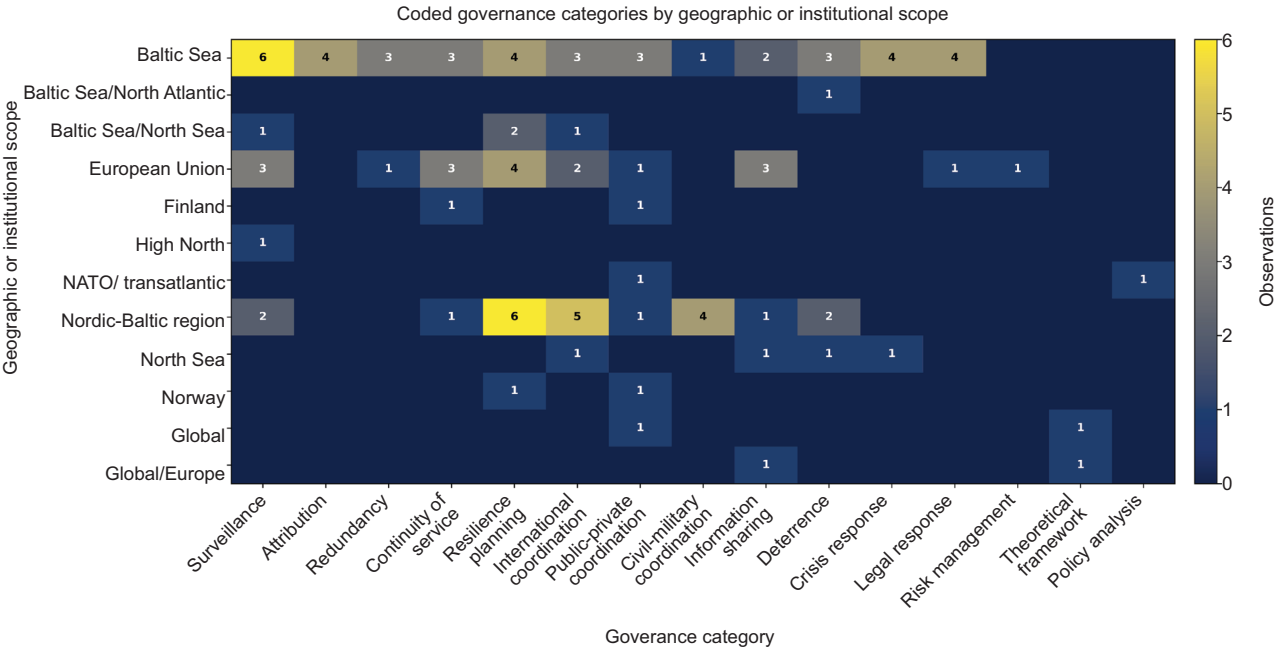
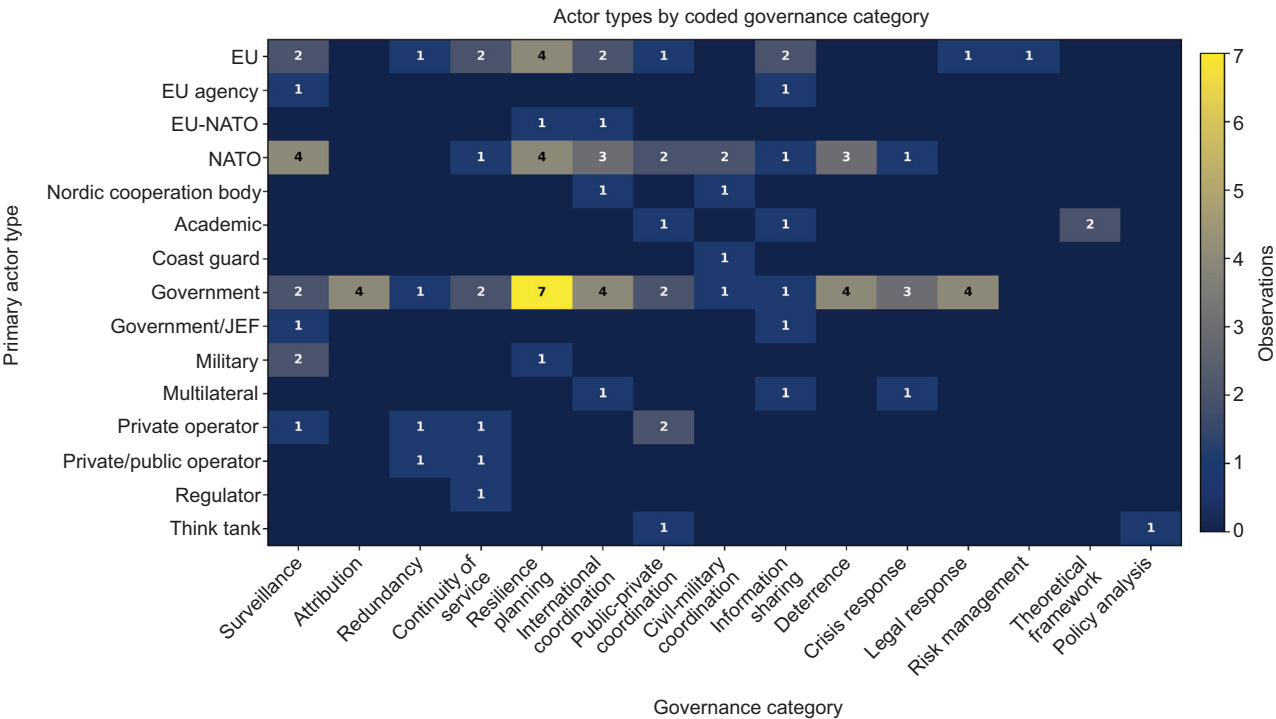


