Sutherland, Ewan

Conference Paper

The Yi Peng 3 and Eagle S incidents - cutting cables in the Baltic Sea

ITS 33rd European Conference 2025: "Digital innovation and transformation in uncertain times", Edinburgh, UK, 29th June – 1st July 2025

Provided in Cooperation with:
International Telecommunications Society (ITS)

Suggested Citation: Sutherland, Ewan (2025) : The Yi Peng 3 and Eagle S incidents - cutting cables in the Baltic Sea, ITS 33rd European Conference 2025: "Digital innovation and transformation in uncertain times", Edinburgh, UK, 29th June – 1st July 2025, International Telecommunications Society (ITS), Calgary

This Version is available at:
https://hdl.handle.net/10419/331307

33rd ITS Europe Conference
Edinburgh, 30th June and 1st July 2025
https://itseurope.org/2025/edinburgh/

The *Yi Peng 3* and *Eagle S* incidents - cutting cables in the Baltic Sea

Ewan Sutherland‡
LINK Centre, University of the Witwatersrand

Abstract

In November 2024, the Chinese registered bulk carrier, the *Yi Peng 3* was found to have been the only vessel in the area where cuts had been made in two telecommunication cables in the Baltic Sea, between Gotland and Estonia. With unexpected rapidity, the *Yi Peng 3* was stopped by the Royal Danish Navy and, after delays by Chinese authorities, their officials arrived for a cursory examination, then the ship was released. The two cables had already been repaired and evidence collected about the damage, together with evidence of previous attempts by the same vessel to cut electricity and telecommunication cables. Then in December 2024, a vessel belonging to the 'shadow fleet' used by Russia to breach oil sanctions cut an electricity interconnector and four telecommunications cables in the Gulf of Finland. The *Eagle S*, registered in the Cook Islands, was ordered into Finnish territorial waters, where it was boarded by special forces and taken to a port. These incidents highlighted the challenges of responding to attacks on undersea cables conducted by Russia as part of its undeclared war against NATO. It requires rapid notification of breaks to the national authorities (e.g., CERT), passed immediately to coast guard and navy, and consultation with prosecutors, before making immediate interventions to seize the vessels concerned and gather evidence, followed by quick repairs to the broken cables. This is possible only with careful administrative, judicial and political coordination in a complex system of polycentric governance. The international conventions, especially in the Danish Straits, make it difficult for coastal states to arrest vessels and to protect cables, especially beyond territorial waters. Nonetheless, the *Eagle S* incident demonstrated that a rapid response can be effective. In the longer term such threats require improvements to network resilience and better coordination amongst operators, government agencies and countries, given the difficulties in changing international conventions. One crucial change could be the inclusion of cable cutting in the definition of piracy.

Keywords: Infrastructure, Russia, Sabotage, Submarine cables, Telecommunications.

‡ http://ssrn.com/author=927092 http://orcid.org/0000-0001-5220-9605

Introduction

The first ever undersea cable was laid between Great Britain and France in 1850, but lasted only a few hours, before either being cut by a fisherman or being broken by wave action against rocks. Fishermen were to prove an enduring problem, trawling their nets along the seabed, together with the occasional theft of sections of cable for the resale value of the copper wire. From the 1850s, some protection was provided by burying cables in shallower waters, and by notifying merchant ships and fishermen of the location of cables in the expectation they would not drag anchors or trawl nets. The need emerged for more resilient cables and for specialist ships to grapple those cables from the seabed in order to repair them. While some breakages appeared to occur naturally, it was over a century before these were understood in terms of geology. In wartime, cables were cut to limit the ability of enemies to communicate with their armed forces, their allies, and potential suppliers of armaments, together with limiting their ability to disseminate propaganda. New threats have emerged from the use of autonomous underwater vehicles (AUVs), though evidence of their deployment remains scant, and, much more crudely, from the dragging of anchors across the seabed. The question addressed in this paper concerns the governance of undersea cables as critical infrastructure, examining two recent incidents in the Baltic Sea in the second half of 2024.

