University of Nottingham
Taiwan Research Hub

POLICY PAPER

Threats to Critical Undersea Infrastructure in the Baltic Sea and the Taiwan Strait

Toomas Hanso

University of Nottingham
Taiwan Research Hub

POLICY PAPER SERIES 2025/2026

Policy Paper No. 4, March 2026

Threats to Critical Undersea Infrastructure in the Baltic Sea and the Taiwan Strait

Author: Toomas Hanso
Editors: Dominika Remžová, Mark Murphy, Chun-yi Lee
Design: Mandy Felton
Citation: Toomas Hanso. *Threats to Critical Undersea Infrastructure in the Baltic Sea and the Taiwan Strait*. (Nottingham: Taiwan Research Hub, March 2026).

TAIWAN RESEARCH HUB (TRH)
University of Nottingham
University Park
Nottingham, NG7 2RD
United Kingdom

Table of Contents

Executive Summary 4
Policy Recommendations 5
Introduction 6
The Layout of the Baltic and Taiwanese CUI 7
Approaches to CUI Protection 9
Cases of Damage to the Baltic Sea CUI 11
Cases of Damage to the Taiwan Strait CUI 13
CUI Damage – Sabotage or Accident? 15
Final Conclusions 16
About the Author 17
Endnotes 18

Executive Summary

1 **Damage to Critical Undersea Infrastructure (CUI) has increased in both the Baltic Sea and the Taiwan Strait**, not least due to shallow waters, dense cable networks, and heavy maritime traffic. While many incidents may be accidental, the scale and frequency of disruptions raise **concerns about hybrid activities** and highlight growing vulnerabilities for regional security.

2 **Baltic states rely on NATO's expanding CUI-protection efforts**, yet repeated incidents show the limits of multinational monitoring. **Taiwan, without comparable alliances, depends on domestic enforcement**, legal reforms, and new international cooperation initiatives to protect its telecom and energy cables.

3 **Despite differing geopolitical contexts, both regions face similar challenges**: persistent hybrid threats, difficulty in attribution, and the economic and security risks posed by disrupted CUI. Taiwan can draw **lessons from Baltic experiences** but must tailor its approach to avoid escalation in the more sensitive strategic environment of the Taiwan Strait.

Policy Recommendations

1 **Increase international visibility of CUI incidents to strengthen deterrence.** Taiwan should elevate international awareness of its CUI incidents to raise the political and reputational costs of sabotage. Baltic cases naturally draw global attention because they often involve multiple states, while Taiwan's incidents are mostly domestic due to the structure of its CUI links with outlying islands. By proactively engaging international media and partners, Taiwan can increase scrutiny and create a stronger deterrence against malicious interference.

2 **Strengthen domestic rapid-response capacity for CUI incidents.** The Baltic experience shows that even robust international frameworks, like NATO cooperation, do not prevent CUI damage. Taiwan, lacking comparable alliance structures, cannot rely on external support in a crisis. This makes strengthening domestic monitoring, repair, and emergency-response capabilities essential for minimising downtime and damage.

3 **Carefully calibrate post-incident responses to avoid escalation.** Taiwan must adopt a more cautious approach to post-incident actions than some Baltic states. Measures seen as firm but manageable in Europe, like the Finnish response to the *Eagle S* tanker case, carry significantly higher escalation risks in the Taiwan Strait. Taiwan can draw lessons from Baltic practices but must adapt them to its more sensitive strategic environment to avoid unintended escalation.

Introduction

Since 2020, the Baltic Sea and the Taiwan Strait have seen increasingly frequent instances of damage to Critical Undersea Infrastructure (CUI), also known as “cable cutting.” The most recent Baltic Sea case was recorded on the final day of 2025, highlighting the threat’s persistent nature. Many researchers increasingly attribute such activities to hybrid warfare conducted by China and Russia, whereby Chinese and Russian merchant ships may be engaging in sabotage operations.[1] Intelligence agencies highlight an unclear picture.