Figure 3. Actor types by coded governance category.



The actor-category matrix also differentiates institutional comparative advantage. Government documents carry most attribution, crisis response, legal response, and resilience-planning observations. NATO is especially visible in deterrence, international coordination, surveillance, and resilience planning. EU documents are prominent in continuity of service, information sharing, redundancy, resilience planning, and risk management. Private operators are most visible where public–private coordination, redundancy,

and continuity are documented. These patterns support the claim that CUI protection cannot be reduced to naval patrols or a single command chain.

### Civil–military and public–private interfaces

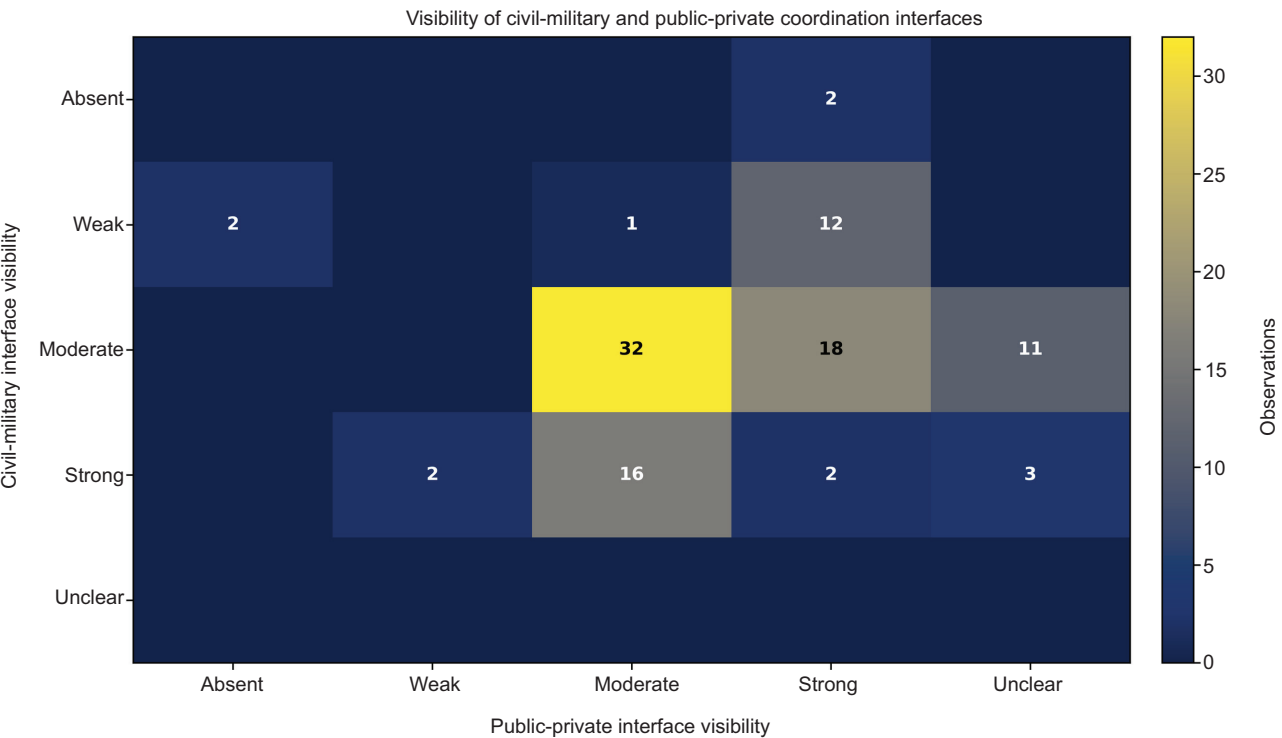
Figure 4 cross-tabulates two separately coded dimensions: civil–military interface visibility on the vertical axis and public–private interface visibility on the horizontal axis. The largest cell combines moderate visibility on both interfaces, with thirty-two observations. Moderate civil–military and strong public–private visibility accounts for eighteen observations, while strong civil–military and moderate public–private visibility accounts for sixteen observations. Other combinations include twelve observations with weak civil–military but strong public–private visibility and eleven observations with moderate civil–military but unclear public–private visibility.