The original 1850 cable was a simple copper conductor insulated with *gutta percha,* made up of jointed lengths of about 100 metres. Permissions had been granted by the two governments to operate the service, with the two navies aiding the laying of the cable, but without any legal or physical measures to protect the cable, despite the large volumes of fishing and shipping in the English Channel. Its successor in 1851, was a single continuous cable protected with steel armouring, applied using a process developed to make wire rope, reducing the risk of breakages. Rapid advances were made in the conductors, insulation, armouring, cable laying machinery, and in the capacity to locate faults, grapple the cables and bring them to the surface to make repairs. Throughput was increased by 'loading' cables, which also enabled voice telephony, and their range was extended by use of underwater repeaters. A significant breakthrough came with the replacement of copper with fibre optics, enormously increasing throughput, further increased by dense wavelength division multiplexing (DWDM).

A major scientific advance came with the development of the theory of plate tectonics, which provided the first systematic explanation of continental drift, a true scientific revolution (Kuhn, 1962). Through the twentieth century there had been a gradual accumulation of evidence that continents had moved over millions of years and a growing understanding of mechanisms that enabled such movements, including the spread of seafloors and the subduction of plates. An almost trivial aspect of this was the explanation of breaks in undersea cables, for example, because the African plate was moving northwards it damaged cables laid in the Mediterranean Sea, while subduction explained the location of undersea earthquakes and some resulting underwater landslides. (Pichon *et al*., 2013)

Since its invasion of Ukraine in 2014, Russia has expanded its use of cyber and physical attacks on telecommunications and energy infrastructure against other states, sometimes termed 'hybrid warfare', a designation over which there are considerable disputes, making its use for analysis problematic. While not having declared war, Russia has engaged in a variety of attacks on other countries, notably those it considers to be aiding Ukraine, with which it is at war and which it seeks to assimilate. These tactics were developed following the ascent of V V Putin to the Presidency, partly in response to the colour revolutions in Georgia in 2003 and Ukraine in 2004, drawing on the historic approaches of the USSR and Comintern. Russia sought to avoid deploying conventional military forces, preferring asymmetric warfare comprising:

- Disinformation;
- Espionage;
- Sabotage;
- Subversion, and
- Use of private military companies (PMCs).

All of these it would deny, though often implausibly. Russia created frozen conflicts in Georgia, Moldova, and, for a time, in Crimea. It also sought to influence politics in NATO countries, including election outcomes, by exploiting press and social media freedoms, and its supply of natural gas. Russia has interfered with the operation of GPS, the US global satellite navigation system, endangering aircraft and ships (SVT, 2025). It has repeatedly made threats of conventional military action and even of using nuclear weapons against countries it considers to be threats. Generally, Russia has sought to keep conflicts below the level of outright military warfare, but nonetheless tried to achieve strategic results. Its second invasion of Ukraine turned from a 3-day special military operation into a brutal slogging 'conventional' war, albeit with the novel use of a great many drones, notably Operation Spiderweb. There have also been cyber attacks on telecommunication systems in Ukraine, many of which have been successfully resisted. To counter sanctions against the purchase of oil and gas from Russia, a 'shadow fleet' of elderly tankers has been deployed, owned by firms and listed in shipping registries, both of which are chosen to be opaque. (Clark, 2020; Person *et al*., 2024)

The next section examines international law as it relates to the laying, cutting and protection of undersea cables. This is followed by a short historical account of the military cutting of cables since the 1870s. An incident in the waters between the Gulf of Aden and the Red Sea is briefly described. There is then an account and analysis of two incidents in the Baltic Sea in November and December 2024, when the Yi Peng 3 and Eagle S cut cables on behalf of Russia. Next there is a consideration of international law relating to the two incidents in the particular circumstances of the Baltic Sea. Finally, conclusions are drawn and issues identified for further research.