Former Estonian intelligence officers have cited local incidents as accidental, owing to coinciding factors like heavier ship traffic and poorly maintained vessels with low crew competence.[2] This diverges from perceptions of local incidents by Taiwanese intelligence – although public attribution has not been made, Taiwan’s National Security Bureau has been involved in discussing cable cutting as part of hybrid warfare, with non-accidentality implicit.[3] Despite difficulties in defining intentionality and attribution, damage to critical infrastructure must be addressed.

Similarities make for a worthwhile comparison. In addition to the Baltic Sea and the Taiwan Strait being global hotspots for cable-cutting incidents, certain similarities in physical geography further increase the value of comparison. The average depth of the Baltic Sea is 55m, while that of the Taiwan Strait is 60m – this relatively shallow depth is a key factor in increasing the vulnerability of CUI. In terms of area and size, the Baltic Sea’s north-eastern section, the Gulf of Finland (30,000 km²), is comparable to the Taiwan Strait in total area (55,000 km²). Therefore, this analysis will compare recent incidents of damage to CUI, looking at the similarities and differences between these incidents and variation in regional responses.

The Layout of the Baltic and Taiwanese CUI

Critical Undersea Infrastructure consists of submarine energy pipelines, power and communication cables. These are vital to energy security, communications, financial systems, and therefore overall economic prosperity. While very important to littoral states like the Baltics, undersea infrastructure is especially critical for Taiwan, which as an island, does not have the luxury of relying on overland connectivity.

The Baltic Sea in North-East Europe covers an area of 377,000 km². Eight countries sit on its coast: Denmark, Estonia, Finland, Germany, Latvia, Lithuania, Poland, Russia and Sweden. It is a busy trade route with 15% of the world's container shipping passing through. While the dual accession of Finland and Sweden to NATO has increased the international perception of the Baltic Sea as a "NATO lake," Russia maintains Baltic Sea presence via Leningrad Oblast on the north-eastern shores and Kaliningrad Oblast on the southern shores.

Given that eight countries lie around it, the Baltic Sea is home to a dense network of CUI. In the Gulf of Finland specifically, infrastructure includes the Finland-Estonia 2 and Finland-Estonia 3 fibre-optic cables, the Balticconnector gas pipeline, and the EstLink 1 and 2 electricity cables. In the wider Baltic Sea region, the total number of undersea cables for energy and communications may total around 40-50 individual lines.

The Taiwan Strait, covering 55,000 km², is smaller in area, but far busier than the Baltic Sea when it comes to shipping – nearly 50% of global container shipping transits through the Strait. This is very significant for a Strait that is 180 km wide and 350 km long. While at first glance the Baltic Sea may seem more complex due to the high number of littoral countries, the Taiwan Strait is also not a simple area, considering the current complexity of Taiwan's international status and its territorial waters. Much CUI is housed on the seabed of the Taiwan Strait.

The majority of Taiwanese CUI consists of telecom cables which connect Taiwan to its outlying islands: Strait Express-1, Taiwan-Matsu No. 4, Taiwan-Penghu-Kinmen-Matsu No. 2, Taiwan-Penghu-Kinmen-Matsu No. 3, and more.

Energy CUI is also present in the area, represented by the currently operational undersea gas pipeline between Kaohsiung and Miaoli, while the construction of a new gas pipeline from Taichung to Miaoli was signed in January 2025.[4]

Finally, the Taiwan-Penghu 161kV subsea power cable, completed in 2021, brings power from Yunlin to the Penghu archipelago, 50 km away from the main island of Taiwan. Overall, the Taiwan Strait probably has 25-35 individual cables and lines, with the Taiwanese Coast Guard guarding the security of the Taiwanese undersea infrastructure.

8 Threats to Critical Undersea Infrastructure in the Baltic Sea and the Taiwan Strait

Approaches to CUI Protection

The Baltic Sea states aim to protect their CUI primarily through NATO initiatives, while Taiwan has taken the approach of launching its own international coordination formats and strengthening certain domestic responses, especially in the legal field.

