The Attribution Problem at Sea

28 APRIL 2026

Elisabeth Schäfer



Introduction

Between October 2023 and January 2025, four incidents of damage to critical underwater infrastructure (CUI) occurred in the Baltic Sea. In each case, vessels dragged their anchors across the seabed. It remained unclear whether these incidents were accidental or deliberate (Kirchberger, 2025). The case of the Yi Peng 3 illustrates this ambiguity: while technical evidence identified the vessel as the most likely suspect, uncertainty about intent and legal and political constraints limited attribution. This ambiguity creates fundamental challenges for policymakers, as limited attribution constrains both responses and deterrence.

This brief examines whether the concept of the "attribution problem", originally developed in cybersecurity policy, can be applied to sabotage of CUI in the Baltic Sea. It argues that CUI sabotage is shaped less by technical uncertainty than by political, legal, and discursive constraints. By applying the "Q-Model" by Rid and Buchanan (2015), the analysis shows that attribution unfolds as a multi-layered process in which ambiguity persists across all stages, reducing the effectiveness of deterrence.

Conceptual Framework: Attribution and the Q-Model

To better understand these challenges, the following section introduces the concept of the attribution problem and its operationalisation in the Q-Model by Rid and Buchanan (2015).

In cybersecurity policy research, attribution describes the process of assigning responsibility for a cyberattack to a specific actor. It encompasses three interrelated dimensions: technical, legal, and political attribution, commonly referred to as the "politics of attribution" (Bendiek & Schulze, 2021). Technical attribution involves the collection and analysis of forensic evidence, Indicators of Compromise (IoC), to reconstruct an attack and generate hypotheses about perpetrators. Political attribution focuses on identifying responsible actors based on political factors and strategic considerations. While remaining sensitive to evidentiary limitations and escalation risks, it often employs mechanisms such as "naming and shaming" (Bendiek & Schulze, 2021). Legal attribution requires a higher evidentiary standard and enables formal accountability, such as criminal prosecution (Bendiek & Schulze, 2021). Attribution decisions across these dimensions can diverge. States may engage in political attribution despite limited technical or legal evidence when it is strategically advantageous (Bendiek & Schulze, 2021), whereas failure to attribute can undermine deterrence and misattribution may lead to unintended conflict escalation (Finlay & Payne, 2019; Taddeo, 2018).

This multidimensional understanding of attribution is further specified in Rid and Buchanan's (2015) "Q-Model", which conceptualises attribution as a layered process across four levels: tactical/technical, operational, strategic and communication. At the tactical level, investigators analyse technical evidence to understand how an intrusion occurred. The operational level combines these findings with contextual information, such as geopolitical factors, to develop competing hypotheses that explain the incident (Rid & Buchanan, 2015). At the strategic level, these hypotheses are evaluated to determine responsibility, assess the underlying rationale and the attack's significance, and determine an appropriate response. "*The more severe the consequences of a specific incident, and the higher its damage, the more resources and political capital will a government invest in identifying the perpetrators.*" (Rid & Buchanan 2015, p.30). Finally, the communicative layer addresses the public communication of attribution. While publicising intelligence can harm both sources and methods, according to Rid and Buchanan (2015), greater transparency can improve credibility, attribution,

and defensive measures. Together, the approaches highlight that attribution is not merely a technical exercise, but a politically embedded and strategically contested process.

Applicability to CUI Sabotage in the Baltic Sea

To test the relevance of the attribution problem beyond cyberspace, the following section applies it to CUI sabotage in the Baltic Sea.

CUI, like undersea cables, pipelines, and energy installations, is essential for global communication, energy supply and economic stability (Frenzel, 2025). Despite its strategic importance, this infrastructure remains vulnerable to accidents and intentional sabotage. Between October 2023 and December 2024, four incidents of CUI damage occurred in the Baltic Sea, specifically within the Exclusive Economic Zones (EEZs) of Finland, Estonia, and Sweden. In all cases, vessels damaged CUI by dragging anchors along the seabed (Kirchberger, 2025). According to Kirchberger (2025), these incidents highlighted "*the difficulty of quickly attributing damage to a particular actor, of legally proving intent, of claiming and receiving damages, and ultimately of deterring future acts of vandalism*" (p. 179). Spatial ambiguity characterises both CUI sabotage and cyber operations, as both domains are difficult to control and regulate. These similarities suggest that the attribution problem can be meaningfully transferred to the context of CUI sabotage. However, the nature of attribution differs across domains. Unlike damage in cyber operations, physical damage is often easier to detect (Rid & Buchanan, 2015). Nevertheless, attribution challenges in the context of CUI sabotage are less a matter of technical impossibility than of political, legal, and strategic ambiguity.