International conventions and treaties

While the early national telegraph networks were mostly provided and operated by governments,[1] international cables were largely private ventures centred on London, where the cables were manufactured and the finance was raised. There were two principal international conglomerates:

- Eastern Group led by John Pender in London; and
- *Det Store Nordiske Telegraf-Selskab* led by C F Tietgen in Copenhagen.[2]

Laying cables beyond the territorial limit of states, at that time only 5.5 kilometres, was presumed to be permissible as part of the freedom of navigation of the high seas. Companies obtained permission to land cables from national governments, often being granted a monopoly and sometimes a subsidy, building up routes where they considered there would be profitable traffic. Operators accepted occasional cable breaks, notably from fishing, developing techniques to identify their location and make repairs.

To interconnect national networks, European governments formed regional unions and eventually the larger International Telegraph Union (ITU), which set rates and conditions. In 1869, only three years after the successful completion of the first effective transatlantic service, the USA proposed international action to protect undersea cables, suggesting that cable cutting might be treated as piracy. The issue was considered by *l'Institut de droit international*, which proposed that responsibility for a break should lie with the nation to which the vessel or the responsible individual belonged, with each nation having appropriate universal jurisdiction (*7e Commission d'étude*, 1879). The designation of piracy was rejected because penalties included execution and life imprisonment with hard labour. In 1884, at a meeting in Paris, a group of nations finalised and signed the Convention for the Protection of Submarine Telegraph Cables.

One of the obligations of the 1884 Convention was criminalisation of breaking cables, with Article VIII making the responsible legal tribunal that of the flag flown by the vessel and requiring that nation to have given itself global jurisdiction. For example, US federal law empowers courts to impose penalties of imprisonment for a term not exceeding two years, or a fine not exceeding US$5,000, or both, for intentionally breaking a cable (47 USC Ch. 2: Submarine Cables).[3] In the United Kingdom, the Submarine Telegraph Cables Bill, which transposed the Convention into law, was debated in both houses of parliament, generating considerable criticism, including petitions from the major transatlantic cable companies. It became the Submarine Telegraph Act 1885,[4] which made the wilful breaking of cables a misdemeanor subject to a penalty of up to five years imprisonment, optionally with hard labour, and a fine, or if it had been culpable negligence then up to three months imprisonment

[1] An obvious exception was Western Union in the United States.
[2] Most of the capital for Great Northern had been raised on London markets.
[3] https://www.law.cornell.edu/uscode/text/47/chapter-2
[4] https://www.legislation.gov.uk/ukpga/Vict/48-49/49/contents

and a fine of up to £100. Exemptions were granted when preserving human life or the vessel itself.

Article X of the 1884 Convention allows a warship of a signatory state to board a vessel suspected of intentionally breaking a cable to require its master to provide documentation proving its nationality. The country boarding the vessel was then to make a report to the flag state with a view to prosecution.

There followed a series of general discussions of international maritime law, with a codification adopted in 1930. After the Second World War there were three rounds of international meetings under the banner of the United Nations Convention on the Law of the Sea (UNCLOS), resulting in treaties signed in 1958, 1960 and 1982, with the notable omission of the United States.

The 1958 Convention on the High Seas outlined four fundamental freedoms:

- Freedom of navigation;
- Freedom of fishing;
- Freedom to lay submarine cables and pipelines; and
- Freedom of overflight.

UNCLOS III lasted from 1973 to 1982, finally establishing a comprehensive framework, including a dedicated regime for submarine cables. It categorised waters as follow:

- Internal waters (e.g., bays, inlet and rivers);
- Territorial seas (up to 12 nautical miles);
- Exclusive economic zone (EEZ) (up to 200 nautical miles); and
- High seas.

Freedom of navigation, including the laying of cables, is permitted in the last three, though it may be regulated, but requires permission in the first. In its EEZ the coastal state has the right to deny economic activities by other states.