Following NATO's 2023 Vilnius Summit, the NATO Maritime Centre for Security of Critical Undersea Infrastructure (NMCSCUI) was established at NATO's Maritime Command (MARCOM) in the UK to protect this critical undersea infrastructure — principally submarine cables, pipelines, and energy interconnectors. NMCSCUI assists NATO Allies in making decisions and coordinating action relating to CUI protection and response. In 2025, NATO announced 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.[5]

The first contributing nations to the NMCSCUI were Denmark, Germany, Norway, Poland, Türkiye, the UK and the USA, with Greece, Portugal and Sweden joining later. While the Baltic states are not listed as contributors, the importance of the Baltic Sea is shown by the presence of Baltic Sea countries, namely Denmark, Germany, Poland and Sweden.[6]

According to the statements, NATO continues to invest in the latest military technology, including Artificial Intelligence, to detect and minimise threats to CUI, as well as specialised sonar systems, unmanned underwater vehicles, and advanced sensors for real-time intelligence on underwater activity. Yet despite NATO operations, persistent damage has occurred to the Baltic Sea CUI. Indeed, in 2023, the US-based Center for Strategic and International Studies (CSIS) assessed that NATO was "not ready to mitigate" increasingly prevalent Russian aggression against European CUI.[7]

Taiwan cannot rely on military alliances like NATO, so its options include starting its own initiatives, as well as strengthening domestic capabilities. In terms of the former, Taiwan launched the global initiative on security of undersea cables in 2025,[8] known as the RISK Management Initiative on International Undersea Cables.

The initiative aims to mitigate risks, share information, reform systems, and build knowledge. Domestically, Taiwan is tightening laws, as evidenced by the amending of seven submarine cable laws, serving up to seven years in prison for intentional damage.[9] Taiwan already implemented such legal responses, with the Tainan District Court sentencing a Chinese national to three years for causing damage to an undersea cable.[10] As for Taiwanese physical responses, these are led by Taiwan's Coast Guard Administration, in close coordination with other domestic actors.

