PROTECTING CRITICAL UNDERSEA INFRASTRUCTURE IN THE BALTIC SEA: LESSONS FROM THE BALTICCONNECTOR, ESTLINK 2, AND YI PENG 3 INCIDENTS

George Burden

Abstract. This article is written based on the author's dissertation[1], where he examined the vulnerability, attribution challenges, and resilience of the critical undersea infrastructure (CUI) in the Baltic Sea, using the Balticconnector, Yi Peng 3, and EstLink 2 incidents as case studies. Since the Nord Stream pipeline damage in 2022, the Baltic Sea region has seen a growing number of "accidents" damaging CUI. These events illustrate the growing realisation that CUI is vulnerable to hostile sabotage, whether these Baltic instances were accidents or not. Using a qualitative, comparative case study approach that combines process tracing, document analysis, and expert interviews, the study examines whether Russia was responsible for these incidents and what lessons can NATO states draw to better protect CUI. It finds that although Russia's motives and capabilities cannot be dismissed, conclusive attribution remains elusive. The cases highlight gaps in the international law that limit enforcement in exclusive economic zones, difficulties in proving intent, and the risk that uncertainty may embolden probing behaviour by state or state-linked actors. They also show that redundancy and preparedness have so far absorbed isolated disruptions but may not withstand instances of sustained or coordinated sabotage. The author argues that CUI protection should be treated as a strategic priority, requiring layered measures of legal reform, improved surveillance and attribution, credible enforcement, and coordinated investment in redundancy and resilience. By framing the seabed as a contested security domain, the study contributes to debates on hybrid warfare and offers a baseline for policymakers confronting emerging threats to CUI.

Keywords: critical undersea infrastructure, submarine cables, Balticconnector, EstLink 2, Russian sabotage, Baltic Sea, Eagle S, undersea warfare

Võtmesõnad: elutähtis veealune taristu, veealused kaablid, Balticconnector, Estlink 2, Venemaa sabotaaž, Läänemeri, Eagle S, allveesõjapidamine

[1] The master's thesis was submitted to King's College London on 26 August 2025. The final version of the article was submitted to *Sõjateadlane* (Estonian Journal of Military Studies) on 3 November 2025.

1. Introduction

Critical Undersea Infrastructure (CUI) plays a vital yet sometimes overlooked role in sustaining a globalised world. Submarine telecommunications cables, electricity interconnectors, and pipelines underpin the global digital economy and energy trade. 97–99% of global internet traffic passes through a network of only a few hundred submarine telecommunications cables (Black et al., 2025, p. 4; Ganz et al., 2024, p. 2; Telegeography, 2025). Estimates suggest that more than 10 trillion USD in financial transactions are transmitted across these cables daily (Besch & Brown, 2024, p. 3). Since Russia's full-scale invasion of Ukraine in February 2022, the Baltic Sea region has witnessed a series of high-profile incidents involving a suspected sabotage of CUI. Damage to cables and pipelines is not a new phenomenon, with fishing gear, anchors, and poor weather events historically posing risks. However, the rising frequency of incidents in the Baltic Sea combined with heightened tensions between Russia and NATO has fuelled suspicion that Russia is conducting a campaign of CUI sabotage under a veil of plausible deniability. Merchant vessels linked to Russia and China have been observed manoeuvring suspiciously and dragging anchors over cables, later citing technical faults, maintenance issues, or poor weather. Whether accidents or intentional acts, these episodes have caused real damage. In the long term, there is a strategic concern that in a period of escalation or conflict, Russia could conduct a coordinated campaign of sabotage against Europe's CUI, throttling energy grids, gas supplies and access to the internet.

This study investigates three incidents of suspected sabotage in detail. First, the Balticconnector pipeline rupture in October 2023, caused when the Hong Kong-flagged Newnew Polar Bear dragged its anchor across the pipeline and adjacent telecom cables. Second, the Yi Peng 3 incident in November 2024, in which a Chinese-flagged vessel captained by a Russian national was implicated in cutting two submarine telecommunications cables in Sweden's Exclusive Economic Zone (EEZ). Third, the EstLink 2 incident in December 2024 when the Eagle S, a tanker linked to Russia's shadow fleet, dragged its anchor across the EstLink 2 electricity interconnector and multiple submarine telecommunications cables, prompting Finnish authorities to board the vessel and launch criminal proceedings. These cases span the three principal categories of CUI and offer valuable insight into the vulnerabilities, attribution challenges, impact and response measures associated with cases of suspected sabotage to CUI. This article is written based on the

author's dissertation where he examined publicly available information, supplemented by expert interviews, to assess whether Russia orchestrated these incidents. It also identifies lessons that serve as a foundation for policy researchers, NATO, and member states seeking to protect CUI.

The research was approached with the following question in mind: "What lessons can NATO states draw from the Balticconnector, Yi Peng 3, and EstLink 2 incidents regarding the vulnerability, attribution, and protection of CUI in the Baltic Sea region?" It also seeks to answer the following questions:

- What measures taken by the affected states were effective in preventing and mitigating damage to CUI?
- Is Russia responsible for these instances of damaging CUI, and how should the affected states respond?
- What legal and jurisdictional constraints limit the states' ability to respond to incidents of suspected sabotage against CUI, and what reforms or adaptations might address them?

This article argues that while the question of Russia's responsibility is important, the available evidence does not permit a definitive conclusion. At present, no conclusive proof links the Balticconnector, Yi Peng 3, or EstLink 2 incidents directly to the Kremlin, Russian intelligence services or other apparatus of the Russian state. However, Russia's emphasis on the seabed as a domain of strategic competition, its track record of targeting European critical national infrastructure (CNI), and its ongoing confrontation with NATO mean that future sabotage is a significant risk. Whether the result of deliberate sabotage or crew negligence, these events nonetheless expose serious vulnerabilities. They should be understood less as isolated disruptions and more as stress tests, revealing the fragility of existing legal, institutional, and operational frameworks. The case studies demonstrate that isolated damage to critical undersea infrastructure (CUI) does not entail catastrophic disruption. Redundancy, integration, and preparations by telecommunications and energy companies have so far absorbed isolated shocks in the Baltic incidents. However, this resilience should be seen as a short-term buffer rather than a long-term solution. In a potential future scenario of coordinated or sustained targeting, current CUI redundancy levels could be overwhelmed, exposing the NATO states to severe economic, political and societal disruption. As such, lessons need to be learned from these incidents to proactively enhance the protection and resilience of CUI.

This research demonstrates that limitations within the international law and state response systems prevent coastal states from acting decisively against suspect vessels, constraining enforcement options beyond territorial waters. Additionally, attributing intent in an instance of damage also proves difficult. These factors can create permissive conditions for adversaries to probe for weaknesses and test boundaries. In a scenario of deliberate and coordinated sabotage, such legal and institutional gaps would leave NATO states dangerously exposed. In line with the prevailing literature, this article argues that the protection of CUI cannot be achieved through any single measure but requires a multi-layered approach. It stresses the importance of making interference costly through credible enforcement mechanisms, of pursuing reform and creative adaptation of international law, improving surveillance and attribution capabilities, and of strengthening multilateral collaboration. Taken together, these measures provide the basis for enhancing long-term resilience and deterring future attacks, regardless of whether the immediate cause of the Baltic incidents was an accident or an incident of sabotage.

The article proceeds as follows. Chapter Two reviews the existing literature on CNI and CUI, situating current debates within broader theories of security, vulnerability, and "hybrid warfare". Chapter Three outlines methodology; Chapter Four presents the Balticconnector, Yi Peng 3, and EstLink 2 case studies; Chapter Five examines attribution and Russian involvement; Chapter Six discusses patterns, contradictions, and lessons from the case studies.

2. Literature Review

2.1. Defining Critical National Infrastructure and Critical Undersea Infrastructure

Definitions of CNI differ across states. Broadly, CNI refers to systems and assets for which disruption would seriously harm the economic, government or security functions of a state. Newbill (2019, p. 764) observes that while terminological and legal differences exist, the overarching premise of safeguarding vital societal functions transcends borders. For instance, the UK's National Protective Security Authority (2023) defines CNI as:

"Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:

a) Major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or
b) Significant impact on national security, national defence, or the functioning of the state."

The United States' definition closely resembles that of the UK. It focuses on infrastructure, whether physical or virtual, where the "incapacitation or destruction would have a debilitating effect on national security, economic security, national public health or safety, or any combination thereof." (The White House, 2024) This is set to develop under the Trump administration following Executive Order 14239 which signifies a move away from an "all-hazards" approach toward a "risk-informed" model, prioritising specific, high-probability threats over broad resilience planning, decentralising decision-making authority to state and local governments (The White House, 2025). At present, the implications of this shift remain ambiguous. The European Union (EU) defines critical infrastructure as assets or systems, whether physical or digital, that are essential to the delivery of services vital to societal functions, the economy, public health and safety, or the environment (European Union, 2022). There is less of an emphasis on national security, but that is to be expected considering the EU is a multilateral organisation which is not principally concerned with defence. Although there is no universal definition for CNI under international law, Western governments' definitions are largely consistent. Take the following examples to understand the rationale. The failure of energy infrastructure can endanger lives by disabling heating or medical equipment, while hospital system outages may directly compromise patient care. Similarly, large-scale internet disruptions can result in significant financial losses and impair access to essential services. Governments, therefore, place a premium on protecting CNI as prolonged and widespread damage can lead to substantial loss of life, economic disruption, and national security vulnerabilities.

The term CUI is more recent, gaining traction in governmental and academic discourse as recognition grows that these assets are vulnerable to both accidental damage and deliberate attack. CUI is conceptually linked with

both CNI and maritime infrastructure. Monaghan et al. (2023, p. 6) define maritime infrastructure as the network of assets and facilities, such as navigational aids, ports, energy installations, and pipelines, that support resource extraction, maritime transport, and essential services, and whose disruption can cause significant economic, societal, and security consequences. Maritime infrastructure covers all sea-related assets, whereas CUI refers specifically to infrastructure below sea level (Brooke-Holland, 2023; European Commission, 2023, pp. 5, 7; Ministry of Defence, 2025, pp. 19, 74, 89). Writing for the RAND Corporation, Black et al. (2025, p. 4) identify the three types of CUI as submarine telecommunications cables, undersea oil and gas pipelines, and submarine electricity cables. Submarine telecommunications cables are fibre-optic cables that are used to transmit data over long distances (p. 4). Undersea oil and gas pipelines are hollow pipes that can transport oil and gas over long distances (p. 6). Submarine electricity cables can be as simple as a cable linking an offshore wind farm to a national grid, or a high-voltage interconnector cable connecting the electricity grids of different countries (p. 7). These assets underpin global energy and information systems, enabling states to balance electricity demand and exchange oil and gas efficiently, whilst providing the bandwidth and connectivity necessary for mass internet access (Douglas R. Burnett, 2013, pp. 1–3; Larsson, 2024, pp. 400–401).

The vulnerability of CUI is particularly stark considering its criticality. Yet, these vulnerabilities have long been recognised. Sutherland (2025, p. 9) cites Arthur Balfour's 1898 speech to the House of Commons in which he denounced the idea that an adversary could justly cut a state's telegraph cables during wartime. This concern has since become mainstream, reflecting a growing trend among major powers to treat the seabed as a domain of strategic competition (Bueger & Liebetrau, 2021; Runde et al., 2024). Murphy et al. (2016, pp. 15–16) identify that submarine cables are susceptible to intentional interference and damage. There are several reasons for this. Kraska and Pedrozo (2022, pp. 180–181) argue that the vulnerability of undersea cables stems from the fact that their routes and landing locations are well-known and many are concentrated in maritime chokepoints. Bueger and Liebetrau (2023, p. 3) highlight that the vastness of the ocean makes policing and surveillance inherently challenging. Additionally, most submarine cables are privately owned and maintained, placing repair and initial response responsibility on commercial entities (Murphy et al., 2016, p. 16). Once damage occurs, CUI requires extensive time to repair and can cause widespread disruption within the affected state (Bueger & Liebetrau, 2021; Murphy & Pearl, 2025). Although

many authors focus on submarine cables, similar vulnerabilities apply to pipelines. Like cables, they are fixed, spread over vast distances, commercially owned, and require specialised, time-intensive repairs when damaged.

2.2. The Security Environment of CUI

Regarding the threats to and security implications of CUI to NATO in Europe, two distinct but interconnected strands have emerged. The first focuses on the growing number of CUI-related incidents in the Baltic and North Sea. The second addresses the longer-term threat posed by hostile state actors who may deliberately target CUI in the context of heightened geopolitical tensions or armed conflict. Focusing on the first, Lott (2024, p. 127) notes that historically, damage to CUI was the result of accidents such as fishing activity or anchoring mishaps. Runde et al. (2024, p. 2) identify that accidents are responsible for the majority of the 100–150 annual submarine cable breakages. However, since 2021, there has been a noticeable increase in cases where intentional damage is suspected, if not conclusively proven (Lott, 2024, pp. 125–128). High-profile cases include the removal of a section of a fibre-optic cable connecting Svalbard to Norway in 2021, the cutting of two cables in Estonia's Exclusive Economic Zone (EEZ) that linked Estonia to Sweden and Finland in 2023, and, perhaps most infamously, the explosions that damaged the Nord Stream pipelines in 2022 (Monaghan et al., 2023, p. 1). These incidents have prompted both public and private stakeholders to take the protection of CUI more seriously, leading to increased efforts to enhance protection measures and develop strategies to deter damage.