The matrix indicates that coordination is commonly acknowledged but less often documented as strong across both interfaces. Public sources more readily state that cooperation exists than explain how authority, data exchange, repair capacity, and crisis decisions are integrated. This is significant because private actors possess much of the technical capability needed for restoration, while public authorities carry legal and strategic responsibility.

### Temporal pattern and uncertainty

Figure S1 covers the 2021–2026 period and shows the concentration of visibility after 2022: resilience planning and international coordination peak in 2023, deterrence and

**Figure 4. Visibility of civil–military and public–private coordination interfaces.** Cell values represent the number of coded documentary observations at each combination of civil–military and public–private interface visibility (N = 101).



civil–military coordination rise in 2024, and surveillance and continuity become more visible in 2025 ([Associated Press, 2025b](#); [Cinia, 2025](#); [Fingrid, 2025](#); [NATO, 2025](#); [Reuters, 2025a](#)). The pattern is incident-driven but also reflects institutionalisation through NATO, EU, and national initiatives.

Uncertainty is substantial: forty-one observations have no uncertainty flag, thirty-eight contain partial information, twenty-one require verification, and one records disputed attribution. This supports treating uncertainty as a governance variable and phrasing results as documentary visibility rather than verified intent or capability.

## **Discussion**

### **Critical undersea infrastructure protection as hybrid-threat governance**

The findings show that CUI protection is best understood as hybrid-threat governance. The problem is not simply whether an asset can be damaged; it is whether institutions can maintain awareness, manage attribution, preserve alternative capacity, and sustain essential services while intent remains uncertain. The four functions expose different failure modes. A system may monitor effectively but hesitate over legal responsibility. It may attribute an incident but lack visible backup capacity. It may restore service rapidly without clarifying whether lessons have been converted into lasting preparedness. Treating the functions separately makes resilience analytically specific rather than rhetorical.

This functional view also clarifies deterrence. Surveillance and attribution contribute to the credibility of detection and accountability, whereas redundancy and continuity reduce the strategic payoff of disruption. Together they combine deterrence by prospective response with deterrence by denial. The public record, however, is weighted towards the first part of this bundle: monitoring, alliance presence, and general preparedness are more readily disclosed because they can signal activity without revealing sensitive contingency arrangements. A mature governance architecture may therefore be stronger than its public documentation, but the asymmetry can also conceal genuine gaps.

### **Strategic significance of public-source visibility**

Public-source visibility performs governance functions: official statements justify initiatives, reassure allies, signal resolve, and set expectations ([Council of the European Union, 2023](#); [European Commission, 2024](#); [European Union, 2022a, 2022b](#); [NATO, 2023a, 2024b, 2025](#); [Office of the President of the Republic of Finland, 2025](#)). Yet governments, operators, militaries, and investigators also withhold intelligence, commercial data, surveillance patterns, or legal evidence. The method therefore treats visibility as a partial governance signal, records uncertainty, and avoids equating silence with incapacity.

### **Explaining visibility differences across the four core functions**

The function gap is substantively meaningful. Surveillance measures are often suitable for public signalling because they demonstrate attention and presence without requiring disclosure of every capability. They can reassure publics and partners while contributing to deterrence. Attribution is more difficult because evidence must travel through

investigative, intelligence, diplomatic, and legal channels. Premature attribution can damage credibility or create escalation pressure. The low attribution count therefore reflects the institutional difficulty of converting suspicion into an authoritative public claim.

Redundancy is constrained for different reasons. Alternative routes, reserve capacity, repair contracts, and dependency maps may be commercially sensitive or operationally risky to disclose. Continuity of service occupies an intermediate position: operator notices can make rerouting or restoration visible after disruption, while prospective continuity arrangements remain less detailed ([Cinia, 2025](#); [Fingrid, 2025](#)). This highlights a policy communication dilemma: authorities need to demonstrate resilience without advertising where backup arrangements remain thin. Future assessments may therefore be enhanced by combining public governance analysis with authorised expert review or classified evaluation, rather than asking the public record to carry the full evidentiary burden.

## Civil–military and public–private implications

Protection is layered: NATO contributes deterrence and military coordination; the EU provides legal, market, cyber, and resilience frameworks; governments provide sovereignty, investigation, and crisis management; operators provide technical knowledge and restoration; and NORDEFCO and the Joint Expeditionary Force provide regional channels ([NORDEFCO, 2024](#); [UK Government and Joint Expeditionary Force, 2025](#)). The core risk is a translation failure across these actors: surveillance data, legal findings, operator knowledge, and military awareness must reach the authorities able to act. Industry-facing work likewise shows that different priorities, fragmented regulation, and unstable policy can complicate cooperation ([Channer, 2024](#); [International Cable Protection Committee, n.d.](#)).