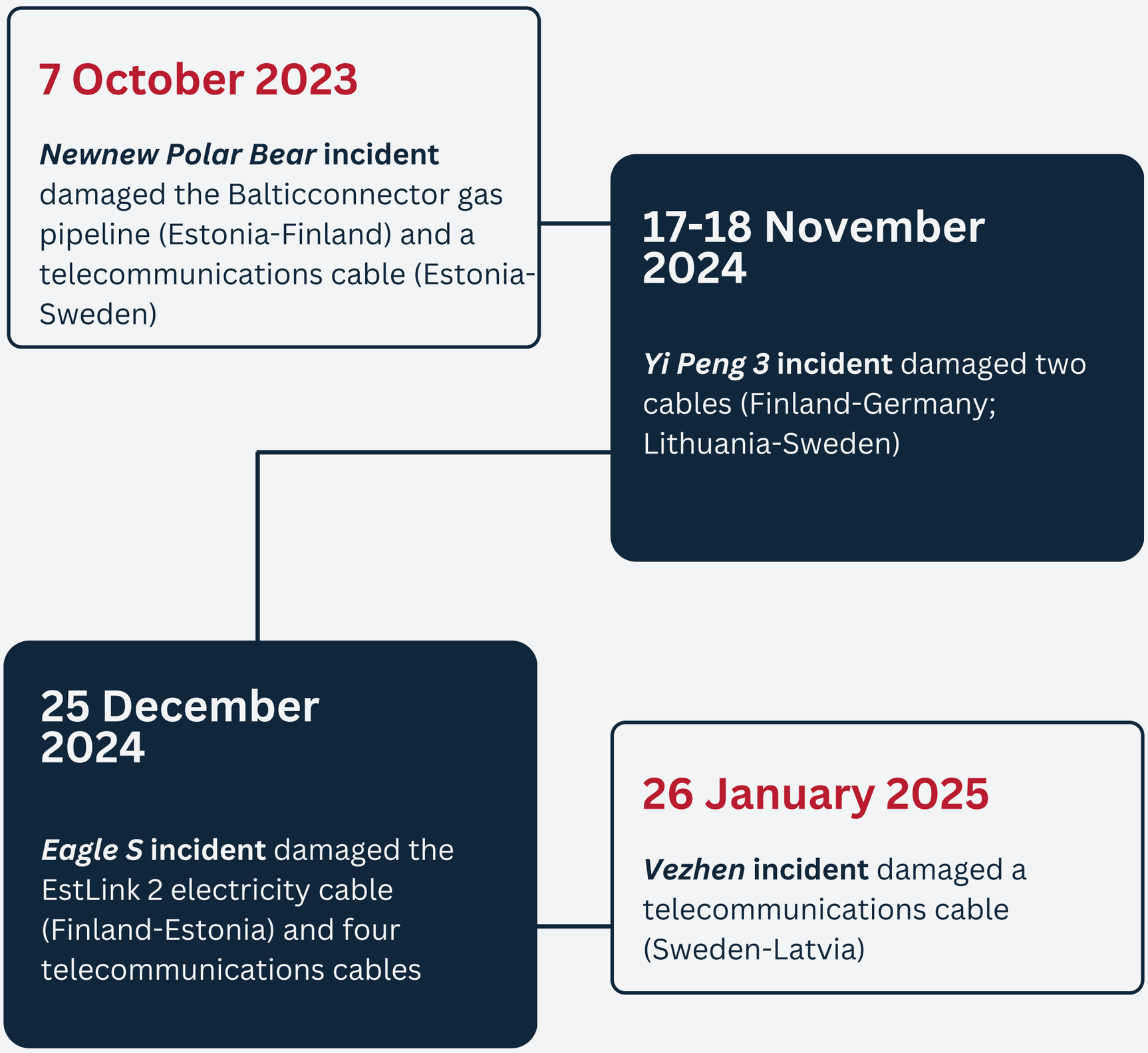

Fig.1: Recent Cases of CUI Damage in the Baltic Sea

Cases of Damage to the Baltic Sea CUI

Several incidents since 2023 have increased the threat perception of NATO member states around the Baltic Sea. The most recent case occurred on 31 December 2025, when telecommunications provider Elisa's cable was damaged in Estonia's Exclusive Economic Zone (EEZ), in the Gulf of Finland. Following the damage, the responsible vessel was located in Finland's EEZ, with the vessel's anchor chain found to be lowered into the sea. Finnish authorities took control of the vessel, and investigations are ongoing.[11] The perpetrator is yet to be confirmed.

Underwater telecommunications cables in the Baltic Sea have also sustained damage in multiple other incidents. On 26 January 2025, a cable connecting Sweden to Latvia was damaged. Authorities initially cited "external influence." Following a joint investigation and the involvement of NATO patrol ships under operation Baltic Sentry, a bulk carrier *Vezhen* flying the Malta flag was taken into custody. However, Swedish prosecutors later concluded the incident to be accidental.[12] The 25 December 2024 incident involving the *Eagle S* tanker (see below) of Russia's shadow fleet caused damage to four cables between Estonia and Finland.

The 17-18 November 2024 incident involving China's *Yi Peng 3* ship, damaged two cables simultaneously, one between Finland and Germany, and one between Lithuania and Sweden. Swedish authorities reported that their lead prosecutor was not allowed to board the ship, and the vessel later departed the area, prompting calls for fuller cooperation from China in the investigation. As of April 2025, a Swedish probe found no conclusive evidence to suggest that the ship deliberately dragged its anchor to damage the cables.[13]

Damage to the Baltic Sea electricity cables occurred during the 25 December 2024 incident involving the Cook Islands-flagged *Eagle S* tanker. The submarine electricity cable EstLink 2, which connects Finland and Estonia, was damaged in Finland's EEZ, in addition to four telecommunications cables. Repairs on EstLink 2 were completed in June 2025.

The Cook Islands-flagged oil tanker *Eagle S*, suspected of carrying out the damage, was ordered to raise its anchor and enter Finnish territorial waters by Finnish patrol ship *Turva*. While the incident caused a major disruption to cross-border energy and data connections in the Baltic Sea region, telecommunications traffic and electricity flows were rerouted wherever possible.[14]

Finally, undersea gas infrastructure in the Baltic has also sustained damage. On 7 October 2023, several pieces of vital underwater infrastructure in the Baltic Sea were damaged, including the Balticconnector gas pipeline between Estonia and Finland, which was ruptured. On the same day, a telecommunications cable between Estonia and Sweden was affected by an external mechanical force or tampering. A damaged ship's anchor was recovered from the seabed near the affected infrastructure, with gouge marks indicating its trajectory across the seabed.