The literature identifies several persistent challenges in preventing and responding to instances of suspected CUI sabotage. Several authors argue that the challenge is exacerbated by a persistent lack of knowledge and understanding of CUI among policymakers. Bueger and Liebetrau (2021, pp. 391–392) highlight the limited awareness of policymakers regarding the operation, control, and protection of submarine cables. Larsson (2024, pp. 414–416) deepens this critique through his concept of "sea blindness", arguing that political and military leaders often fail to grasp the strategic significance and vulnerability of CUI to deliberate sabotage. Also important is the question of attribution. The pattern and timing of these incidents align closely with deteriorating relations between Russia and the West, as well as a broader increase in suspected Russian sabotage operations across Europe (Richterova et al., 2024, pp. 10–11).

In many recent cases, malicious intent from a state actor, namely Russia, is suspected but often unconfirmed (Bashfield, 2024, pp. 4–6; Loik, 2024, pp. 8–9). If proven state-sponsored, such incidents could be construed as attacks, prompting national and potentially NATO responses. However, in the absence of verifiable evidence, legal and political constraints make a direct response difficult, even if foul play is suspected.

Another critical challenge lies in the ambiguity and limitations of existing international legal frameworks. As Kraska and Pedrozo (2022, pp. 182–186) argue, the international laws governing CUI, including the 1884 Submarine Cables Convention, the 1958 High Seas Convention, and the 1982 United Nations Convention on the Law of the Sea (UNCLOS), are inadequate for protecting submarine cables. This naturally extends to undersea pipelines due to their shared characteristics. Kraska and Pedrozo (2022, pp. 184–185) argue that, as these conventions contain no provisions for armed conflict, there is an even wider gap in legal authority under conditions of escalation. Although it is important to recognise that in armed conflict, rules and regulations are often overridden by the necessity of victory. Therefore, most authors tend to focus on the legal protection of cables in the event of suspected sabotage or damage through negligence. Kraska and Pedrozo (2022, p. 183) note that beyond the territorial sea, effective enforcement often rests with the flag state rather than the impacted coastal state. Under UNCLOS Article 92, ships on the high seas fall under the exclusive jurisdiction of their flag state, limiting coastal-state intervention even amid instances of suspected sabotage (United Nations Law of the Sea, 1982, p. 58). Article 113 further places on the flag state the duty to criminalise and prosecute the breaking or injury of submarine cables by ships flying its flag or persons under its jurisdiction (p. 64). This duty is tied to the principle of exclusive flag-state jurisdiction, which applies beyond national waters starting immediately outside the 12 nautical mile territorial sea (p. 27). It does not include the EEZ where the state retains exclusive fishing and mineral rights, or the extended continental shelf where the coastal states retain just exclusive fishing rights. In effect, this means that if a ship suspected of damaging submarine cables is located outside a state's territorial waters (even though it may be in its sovereign territory), enforcement action is contingent on the cooperation and legal diligence of the flag state. Any unilateral attempt to board or seize a suspect vessel for investigation risks breaching international law. While the 1958 Convention on the High Seas obliges states to adopt domestic legislation to both protect submarine cables and pipelines and provide compensation mechanisms for damage, it offers no guarantee that

the states will effectively implement or enforce such measures (Convention on the High Seas, 1958). As a result, the states affected by damaged CUI, beyond their territorial seas, must rely on two conditions: first, that the flag state has enacted adequate domestic legislation; and second, that the flag state is willing to cooperate in enforcing it. Schaller (2024, p. 214) notes that this is particularly problematic "where the flag State approves or even controls the ship's illegal conduct..." Seeking to protect CUI in international waters is a challenging endeavour, and the literature is largely in agreement that the existing international legal frameworks are inadequate for its protection.

2.3. The Strategic Threat

A historical precedent for targeting CUI exists; as early as 1898, the United States severed Spanish telegraph cables during the Spanish-American War (Sutherland, 2025, p. 9). However, there is growing concern that NATO's adversaries, namely Russia and China, will target CUI in a potential conflict scenario. This analysis primarily focuses on Russia within the NATO European context, though China will be considered where relevant. At an institutional level, NATO acknowledges Russia's capability to disrupt CUI, such as through the use of submarines equipped to sever cables or neutralise pipelines (Loik, 2024, p. 2). Trakimavičius (2021, p. 3) reveals Russia's collection of "special mission ships" or "oceanographic vessels" that are outfitted with manned deep-sea submersibles which may be employed in "cable cutting, laying of taps on undersea cables and other special tasks operating". One vessel that has ascended to infamy is the Russian Navy's "Yantar" ship, spotted loitering near submarine cables off the coasts of Canada, the United States, and Portugal, among others (p. 3). Schaller (2024, pp. 204-206) notes that these special-purpose ships are mapping CUI locations and routes. Wasiuta (2023, p. 364) identifies a plethora of public statements from NATO officials concerned about the activity of Russia's ships and the vulnerability of CUI, yet observes a notable absence of corresponding action. The concern is not only about Russia's capabilities but also its intent to use CUI disruption as a tool of coercion or warfare (Bashfield, 2024, pp. 1–2; Loik, 2024, p. 2; Monaghan et al., 2023, p. 2).

2.4. Sabotage of CUI within the framework of "Hybrid Warfare"

Existing scholarship often frames the threat of sabotage, along with current suspicious instances of damage to CUI, within the broader discourse of "hybrid threats" and "hybrid warfare" (Loik, 2024; Lott, 2024, pp. 127, 128; Miętkiewicz, 2025, pp. 36–37; Praks, 2024, pp. 1-7). Official government documents, NATO sources and think tank articles stress this further and have explicitly framed recent damage to CUI within the context of a Russian "hybrid" campaign in the Baltics (Maritime Security Centre of Excellence, 2024, p. 190; Ålander et al., 2024, p. 4; Doughty, 2025; European Parliament, 2025; Praks, 2024, p. 6). Casey-Maslen et al. (2024, p. 26) emphasise the strategic function of such attacks, noting that hybrid operations targeting CUI may not only serve to expose vulnerabilities but can also be designed to "create a supply crisis", thereby "laying the ground for popular unrest and destabilisation of the political environment in the affected countries." Recently, scholars have begun to critically assess the competing interpretations and definitions of "hybrid threats" and "hybrid warfare".

Frank Hoffman (2007, p. 7) used the term "hybrid warfare" to capture the convergence of conventional and irregular modes of war, as demonstrated by Hezbollah's use of advanced weaponry and guerrilla tactics. Hoffman argued that state and non-state actors would increasingly develop state-level military capabilities with asymmetric methods such as terrorism and cyber operations (Hoffman, 2007, pp. 8, 28). This concept can apply to the maritime domain and fits relatively well with the conflict on the Black Sea between Russia and Ukraine. Ukraine has successfully employed asymmetric capabilities, such as the use of unmanned surface vehicles, to challenge Russia's naval superiority in the Black Sea despite Ukraine having virtually no navy (Habib & Shamrir Al Af, 2025, pp. 36–37). However, the applicability of Hoffman's model becomes more tenuous when analysing instances of CUI of suspected sabotage in the Baltic Sea. If recent incidents indeed reflect sabotage, these instances lack the overt kinetic or operational fusion typical of hybrid warfare as Hoffman envisioned it. Rather than blending irregular and conventional tactics in a theatre of open conflict, these acts would be clandestine, deniable, and occurring in peacetime. The concept may be more applicable to a warfighting scenario where CUI is targeted as part of a broader maritime campaign.

Modern definitions of "hybrid warfare" differ substantially from Hoffman's original theory. "Hybrid warfare" gained renewed popularity following Russia's annexation of Crimea and intervention in the Donbas region,

as analysts sought to account for the success of Russian strategy. In Crimea, for instance, Russia's "little green men" played a central role in the territorial occupation, supported by disinformation campaigns, cyber-attacks, and psychological operations. Writing for the NATO Defence College, Larsen and Lasconjarias (2015, p. 3) defined hybrid warfare as "the true combination and blending of various means of conflict… dominating the physical and psychological battlefield with information and media control." Another frequently cited analysis, grounded in the context of the 2014 NATO Wales Summit, characterises Russian hybrid warfare as a "combination and orchestration of different actions that achieves a surprise effect and creates ambiguity, making an adequate reaction extremely difficult, especially for multinational organisations that operate on the principle of consensus." Fridman (2018, pp. 104-106) argues that the term has since grown to encompass everything above, but also nearly every element of strategic competition below the threshold of war. That includes the use of cyber-attacks, the manipulation of information in the media space, political subversion, the manipulation of energy resources, among several other military and non-military means, both in peacetime and wartime. An increasing body of literature criticises the banner of "hybrid warfare" and "hybrid threats" (Fridman, 2018; Galeotti, 2019). Fridman (2018, pp. 154–160) argues that both "Gibridnaya Voyna" (Russian for hybrid war) and "hybrid warfare" are analytically imprecise and frequently misrepresent the strategic thinking of the "Other" as Russia and the West, respectively. He demonstrates how these terms have been politicised, often serving more to construct threat perceptions than to enable rigorous strategic analysis of a way of warfare (Fridman, 2018, pp. 125, 151, 152). Fridman (2018, pp. 157–158) further observes a growing trend within the military circles and academic literature toward abandoning these ambiguous labels in favour of more precise terminology that better reflects the nature and context of specific behaviours. In line with this critique, this analysis avoids reliance on such terms (including grey zone and sub-threshold warfare). Instead, it focuses specifically on the strategic and operational environment through which they occur and the key debate as to whether instances of CUI are the result of accidental damage or state-sponsored sabotage.

2.5. How to protect CUI

The literature presents several potential solutions to protecting and deterring the hostile targeting of CUI. Some authors focus narrowly on specific domains, such as international law, while others advocate comprehensive, multi-layered strategies. For instance, Black et al. (2025, pp. 22–24) emphasise that safeguarding CUI requires a multi-layered, multi-actor approach spanning national governments, the private sector, the EU, NATO, and Joint Expeditionary Force (JEF). As the nature of the problem spans multiple domains, multi-layered solutions are the most popular among scholars and policymakers. A comprehensive breakdown of specific recommendations is beyond the scope of this research; however, the measures suggested in the literature can be loosely categorised into three groups.

International Law

Within the legal domain, proposed solutions can be grouped under international law reform and adaptation. These often target issues such as flag state jurisdiction, investigative authority, and the allocation of financial responsibility for damage. For instance, Frazier (2022, p. 36) supports the idea that protecting submarine cables requires a tiered fine system that differentiates between corporate actors and smaller operators, escalates penalties for repeat violations, and mandates direct compensation for repair costs. Frazier also advocates amending UNCLOS Article 113 and establishing a universal jurisdiction to close legal enforcement gaps and address the global security risks posed by intentional cable damage (p. 36). Pedrozo (2025, p. 162) argues that instead of pursuing the politically and procedurally burdensome route of amending UNCLOS, states should negotiate a new implementing agreement, modelled on prior successful instruments under the convention, that extends legal protections for submarine cables and pipelines beyond the territorial sea while expressly preserving belligerent rights during armed conflict. Ringbom and Lott (2024) favour working within existing legal frameworks, including the creative reinterpretation and application of current laws and conventions, rather than pursuing new treaty instruments.

Resilience and Response Measures

Resilience and response refer to the actions that states can take to prevent and prepare for the sabotage of CUI, as well as to mitigate the damage when such incidents occur. This can occur through legislation, risk management, investment, and preparing law enforcement and military organisations to respond to instances of sabotage when they occur. Regarding domestic legislation, Sari (2025, p. 36) highlights that states need to update their domestic laws in order to make full use of their rights under UNCLOS and to harmonise their legislations to allow for cooperation across jurisdictional boundaries. Some authors suggest prioritising private sector resilience and public-private collaboration (Black et al., 2025, p. 23; Runde et al., 2024, p. 10). There are also physical resilience measures that focus on tangible actions to enhance CUI redundancy. For instance, Frazier (2022, p. 36) suggests that laying more "dark" cables is worth consideration. These "dark" cables are deliberately omitted from publicly available maps to reduce their visibility to hostile actors. Concealing their locations reduces the likelihood of targeted sabotage by making critical routes harder to identify. Cao et al. (2022) suggest optimising burial depth to protect against anchor strikes, noting the lack of universal standards. There are also technological measures, including the use of acoustic, magnetic, optical, and oceanographic sensors, which Eleftherakis and Vicen-Bueno (2020, pp. 33-35) identify as capable of detecting threats such as fishing gear, anchors, submarines, divers, and environmental anomalies along cable routes.

Multilateral Security Frameworks

Multilateral security frameworks highlight shared responsibility between states through organisations such as the EU, NATO, and JEF in protecting and deterring attacks on CUI. For instance, Black et al. (2025, pp. 23–24) advocate for the shared responsibility for CUI protection, with the EU focusing on regulatory frameworks, coordinated risk assessments, and cross-border information sharing, and NATO enhancing patrolling, cyber defence, and innovation capabilities. Monaghan et al. (2023, pp. 12–13) argue that NATO should protect CUI through immediate actions, such as a dedicated maritime group, and longer-term measures, including resilience strategies, preparedness goals, and risk-based planning.