Professional practice should consequently use the four functions as a bundle. Exercises and planning should ask who owns the relevant information, who can authorise action, what alternative capacity exists, how essential services will be sustained, and how uncertainty will be communicated. The framework can support staff education and cross-sector exercises without relying on technical exposure. It directs attention towards institutional handoffs, which are often where hybrid threats seek to generate delay, confusion, and political friction. In other words, institutional handoffs are the points at which information, authority, or operational responsibility pass between operators, regulators, investigators, governments, military organisations, and alliance structures.

## Global dimension and transferability beyond the Nordic–Baltic case

Although not statistically representative, the Nordic–Baltic case addresses a global governance problem: privately operated cables and offshore energy networks cross jurisdictions and support civilian and defence activity. Other regions differ in alliances, markets, and threats but face the same questions of surveillance, attribution, redundancy, and continuity of service ([Bueger and Liebetrau, 2021, 2023](#)).

The framework can support comparison across the North Atlantic, the Mediterranean, Indo-Pacific corridors, Arctic, and offshore-energy settings when local authorities, markets, alliances, and repair access are incorporated. Its transferable contribution is procedural—decompose resilience into functions, retain uncertainty, map actors and interfaces, and trace claims to evidence—not a claim of universal institutional weakness or effectiveness. Future applications could examine whether similar functional and coordination

asymmetries appear in the Red Sea, the Taiwan Strait, other Indo-Pacific corridors, or the Mediterranean (Govella, 2025; Watson, 2025).

## Limitations

The study has six principal limitations. First, it relies on public documentation and excludes classified intelligence, operational plans, and commercially protected contingency arrangements. Second, the dataset measures documentary visibility rather than institutional capability. Third, the empirical evidence is regionally bounded to the Nordic–Baltic case and connected EU/NATO policy spaces; it is not a global sample. Fourth, the corpus spans 2021–2026 but is concentrated from 2022 onwards, especially in the Baltic Sea. Fifth, natural hazards form part of the wider CUI risk environment but are not included in this hybrid-threat corpus, and the framework has not been tested against them. Sixth, some incident entries rely on public reporting because official investigations remain incomplete or fragmented across jurisdictions; these entries are flagged and should be corroborated as official material becomes available.

Coding was conducted by the author and not assessed independently through inter-rater reliability. This limitation is mitigated through an explicit codebook, source-level traceability, observation-level evidence, decision rules, uncertainty flags, and an open replication package, but future work should include delayed or independent recoding. The clarified scope labels and interface levels improve transparency without converting documentary visibility into a measure of actual coordination quality. The analysis is descriptive-comparative and does not support causal claims about policy effectiveness, exhaustive coverage, or operational validation.

## Conclusions

This study examined how public-source evidence can be used to compare security and defence governance for CUI protection under hybrid-threat conditions. Open documentation becomes analytically useful when it is organised by function rather than treated as a collection of incidents. The four-function framework distinguishes surveillance, attribution, redundancy, and continuity of service, while actor, scope, and interface coding show where those functions and their enabling mechanisms are located institutionally.

The Nordic–Baltic corpus reveals uneven visibility. Resilience planning, a cross-cutting mechanism, surveillance, and international coordination are prominent in the public record; attribution and redundancy are comparatively sparse. Government, NATO, and EU actors dominate the public record, while operators and military organisations appear more selectively as primary actors. Coordination is frequently acknowledged but less often documented as strong across both civil–military and public–private interfaces. These findings indicate that CUI protection is a layered governance problem involving warning, accountability, alternative capacity, and service preservation—not a purely technical or naval task.

The main contribution is a non-sensitive, reproducible method for studying partial evidence without exposing operational vulnerability. The Nordic–Baltic case demonstrates the framework; future research should independently recode the data, incorporate authorised practitioner perspectives, compare public visibility with institutional maturity, and test the framework in another geographical region. The findings are robust for the public governance record, not a measure of hidden capability.

### Funding

No funding was received for conducting this study or preparing this manuscript.

### Data Availability Statement

The source documents used in this study are publicly available. The coded analytical dataset, codebook, source matrix, analysis notebook, exported figures, supplementary tables, and audit files are provided in an anonymised Open Science Framework (OSF) view-only replication package for peer review: [https://osf.io/zr2dk/overview?view\\_only=49fd2cdbc7944fe5b9ef0960f5b4651d](https://osf.io/zr2dk/overview?view_only=49fd2cdbc7944fe5b9ef0960f5b4651d). The package excludes operationally sensitive information, including precise infrastructure coordinates, cable routes, patrol patterns, sensor locations, and technical vulnerability details.