The damage was linked by investigators to the Hong Kong-flagged vessel *Newnew Polar Bear*, found to be missing one of its anchors. In August 2024, Chinese authorities acknowledged that the vessel had caused the damage, describing the incident as accidental and attributing it to severe weather.[15] Investigations by Finnish, Estonian and Swedish authorities continued following the incident, with NATO increasing maritime and air surveillance activities in the Baltic Sea.

Cases of Damage to the Taiwan Strait CUI

The Taiwan Strait has also seen multiple incidents of cable damage – some suspected sabotage, and some assumed to be natural deterioration.[16] In the Strait, incidents to date have primarily involved damage to telecommunications CUI. For Taiwan, telecommunications infrastructure is critical, given that, as an island, it can be more easily isolated.

Incidents where no sabotage is suspected include the natural deterioration of Taiwan-Matsu No. 2 (15 January 2025) and Taiwan-Matsu No. 3 (22 January 2025). Taiwan's Chunghwa Telecom said the Taiwan-Matsu No. 3 cable was "completely disconnected" on the afternoon of 15 January, while the Taiwan-Matsu No. 2 cable was found to be disconnected on the morning of 22 January. Communication traffic has been rerouted to microwave circuits.[17] Similarly, on 16 February 2025, the No. 2 undersea cable connecting Taiwan and Matsu broke at multiple points, causing a complete outage, according to Taiwan's Ministry of Digital Affairs.[18]

Two recent incidents, which include Chinese ships sailing under African flags, have been suspected of sabotage. On 25 February 2025, a telecommunications cable connecting the main island of Taiwan and Penghu was severed. Authorities traced the incident to a nearby cargo ship.[19] The *Hong Tai 58* was Togolese-flagged and crewed by eight Chinese nationals. Taiwan's coast guard detained the vessel after it failed to respond to repeated communications and was found anchored near the cable site just before the disruption was discovered. Prosecutors formally accused the captain of the *Hong Tai 58* of purposefully damaging the underwater cable in April 2025, marking the first time Taiwan has filed criminal charges in an incident of this nature.

The captain of *Hong Tai 58* was sentenced to three years in prison for destroying cables under the Telecommunications Management Act.[20] A month and a half earlier, one of Taiwan's undersea communication cables off the northern coast was damaged on 3 January 2025. Taiwan's Coast Guard identified the *Shunxing 39* operating near the cable at the time of the disruption. The vessel was registered under a Cameroon flag and linked to a Hong Kong-based company. Due to poor weather conditions, coast-guard personnel were unable to board the ship for inspection, and it subsequently left the area en route to South Korea.

In February 2023, Matsu was left without internet due to incidents which occurred about a week apart, on the second and eighth days of the month. The initial disruption occurred when a Chinese fishing vessel operating close to the cable route damaged a cable, resulting in a significant reduction of internet and telecommunications services for residents of the Matsu Islands, who had to rely on limited microwave transmission links as an emergency substitute.

The following week, another one of Matsu's telecommunications was damaged, this time by a Chinese-flagged cargo ship passing through the area. With both cables out of service, Matsu temporarily lost nearly all stable external connectivity. Essential communication services were severely impacted until repairs could be arranged, leading to several weeks of restricted and unstable access before full service was restored.[21]