Article 87(1)(c) of the Law of the Sea Convention (LOSC) granted states parties the freedom to lay submarine cables. This is an odd provision, since few cables are laid by states, with the vast majority being laid by contractors acting either for a private cable operator or for a consortium of providers. Governments have rarely done more than licence landing rights, leaving the design, operation and even the location of landing stations to the consortia. Thus the practice of laying cables is only tenuously linked to Article 87(1)(c), perhaps through the flags of cable-laying vessels. Theoretically, a state could licence the laying of cables in its EEZ, potentially bringing them within the scope of Article 87.

Like the 1884 Convention, UNCLOS required states parties to enact laws criminalising the breaking of undersea cables by vessels flying their flags However, it provided no enforcement power for the large number of states that have not done so or those that fail to enforce the legislation.

The 1972 Convention on the International Regulations for Preventing Collisions at Sea (COLREGS), provides in Rule 3(g)(i) that a vessel engaged in laying or repairing a cable is considered a "vessel restricted in its ability to manoeuvre". Rule 18 requires other vessels to "keep out of the way of" such a ship, though without specifying the distance. Whereas the 1884 Convention specified one quarter of a nautical mile or about 500 metres.

UNCLOS III expanded territorial waters from three to twelve nautical miles, that is from 5.5 to 22.2 kilometres. Additionally, EEZs were possible up to 200 nautical miles or 370 kilometres, enabling exploitation of the seabed, based on rights contained in the 1958 Geneva Continental Shelf Convention. While a nation can exploit its EEZ it has very limited legal powers over foreign ships sailing there. In the case of the Baltic, Mediterranean and North Seas, their small size required the drawing of borders, mostly median lines, though some demarcations also considered history and traditional uses of the waters. There is a long running dispute over the South China Sea, with China claiming most of that body of water, within the 'nine-dash line'.

UNCLOS restricts the boarding of vessels by the crews of warships and coast guard vessels outside their territorial waters. It is permitted only where a vessel is refusing to fly its flag or can reasonably be suspected of engaging in piracy or the slave trade.

While it is known that AUVs are being developed and have been deployed, their legal status is unclear. If they are for military purposes and deployed from a military vessel, then under UNCLOS they are designated as naval. However, if their purposes are less clear or they are deployed from a civilian vessel or one that presented itself as civilian, then their status is very much less clear. Given they can now be deployed, it is necessary to have a legal framework to deal with them.

An important addition to the scope of the law of the sea arose from concerns about pollution amongst coastal states. A key incident had been the sinking of the *SS Torrey Canyon* off the far south-west coast of the United Kingdom on 18th March 1967, with its cargo of 120,183 tonnes of crude oil. The result was the adoption of the International Convention for the Prevention of Pollution from Ships (MARPOL) of 1973, modified by protocols in 1978 and 1997, and by the addition of two annexes in 1983. MARPOL includes regulations to prevent and minimise pollution from ships, whether by accident or in the course of routine operations, notably the requirement that oil tankers have double hulls. Additionally, there is the Helsinki Convention on the Protection of the Baltic Sea Environment, originally adopted in 1974, but replaced by a second Helsinki Convention in 1992. This is supported by the intergovernmental Baltic Marine Environment Protection Commission, also known as the Helsinki Commission (HELCOM, 2025).

The 1976 Convention on Limitation of Liability for Maritime Claims (LLMC) replaced the 1957 Convention Relating to the Limitation of the Liability of Owners of Seagoing Ships. The effect of LLMC is to limit the amount for which the owners of a vessel are liable, potentially far less than the damage caused. For vessels not exceeding 2,000 gross tonnage it is:[5]

[5] At the time of writing 1 SDR = €1.23

- 3 million SDR for claims for loss of life or personal injury; and
- 1.51 million SDR for property claims.

However, Article 4 states:

> A person liable shall not be entitled to limit his liability if it is proved that the loss resulted from his personal act or omission, committed with the intent to cause such loss, or recklessly and with knowledge that such loss would probably result.

Thus intentional damage is unlimited, if it can be proved.