This chapter has examined the literature on CUI, ranging from how it is defined and categorised, to its economic and strategic importance, to the vulnerabilities and threats it faces. The literature reflects growing concern over both accidental damage and suspected sabotage, with Russia emerging as NATO's greatest threat in the CUI domain. Protecting CUI presents several issues, including gaps in international law, inherent vulnerabilities, and the challenge of determining whether damage is intentional or accidental. Scholars diverge over whether recent incidents should be seen as part of instances of "hybrid warfare" or whether such terms obscure more than they clarify. While a range of solutions are proposed, from legal reforms and technological measures to resilience strategies and multilateral security frameworks, consensus is limited, and their effectiveness remains uncertain.

3. Methodology

This research adopts a qualitative, comparative case study methodology to examine the impact, attribution, and state responses to suspected CUI sabotage. It aims to identify the challenges encountered and the measures employed, extracting lessons applicable to defence and infrastructure resilience policies. It is primarily aimed at NATO states in northern Europe as they share an adversarial relationship with Russia and a similar operational environment.

3.1. Case Studies of Sabotage Incidents

Chapter Four examines three prominent case studies in the Baltic Sea where Russia is suspected of sabotaging CUI. The first is the 2023 Balticconnector pipeline incident, the second is the 2024 EstLink 2 incident, and the third is the 2024 Yi Peng 3 incident. These cases were selected for their prominence, the availability of credible open-source reporting, and representation of the three forms of CUI. Each case study is analysed through a process-tracing approach to assess:

- The nature and circumstances of the incident;
- The impact of the incident;
- The investigation into the incident;
- The strategic and operational responses adopted by the affected states.

3.2. Discussion & Lessons

Chapters Five and Six consist of a discussion where the findings from the case studies are interpreted considering broader literature and interviews. This section develops key themes from the literature, most notably the challenge of attribution in incidents of damage to CUI. Here, the cases are used to illustrate both the grounds for suspecting Russia's involvement and the limitations of the available evidence, drawing on expert interviews to highlight the tension between technical plausibility and legal proof. The discussion then moves beyond attribution to examine the broader implications of these incidents for European security. Finally, the discussion identifies several lessons that can be drawn from the Baltic experience, including the importance of deterrence, the need for more effective legal instruments, and the strengthening of multinational coordination for protecting CUI. The aim is not to provide comprehensive policy recommendations, but to suggest the "direction of travel".

3.3. Research Methods

The primary methodological tools for this research include:

- Process tracing to reconstruct the sequence of events, policy decisions, and operational responses in selected CUI incidents.
- Thematic analysis of official documents, enabling the identification of patterns and divergences in national policy responses.
- Semi-structured expert interviews, designed to provide insight into strategic thinking, threat perceptions, and inter-agency coordination in the Baltic states and NATO.

This research uses a wide variety of resources, particularly when reconstructing events. It draws from the following:

- Policy and strategy documents from Baltic state governments, defence ministries, and regional organisations such as the EU and NATO;
- Academic literature and policy reports on CUI threats and infrastructure resilience;
- Open-source intelligence (OSINT) relating to CUI incidents;
- Press releases by governments, ministries and military officials;
- Contemporary media reporting and investigations;

- Press releases and annual reports from CUI operators;
- Expert testimony gathered through interviews.

Semi-structured interviews will be conducted with subject matter experts in maritime security and CUI protection. The first is Commander (CDR) Pål Bratbak, the Branch Head for the NATO Maritime Centre for the Security of Undersea Infrastructure (NMCSCUI). The second is CDR Taavi Urb, the Joint Maritime Operations Lecturer at the Baltic Defence College. He has a background in naval mine warfare and was the Estonian national representative during his time as an officer at NATO's Maritime Command (MARCOM). Each interviewee approved selected quotations for use to avoid misinterpretation. Both interviewees agreed to be named in this research.

3.4. Conceptual Definitions and Framing

For the purpose of this research, CUI refers to undersea infrastructure, the loss or degradation of which would significantly impair the delivery of essential services, national security, or core state functions. It explicitly considers three forms: submarine telecommunications cables, submarine electricity interconnectors, and undersea oil and gas pipelines. Sabotage is defined as an intentional act designed to damage, destroy, or disrupt foreign infrastructure in a manner consistent with coercive or strategic objectives. Russia is understood as the primary threat to NATO Europe in the CUI domain, based on its capabilities, strategic posture, and regional commitments. This framing aligns with prevailing threat assessments in the literature and among NATO allies. This study consciously avoids analytical reliance on terms such as hybrid warfare, grey-zone threats, or sub-threshold conflict, due to their limited conceptual precision.

4. The Baltic Case Studies

4.1. The Balticconnector Incident

On 8 October 2023, a leak was detected in the Balticconnector gas pipeline and an adjacent telecom cable between Finland and Estonia (Council of the European Union, 2023, p. 2). The same night, faults were reported in the nearby

Estonian-Swedish, Russian, and Estonian-Finnish submarine telecommunications cables (Ringbom & Lott, 2024, p. 1). These faults all occurred nearby the Balticconnector breach and inside Finland's EEZ. Suspicion centred on the Hong Kong-registered and Chinese-owned Newnew Polar Bear as the ship crossed the Balticconnector at the time when seismic activity, consistent with an anchor drag, was detected (Ringbom & Lott, 2024, p. 1). The Finnish Border Guard made radio contact with the Newnew Polar Bear in the Gulf of Finland on its westward journey following a stay in St. Petersburg (p. 2). However, the vessel did not cooperate. Finnish authorities ultimately took no action, as their enforcement powers did not extend beyond territorial waters and the damage had occurred in the EEZ. As a result, the ship was able to depart unimpeded, first calling at St. Petersburg before continuing to China.

Finland headed the criminal investigation into the incident with support from Estonia. Amid the mounting evidence against the Newnew Polar Bear, requests were made to the Chinese authorities for cooperation and legal assistance regarding the case (Poliisi, 2023). In August 2024, Chinese media reported Beijing's admission that the Newnew Polar Bear damaged the Balticconnector, attributing the rupture to "a strong storm" and classifying it as an accident following its own internal investigation (Bermingham, 2024). This admission added little to what Finnish investigators already suspected, especially as they had by then recovered the vessel's anchor from the seabed (YLE, 2023). Additionally, the joint Finnish-Estonian investigation could not use China's report as admissible evidence. Without direct jurisdiction over the vessel or its crew, both lacked meaningful leverage to conduct their own criminal investigations. In order to establish whether the incident was intentional, Estonian prosecutors submitted a mutual legal assistance (MLA) request to China, asking its law-enforcement authorities to undertake investigative measures related to the vessel and its crew (Sytas, 2024). China did not respond to this request; however, it did cooperate to a limited extent. Cooperation between China and Finland is reportedly ongoing, although it remains unclear whether China has fulfilled the full extent of Estonia's MLA request (Poliisi, 2025b). As of July 2025, the ship's captain, Wan Wenguo, has been formally charged in Hong Kong with criminal damage and maritime safety violations and remains in pre-trial custody (Reuters, 2025a). There appears to have been no attempt to investigate the possibility of sabotage.

The damage to the Balticconnector had surprisingly little immediate effect on the retail energy supplies of Finland and Estonia. Pre-existing redundancy measures meant that the alternative energy infrastructure absorbed

most of the lost throughput. Grid integration with Latvia ensured the Estonian gas supply through the Inčukalns underground gas storage facility, in addition to top-ups from the Klaipeda Liquefied Natural Gas (LNG) terminal and the Lithuanian-Polish interconnection GIPL (Elering, 2025a, p. 11). For Finland, the LNG terminal in Inkoo had sufficient capacity to cover gas imports while the Balticonnector was down (Elering, 2025a). That said, the market reaction was asymmetric. Finnish wholesale prices surged in the immediate aftermath, underlining Finland's near-total reliance on LNG imports, while Estonia's storage cushion and European connections muted domestic price exposure (A'Hearn, 2024, p. 9; Ots, 2024). Repairs were costly and slow. The Balticconnector took over six months to repair at an estimated cost of 35 million EUR, according to annual reports from GasGrid (GasGrid, 2024, pp. 9, 102; GasGrid, 2025, p.18). That cost was to be split between both GasGrid and Estonia's national grid operator Elering. In the case of GasGrid, insurance covered 7.5 million EUR of the repair fees (GasGrid, 2025, p. 89). Elering's 2024 annual report indicated that the Balticconnector repair strained both the financial and manpower resources of the gas operator (Elering, 2025a, p. 6).

Some Western officials and commentators vaguely speculated that Russia might be behind the Balticconnector damage, but those suspicions were never confirmed. For instance, Latvian President stated in a TV interview that if Russia were proven responsible, NATO should shut off Russian access to the Baltics (Reuters, 2023). However, nothing substantial suggested confirmation of Russian involvement. Putin's spokesperson Dmitry Peskov refuted all claims of Russian involvement, declaring the Latvian President's comments "unacceptable" (Reuters, 2023). A Finnish tabloid quoted inside security policy sources that the Finnish government and Defence Forces suspected Russia of attacking the pipeline (Iltalehti, 2023). To date, no NATO head of state, cabinet minister, or senior military officer has publicly and formally attributed the incidents to Russia. The investigation focused on a Hong Kong–flagged vessel, and Chinese authorities reportedly charged the ship's captain with negligence (Reuters, 2025a). While Beijing did not fully cooperate, it did act within international law and took necessary measures to hold the captain responsible. Taken together, there is limited evidence suggesting Russian sabotage. However, Finland and Estonia were never able to conduct their own full inspection of the vessel, leaving some questions unanswered. Both the EU and NATO took the incident seriously, taking measures to aid in the response and for deterrence measures. The EU released 800,000 EUR

from the Internal Security Fund to the Finnish Border Guard and Navy to secure the area and support the investigation. While in terms of government budgets, the sum is small, it was likely to help accelerate an immediate investigation. In response to the Nord Stream sabotage and the Balticonnector incident, NATO increased air and naval patrols in the Baltic Sea and established the Maritime Centre for the Security of Critical Undersea Infrastructure (NMCSCUI) under NATO's Maritime Command (MARCOM) (NATO, 2023). This swift action taken by both organisations reflects the growing concern about the vulnerability of CUI. While the evidence tying Russia directly to the Balticconnector damage remains inconclusive, the scale and speed of the EU and NATO responses nevertheless imply an underlying suspicion of Russian involvement. At the same time, it demonstrates a prepared and increasingly aware posture of the vulnerability of CUI in the Baltic region.

4.2. The Yi Peng 3 Incident

The BCS East-West Interlink is a 218-kilometre submarine telecommunications cable running between Šventoji (Lithuania) and Katthammarsvik (Gotland, Sweden). It is operated by the Swedish telecommunications company Arelion, with Telia responsible for transmitting internet traffic to Lithuania. On 17 November 2024, Telia reported that the cable was severed at roughly 08:00 UTC (Moss, 2024). On 18 November, Cinia (2024) reported a fault in the nearby C-Lion 1 cable (Finland-Germany), occurring around 02:04 UTC. German defence minister stated that the incident looked like sabotage, without naming a perpetrator (Astier & Kirby, 2024). Swedish and Lithuanian defence ministers were more overt. In a joint statement on 19 November, they noted that the incident must be "assessed with the growing threat posed by Russia in our neighbourhood as a backdrop." (Government of Sweden, 2024) These statements demonstrate a wariness amongst policy circles in the Baltic Sea regarding recent incidents of damaged CUI and the potential role of Russia. As expected, the Kremlin's spokesperson, Dmitry Lavrov, refuted the claims for lack of evidence (Faucon et al., 2024).