### Ethics Statement

Ethics approval was not required because the study analysed publicly available documentary sources and did not involve human participants, private personal data, interviews, fieldwork, or intervention.

### Conflict of Interest

The author has no relevant financial or non-financial interests to disclose.

### AI Use Statement

Generative AI tools were used to support project structuring, source organisation, data-processing code, analytical checking, and language development. The author selected and verified the sources and references, reviewed the code and outputs, made all coding and scientific decisions, and accepts full responsibility for the manuscript.

## References

**Associated Press** (2024) *Germany and Finland investigate a severed data cable through the Baltic Sea*, 18 November. Available at: <https://apnews.com/article/9b231aa47501545690a26a442fe106a5> (Accessed: 18 June 2026).

**Associated Press** (2025a) *Sweden seizes vessel suspected of sabotage after undersea data cable rupture in Baltic Sea*, 27 January. Available at: <https://apnews.com/article/63da5ef0d577bca12bbe118d527d3a14> (Accessed: 18 June 2026).

**Associated Press** (2025b) *Sweden to contribute up to 3 warships to reinforced NATO presence in the Baltic*, 12 January. Available at: <https://apnews.com/article/5e47dd20f19da2b5c5e0cccaed71e119> (Accessed: 18 June 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](https://doi.org/10.1080/13523260.2021.1907129).

**Bueger, C. and Liebetrau, T.** (2023) 'Critical maritime infrastructure protection: What's the trouble?', *Marine Policy*, 155, art. no. 105772. doi: [10.1016/j.marpol.2023.105772](https://doi.org/10.1016/j.marpol.2023.105772).

**Channer, H.** (2024) 'Improving public–private partnerships on undersea cables: Lessons from Australia and its partners in the Indo-Pacific', *Indo-Pacific Outlook*, 1(2), pp. 1–10. Available at: <https://manoa.hawaii.edu/indopacificaffairs/article/improving-public-private-partnerships-on-undersea-cables-lessons-from-australia-and-its-partners-in-the-indo-pacific/> (Accessed: 30 July 2026).

**Cinia** (2025) *Cinia's C-Lion1 submarine cable fully restored*. Available at: <https://www.cinia.fi/en/news/cinia-s-c-lion1-submarine-cable-fully-restored/> (Accessed: 18 June 2026).

**Constantinescu, M.** (2023) 'Measuring economic resilience for the CEE and Black Sea countries in the framework of comprehensive defense', *Security and Defence Quarterly*, 44(4), pp. 55–83. doi: [10.35467/sdq/175379](https://doi.org/10.35467/sdq/175379).

**Council of the European Union** (2023) *Council recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure*. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023H0120%2801%29> (Accessed: 18 June 2026).

**European Commission** (2024) Recommendation on secure and resilient submarine cable infrastructures. Available at: <https://digital-strategy.ec.europa.eu/en/library/recommendation-secure-and-resilient-submarine-cable-infrastructures> (Accessed: 18 June 2026).

**European Commission and High Representative of the Union for Foreign Affairs and Security Policy** (2023) *Joint communication on the update of the EU maritime security strategy and its action plan*. Available at: [https://oceans-and-fisheries.ec.europa.eu/publications/joint-communication-update-eu-maritime-security-strategy-and-its-action-plan-enhanced-eu-maritime-security\\_en](https://oceans-and-fisheries.ec.europa.eu/publications/joint-communication-update-eu-maritime-security-strategy-and-its-action-plan-enhanced-eu-maritime-security_en) (Accessed: 18 June 2026).

**European Commission and High Representative of the Union for Foreign Affairs and Security Policy** (2025) EU action plan on cable security. Available at: <https://digital-strategy.ec.europa.eu/en/library/eu-action-plan-cable-security> (Accessed: 18 June 2026).

**European Commission and NATO** (2023) *EU-NATO Task Force on resilience of critical infrastructure: Final assessment report*. Available at: [https://commission.europa.eu/system/files/2023-06/EU-NATO\\_Final%20Assessment%20Report%20Digital.pdf](https://commission.europa.eu/system/files/2023-06/EU-NATO_Final%20Assessment%20Report%20Digital.pdf) (Accessed: 18 June 2026).

**European Maritime Safety Agency** (2024) *Common Information Sharing Environment (CISE)*. Available at: <https://emsa.europa.eu/cise.html> (Accessed: 18 June 2026).

**European Union** (2022a) *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union*. Available at: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj> (Accessed: 18 June 2026).

**European Union** (2022b) *Directive (EU) 2022/2557 on the resilience of critical entities*. Available at: <https://eur-lex.europa.eu/eli/dir/2022/2557/oj> (Accessed: 18 June 2026).

**Federal Government of Germany** (2023) *Integrated security for Germany: National security strategy*. Available at: <https://www.nationalesicherheitsstrategie.de/National-Security-Strategy-EN.pdf> (Accessed: 18 June 2026).