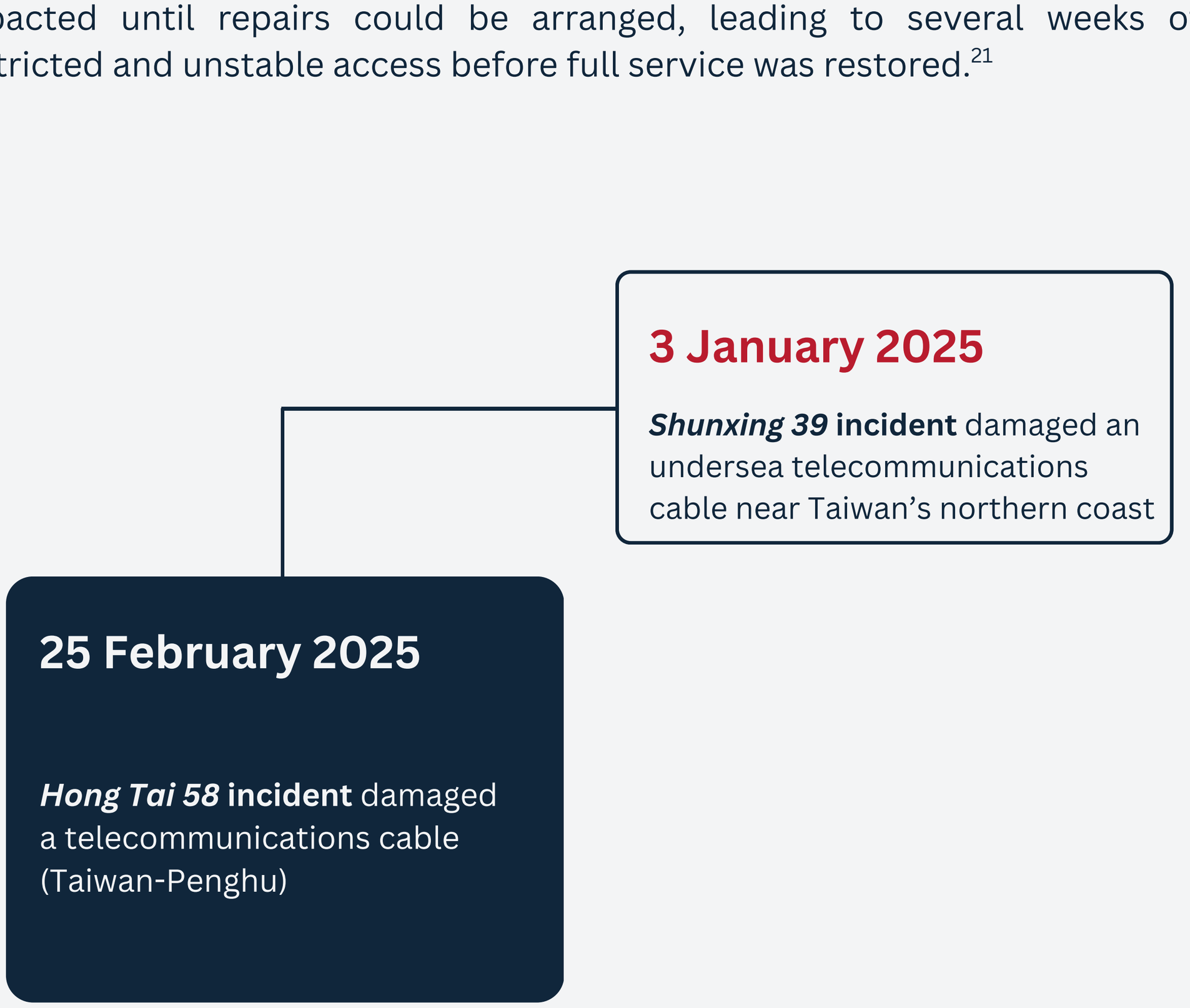

Fig.2: Recent Cases of CUI Damage in the Taiwan Strait

CUI Damage – Sabotage or Accident?

Whether sabotage is ongoing cannot be directly proven. On one hand, the increasing frequency of incidents in both areas suggests that they cannot all be purely incidental. Yet a rise in accidents can also be explained.