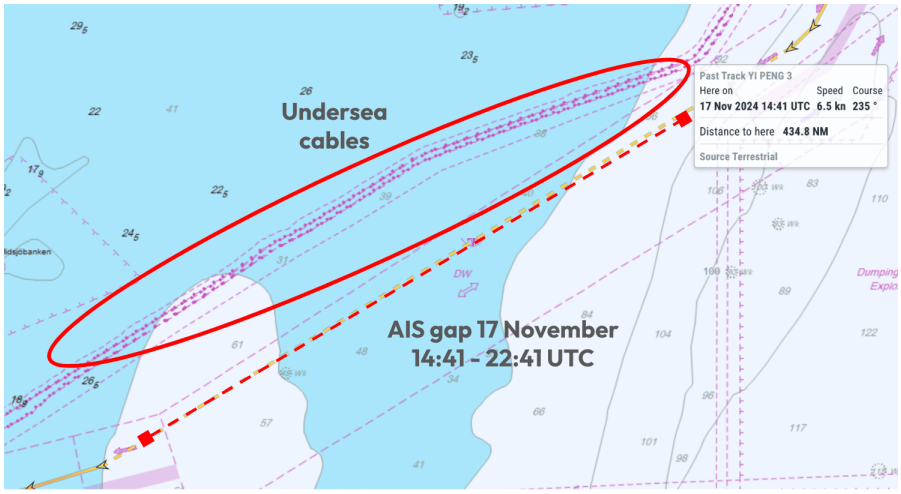

Figure 1. Diagram released by the maritime analytics provider Marine Traffic. The bold dotted line shows the area where AIS was lost (from 14:41 UTC to 22:41 UTC on 17 November). The bold circle shows the area of the C-Lion 1 and BCS East-West Interlink cables. Source: (Ampatzidis, 2024)

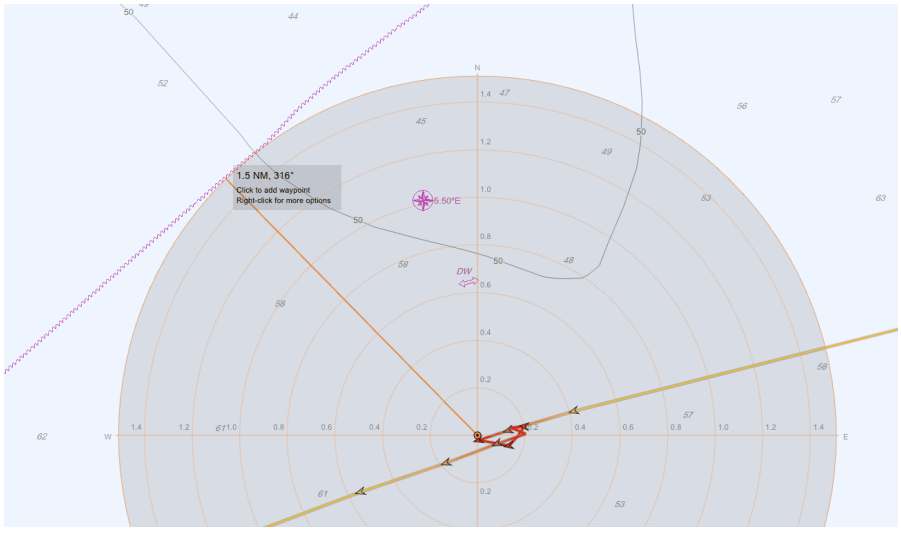

Figure 2. AIS tracking data released by Marine Traffic shows the Yi Peng 3 drifting near the cable for 65 minutes. Source: (Ampatzidis, 2024)

The Yi Peng 3, a Chinese-flagged vessel with a Russian captain, became the primary suspect for the damage. Publicly available Automatic Identification System (AIS)[2] data placed it as the closest vessel to the locations of the severed Baltic Sea cables, showing its course intersecting directly with those damage sites in Sweden's EEZ. During this period, the ship's AIS signal went dark for about 7.5 hours, creating a gap in the publicly available track just hours before cable faults were reported, as seen in **Figure 1** (Ampatzidis, 2024; LRT, 2024; Paasch, 2024; Reuters, 2024). Additionally, upon the AIS resuming, the vessel was recorded drifting for 65 minutes, 1.5 nautical miles from the undersea cables seen in **Figure 2**. The combination of the Yi Peng's 3's proximity to the cables at the time of breaking, the suspicious AIS behaviour, and unusual movement patterns warranted suspicion on the part of the affected states.

On 26 November, Lithuania, Finland, and Sweden created a joint investigation team under the coordination of Eurojust, the EU agency responsible for supporting cross-border criminal cases (LRT, 2024). Despite mounting suspicions, the Yi Peng 3 continued toward the North Sea. A Danish Navy patrol vessel shadowed the vessel before intercepting it in the Kattegat Strait (Ampatzidis, 2024). The ship anchored under Danish observation. The Danish ships did not board the vessel and allowed it to sail through Denmark's territorial sea, only inhibiting its movement once it was anchored in international waters. Reuters (2024) reported that around this time, Sweden formally requested that the ship enter its territorial waters. This would have provided a clear legal basis for a Swedish-led criminal investigation. The crew refused, and by remaining outside both Danish and Swedish territorial seas, placed itself beyond the immediate jurisdiction of the coastal states. Under international law, the responsibility for investigation therefore reverted to the flag state, China. In practice, this meant that any meaningful legal process depended on Beijing's willingness to cooperate. Although not compelled to do so, Chinese authorities agreed to a joint inspection with Sweden and other observers.

The investigation was headed by the Swedish Accident Investigation Authority (SHK), upon receiving a request from the corresponding Chinese

[2] The Automatic Identification System (AIS) is a maritime tracking system that allows vessels to automatically identify and exchange key data with each other and with shore-based stations. AIS tracking is mandatory for most larger ships and all passenger ships. Companies such as Marine Traffic compile this data into maps that track, analyse, and display live AIS data.

body on 21 November (Statens Haverikommission, 2025, p. 1).[3] By approaching the SHK instead of the Swedish authority handling the criminal investigation, China ensured that the inquiry did not assume a criminal character. The SHK inspected the vessel alongside Chinese representatives and observers from Germany, Finland, and Denmark. The investigation found that the ship had been dragging its port side anchor for one and a half days over approximately 330 kilometres (p. 3). The crew acknowledged this but claimed it was accidental (p. 3). Therefore, the investigation hinged on whether the anchor had been intentionally discharged or accidentally released due to negligence and poor seamanship. Based on the available evidence, including interviews, the ship's logbook, and an inspection of the anchor, the investigation could not definitively rule out either possibility (pp. 15–16). A full review of every aspect of the investigation is beyond the scope of this research; however, neither the brief AIS outage nor the drifting period drew particular attention in the final report. This may reflect the fact that the crew had already acknowledged anchor dragging and that suspicions centred more on the vessel's position and timing rather than on anomalies in the tracking data.

Several factors limited the scope and intensity of the investigation, likely preventing a definitive outcome. First, the on-board inspection took place over a month after the incident, limiting access to key evidence such as electronic material. Second, Chinese officials were present during all interviews and forbade any recordings (pp. 2–3). Third, bad weather restricted the time available for inspection, meaning certain procedures, including testing of the port side anchor, had to be accelerated or could not be completed (pp. 2–3). The investigation was ultimately limited in scope and carried out more as a formality than as a fully open and impartial inquiry. While CDR Bratbak (2025) expressed surprise at the extent of the Yi Peng 3 investigations, he suggested that this may reflect China's desire to maintain its image as a responsible shipping state. Whatever the motive, Chinese authorities clearly demonstrated a desire to prevent criminal charges in Finnish or Estonian courts and prove the crew's innocence.

The impact of the Yi Peng 3 incident was limited compared to the Balticonnector rupture. Belson (2024) indicates that neither the severance of the C-Lion 1 nor the BCS East-West Interlink had any noticeable impact on network traffic, HTTPS requests, and bandwidth in any of the affected

[3] The investigation's findings are only available in Swedish. These were carefully translated using a large language model, and the output was compared against secondary reporting.

countries. Belson (2024) attributes this to the effective rerouting of internet traffic through alternative cables. This implies that isolated damage to submarine telecommunications cables has a limited impact on the availability of internet services where sufficient alternative cables exist. The impact on grid operators was also limited. Cinia's annual report notes that the C-Lion 1 cable was swift and cheap to repair due to preexisting arrangements with repair contractors (Cinia, 2025, pp. 23, 87). By contrast, there is little publicly available evidence from Arelion regarding the costs of repairing the BCS East-West Interlink, which suggests that any expenses were either covered by existing arrangements or not material enough to require disclosure.

4.3. The EstLink 2 Incident

EstLink 2 is the second high-voltage direct current interconnector linking the Estonian and Finnish power grids. It runs between the Püssi converter station in Estonia and the Anttila converter station in Finland. With a capacity of 650 megawatts, it is one of the highest-capacity interconnectors in the Baltic region (Elering, 2025a, p. 49). Ownership is equally divided between Estonia's Elering and Finland's Fingrid. EstLink 2 is a key link for regional energy security, helping to maintain a reliable electricity supply and stable prices in both Finland and Estonia (Elering, 2025a, p. 16). Before the incident, the cable had already experienced a technical fault that shut down operations and required replacing a 300-metre segment, a process that took about eight months (Elering, 2025a, pp. 16–17). On 25 December 2024, Fingrid reported a further failure of EstLink 2 to Finnish authorities (Fingrid, 2024). Shortly afterwards, four submarine telecommunications cables were damaged, including two operated by Elisa (Finland-Estonia), another by CITIC (Finland-Estonia), and Cinia's C-Lion1 cable (Finland-Germany) (Traficom, 2024). Unlike the initial technical fault earlier in 2024, the timing and nature of the new fault suggested external interference.

The Eagle S oil tanker became the prime suspect. The tanker, registered under the Cook Islands flag and owned by a United Arab Emirates-based company, had been publicly described by Finnish Customs officials as linked to Russia's "shadow fleet" (Reuters, 2025b). At the time of the incident, it was departing from St. Petersburg and was en route to Port Said, Egypt. AIS tracking data from the Marine Traffic website, compiled by media organisations including Finland's YLE News, indicated that the tanker passed directly

Figure 3. Movement of the Eagle S in the Gulf of Finland plotted using AIS tracking data from Marine Traffic. Source: [YLE, 2024]

over the EstLink 2 cable as well as the other damaged telecommunications cables at the time the damage was reported (YLE, 2024). Moreover, the data revealed that the Eagle S looped back on itself shortly after crossing the cables (YLE, 2024), an unusual manoeuvre that raised questions about the vessel's intentions. Like with the Yi Peng 3, the combination of the precise timing and atypical navigation patterns made the ship the logical focus for Finnish authorities. The Eagle S complied with subsequent orders to enter Finnish territorial waters (Cook & Milne, 2025), allowing authorities to take enforcement action. During the night between 25 and 26 of December, the police special intervention unit Karhu, together with the Border Guard's special intervention unit, descended from helicopters to take control of the tanker (Poliisi, 2025d). On 28 December, Finnish authorities moved the Eagle S to an inner anchorage within national jurisdiction to facilitate investigation, and on 3 January 2025, the country's Maritime Court formally ordered its seizure under suspicion of damaging the EstLink 2 (Fingrid, 2025, p. 19; Poliisi, 2024).

On 6 January 2025, Finland retrieved the anchor suspected of causing the damage. The Eagle S was missing an anchor when boarded, having dragged it over 90 kilometres along the seabed when the damage occurred (Poliisi, 2025a; National Prosecution Authority Finland, 2025). On 13 June 2025, Finland's National Bureau of Investigation (NBI) completed its investigation. The Police of Finland reported that "Based on the material collected from the

Figure 4. The anchor suspected of rupturing the EstLink 2 is hoisted onto the deck of HMS Belos (Poliisi, 2025)

vessel, the examination of the seabed, and the interviews conducted with the crew, senior officers of the tanker Eagle S are suspected of aggravated criminal mischief and aggravated interference with telecommunications." (Poliisi, 2025c) The Head of Investigation, Detective Chief Inspector Sami Liimatainen stated, "Among the suspects are the master, the chief mate and the second mate, who were responsible for the safe passage, navigation and operation of the vessel." (Poliisi, 2025c) The outcome of the case may set a regional precedent for criminal liability and state jurisdiction over foreign-flagged vessels that damage CUI in a country's EEZ.

Finland's National Prosecution Authority announced that the damage to the EstLink 2 cable cost the operators at least 60 million EUR in repair expenses alone (National Prosecution Authority Finland, 2025). This figure does not account for additional costs associated with downtime or lost capacity. Elering (2024) reported that the EstLink 2 fault did not impede the Baltic States' desynchronisation from the Russian energy grid, as alternative European interconnectors were able to handle extra demand. Fingrid (2025, p. 19) confirmed that it would pursue legal action to recover damages, which was seconded by Elering (2025b). The two Elisa submarine telecommunications cables that were severed were repaired successfully in early January (Elisa, 2025b). Elisa's annual review suggests that the cost and duration of the repairs were not significant and that the incident did not materially disrupt

telecommunications services (Elisa, 2025a, p. 8). The report does not disclose specific costs, which aligns with common practice among listed companies, where one-off operational events are only detailed if they materially affect financial results. As noted in the Yi Peng 3 case study, the C-Lion 1 was repaired quickly, likely with insignificant costs. Information regarding the CITIC cable remains unclear.

A report by Estonia's ERR news compiled regional leaders' reactions to the incident. Most suspected sabotage and called for greater protection for CUI, others hinted at Russian involvement but refrained from direct accusations. For instance, Finland's President and Prime Minister both stated it was too early to determine whether Russia was responsible (Wright, 2024). Estonia's president acknowledged that "Repeated damage to Baltic Sea infrastructure signals a systemic threat, not mere accidents." (Wright, 2024) These statements indicate that regional leaders viewed the incident as serious and likely intentional but were cautious about making premature judgments regarding Russian involvement. Nevertheless, NATO and the EU mobilised concrete measures. The UK-led JEF launched Operation Nordic Warden in direct response to the EstLink 2 damage (Ministry of Defence and Foreign, Commonwealth & Development Office, 2025). The operation harnesses and analyses data streams such as AIS tracking data to assess vessels graded as a threat, warning JEF and NATO members in real time if certain ships pose a risk to CUI. NATO launched operation Baltic Sentry, "a multi-domain vigilance activity aimed at increasing maritime situational awareness in the Baltic Sea to deter and defend against attacks on CUI" (NATO, 2025b). Together, these actions reflect that NATO and JEF have recognised the pattern of repeated incidents and are treating the Baltic undersea environment as a strategic domain requiring proactive monitoring and rapid response. The operational response signal to state and non-state actors that any potential attacks targeting CNI will be met with coordinated, alliance-level situational awareness and enforcement capability. In doing so, NATO and JEF are effectively institutionalising a posture of preparedness and resilience, acknowledging the evolving threat environment in which human damage to CUI is becoming a recurring concern.