In 1948, an international conference in Geneva adopted a convention establishing the Inter-governmental Maritime Consultative Organization (IMCO), focused on safety at sea, which in 1982 became the International Maritime Organization (IMO).

The International Convention for the Safety of Life at Sea (SOLAS) of 1974, was the result of a series of improvements to earlier conventions of the same name dating from 1914, 1929, 1948, and 1960.

The International Cable Protection Committee (ICPC, 2024) was founded in 1958 as an industry body to bring together governments, state telecommunication providers and the firms manufacturing and operating undersea cables and cable ships. It later added firms and organisations involved in submarine electric cables:

> The primary purpose of the ICPC is to help its Members to improve the security of undersea cables by providing a forum in which relevant technical, legal and environmental information can be exchanged.

However, its press releases on the cable cutting in the Red and Baltic Seas indicate that there is little, if anything, the ICPC can do.

In late 2024, the International Telecommunication Union (ITU), successor to the International Telegraph Union, and the ICPC announced work to improve the resilience of cables, creating an International Advisory Body for Submarine Cable Resilience (ITU, 2024). The inaugural Submarine Cable Resilience Summit was held on 26th and 27th February 2025 in Abuja, Nigeria, strangely distant from the sea (ITU, 2025). However, resilience will be an expensive exercise for most countries, since it requires duplicate cables and landing stations, overland connections to neighbouring countries, stockpiles of cables, additional cable repair ships, and the creation of systems to respond rapidly to cut cables. Much will depend on making realistic assessments of the risks of damage to cables and of the costs, both economic and social.

The International Law Association Committee on Submarine Cables and Pipelines under International Law has produced reports that suggest there is little that can be done (ILA, 2024). Azaria (2025), had made the very peculiar suggestion that the 1884 Convention covers telegraphic but not telecommunication cables, seemingly distinguishing electrons from photons, a position that would not be held by any well informed court.

A short history of cutting cables

In the nineteenth century, the introduction of undersea telegraph cables enabled communications between colonies and imperial capitals, which combined with fast steamships and coaling stations facilitated the deployment of warships and armies to counter internal threats and external enemies. Undersea cables also supported global commerce and trade, empowered financial markets and provided stories for newspapers, helping to inform financial markets. Damage to cables could delay diplomatic and military responses, with the result that the major operators went to the expense of increasing the resilience of networks by laying additional cables, ideally in the comparative safety of very deep water. For example, from the early 1870s the United Kingdom had two routes to Hong Kong, one using undersea cables provided by the Eastern Group running via Gibraltar, Egypt, India and Singapore, and another by Great Northern via Copenhagen and St Petersburg, then overland to Vladivostok, and finally by undersea cable via Nagasaki and Shanghai. Further resilience was added by additional cables to South Africa and Australia, then north to Singapore, and later across the Pacific to China and Japan. A major concern was whether the transmission of telegrams, especially in cipher, would be permitted by neutral countries during wartime, with the British Empire going to great lengths to have 'all-red' cable routes, avoiding other countries.[6]

In 1898, Arthur Balfour explained to the House of Commons one limitation of the 1884 Convention:

> … by Article XV thereof in time of war a belligerent, signatory to the convention is free to act with respect to submarine cables as if the convention did not exist. I am not prepared, therefore, to say that a belligerent, on the ground of military exigency, would, under no circumstances, be justified in interfering with cables between the territory of the opposing Power and any other part of the world. (Hansard, 1898)