This ambiguity is reinforced by several structural factors. First, vessels involved in suspected sabotage are often linked to Russia's "shadow fleet", which operates through complex ownership structures designed to obscure responsibility and hinder attribution to a state actor (Kirchberger, 2025). Second, legal constraints limit states' ability to investigate and respond. Coastal states have restricted rights of intervention beyond their EEZs, and legal frameworks such as Article 113 of UNCLOS (1982) do not grant warships the right to board suspected vessels in international waters (Frenzel, 2025). A further dimension of this ambiguity is the emergence of a "war of narratives", in which incidents are interpreted either as accidents or deliberate sabotage (Kirchberger, 2025). This debate allows actors to exploit uncertainty and reinforces plausible deniability, thereby complicating both attribution and deterrence.

To illustrate these dynamics, the Q-Model is applied to the Yi Peng 3 case from November 17th, 2024, in which the vessel dragged its anchor across the seabed, damaging CUI in the Swedish EEZ near Gotland. The case was chosen as it is the most extensively documented incident of CUI damage in the Baltic Sea (Sutherland, 2025), and clearly demonstrates the attribution challenges discussed above. The Q-Model is well-suited for the following analysis, as it was explicitly developed to explain, guide, and improve the

process of attribution (Sahrom et al., 2018). It thereby allows for a structured analysis of how attribution unfolds in a context where evidence is available, but conclusions remain constricted.

At the technical level, investigators reconstructed the incident using physical and digital evidence. Data from the Automatic Identification System (AIS) and OSINT revealed that the ship had followed an unusual route over the affected cables, including patterns inconsistent with normal navigation, autopilots, or weather conditions (Sutherland, 2025). Moreover, the temporary deactivation of AIS signals and the repeated dragging of an anchor across the seabed further increased suspicion (Kirchberger, 2025).

At the operational level, this evidence was combined with contextual information to develop competing hypotheses. The vessel was Chinese-owned and flagged, with a Chinese crew and Russian captain, and had departed from the Russian port of Ust-Luga (Sutherland, 2025). While these factors raised suspicions of potential state involvement, alternative explanations remained plausible. The crew claimed that the anchor had become loose accidentally, but this explanation was inconsistent with the collected evidence (Sutherland, 2025). Still, there was no proof of intentional damage, leaving authorities with no definitive conclusion regarding intent.

At the strategic level, the limitations of attribution became even more apparent. Although several Baltic states launched a joint investigation and considered charges such as sabotage or terrorism, legal attribution was constrained by jurisdictional limitations and the need for cooperation with China, the vessel's flag state (Sutherland, 2025). In response to a formal request from Sweden, China agreed to some cooperation in the investigation, but denied the request for the vessel to sail into Swedish waters (Sutherland, 2025). Therefore, the ship remained outside territorial waters for much of the investigation, limiting direct intervention. Although China eventually consented to a formal inspection in the presence of European authorities, the investigation only took place on November 29th, weeks after the incident, and failed to produce conclusive evidence (Kirchberger, 2025).

Regarding communication, political responses remained cautious and reflected broader security concerns rather than clear political attribution. Nordic and Baltic leaders condemned the Russian Federation's increasing use of hybrid warfare and made a specific call for naval patrols in the Baltic Sea, without directly assigning responsibility (Sutherland, 2025). The Yi Peng 3 incident thus demonstrates that attribution is a complex and layered process in which ambiguity persists at every stage. Although technical attribution was possible, political, legal and discursive factors limited political and legal attribution.

Benefits and Limitations of the Framework

The framework offers several analytical benefits, most notably its ability to structure a highly complex phenomenon. By distinguishing between different layers of attribution, the Q-Model clarifies how technical evidence, contextual factors, and political decision-making interact. As the Yi Peng 3

case demonstrates, incidents may be attributed technically, while political action remains cautious and legal frameworks complicate enforcement. By emphasising political attribution and communication, it shows that attribution depends not only on evidence, but also on strategic considerations, and that attribution is a multidimensional process in which different types of evidence sometimes produce conflicting conclusions.

The framework also bridges different subfields of security policy research. Both cyber operations and CUI sabotage can be understood as forms of hybrid warfare, characterised by ambiguity, plausible deniability, and the use of civilian actors. Applying the framework allows for identifying recurring patterns across different contexts. In this sense, the framework not only transfers a concept but also helps integrate previously separate strands of research into a more coherent understanding of hybrid warfare.

At the same time, this framework has limitations. Most notably, the technical dimension of attribution does not fully translate to the maritime domain. Unlike cyberattacks, where identifying the source of an attack can be highly complex (Rid & Buchanan, 2015), physical damage to CUI is often easier to detect and link to a specific vessel. Attribution challenges in this context are less about technical uncertainty than legal and discursive factors that constrain political and legal attribution.