5. The Dilemma of Attribution

Two questions underlie each case study. First, was the CUI damaged intentionally? Second, is Russia somehow involved? The correct attribution is critical because it determines how states and NATO can respond legally, militarily, and diplomatically. If a state is involved, without attribution it limits the measures both states and NATO can take to respond. Conversely, attributing such incidents to a state actor carries the risk of miscalculation if these are, in fact, the result of negligence, poor weather, or accidents. When asked whether these instances of CUI damage were accidental, both CDR Urb and CDR Bratbak expressed scepticism. CDR Urb (2025) stated, "You have to lower it [the anchor] very carefully or it will snap before you can drag it. So, I would say it's implausible that it's an accident, but well, you can't prove it." Similarly, CDR Bratbak (2025) found it "very strange" that multiple ships could drag their anchors for long distances without noticing. Yet, like CDR Urb, he acknowledges there is no conclusive proof of intent. On the other hand, some academics argue more fervently that Russia is conducting sabotage in the Baltic Sea. For instance, Sutherland (2025, p. 27) asserts bluntly that "the Yi Peng 3 and Eagle S cut cables on behalf of Russia," in order to destabilise the Baltic region.

The issue is that sabotage is particularly difficult to prove because plausible deniability is built into sabotage operations. Galeotti (2019, pp. 60–62) offers a useful perspective on how the Kremlin achieves plausible deniability in both covert and overt operations. Galeotti describes a decentralised ecosystem in which intelligence services, private actors and commercial platforms act in anticipation of Kremlin intent rather than through direct orders. Successful operations can be quietly endorsed; failures can be disavowed, preserving deniability. Sometimes directives originate from the top, but often opportunistic actors move independently. In practice, it could be as simple as an ambitious FSB or GRU officer bribing a crew member to drop the anchor at an opportune moment. That crew member would likely know that accidents at sea occur often and jurisdictional protections complicate enforcement. Note that this is a hypothetical case that speculates how Russia could maintain plausible deniability whilst sabotaging CUI.

While plausible deniability explains how Russia could carry out sabotage whilst limiting direct evidence, such a mechanism is only relevant because Russia possesses both the capability and historical precedent to conduct these operations. As shown in the literature review section, Russia has invested

in developing different capabilities to map, target, and sabotage CUI. Kremlin officials likely already know of the vulnerability and the locations of key CUI. Additionally, there is strong evidence that Russia has targeted CNI on several occasions. For instance, Moscow was linked to the 2007 Estonian cyber-attacks (Czosseck et al., 2013, pp. 73–75) as well as several arson attacks against warehouses and shopping centres in NATO states (Counter Terrorism Policing, 2025; Walker, 2025). Given this context, it would not be unprecedented for such instances of sabotage to extend to CUI. Having established that Russia has both the capability and precedent, the next question is whether it would be motivated to use these capabilities against CUI in the Baltic Sea.

Based on the geopolitical situation in the Baltic region, there is a rationale for why Russia may sabotage CUI. The Estonian Foreign Intelligence Service's annual public report (2025, p. 37) states that Russia is critically reliant on Baltic ports for around 60% of its oil exports and for access to the Kaliningrad Oblast. Therefore, maintaining the Baltic Sea access is critical for Russian economy and, to an extent, its territorial integrity. Eight of the nine states which have a Baltic coastline are now NATO member states, with the accession of Sweden and Finland reinforcing Moscow's perception of encirclement. In particular, Russian officials have framed NATO as an aggressor in the region, with Deputy Foreign Minister Alexander Grushko accusing the Alliance of trying to turn the Baltic into an "internal sea of NATO" (Izvestia, 2025). Regardless of Russia's responsibility in creating this standoff, NATO remains an adversary, with each of these states contributing directly to Russia's struggles in Ukraine through military and financial aid. Russia could therefore be seeking to contest NATO's growing maritime dominance in the Baltic and, simultaneously, to raise the costs of Western support for Ukraine by signalling that proximity to the conflict entails risk to one's own infrastructure. However, if either of these were the case, the results would have been predictably counterproductive. The recent damage to CUI has not had a significant impact on the countries supporting Ukraine, with NATO member states now committing to 5% of GDP for defence spending and reaffirming support for Ukraine as agreed at the Hague Summit (NATO, 2025a). Additionally, the Baltic Sea states continue to rank among the highest donors of bilateral aid to Ukraine as a percentage of GDP, despite several instances of damaged CUI (Ukraine Support Tracker, n.d.). Evidence shows that instead of weakening security, the recent incidents prompted NATO to intensify surveillance and patrols and strengthen cohesion in the Baltics.

A recent Publication by the Institute for the Study of War, following multiple drone incursions into NATO airspace over airports in Denmark, Norway, Germany, Sweden and Poland, interprets the rationale behind Russia's hostile actions towards NATO at a more strategic level. It argues that Russia is increasing the number of covert and overt attacks against NATO states in order to "create fear throughout the European population and fragment NATO's resolve." (Barros et al., 2025) It states that Russia appears to be "accelerating the informational and psychological condition setting phase — "Phase 0" — of its campaign to prepare for a possible NATO-Russia war in the future." While there is no guarantee that Russia will go to war with NATO, it demonstrates that it is aware of the possibility, and thus, the Kremlin is trying to put Russia in the best possible position should there be a war. This, in turn, demonstrates a rationale for why Russia would sacrifice a NATO build-up in the Baltic by theoretically sabotaging CUI. Doing so would effectively mean that Russia is tolerating setbacks in the Baltics to serve its long-term interests of weakening coherence within the alliance.

The primary issue remains that suspicion does not amount to proof. While precedent, capability, circumstantial evidence, and speculative strategic rationale create grounds to suspect Russia, it is not sufficient to assign responsibility. This duality is illustrated by CDR Urb's comment that Russia's "'poking' has been ongoing and intensified since the war [in Ukraine]. Incidents may cause automatic suspicion of Russia, even if it is not guilty." The Nord Stream sabotage in 2022 should serve as a lesson. Initial Western accusations against Russia have since given way to evidence implicating a Ukrainian-linked team, though without definitive state-level attribution (Bundesanwaltschaft, 2025; Duffy, 2022; Olsen, 2024; Pancevski, 2024). The Nord Stream case highlights how difficult attribution can be, as even Europe's most heavily investigated and overt act of CUI sabotage has produced no definitive findings. At the time, Russia was capable and suspected of carrying out the sabotage, but the evidence suggests that it did not. Lessons from the Nord Stream need to be carried forward. Russia may often be the path of plausibility when attempting to explain man-made damage to CUI, particularly in the Baltic region, but to accuse Russia without sufficient proof is strategically counterproductive. It risks damaging the accuser's credibility, escalating tension unnecessarily, and plays into Russian disinformation. Where evidence of Russian involvement exists, high-level government actors tend to expose it. For example, in relation to the recent drone incursions over European airports, high-level state leaders, such as Friedrich Merz, and a resolution adopted by the European Parliament

directly attributed the incursions to Russia (Barros et al., 2025; *MEPs demand a unified EU response to Russian violations and hybrid warfare threats*, 2025). By contrast, high-level political leaders were markedly more cautious in blaming Russia in each case study, and there was no definitive consensus in this regard. Expert assessments reflect this ambiguity. Both CDR Urb (2025) and CDR Bratbak (2025) acknowledge that Russia could benefit from sabotaging CUI and might be responsible but stressed that this does not change the fact that there is no definitive evidence.

The ambiguity in trying to understand the rationale necessitates that the possibility of sabotage should be rooted in the facts on the ground. In the case of the Newnew Polar Bear, there is little open-source evidence linking the vessel to Russia other than the fact that it was heading to a Russian port (a normal act of trade or transit between two friendly countries), and was sailing under the flag of a state friendly to Russia. Given that a Russian cable was damaged during the incident, such an outcome would be inconsistent with the vessel acting entirely in Russia's interest, suggesting that a deliberate state-directed attack is difficult to substantiate based on the available evidence. The prosecution by China does not necessarily support either argument. If Beijing believed there was state-level intent behind the incident, then charge could serve as a form of damage control; alternatively, it could have been avoided entirely to prevent generating unnecessary international attention and scrutiny. The Yi Peng 3 case is more ambiguous because the signals from China were mixed. The vessel's conduct appeared unusual given the regional context, raising questions among investigators. At the same time, China's reluctance to allow foreign prosecutors full access could simply reflect sovereignty concerns, diplomatic caution, or mistrust of Western intentions. Alternatively, it could indicate a desire to limit scrutiny of the vessel's activities. Suspicion was heightened by the fact that, despite these concerns, the captain was not criminally charged in China, even though investigators noted that if the incident was not deliberate sabotage, it was likely the result of negligence and poor seamanship. This case remains ambiguous, aligning with the findings of the Swedish investigation. Intentional sabotage cannot be ruled out, but links to Russia remain speculative. The Eagle S is the strongest candidate for sabotage and possible Russian involvement. As noted, the vessel has been linked to Russia's so-called "shadow fleet", a network of ships often used to circumvent sanctions. Additionally, Sutherland (2025, p. 26) notes that the Eagle S was carrying sanctioned Russian fuel and had previous associations with the FSB. The scale and nature of the damage are also noteworthy,

as multiple cables were severed at a time of heightened regional sensitivity around CUI, making a simple accident less convincing. Overall, the evidence across these incidents remains largely circumstantial. While each case raises questions, particularly the Eagle S, which shows the strongest links to Russia, there is still no conclusive proof that any of the vessels intentionally dropped their anchors on behalf of Russia.

The pattern of recurring vulnerability is less ambiguous and deserves more focus. Multiple major incidents involving both pipelines and telecommunications cables have taken place within two years in the same maritime corridor. Irrespective of whether Russia is responsible, the consequences have been costly, with Balticconnector and EstLink 2 requiring expensive, time-consuming repairs that disrupted energy flows. These outcomes justify precautionary responses, which can be directed at ships, their crews, and operating companies to discourage negligent or reckless behaviour, even when state involvement cannot be proven. Concurrently, states are right to remain alert to the broader strategic danger. Russia possesses both the capability and could very well target CUI in a period of escalation. Thus far, the damage has been episodic and repairable, but the same methods could easily be scaled and coordinated by a more hostile Kremlin. Civilian vessels dragging their anchors have already shown the fragility of seabed infrastructure. Therefore, a synchronised campaign against multiple interconnectors or several telecommunications cables at once could be devastating. In peacetime, accidents may be disruptive but containable, whereas in wartime, such activity could present fundamental challenges to economies, state apparatus, and even people's lives. In some ways, these incidents are actually a gift to NATO. They create enough concern and demonstrate a critical vulnerability to prompt renewed investment and attention in protecting CUI, without the shock and cost of a full-scale, coordinated sabotage campaign.

6. Lessons and Recommendations for the Protection of CUI

The preceding analysis highlights recurring vulnerabilities in both national and allied responses. The following section distils these observations into lessons and recommendations for strengthening the protection of CUI.

6.1. Punishment and Deterrence

Deterrence in the protection of CUI rests on the credible imposition of costs for vessels that damage it. Unless ships perceive that damaging cables or pipelines, whether through negligence or intent, carries real and unavoidable consequences, the incentives for carelessness or malign action remain unchanged. In this sense, preventing human damage to CUI depends on visible precedent. The EstLink 2 incident remains instructive. Finnish authorities acted swiftly by boarding the Eagle S and initiating criminal proceedings. The subsequent seizure of the vessel not only secured evidence but also imposed reputational and legal costs on the crew. By contrast, both the Balticconnector and Yi Peng 3 incidents illustrate what happens when this chain fails. In the Balticconnector case, it was believed that Finland lacked jurisdiction over the Newnew Polar Bear in its EEZ, leaving the vessel unchallenged and preventing a domestic investigation. In the Yi Peng 3 case, China asserted control over inspection procedures, effectively insulating the vessel from external scrutiny. The case study comparisons reveal that deterrence requires two linked capacities. First is the immediate responsiveness at the operational level. If sabotage is suspected, the ability to gather evidence is crucial. The most reliable way to do this is by boarding the ship to investigate physical evidence and interrogate the crew as with the Eagle S. CDR Urb (2025) suggests that perhaps the only way to establish proof in an instant of state-sponsored sabotage is via a confession from a crew member, captain or relevant person. This requires having the crew in custody. Second, the capability and willingness to impose a cost on the perpetrator. In the cases of complete negligence, where improper inspections or poor seamanship occur, legal proceedings should be seriously considered. Nevertheless, states should exercise restraint and avoid a maritime witch hunt, which would hinder freedom of navigation. Sweden has set a good precedent for this. In January 2025, Sweden seized a Maltese-flagged vessel suspected of sabotaging a telecommunications cable between Sweden and Estonia (Åklagarmyndigheten, 2025). The vessel was released after it was determined that the damage was clearly not an instance of sabotage (Säkerhetspolisen, 2025).