**Fingrid** (2025) *Estlink 2 submarine cable repairs complete: Cross-border transmission capacity between Finland and Estonia restored*. Available at: <https://www.fingrid.fi/en/news/news/2025/estlink-2-submarine-cable-repairs-complete--cross-border-transmission-capacity-between-finland-and-estonia-restored/> (Accessed: 18 June 2026).

**Gasztold, A. and Akrap, G.** (2022) 'Introduction to the special issue: Critical infrastructure protection—The challenge of resilience', *Security and Defence Quarterly*, 39(3), pp. 1–5. doi: [10.35467/sdq/154046](https://doi.org/10.35467/sdq/154046).

**Godzimirski, J.M.** (2022) 'Protection of critical infrastructure in Norway—Factors, actors and systems', *Security and Defence Quarterly*, 39(3), pp. 45–62. doi: [10.35467/sdq/151964](https://doi.org/10.35467/sdq/151964).

**Govella, K.** (2025) 'Undersea cables, geoeconomics, and security in the Indo-Pacific: Risks and resilience', *Marine Policy*, 180, art. no. 106809. doi: [10.1016/j.marpol.2025.106809](https://doi.org/10.1016/j.marpol.2025.106809).

**Government of Finland** (2022) *Government report on changes in the security environment*. Available at: <https://julkaisut.valtioneuvosto.fi/handle/10024/164024> (Accessed: 18 June 2026).

**Government of Finland** (2024) *Government Defence Report 2024*. Available at: <https://julkaisut.valtioneuvosto.fi/handle/10024/165820> (Accessed: 18 June 2026).

**Government of Norway** (2023) *Now it is serious: Prepared for an uncertain future*. Available at: <https://www.regjeringen.no/en/dokumenter/nou-2023-17/id2982767/> (Accessed: 18 June 2026).

**Government of Norway** (2024) *The Norwegian defence pledge: Long-term defence plan*. Available at: <https://www.regjeringen.no/en/dokumenter/prop.-87-s-20232024/id3032217/> (Accessed: 18 June 2026).

**Government Offices of Sweden** (2024) *Sweden's National Security Strategy*. Available at: <https://www.government.se/information-material/2024/07/sweden-national-security-strategy/> (Accessed: 18 June 2026).

**International Cable Protection Committee** (n.d.) *Government best practices for protecting and promoting resilience of submarine telecommunications cables*. Version 1.2. Available at: <https://www.iscpc.org/documents/?id=3733> (Accessed: 30 July 2026).

**Ionita, C.-C.** (2023) 'Conventional and hybrid actions in Russia's invasion of Ukraine', *Security and Defence Quarterly*, 44(4), pp. 5–20. doi: [10.35467/sdq/168870](https://doi.org/10.35467/sdq/168870).

**Juberte Krūmiņa, L.** (2024) 'Role of the private sector within Latvia's strategic defence documents: Dimensions of psychological resilience and strategic communication', *Security and Defence Quarterly*, 47(3), pp. 19–37. doi: [10.35467/sdq/186719](https://doi.org/10.35467/sdq/186719).

**Ministry of Defence of Denmark** (2023) *Agreement on Danish Defence 2024–2033*. Available at: <https://www.fmn.dk/en/topics/agreements-and-economy/agreement-on-danish-defence-2024-2033/> (Accessed: 18 June 2026).

**Ministry of Defence of Latvia** (2023) *National security concept of Latvia*. Available at: <https://www.mod.gov.lv/en/documents/national-security-concept> (Accessed: 18 June 2026).

**Ministry of National Defence of Lithuania** (2021) *National security strategy of Lithuania*. Available at: <https://kam.lt/en/national-security-strategy/> (Accessed: 18 June 2026).

**Monaghan, S., Svendsen, O., Darrah, M. and Arnold, E.** (2023) *NATO's role in protecting critical undersea infrastructure*. Washington, DC: Center for Strategic and International Studies. Available at: <https://www.csis.org/analysis/natos-role-protecting-critical-undersea-infrastructure> (Accessed: 18 June 2026).

**Nordic Defence Cooperation (NORDEFCO)** (2024) *Vision for Nordic Defence Cooperation 2030*. Available at: <https://www.nordefco.org/the-vision-for-nordic-defence-cooperation> (Accessed: 18 June 2026).

**North Atlantic Treaty Organization (NATO)** (2022) *NATO 2022 strategic concept*. Available at: <https://www.nato.int/strategic-concept/> (Accessed: 18 June 2026).

**North Atlantic Treaty Organization (NATO)** (2023a) *NATO stands up undersea infrastructure coordination cell*. Available at: <https://www.nato.int/en/news-and-events/articles/news/2023/02/15/nato-stands-up-undersea-infrastructure-coordination-cell> (Accessed: 18 June 2026).