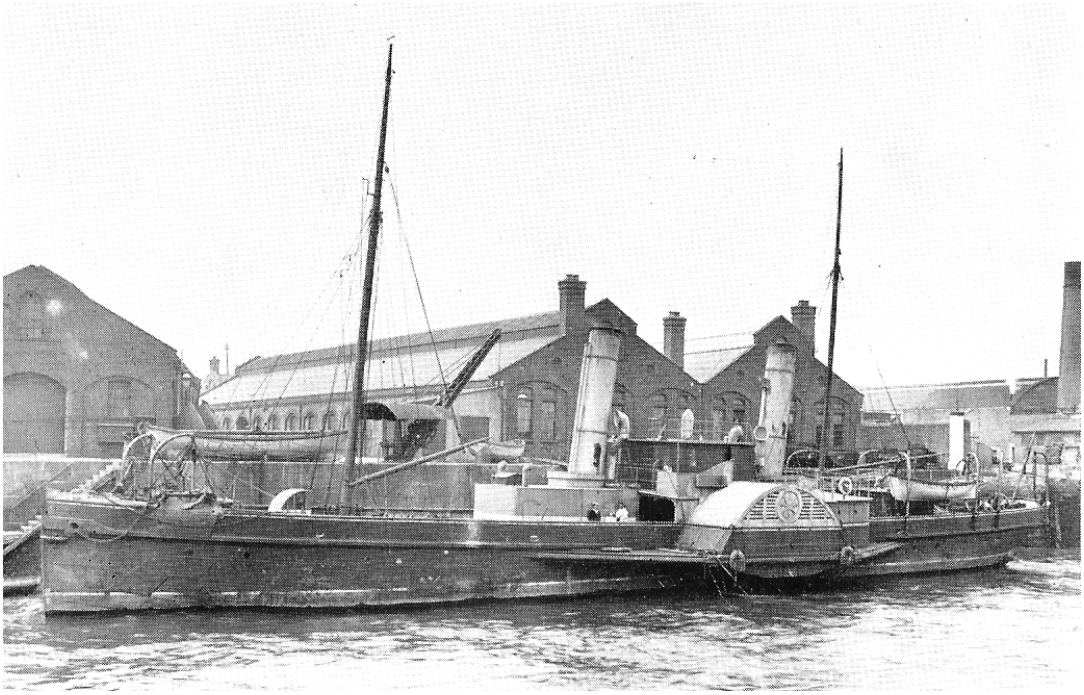
The issue again arose in the House of Commons from the adoption by the United States of its Naval War Code, giving considerable latitude for the cutting of cables connecting belligerents and other cables in the territorial waters of those belligerents. The concern was that the US Navy might be cutting cables owned by British firms. (Navy Dept, 1900; Hansard, 1901)

The US Navy had 'ridden shotgun' for a commercial cable operator as it lifted and redirected a cable off the coast of Chile in 1891, connected with a civil war. In 1898, the US Navy cut cables during the Spanish-American War. After the US Congress declared war against Spain, the Pacific Squadron of the US Navy sailed from Hong Kong to invade the Philippines. As it approached Manila one ship cut the Eastern Group cable connecting it to Hong Kong, with the effect of breaking communications between the colony and Madrid. Similarly, the US Navy cut cables in the waters around Cuba, to deprive Madrid of information about its activities and to impair coordination of its forces within the island, which had relied on coastal cables. Litigation concerning damages to the commercial cables took many years, with the operators finally being refused compensation (Fromageot, 1924a, 1924b).

[6] Nonetheless, many cables passed through Portuguese landing stations, considered a very reliable ally.

The First World War saw a series of actions that illustrate the opportunities and challenges from naval cable cutting. The United Kingdom had anticipated the outbreak of war and within hours of the formal commencement of hostilities the cable ship *CS Alert* (see Figure 1) cut five German cables that ran through the English Channel, including its connections to the United States. One cable was later diverted to France and another to Great Britain. This forced the Germans to use wireless telegraphy, which the British endeavoured to intercept and decipher. The *Kaiserliche Marine* reciprocated, by attacking cable landing stations on remote islands in the Indian and Pacific Oceans, which were soon made good. One German cruiser was forced to run aground and was lost, while the rest of the squadron had to leave the region for lack of access to coal. The *Kaiserliche Marine* also cut cables between Russia, Denmark and Sweden in the Baltic Sea, then refused to permit repairs despite the cables belonging to Great Northern, a private company based in a neutral country. This forced the British to lay a cable to Archangel, both to restore its link to its ally and to increase telegraphic capacity to India, since overland routes through Germany and Turkey had been lost.