6.2. Building a Picture

Underlying the ability to impose costs is the challenge of detection. States must be able to link physical damage to specific vessels, and to do so quickly enough that follow-up action remains feasible. CDR Bratbak (2025) stressed, "Priority should be on building a clear maritime situational picture showing where vessels are and what they are doing. NATO needs to know where and when cable breaks occur so it can respond as necessary. Legal frameworks must allow responsibility to be assigned to actors. Infrastructure operators should have well-rehearsed protocols detailing who to call when a break occurs, and these procedures should be trained in advance to ensure rapid, coordinated action." The EstLink 2 case demonstrates how an effective maritime picture can shape favourable outcomes. The rapid reporting of the fault to authorities enabled a prompt and coordinated response, preventing the Eagle S from dragging its anchor over the EstLink 1 (Bratbak, 2025). The lesson here is that deterrence is inseparable from surveillance capacity. Technical monitoring systems such as sonar and acoustic detection in busy or shallow seas can improve the attribution chain, but only if integrated with clear reporting protocols and rehearsed escalation procedures. As CDR Bratbak (2025) highlighted, infrastructure operators must know "who to call when a break occurs", and states must ensure that these calls trigger pre-defined, rapid responses.

6.3. Legal Reform and Jurisdiction

The most persistent obstacle to deterrence remains legal jurisdiction. International frameworks such as UNCLOS and the 1884 Submarine Cables Convention leave enforcement primarily in the hands of flag states. As the Yi Peng 3 case illustrated, this enables states to shield vessels from scrutiny by invoking exclusive jurisdiction. As most states depend on CUI in some shape or form, there is likely a common interest in enhancing legal protection through multilateral channels like the United Nations. However, ironing out the details and establishing consensus could take years. Where more immediate action can be taken, it should. There are legal arguments for states to enforce measures against ships in their EEZ, and not just the territorial sea. For instance, although Finland believed it did not have jurisdiction to take enforcement measures over the Newnew Polar Bear, there were arguable legal

grounds. Ringbom and Lott (2024) justify that Finland possessed legal arguments to take enforcement measures in its EEZ against the Newnew Polar Bear by interpreting UNCLOS dynamically, stressing that Articles 56, 73, 79, 113, 220 and 221, when read in light of the Convention's object and purpose, support coastal state jurisdiction to investigate and even interdict vessels suspected of damaging pipelines on the continental shelf.

However, the most pertinent solution can come from domestic laws. CDR Urb (2025) observed that prior to reforming it, maritime law was a "mess" that actively hindered intervention, but subsequent changes have given the Estonian Navy clearer rights to act. He was referring to amendments to Estonia's Defence Forces Organisation Act and the Exclusive Economic Zone Act in April 2024. These amendments grant the Estonian Defence Forces (EDF) the authority to use force in maritime security operations in Estonia's EEZ, including the right to sink civilian vessels if deemed a threat to critical infrastructure, national defence objects, ports, structures, equipment, or vessels when other means fail (Riigikogu, 2025a, 2025b). In effect, this removes legal ambiguity, creates a deterrent effect if properly enacted, and legitimises actions to protect CUI in the EEZ. It provides a strong model for other states to consider adopting.

6.4. Enforcement

Even if detection is flawless and legal frameworks robust, deterrence fails without credible enforcement. As CDR Urb (2025) stated, "Reporting is important, but you still need credible force to stop ships." The EstLink 2 incident again provides the best example. Finland's ability to compel the Eagle S to comply by boarding demonstrated that interdiction was operationally feasible. Similarly, Denmark's decision to position naval assets around the Yi Peng 3 signalled both capacity and intent to act. Nevertheless, for smaller states such as Estonia, enforcement capacity remains limited. CDR Urb (2025) gives two cases where stateless merchant ships traversed Estonia's EEZ. In one instance, the vessel obeyed orders to divert to an Estonian port; on a separate occasion, the ship refused, and Estonia lacked a vessel capable of stopping it. The ship continued its path unimpeded. Although not related to CUI, the episodes demonstrate how legal rights without sufficient naval presence are meaningless. NATO's presence may offset these gaps, yet as CDR Urb (2025) noted, NATO's rules of engagement are unlikely to extend to cases of criminal

damage. Enforcement, therefore, begins at the domestic level, with states needing to ensure their own naval and coast guard have adequate capacity to render legal rights enforceable.

6.5. Resilience

Deterrence, however, cannot eliminate all risk. States must also invest in resilience, ensuring that systems have multiple points of failure and damage resistance built in. The case studies show a clear divergence between telecommunications cables and energy infrastructure. Telecommunications networks already benefit from greater redundancy because traffic can be rerouted across alternative lines with minimal disruption (Belson, 2024). The case studies evidently show that their repair cycles are both quicker and cheaper than pipelines or interconnector cables. However, resilience must be designed with deliberate sabotage in mind. If multiple cables or pipelines were targeted simultaneously, peacetime redundancy could quickly evaporate, potentially leading to blackouts or communication outages across entire regions. Internet traffic can only be rerouted to the extent that alternative and functional telecommunications cables can handle the additional capacity. Laying additional cables can contribute to resilience by creating additional points of failure, but it is an expensive and static solution. Enhancing repair capacity could provide a more flexible solution as dedicated repair ships can be deployed to restore services wherever damage occurs, reducing downtimes in the event of multiple breakages.

The case studies indicate that pipelines and interconnectors tend to be more vulnerable than submarine telecommunications cables. The Balticconnector rupture disrupted gas supplies and revealed Finland's dependence on a narrow set of alternatives, while Estonia's more diversified energy system proved considerably more resilient. In both peacetime and wartime, energy import diversification is essential, and states would be wise to emulate Estonia's model. This means investing in multiple interconnectors, LNG terminals, and other alternative supply routes to ensure that the loss of even multiple assets does not lead to energy shortfalls. This could occur at the national level, or, as in Estonia's case, alongside regional partners within NATO. Strategic reserves of natural gas and oil are a particularly valuable resilience measure, as shown in the Balticconnector case study. They allow flows to continue even when imports are interrupted, providing governments with time

to organise repairs or shift to alternative sources, while keeping prices stable. By maintaining such reserves as a backstop, states can ensure that even severe disruptions are absorbed with relatively low risk. NATO members are well placed to take this agenda forward. At the Hague Summit Declaration, the states agreed to increase defence spending to 5% of GDP, with 1.5% allocated to areas including the protection of critical infrastructure (NATO, 2025a). Using this commitment to expand import redundancy, build strategic reserves, and build emergency capacity would strengthen national energy security while allowing states to fulfil NATO obligations.

6.6. Multilateral Security Frameworks

Coordination with allies has been central to the Baltic Sea states' responses since these incidents began. In both the Yi Peng 3 and Eagle S cases, the vessels involved sailed under foreign flags and operated across multiple EEZs, limiting the jurisdiction of any single authority. Effective investigation and enforcement, therefore, was aided by cooperation between allies. This applied across resilience, enforcement, and deterrence. For instance, the Balticconnector rupture highlighted the value of prior EU-backed integration, as Estonia relied extensively on its new integration with the EU energy grid. Similarly, the Eurojust-led Joint Investigation Team on the Yi Peng 3 incident provided a cross-border framework that lent credibility to the inquiry and signalled European unity, even when jurisdictional obstacles constrained access to evidence. Denmark's shadowing of the vessel, without exercising a right of boarding, underscored the limits of unilateral enforcement but also showed how coordination can apply pressure for subsequent cooperation.

NATO's response has so far been measured and proportional, increasing surveillance, patrolling and developing institutional structures focused on protecting CUI. For instance, the UK-led JEF launched Operation Nordic Warden on three occasions after the CUI was damaged in the Baltic Sea. The most recent operation followed the EstLink 2 incident and integrated sensor technology, anomaly detection, and real-time intelligence-sharing across 22 maritime zones in northern Europe (Ministry of Defence and Foreign, Commonwealth & Development Office, 2025). These acts of surveillance combined with physical deterrence have been reinforced by institutional developments that seek to increase to improve the understanding, responsiveness, and resilience of CUI. At the NATO level, there are initiatives including the

standing NATO Maritime Group One and the NMCSCUI, and at the EU level, measures such as the EU Action Plan on Cable Security and the EU-NATO Task Force on the Resilience of Critical Infrastructure (2023). These steps indicate that NATO and the EU are moving in the right direction and taking the threat to CUI seriously. Both organisations must lead on regional strategies, combining persistent surveillance, targeted research, and coordinated patrolling. Without such measures, CUI will be more vulnerable to malign actors and careless vessels.

Baltic Sentry and Nordic Warden were large military responses, suggesting an understanding that the threats to CUI extend beyond the civilian domain. These cases sit within a broader allied effort to monitor and deter sabotage. The effective result of the measures is that, since the Nord Stream sabotage, the Baltic Sea has transitioned into a body of water bristling with surveillance equipment, maritime patrols bolstered by response frameworks. This correlates with an increasingly serious response to further CUI incidents. In this regard, in the direction of travel with multilateral frameworks, NATO and the EU have responded adequately and should maintain their current course. However, multilateral solutions should not lead to domestic complacency. It must be remembered that the Eagle S response, although having support from states like Estonia, was spearheaded by domestic Finnish action. Resilience measures need to be integrated into the domestic industrial strategy and cannot be purely offshored to NATO.

7. Conclusion

This article has analysed three cases of damage to CUI in the Baltic Sea in order to draw lessons for policy. The Balticconnector, Yi Peng 3, and EstLink 2 incidents illustrate both the fragility of CUI and the difficulties NATO faces in proving intent and assigning responsibility when they suspect sabotage. While suspicion frequently falls on Russia, given its capabilities and incentives, attribution currently remains contested and legally unproven. The central challenge revealed by this research is therefore not the confirmation of responsibility, but the protection of CUI under conditions of uncertainty. Yet the danger extends further. Russia has placed sustained emphasis on the seabed as a domain of strategic competition and retains both the motive and the capability to target CUI more deliberately in the future, particularly in a period of heightened escalation or war. If such attacks were coordinated

and sustained, they could overwhelm redundancy and transform manageable disruptions into severe strategic crises for NATO states.

The wider implication is that CUI protection must be treated as a strategic priority for NATO. This study supports the consensus that layered approaches are the best path forward. These include credible deterrence through enforcement, stronger attribution and surveillance mechanisms, reforms to close legal enforcement gaps, and sustained investment in redundancy and resilience. NATO and the EU play a vital coordinating role for responding to incidents, coordinating investigations, and building cross-border resilience. Nevertheless, states must take action at the domestic level to strengthen enforcement inside their EEZs and build national energy reserves. NATO's renewed spending commitments provide an opportunity to direct resources toward this agenda, ensuring that infrastructure security complements traditional defence capabilities. The incidents examined in this study also show that techniques which have so far resulted only in episodic and repairable damage could readily be scaled into a coordinated campaign of disruption. By taking protective measures now, European states will not only reduce the risk of present-day interference but also harden their infrastructure against more sophisticated threats in the future.

Future research should compare Baltic case studies with those in other global theatres. Instances of sabotage, or suspected sabotage, have been reported in both the Red Sea and the South China Sea. Comparing the lessons from the Baltic Sea with cases from other regions could determine if there are generalisable lessons for protecting CUI that apply to states worldwide. While this research reveals lessons for CUI policy, policy proposals should be investigated in greater depth to assess for effectiveness and implementation strategies. If this work were to be extended, a deep engagement with the literature on deterrence theory would be necessary and could help flesh out lessons into full policy proposals.

Bibliography

A'Hearn, B. (2024). Finland and the Baltics without the Balticconnector: market impact and outlook for the rest of winter 2023–24. In The Oxford Institute for Energy Studies.

Åklagarmyndigheten. (2025). *Preliminary investigation launched after cable break in the Baltic Sea.* Retrieved 11 October 2025 from https://www.aklagare.se/for-media/pressmeddelanden/2025/januari/forundersokning-inledd-efter-kabelbrott-i-ostersjon/

Ålander, M., Eggen, K.-A., Kjartansson, B. B., Kohv, M., Bērziņa, I., Oksanen, A. P., Roževič, A., & Serritzlev, J. (2024). *Tracking the Russian Hybrid Warfare – Cases From Nordic-Baltic Countries.* Stockholm Free World Forum. https://frivarld.se/rapporter/tracking-the-russian-hybrid-warfare-cases-from-nordic-baltic-countries/

Ampatzidis, D. (2024, December 5). *Damage to Baltic Sea Communication Cables.* Marine Traffic. Retrieved 22 August 2025 from https://www.marinetraffic.com/en/maritime-news/34/risk-and%20compliance/2025/11692/damage-to-baltic-sea-communication-cables

Astier, H., & Kirby, P. (2024). *Germany suspects sabotage behind severed undersea cables.* BBC News. Retrieved 18 August 2025 from https://www.bbc.co.uk/news/articles/c9dl4vxw501o

Barros, G., Harward, C., Iredale, V., Matthews, I., Olmsted, J., & Young, J. (2025, October 6). *Russian Offensive Campaign Assessment.* Institute for the Study of War. Retrieved 10 October 2025 from https://understandingwar.org/research/russia-ukraine/russian-offensive-campaign-assessment-october-6-2025/

Bashfield, S. (2024). Defending seabed lines of communication. *Australian Journal of Maritime & Ocean Affairs, 17*(4), pp. 1–13. Retrieved 19 August 2025 from https://doi.org/10.1080/18366503.2024.2363607

Belson, D. (2024, November 20). *Resilient Internet connectivity in Europe mitigates impact from multiple cable cuts.* Cloudflare. Retrieved 19 August 2025 from https://blog.cloudflare.com/resilient-internet-connectivity-baltic-cable-cuts/

Bermingham, F. (2024, August 13). Beijing admits Hong Kong-flagged ship destroyed key Baltic gas pipeline 'by accident'. *South China Morning Post.* Retrieved 18 August 2024 from https://www.scmp.com/news/china/diplomacy/article/3274120/china-admits-hong-hong-flagged-ship-destroyed-key-baltic-gas-pipeline-accident

Besch, S., & Brown, E. (2024). Securing Europe's Subsea Data Cables. In Carnegie Endowment for International Peace. https://www.jstor.org/stable/resrep65605

Black, J., Retter, L., Soest, H. v., & Fine, H. (2025). Evolving threats to critical undersea infrastructure: Implications for European security and resilience. *RAND: Expert Insights.* https://www.rand.org/pubs/perspectives/PEA3800-1.html

Bratbak, C. P. (2025). *Interview with Commander Pål Bratbak regarding damage to CUI in the Baltic Sea* [Interview].