**North Atlantic Treaty Organization (NATO)** (2023b) *Vilnius summit communiqué*. Available at: [https://www.nato.int/cps/en/natohq/official\\_texts\\_217320.htm](https://www.nato.int/cps/en/natohq/official_texts_217320.htm) (Accessed: 18 June 2026).

**North Atlantic Treaty Organization (NATO)** (2024a) *Resilience, civil preparedness and Article 3*. Available at: [https://www.nato.int/cps/en/natohq/topics\\_132722.htm](https://www.nato.int/cps/en/natohq/topics_132722.htm) (Accessed: 18 June 2026).

**North Atlantic Treaty Organization (NATO)** (2024b) *Washington Summit Declaration*. Available at: [https://www.nato.int/cps/en/natohq/official\\_texts\\_227678.htm](https://www.nato.int/cps/en/natohq/official_texts_227678.htm) (Accessed: 18 June 2026).

**North Atlantic Treaty Organization (NATO)** (2025) *NATO launches Baltic Sentry to increase critical infrastructure security*. 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: 18 June 2026).

**Office of the President of the Republic of Finland** (2025) *Joint statement of the Baltic Sea NATO allies summit*. Available at: <https://www.presidentti.fi/en/press-release/joint-statement-of-the-baltic-sea-nato-allies-summit/> (Accessed: 18 June 2026).

**Pajak, K.** (2025) 'Enhancing maritime infrastructure security through AI-driven naval drone operations in the southern Baltic Sea', *Security and Defence Quarterly*, 52(4), pp. 59–77. doi: [10.35467/sdq/211790](https://doi.org/10.35467/sdq/211790).

**Reuters** (2023) 'China cooperating in Balticconnector investigation, Finland says', 31 October. Available at: <https://www.reuters.com/world/china-cooperating-balticconnector-investigation-finland-says-2023-10-31/> (Accessed: 18 June 2026).

**Reuters** (2025a) 'Wary of Russia, Denmark to spend \$600 million on surveillance vessels', 22 April. Available at: <https://www.reuters.com/world/europe/wary-russia-denmark-spend-600-million-surveillance-vessels-2025-04-22/> (Accessed: 18 June 2026).

**Reuters** (2025b) 'Finland completes probe into Baltic Sea cable damage, suspects tanker crew', 13 June. Available at: <https://www.reuters.com/business/media-telecom/finland-completes-probe-into-baltic-sea-cable-damage-suspects-tanker-crew-2025-06-13/> (Accessed: 18 June 2026).

**Riigikogu and Government of Estonia** (2023) *National security concept of Estonia*. Available at: <https://www.riigikogu.ee/en/wpcms/wp-content/uploads/2023/02/National-Security-Concept-of-Estonia.pdf> (Accessed: 18 June 2026).

**Security Committee of Finland** (2025) *Security strategy for society*. Available at: <https://turvallisuuskomitea.fi/en/security-strategy-for-society/> (Accessed: 18 June 2026).

**Sellevåg, S.R.** (2022) 'Abstraction-decomposition space for critical infrastructure systems: A framework for infrastructure planning and resilience policies', *Security and Defence Quarterly*, 39(3), pp. 6–20. doi: [10.35467/sdq/146789](https://doi.org/10.35467/sdq/146789).

**Swedish Prosecution Authority** (2024) *Investigation concerning gross sabotage in the Baltic Sea discontinued*. Available at: <https://www.aklagare.se/en/media/press-releases/2024/february/investigation-concerning-gross-sabotage-in-the-baltic-sea-discontinued/> (Accessed: 18 June 2026).

**UK Government and Joint Expeditionary Force** (2025) *UK-led JEF activates response option to monitor Russian shadow fleet*. Available at: <https://www.gov.uk/government/news/uk-led-jef-activates-response-option-to-monitor-russian-shadow-fleet> (Accessed: 18 June 2026).

**Watson, A.H.A.** (2025) 'Undersea cables: The official perspectives expressed in the Pacific region', *Marine Policy*, 178, p. 106735. doi: [10.1016/j.marpol.2025.106735](https://doi.org/10.1016/j.marpol.2025.106735).

Supplementary Operational definitions

Purpose: This supplement clarifies the labels used in the revised manuscript. It distinguishes physical maritime spaces from institutional policy spaces, separates four core functions from broader governance categories, and defines the interface-visibility levels and coding decision rules. The definitions do not alter the reported 101 coded documentary observations.