Former deputy director of the Estonian Foreign Intelligence Service, Andres Vosman, said in January 2026 that “most of the recent incidents in the Baltic Sea have largely been the result of coinciding factors,” citing heavier ship traffic towards Russia, vessels in poor condition with low crew competence and increased public attention. Reasons for Russia not to engage in such behaviour include the role of the Baltic Sea as a lifeline for Russian trade, which Moscow cannot afford to have closed down. Reportedly, the Rostelecom-owned Baltika telecommunications cable between Russia’s Kingissepp and Kaliningrad has been cut twice; once in October 2023 at the same time as the *New New Polar Bear* incident; second in February 2025.[22] The Baltika telecommunications cable is 1,000 km long and runs through the EEZs of Finland and Sweden for over 700 km.[23]

Finnish statements present a more mixed picture of intentionality. Regarding the *Eagle S* tanker incident, it is difficult to understand the final Finnish assessment. On the one hand, some Finnish intelligence officials said that the incident was likely accidental. Yet, a retired Finnish army general and current Member of Parliament, Pekka Toveri, said that claims of accidental damage are “total B.S. [bullshit],”[24] and the Finnish National Bureau of Investigation said it suspected intent.[25] Meanwhile, Taiwan’s National Security Bureau has discussed CUI damage as a part of hybrid warfare, not directly attributing incidents to China, but also not denying it.[26]

Although factors like higher shipping traffic, old ships and greater attention may partly explain the higher frequency of CUI damage incidents, it is hard to believe that the unprecedented frequency of Baltic Sea incidents is purely accidental. Similarly, in the Taiwan Strait, frequent cable damage can be partially explained by natural deterioration and accidents, although high incident frequency means that sabotage cannot be excluded. Currently, attribution remains difficult. In the future, however, attribution capabilities may be strengthened by improved monitoring capabilities enabled by underwater drone technologies.

Final Conclusions

The Baltic Sea and the Taiwan Strait present different international contexts for deterrence activity and responses, and both waterways face different challenges owing to these regional realities. In the Baltic Sea, deterrence and response must be coordinated between multiple partners, which comes with its own challenges, and this has been evident in the inability to prevent CUI damage incidents from recurring. Taiwan, on the other hand, is left to manage its CUI largely alone, due to its lack of diplomatic partners. This means that planners in Taipei must focus especially on domestic response capabilities, whereas the three Baltic states can afford to count on the support of other regional partners in certain cases.

The Baltic Sea has experienced CUI incidents involving both Chinese- and Russian-linked vessels, while the Taiwan Strait cases have been associated almost exclusively with actors connected to China. The only notable exception occurred in December 2024, when a Russian vessel lingered over a Taiwanese undersea cable without causing damage.[27] Low levels of Russian activity in the Taiwan Strait may reflect Moscow's alignment with Beijing's view of the Strait as a domestic waterway and its reluctance to intervene in what it perceives as China's internal affairs. These differing geopolitical contexts mean the Baltic region must contend with multiple potential actors, whereas Taiwan primarily faces one. Regardless of who is responsible, recurrent CUI damage threatens the geo-economic security of both regions, underscoring the need for stronger infrastructure protection.

Overall, both regions remain hotbeds for CUI damage. First, the similar physical geography of low average depths (55m – 60m) increases CUI vulnerability. Second, both are busy waterways, increasing the likelihood of accidental damage due to shipping volume. Third, hybrid activity is attractive for malign actors in both areas due to the above reasons – CUI is vulnerable, and shipping volume makes attribution difficult. Regardless of intentionality, the increased frequency of incidents highlights the need to do more to protect CUI, which is the backbone of telecommunications security and contributes to energy security in both regions.

About the Author

Toomas Hanso is a Junior Research Fellow at the International Centre for Defence and Security (ICDS), Estonia.

Toomas is a China expert focusing on the PRC's domestic and foreign policy, as well as Sino-Russian and international relations. He holds a first-class MA from the University of Edinburgh in Chinese & Linguistics, also having studied under the Taiwan-Europe Connectivity Scholarship at National Donghwa University in Hualien, Taiwan (2021-2022), and as recipient of the Confucius Institute Scholarship at Yunnan University in Kunming, China (2023-2024), where he passed the HSK6 Chinese-language exam.

Having joined ICDS in October 2024, Toomas regularly comments on China-related news in Estonian media, has published multiple analyses and reports, and represents Estonia at the European Think-tank Network on China (ETNC).

.

Endnotes

1 John Dotson, “Strangers on a Seabed: Sino-Russian Collaboration on Undersea Cable Sabotage Operations,” *Jamestown*, 6 July 2025.