Brooke-Holland, L. (2023). S*eabed warfare: Protecting the UK's undersea infrastructure.* UK Parliament. Retrieved from https://commonslibrary.parliament.uk/seabed-warfare-protecting-the-uks-undersea-infrastructure/

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.* https://doi.org/10.1016/j.marpol.2023.105772

Bundesanwaltschaft. (2025). *Festnahme im Zusammenhang mit der mutmaßlichen Sabotage an den "Nord Stream" Gaspipelines.* Der Generalbundesanwalt beim Bundesgerichtshof. Retrieved from https://www.generalbundesanwalt.de/SharedDocs/Pressemitteilungen/DE/2025/Pressemitteilung-vom-21-08-2025.html

Cao, C., Chen, J., Ge, Y., Li, S., Lu, Z., Zheng, X., & Zhou, P. (2022). Study on Buried Depth Protection Index of Submarine Cable Based on Physical and Numerical Modeling. *Journal of Marine Science and Engineering, 10*(2), 137. https://doi.org/10.3390/jmse10020137

Casey-Maslen, S., Galani, S., Lott, A., & Dahl, A. W. (2024). Hybrid Warfare through the Lens of Maritime Security Law. In A. Lott (Ed.), *Maritime Security Law in Hybrid Warfare* (pp. 7–27). Brill.

Cinia. (2024). *A fault in the Cinia C-Lion1 submarine cable between Finland and Germany.* Retrieved 08 August 2025 from https://www.cinia.fi/en/news/a-fault-in-the-cinia-c-lion1-submarine-cable-between-finland-and-germany

Cinia. (2025). *Ensuring a more certain digital future: Annual Report 2024.* https://www.cinia.fi/hubfs/CN-Julkaisut/Vuosikertomus-Annual-reports/Cinia_Annual_report_2024_final.pdf

Convention on the High Seas. (1958). In United Nations. Retrieved 21 August 2025 from https://treaties.un.org/pages/viewdetails.aspx?src=treaty&mtdsg_no=xxi-2&chapter=21

Cook, C., & Milne, R. (2025, August 11). Finland charges captain of Russian 'shadow fleet' ship over cable cutting. *Financial Times.* Retrieved 19 August 2025 from https://www.ft.com/content/a3110e00-9d4d-4757-9066-7af0ec925b42

Council of the European Union. (2023, October 13). *Balticconnector disruption between Finland and Estonia on 8 October 2023.* In Vol. ENER 543. Retrieved 18 August 2025 from https://data.consilium.europa.eu/doc/document/ST-14089-2023-INIT/en/pdf

Counter Terrorism Policing. (2025). *Group convicted after Russian-ordered arson attack in London.* Retrieved 21 August 2025 from https://www.counterterrorism.police.uk/group-convicted-after-russian-ordered-arson-attack-in-london/

Critical National Infrastructure. (2023). National Protective Security Authority. Retrieved 21 April 2025 from https://www.npsa.gov.uk/critical-national-infrastructure-0

Czosseck, C., Ottis, R., & Talihärm, A.-M. (2013). Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security. In M. Warren (Ed.), *Case Studies in Information Warfare and Security for Researchers, Teachers and Students* (Vol. 1, pp. 72–83). Academic Conferences Limited.

Doughty, S. (2025). *UK and Nordic-Baltic Eight Ministerial Roundtable: Joint Statement.* Gov.UK. Retrieved 04 July 2025 from https://www.gov.uk/government/news/uk-and-nordic-baltic-eight-ministerial-roundtable-joint-statement

Douglas, R., Burnett, R. B., & Davenport, T. M. (2013). *Submarine Cables: The Handbook of Law and Policy.* Martinus Nijhoff Publishers. https://books.google.nl/books?hl=en&lr=&id=LQDXAQAAQBAJ&oi=fnd&pg=PR5&dq=Subsea+cable+damage+claims+%E2%80%93+a+legal+perspective&ots=c4_4jkeBMY&sig=iWe98VhnWdCyt6JpXhR413KECIg&redir_esc=y#v=onepage&q&f=false

Duffy, K. (2022). *German lawmakers break Europe's silence on suspected Nord Stream pipeline saboteur to point the finger at Russia.* Business Insider. Retrieved 19 August 2025 from https://www.businessinsider.com/nord-stream-german-lawmakers-point-finger-russia-sabotage-pipeline-leaks-2022-9

Eleftherakis, D., & Vicen-Bueno, R. (2020). Sensors to Increase the Security of Underwater Communication Cables: A Review of Underwater Monitoring Sensors. *Sensors, 20*(3), 737. https://doi.org/10.3390/s20030737

Elering. (2024). *The suspected fault in EstLink 2 is located on the seabed of the Gulf of Finland.* Retrieved 14 August 2025 from https://elering.ee/en/article/suspected-fault-estlink-2-located-seabed-gulf-finland

Elering. (2025a). *2024 Annual report.* Retrieved 18 March 2025 from https://elering.ee/sites/default/files/2025-04/Elering_Majandusaasta-aruanne_2024_WEB_reso-72_ENG.pdf

Elering. (2025b). *System operators are planning to recover EstLink 2 repair costs through the court.* Retrieved 08 August 2025 from https://elering.ee/en/article/system-operators-are-planning-recover-estlink-2-repair-costs-through-court

Elisa. (2025a). *Elisa Annual Report 2024.* https://elisa.com/corporate/investors/annual-report/

Elisa. (2025b). *Elisa's damaged submarine cables in the Baltic Sea repaired.* Retrieved 14 August 2025 from https://elisa.com/corporate/news-room/press-releases/elisa%E2%80%99s-damaged-submarine-cables-in-the-baltic-sea-repaired/87594841499067/

Estonian Foreign Intelligence Service public report 2025. (2025). Estonian Foreign Intelligence Service. Retrieved from https://www.valisluureamet.ee/en.html

EU-NATO Task Force on the Resilience of Critical Infrastructure: Final Assessment Report. (2023). European Commission. https://commission.europa.eu/system/files/2023-06/EU-NATO_Final%20Assessment%20Report%20Digital.pdf

European Parliament. (2025). *Hybrid War: protection of undersea cables in the Baltic Sea.* Retrieved 4 July 2025 from https://www.europarl.europa.eu/committees/en/hybrid-war-protection-of-undersea-cables/product-details/20250210CHE12922

European Union. (2022). Directive (EU) of the European Parliament and of the Council: on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC 164–198 (2022). http://data.europa.eu/eli/dir/2022/2557/oja

Faucon, B., Pancevski, B., & Rasmussen, S. E. (2024, November 20). Chinese-Registered Ship Is Held in Baltic Sea Sabotage Investigation. *The Wall Street Journal.* Retrieved 18 August 2025 from https://www.wsj.com/world/europe/chinese-registered-ship-is-held-in-baltic-sea-sabotage-investigation-27929472

Fingrid. (2024). *EstLink 2 electricity transmission link between Finland and Estonia has failed, investigation continues.* Retrieved 7 August 2025 from https://www.fingrid.fi/en/news/news/2024/estlink-2-electricity-transmission-link-between-finland-and-estonia-has-failed-investigation-continues2/

Fingrid. (2025). 2024: *Fingrid Annual Review.* https://www.fingrid.fi/en/company/annual-report/

Frazier, K. (2022). Policy Proposals for the United States to Protect the Undersea Cable System. *Journal of Law, Technology & the Internet, 13*(1). https://heinonline.org/HOL/Page?public=true&handle=hein.journals/caswestres13&div=3&start_page=[ii]&collection=journals&set_as_cursor=25&men_tab=srchresults

Fridman, O. (2018). R*ussian "Hybrid Warfare": Resurgence and Politicalisation.* Hurst.

GasGrid. (2024). *Transmitting Energy: Annual Report 2023.* Retrieved from https://gasgrid.fi/wp-content/uploads/Gasgrid_Annual-Report-2023.pdf

GasGrid. (2025). *Transmitting Energy: Annual Report 2024.* Retrieved from https://gasgrid.fi/wp-content/uploads/Gasgrid_Annual-Report-2024_96dpi.pdf

Galeotti, M. (2019). *Russian Political War: Moving Beyond the Hybrid.* Routledge.

Ganz, A., Camellini, M., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2024). Submarine Cables and the Risks to Digital Sovereignty. *Minds and Machines, 34*(3), 31. https://doi.org/10.1007/s11023-024-09683-z

Government of Sweden. (2024). *Statement regarding damaged communications cable by the Swedish and Lithuanian ministers for defence.* (2024). Retrieved from https://www.government.se/press-releases/2024/11/statement-regarding-damaged-communications-cable-by-the-swedish-and-lithuanian-ministers-for-defence/

Habib, M. T., & Shamrir Al Af, S. M. (2025). Maritime asymmetric warfare strategy for smaller states: lessons from Ukraine. *Small Wars & Insurgencies, 36*(1), 29–58. https://doi.org/10.1080/09592318.2024.2397171

Hoffman, F. (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars.* Potomac Institute for Policy Studies.

Iltalehti. (2023, October 10). *Puolustusvoimat on ryhtynyt "toimenpiteisiin", Suomi yhä normaaliolojen valmiudessa – Nämä asiat nyt tiedetään.* Retrieved 20 March 2025 from https://www.iltalehti.fi/politiikka/a/07fa3666-2804-4d9a-98c1-91a3056e2995

Izvestia. (2025). *The Russian Foreign Ministry announced the transformation of the Baltic Sea by NATO into a zone of confrontation.* Retrieved 26 August 2025 from https://en.iz.ru/en/1910682/2025-06-25/russian-foreign-ministry-announced-transformation-baltic-sea-nato-zone-confrontation

Kraska, J., & Pedrozo, R. (2022). Seabed Warfare. In J. Kraska & R. Pedrozo (Eds.), *Disruptive Technology and the Law of Naval Warfare* (pp. 169–201). Oxford University Press. https://doi.org/10.1093/oso/9780197630181.003.0007

Larsen, J. A., & Lasconjarias, G. (2015). *NATO's Response to Hybrid Threats.* NATO Defence College.

Larsson, O. L. (2024). Sea blindness in grey zone preparations. *Defence Studies, 24*(3), 399–420. https://doi.org/10.1080/14702436.2024.2359913

Loik, R. (2024). Undersea Hybrid Threats in Strategic Competition: The Emerging Domain of NATO–EU Defense Cooperation. *Journal on Baltic Security, 10*(2), 1–25. https://doi.org/10.57767/jobs_2024_008

Lott, A. (2024). The Legal Resilience of Critical Offshore Infrastructure to Hybrid Warfare. In A. Lott (Ed.), *Maritime Security Law in Hybrid Warfare* (pp. 125–254). Brill. https:/doi.org/10.1163/9789004707993_007

LRT. (2024). *Chinese ship suspected of deliberately cutting cables in Baltic Sea – media.* Retrieved 18 August 2025 from https://www.lrt.lt/en/news-in-english/19/2426033/chinese-ship-suspected-of-deliberately-cutting-cables-in-baltic-sea-media

Maritime Security Centre of Excellence (2024). Protection of Maritime Critical Infrastructure and the Seabed. *4th Maritime Security Conference Proceedings.* MARSEC COE.