Table S1. Geographic or institutional scope. Interpretive note: There is no standalone “North” category in the dataset presented in the manuscript. “North Sea,” “High North,” and “Nordic–Baltic region” refer to different physical or regional frames. Combined labels are retained where a source explicitly links more than one setting. EU and NATO/transatlantic are institutional policy spaces rather than maritime regions.

| Scope label               | Operational definition                                                                                                                     |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Baltic Sea                | A coded statement centred on the Baltic Sea or its littoral security and infrastructure settings.                                          |
| Baltic Sea–North Atlantic | A statement explicitly linking the Baltic Sea developments with the North Atlantic security or infrastructure settings.                    |
| Baltic Sea–North Sea      | A statement explicitly spanning both the Baltic Sea and the North Sea settings.                                                            |
| European Union            | An EU-wide legal, regulatory or policy frame not confined to one maritime basin.                                                           |
| Finland                   | A national statement or measure whose principal empirical scope is Finland.                                                                |
| High North                | An Arctic or sub-Arctic northern European maritime setting, distinct from the North Sea and from the broader Nordic–Baltic regional frame. |
| NATO/transatlantic        | An alliance-wide or transatlantic policy and security frame not confined to one sea area.                                                  |
| Nordic–Baltic region      | A multi-state regional frame involving Nordic and Baltic countries rather than one physical maritime basin.                                |
| North Sea                 | A coded statement centred on the North Sea maritime setting.                                                                               |
| Norway                    | A national statement or measure whose principal empirical scope is Norway.                                                                 |
| Global                    | A global infrastructure or governance frame without a narrower regional focus.                                                             |
| Global/Europe             | A global frame with an explicit European focus or application.                                                                             |

Table S2. Category-type mapping.

| Category type                     | Governance category         | Clarifying role                                                                                                            |
|-----------------------------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------|
| Core function                     | Surveillance                | Detection and monitoring of risk or disruption.                                                                            |
| Core function                     | Attribution                 | Establishment or communication of cause, responsibility, or plausible culpability.                                         |
| Core function                     | Redundancy                  | Availability of alternative capacity, reserve systems, repair resources, or substitute routes.                             |
| Core function                     | Continuity of service       | Maintenance or restoration of essential functions through rerouting, balancing, emergency procedures, repair, or recovery. |
| Cross-cutting mechanism/interface | Resilience planning         | Planning that may enable all four core functions; not treated as a fifth functional outcome.                               |
| Cross-cutting mechanism/interface | International coordination  | Coordination across states, alliances, or international institutions.                                                      |
| Cross-cutting mechanism/interface | Public–private coordination | Coordination between public authorities and private or mixed operators.                                                    |
| Cross-cutting mechanism/interface | Civil–military coordination | Coordination between civilian and military actors or responsibilities.                                                     |
| Cross-cutting mechanism/interface | Information sharing         | Exchange of information relevant to awareness, evidence, decisions, or response.                                           |
| Cross-cutting mechanism/interface | Deterrence                  | Measures or communication intended to affect an adversary’s expected costs or gains.                                       |
| Cross-cutting mechanism/interface | Crisis response             | Immediate or short-term institutional response following disruption or threat.                                             |
| Cross-cutting mechanism/interface | Legal response              | Legal, investigative, or enforcement action connected to protection or accountability.                                     |
| Cross-cutting mechanism/interface | Risk management             | General risk-management measures not reducible to one core function.                                                       |
| Contextual/analytical category    | Theoretical framework       | Conceptual material used to structure or interpret the governance problem.                                                 |
| Contextual/analytical category    | Policy analysis             | Policy-oriented analysis not coded as a specific function or mechanism.                                                    |

**Table S3. Coding decision rules for ambiguous cases.**

| Decision point                       | Rule                                                                                                                                                                                                            |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Threat framing versus attribution    | A reference to “hybrid threat,” “sabotage,” or “suspected sabotage” does not by itself establish attribution. Attribution requires an explicit statement about cause, responsibility, or plausible culpability. |
| Redundancy versus generic resilience | Redundancy requires explicit alternative capacity, routes, reserves, repair resources, or substitute systems. General resilience language is insufficient.                                                      |
| Continuity versus redundancy         | Continuity requires maintenance, rerouting, restoration, or organisational recovery. Backup capacity alone is coded as redundancy unless service preservation or restoration is documented.                     |
| Multiple observations in one source  | A single source may generate more than one observation only where analytically distinct and traceable statements or actions are documented.                                                                     |
| Uncertainty                          | Incomplete, verification-required, or disputed information retains an uncertainty flag rather than being assigned the strongest available category.                                                             |
| Traceability                         | Each observation remains linked to its source identifier and a short evidentiary trace.                                                                                                                         |

**Table S4. Coordination-interface visibility levels. Note. These levels describe what is visible in public documentation. They do not measure the actual quality, maturity, or effectiveness of civil–military or public–private coordination.**

| Level    | Operational meaning                                                            |
|----------|--------------------------------------------------------------------------------|
| Absent   | The coded passage does not identify the interface.                             |
| Weak     | The interface is mentioned generally or with limited role specificity.         |
| Moderate | Identifiable coordination or role sharing is documented with some specificity. |
| Strong   | Explicit and structured coordination is documented.                            |
| Unclear  | The public source does not permit a defensible classification.                 |