Overall, the attribution problem provides a useful analytical lens, particularly by highlighting the multi-layered and politically complex nature of attribution in the context of CUI sabotage. While the framework can be meaningfully applied to the maritime domain, the drawn conclusions must be adapted and complemented with additional perspectives, such as deterrence strategies, in order to fully capture the dynamics of hybrid conflict in the Baltic Sea. Even though the framework itself does not deal with deterrence, attribution underpins deterrence and shapes strategic responses. While classical deterrence theory is widely deemed inapplicable to cyberspace (Taddeo, 2018), it remains applicable to CUI sabotage. In cyberspace, structural constraints limit deterrence strategies largely to retaliation or punishment. By contrast, CUI sabotage allows for broader deterrence strategies, including extended deterrence via NATO, deterrence by denial, and punishment (Rostoks & Vanaga, 2017), although political attribution remains constrained. If successful, attribution significantly enhances the feasibility of deterrence compared to cyberspace.

Conclusions

This policy brief has shown that the concept of the "attribution problem", originally developed in the context of cybersecurity, can be meaningfully applied to the analysis of sabotage of critical underwater infrastructure (CUI) in the Baltic Sea. While technical indicators may provide relatively clear evidence, attribution remains constrained by political, legal, and discursive factors. The application of the Q-Model to the Yi Peng 3 case demonstrates that attribution is a multi-layered process in which ambiguity can persist across all stages.

For policymakers, this means that technical attribution alone is insufficient. Instead, effective responses to CUI sabotage require addressing legal gaps, strengthening coordination, and developing deterrence strategies that remain viable under conditions of persistent ambiguity.

References

Abu, S., Selamat, S. R., Yusof, R., & Ariffin, A. (2018). An Enhancement of Cyber Threat Intelligence Framework. In *2nd Global Conference on Computing & Media Technology*. https://www.researchgate.net/publication/334697012_An_Enhancement_of_Cyber_Threat_Intelligence_Framework

Bendiek, A., & Schulze, M. (2021). Attribution: A Major Challenge for EU Cyber Sanctions: An Analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW. In *SWP Research Paper* (Vol. 11) [Report]. Stiftung Wissenschaft und Politik. https://doi.org/10.18449/2021RP11

Finlay, L., & Payne, C. (2019). The attribution problem and cyber armed attacks. *AJIL Unbound*, *113*, 202–206. https://doi.org/10.1017/aju.2019.35

Frenzel, S. (2025). Challenges to the Protection of Critical Undersea Infrastructure: NATO MARCOM's Perspective. In M. Doğrul (Ed.), *5th Maritime Security Conference Proceedings: The Impact of Technology on Maritime Security* (pp. 255–264). Maritime Security Centre of Excellence (MARSEC COE). https://www.marseccoe.org/wp-content/uploads/2026/02/5th-Maritime-Security-Proceedings.pdf#:~:text=It%20is%20with%20great%20honour%20that%20I%20present,theme%20%E2%80%9CThe%20Impact%20of%20Technology%20on%20Maritime%20Security.%E2%80%9D

Kirchberger, S. (2025). Combatting the Shadow Fleet: Countering Maritime Sabotage, Surveillance and Disruption. In M. Doğrul (Ed.), *5th Maritime Security Conference Proceedings: The Impact of Technology on Maritime Security* (pp. 177–192). Maritime Security Centre of Excellence (MARSEC COE). https://www.marseccoe.org/wp-content/uploads/2026/02/5th-Maritime-Security-Proceedings.pdf#:~:text=It%20is%20with%20great%20honour%20that%20I%20present,theme%20%E2%80%9CThe%20Impact%20of%20Technology%20on%20Maritime%20Security.%E2%80%9D

Kuerbis, B., Badiei, F., Grindal, K., & Mueller, M. (2022). Understanding transnational cyber attribution: Moving from "whodunit" to who did it. In M. Dunn Cavelty & A. Wenger (Eds.), *Cyber Security Politics* (pp. 220–238). Routledge. https://www.taylorfrancis.com/chapters/oa-edit/10.4324/9781003110224-17/understanding-transnational-cyber-attribution-brenden-kuerbis-farzaneh-badiei-karl-grindal-milton-mueller

Rid, T., & Buchanan, B. (2014). Attributing Cyber Attacks. *Journal of Strategic Studies*, *38*, 4–37. https://doi.org/10.1080/01402390.2014.977382

Rostoks, T., & Vanaga, N. (2017). *Deterring Russia in the Baltic Sea Region: Latvia's defence developments in regional context*. Friedrich-Ebert-Stiftung. Baltic States. Retrieved April 10, 2026, from https://collections.fes.de/publikationen/content/titleinfo/459184

Sutherland, E. (2025). The Yi Peng 3 and Eagle S incidents – cutting cables in the Baltic Sea. *ideas.repec.org*. https://ideas.repec.org/p/zbw/itse25/331307.html

Taddeo, M. (2017). The Limits of Deterrence Theory in Cyberspace. *Philosophy & Technology*, *31*(3), 339–355. https://doi.org/10.1007/s13347-017-0290-2