2 “Former Estonian intelligence official: Baltic Sea cable damage incidental,” *ERR*, 4 January 2026.

3 “台灣海纜遭破壞 蔡明彥：重點關注中共藉權宜輪侵擾,” 中央社, 16 January 2025.

4 Nadja Skopljak, “Emirati company wins $1B contract for subsea gas pipeline in Taiwan,” *Offshore Energy*, 9 January 2025.

5 “NATO’s Baltic Sentry steps up patrols in the Baltic Sea to safeguard Critical Undersea Infrastructure,” *NATO MARCOM UK*, 14 January 2025.

6 “NATO officially launches new Maritime Centre for Security of Critical Undersea Infrastructure,” *NATO MARCOM UK*, 28 May 2024.

7 “NATO’s Role in Protecting Critical Undersea Infrastructure,” *CSIS*, 19 December 2023.

8 “Taiwan launches global initiative on security of undersea cables,” *Focus Taiwan*, 28 October 2025.

9 “Taiwan Amends Seven Submarine Cable Laws, up to 7 Years in Prison for Intentional Damage,” *Submarine Networks*, 31 October 2025.

10 “Taiwan jails China captain for undersea cable sabotage in landmark case,” *BBC*, 12 June 2025.

11 “Police Investigate Cable Damage in the Gulf of Finland in Cooperation with Other Authorities,” *Police of Finland*, 31 December 2025.

12 “Sweden opens sabotage probe into Baltic undersea cable damage,” *Reuters*, 26 January 2025.

13 “Swedish probe finds no conclusive evidence of deliberate cable damage by Chinese ship,” *Reuters*, 15 April 2025.

14 Alexander Lott, “Christmas Day Cable Cuts in the Baltic Sea,” *Blog of the European Journal of International Law*, 31 December 2024.

15 “New Balticconnector pipeline damage facts come to light,” *ERR*, 25 September 2024.

16 Gahon Chia-Hung Chiang, “Countering China’s Subsea Cable Sabotage,” *Global Taiwan Institute*, 19 March 2025.

17 “2 Taiwan-Matsu undersea cables disconnected,” *Taiwan News*, 22 January 2025.

18 “Undersea telecom cable to Matsu breaks again,” *Taipei Times*, 17 February 2025.

19 “Taiwan detains China-linked cargo ship after undersea cable disconnected,” *Reuters*, 25 February 2025.

20 “Taiwan extends penalty range for damaging subsea cables, pipelines,” *Focus Taiwan*, 12 September 2025.

21 “After Chinese Vessels Cut Matsu Internet Cables, Taiwan Seeks to Improve Its Communications Resilience,” *The Diplomat*, 15 April 2023.

22 “Former Estonian intelligence official: Baltic Sea cable damage incidental,” *ERR*, 4 January 2026.

23 “Russia starts repairs of its Baltika data cable in the Gulf of Finland,” *Ministry of Economic Affairs and Employment of Finland*, 6 November 2023.

24 “Washington Post: Finnish intelligence officials believe Eagle S rupture was an accident,” *yle*, 20 January 2025.

25 “KRP Ylelle: Kun poliisi kysyi Eagle S:n miehistöltä ankkurista, vastaus herätti epäilyn tahallisuudesta,” *yle*, 22 January 2025.

26 “台灣海纜遭破壞 蔡明彥：重點關注中共藉權宜輪侵擾,” 中央社, 16 January 2025.

27 “Map Shows Russian Ship Loitering Above Undersea Cables in Pacific,” *Newsweek*, 14 January 2025.

The Taiwan Research Hub (TRH) brings together researchers from different fields and disciplines (including history, cultural studies, sociology, international relations and economy) and career stages (from early-career to senior scholars) to improve the academic and public communities' understanding(s) of Taiwan.

To share our knowledge of Taiwan, we have a book series called *Taiwan and World Affairs* and an online magazine *Taiwan Insight*.

We also have a policy paper series, as part of which we publish six policy papers annually that engage with various Taiwan-related issues and perspectives. The purpose of this series is to provide constructive suggestions for relevant decision-makers on global issues related to Taiwan.

University of Nottingham
Taiwan Research Hub