MEPs demand a unified EU response to Russian violations and hybrid warfare threats. (2025). European Parliament. Retrieved 11 October 2025 from https://www.europarl.europa.eu/news/en/press-room/20251003IPR30664/call-for-a-unified-eu-response-to-russian-violations-and-hybrid-warfare-threats

Miętkiewicz, R. (2025). Hybrid threats in the Baltic Sea. The results of analysis of countermeasure options. In *Terrorism – Studies, Analyses, Prevention, special edition*, (pp. 35–70). Akademia Marynarki Wojennej im. Bohaterów Westerplatte. https://doi.org/10.4467/27204383TER.25.014.21517

Ministry of Defence. (2025). *Strategic Defence Review Making Britain Safer: secure at home, strong abroad.* (2025). Gov.UK. Retrieved from https://assets.publishing.service.gov.uk/media/683d89f181deb72cce2680a5/The_Strategic_Defence_Review_2025_-_Making_Britain_Safer_-_secure_at_home__strong_abroad.pdf

Ministry of Defence and Foreign, Commonwealth & Development Office. (2025, January 6). *Joint Expeditionary Force activates UK-led reaction system to track threats to undersea infrastructure and monitor Russian shadow fleet.* GOV.UK. Retrieved from https://www.gov.uk/government/news/joint-expeditionary-force-activates-uk-led-reaction-system-to-track-threats-to-undersea-infrastructure-and-monitor-russian-shadow-fleet

Monaghan, S., Svendsen, O., Darrah, M., & Arnold, E. (2023). *NATO's Role in Protecting Critical Undersea Infrastructure.* Center for Strategic an International Studies. Retrieved 21 April 2025 from https://www.csis.org/analysis/natos-role-protecting-critical-undersea-infrastructure

Moss, S. (2024). *Lithuania-Sweden subsea cable cut, was 10m from severed Finnish-German cable.* Data Center Dynamics. Retrieved 23 August 2025 from https://www.datacenterdynamics.com/en/news/lithuania-sweden-subsea-cable-cut-was-10m-from-severed-finnish-german-cable/

Murphy, E. L., & Pearl, M. (2025, April 4). *China's Underwater Power Play: The PRC's New Subsea Cable-Cutting Ship Spooks International Security Experts.* Center for Strategic and International Studies. Retrieved 23 May 2025 from https://www.csis.org/analysis/chinas-underwater-power-play-prcs-new-subsea-cable-cutting-ship-spooks-international

Murphy, M., Hoffman, F. G., & Schaub, G. Jr. (2016). *Hybrid Maritime Warfare and the Baltic Sea Region.* Center for Military Studies Universtiy of Copenhagen. https://www.jstor.org/stable/resrep05271.1

National Prosecution Authority Finland. (2025). *Charges have been brought in the case concerning the cutting of submarine cables in the Gulf of Finland during Christmas 2024.* Retrieved 13 August 2025 from https://syyttajalaitos.fi/en/-/charges-have-been-brought-in-the-case-concerning-the-cutting-of-submarine-cables-in-the-gulf-of-finland-during-christmas-2024

NATO. (2023). *NATO Secretary General addresses protection of critical undersea infrastructure, support to Ukraine with EU Defence Ministers.* Retrieved 4 May 2025 from https://web.archive.org/web/20250514043926/https://www.nato.int/cps/en/natohq/news_220058.htm

NATO. (2025a). *The Hague Summit Declaration.* Retrieved from https://www.nato.int/cps/en/natohq/official_texts_236705.htm

NATO. (2025b). *NATO's Baltic Sentry steps up patrols in the Baltic Sea to safeguard Critical Undersea Infrastructure.* Retrieved 20 March 2025 from https://mc.nato.int/media-centre/news/2025/nato-baltic-sentry-steps-up-patrols-in-the-baltic-sea-to-safeguard-critical-undersea-infrastructure

Newbill, C. M. (2019). Defining Critical Infrastructure for a Global Application. *Indiana Journal of Global Legal Studies, 26*(2), 761–780. https://www.repository.law.indiana.edu/ijgls/vol26/iss2/11/

Olsen, J. M. (2024). *Denmark closes probe into Nord Stream blasts saying there's not enough grounds for a criminal case.* AP News. Retrieved 19 August 2025 from https://apnews.com/article/denmark-nord-stream-pipeline-explosion-investigation-sweden-germany-8fe8be53ff1c10b11ec2d0ad1d8dd615

Ots, M. (2024). *Balticconnector rupture led to lower gas prices in Estonia, higher in Finland.* ERR. Retrieved 18 August 2025 from https://news.err.ee/1609287660/balticconnector-rupture-led-to-lower-gas-prices-in-estonia-higher-in-finland

Paasch, K. R. (2024). *Everything you need to know about the Yi Peng 3 and cable damage in the Baltic Sea.* ScandAsia. Retrieved 18 August 2025 from https://scandasia.com/everything-you-need-to-know-about-the-yi-peng-3-and-cable-damage-in-the-baltic-sea/

Pancevski, B. (2024). A Drunken Evening, a Rented Yacht: The Real Story of the Nord Stream Pipeline Sabotage. *The Wall Street Journal.* Retrieved 17 July 2025 from https://www.wsj.com/world/europe/nord-stream-pipeline-explosion-real-story-da24839c

Pedrozo, R. (2025). Implementing Agreement to Enhance Protection of Critical Undersea Infrastructure. *International Law Studies*, *106*. https://digital-commons.usnwc.edu/ils/vol106/iss1/7/

Poliisi. (2023). *Investigations into the gas pipeline damage proceed.* Retrieved 24 August 2025 from https://poliisi.fi/-/kaasuputkivaurion-tutkinnat-etenevat?languageId=en_US

Poliisi. (2024). *The police transfer tanker Eagle S to Kilpilahti on Saturday.* Retrieved 07 August 2024 from https://poliisi.fi/-/eagle-s-sailioalus-siirretaan-kilpilahteen-lauantaina

Poliisi. (2025a). *Anchor allegedly involved in cable ruptures on Christmas day recovered in Gulf of Finland.* Retrieved 23 May 2025 from https://poliisi.fi/en/-/anchor-allegedly-involved-in-cable-ruptures-on-christmas-day-recovered-in-gulf-of-finland

Poliisi. (2025b). *Cooperation in Balticconnector case to continue.* https://poliisi.fi/en/-/cooperation-in-balticconnector-case-to-continue

Poliisi. (2025c). *Criminal Investigation by the NBI into Cable Damage in the Gulf of Finland Concluded.* https://poliisi.fi/en/-/criminal-investigation-by-the-nbi-into-cable-damage-in-the-gulf-of-finland-concluded

Poliisi. (2025d). *Eagle S tanker to move to international waters under Border Guard's control.* Retrieved 7 August 2025 from https://poliisi.fi/en/-/eagle-s-tanker-to-move-to-international-waters-under-border-guard-s-control

Praks, H. (2024). *Hybrid CoE Working Paper 32: Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage.* Hybrid CoE. https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-32-russias-hybrid-threat-tactics-against-the-baltic-sea-region-from-disinformation-to-sabotage/

Reuters. (2023). *Kremlin, asked about damaged Baltic pipeline, says threats to Russia 'unacceptable'.* Retrieved 26 August 2025 from https://www.reuters.com/world/europe/kremlin-asked-about-damaged-baltic-pipeline-says-threats-russia-unacceptable-2023-10-23/

Reuters. (2024). *Sweden urges Chinese ship to return for undersea cable investigation.* Retrieved 22 August 2025 from https://www.reuters.com/world/sweden-asks-chinese-ship-yi-peng-3-move-swedish-waters-pm-says-2024-11-26/

Reuters. (2025a). *Chinese captain in Baltic sea cable damage case appears in Hong Kong court.* Retrieved 25 August 2025 from https://www.reuters.com/world/china/chinese-captain-baltic-sea-cable-damage-case-appears-hong-kong-court-2025-07-04/

Reuters. (2025b). *Tanker seized by Finland over ripped cables won't face cargo sanctions probe.* Retrieved 23 August 2025 from https://www.reuters.com/world/europe/finnish-customs-will-not-pursue-criminal-investigation-eagle-s-crew-2025-01-16/

Richterova, D., Grossfeld, E., Long, M., & Bury, P. (2024). Russian Sabotage in the Gig-Economy Era. *The RUSI Journal, 169*(5), 10–21. https://doi.org/10.1080/03071847.2024.2401232

Riigikogu. (2025a). Amendment to the Estonian Defence Forces Organisation Act. https://www.riigiteataja.ee/en/eli/ee/506012025006/consolide/current

Riigikogu. (2025b). Amendment to the Exclusive Economic Zone Act. https://www.riigiteataja.ee/en/eli/524042025001/consolide

Ringbom, H., & Lott, A. (2024). Sabotage of Critical Offshore Infrastructure: a Case Study of the Balticconnector Incident. In A. Lott. (Ed.), *Maritime Security Law in Hybrid Warfare* (pp. 155–185). https://brill.com/edcollchap/book/9789004707993/BP000019.xml

Runde, D., Murphy, E., & Bryja, T. (2024). *Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition.* Retrieved from http://www.jstor.org/stable/resrep62567

Säkerhetspolisen. (2025). *Seizure of suspected ship for cable breach lifted.* Retrieved 11 October 2025 from https://sakerhetspolisen.se/ovriga-sidor/nyheter/nyheter/2025-02-03-beslag-av-misstankt-fartyg-for-kabelbrott-havs.html

Sari, A. (2025). Protecting maritime infrastructure from hybrid threats: legal options. *Hybrid CoE Research Reports, 14.* https://www.hybridcoe.fi/publications/hybrid-coe-research-report-14-protecting-maritime-infrastructure-from-hybrid-threats-legal-options/

Schaller, C. (2024). Russia's Mapping of Critical Infrastructure in the North and Baltic Seas – International Law as an Impediment to Countering the Threat of Strategic Sabotage? *Nordic Journal of International Law, 93*, 202–236. https://brill.com/view/journals/nord/93/2/article-p202_002.xml?trk=public_post_comment-text

Statens Haverikommission. (2025). SHK:s observationer ombord på det kinesiska lastfartyget YI PENG 3. Retrieved 22 August 2025 from https://shk.se/download/18.ffd11bf19626c638f3623/1744702687838/YP3-PM%20 2025-04-15%20-%20slutlig.docx.pdf

Sutherland, E. (2025). The Yi Peng 3 and Eagle S incidents-cutting cables in the Baltic Sea. In University of the Witwatersrand, LINK Centre.

Sytas, A. (2024). *Estonia says China has not responded to subsea cables probe request.* Reuters. Retrieved 25 August 2025 from https://www.reuters.com/world/estonia-says-china-has-not-responded-subsea-cables-probe-request-2024-05-28/

Telegeography. (2025). *https://submarine-cable-map-2025.telegeography.com/*. Retrieved 22 August 2025 from https://submarine-cable-map-2025.telegeography.com/

The White House. (2024). *National Security Memorandum on Critical Infrastructure Security and Resilience.* Retrieved from https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/

Traficom. (2024). *Traficom and other authorities investigate cable damage in the Gulf of Finland.* Retrieved 14 August 2024 from https://www.traficom.fi/en/news/traficom-and-other-authorities-investigate-cable-damage-gulf-finland

Trakimavičius, L. (2021). The Hidden Threat to Baltic Undersea Power Cables. In NATO Energy Security Centre of Excellence. Retrieved 21 August 2025 from https://www.enseccoe.org/wp-content/uploads/2024/01/2021-12-the-hidden-threat-to-baltic-undersea-power-cables-final.pdf

Ukraine Support Tracker. (n.d.). Kiel Institue for the World Economy. Retrieved 24 August 2025 from https://www.ifw-kiel.de/topics/war-against-ukraine/ukraine-support-tracker/

United Nations Law of the Sea. (1982). In (pp. 7–208). Montego Bay, Jamaica: United Nations.

Urb, C. T. (2025). *Interview with Commander Taavi Urb regarding damage to CUI in the Baltic Sea* [Interview].

Walker, S. (2025). *Poland to close Russian consulate in Kraków over Warsaw fire.* The Guardian. Retrieved 21 August 2025 from https://www.theguardian.com/world/2025/may/12/poland-to-close-russian-consulate-krakow-warsaw-shopping-centre-fire

Wasiuta, O. (2023). Russian Threats to the Submarine Internet Cable Infrastructure. *Zeszyty Naukowe, 87*. https://doi.org/10.5604/01.3001.0053.9127

Wright, H. (2024). *In brief: Estonia-Finland cable disruption.* ERR News. Retrieved 26 August 2025 from https://news.err.ee/1609560782/in-brief-estonia-finland-cable-disruption

YLE. (2023). Niinistö: Nato willing to help with pipeline investigation. Retrieved 3 October 2025 from https://yle.fi/a/74-20054419

YLE. (2024). *Maps reveal the path of the Eagle S on Christmas Day.* Retrieved 15 August 2025 from https://yle.fi/a/74-20133606

Acknowledgement

I would like to express my heartfelt thanks to all the wonderful people who have supported me throughout the long process of completing this research. First and foremost, I am deeply grateful to Dr Ksenia Kirkham, whose guidance, thoughtful reflection, and encouragement helped me shape and refine my ideas. I also extend my sincere appreciation to the Allied Rapid Reaction Corps for sponsoring this dissertation and for inviting me to present my research. In particular, I would like to thank Major Pete Preisinger, who not only connected me with a wide range of subject matter experts but also played a crucial role in helping me build the foundation of this project. His patience with my endless questions on critical infrastructure was invaluable. I am especially thankful to Commander Taavi Urb and Commander Pål Bratbak, who generously took time from their busy schedules to be interviewed. Their expertise and deep experience in the Baltic theatre offered invaluable perspectives, opening new avenues of thought and insight I would not have otherwise been able to explore. Finally, I would like to thank everyone I spoke with over the course of writing this dissertation who are not mentioned by name here. Your reflections, comments, and perspectives (no matter how small) were instrumental in shaping my thinking and strengthening this research.

GEORGE BURDEN, MA (International Conflict Studies)
Response Operations Manager at Solace Global, United Kingdom