Figure 1 ***Post Office Cable ship Alert***



When Italy entered the Second World War its navy cut the Eastern Group cables linking Gibraltar, Malta and Alexandria. This forced the British to use cables around Africa and a wireless link from Great Britain to Egypt, with wireless telegraphy and telex carrying the bulk of military signals traffic during that war

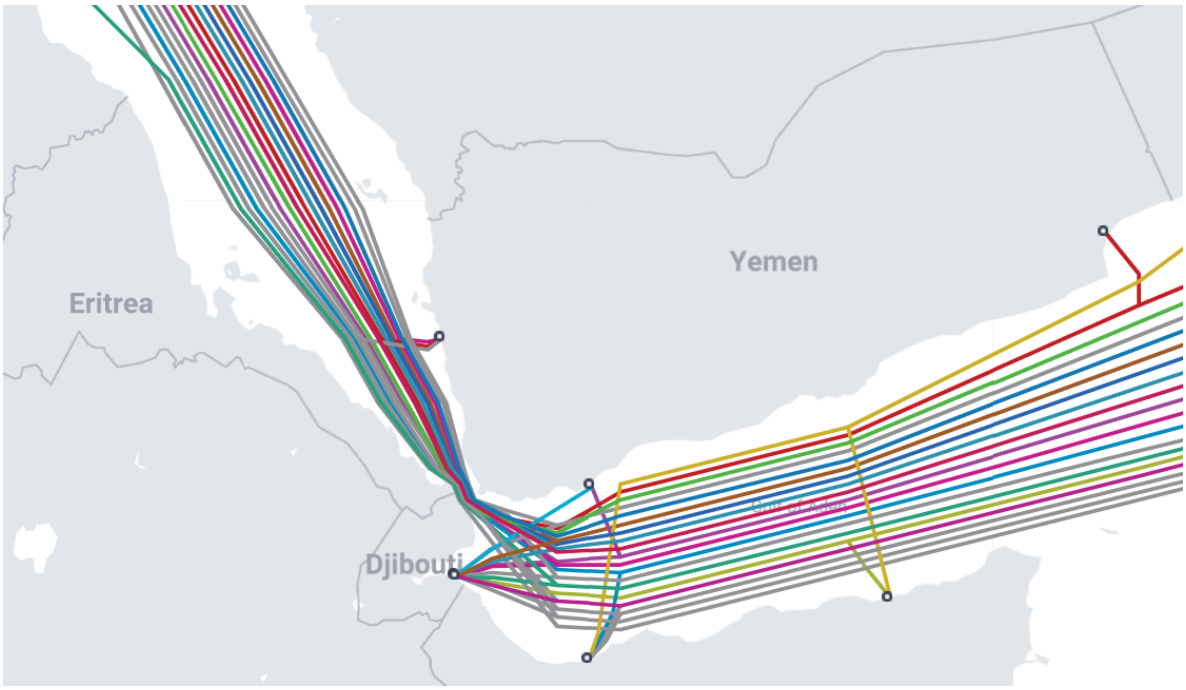
The cutting of undersea cables, both for electricity and telecommunications, has recently become part of the complex doctrine sometimes known by the contested term 'hybrid warfare'. Russia

has engaged in conspicuous mapping of undersea cables and pipelines in the Atlantic Ocean and North Sea, seemingly to intimidate European nations by implying an ability to cut many or all of the cables. It has also worked on the development of submersibles and AUVs capable of cutting cables and placing explosive charges beside gas pipelines (Rossiter, 2025). As yet, it has attacked European undersea infrastructure only in the Baltic Sea and using vessels of other flags, in an effort to obfuscate its direct involvement, even when it was the only plausible belligerent and beneficiary. Large scale cable cutting would be considered an act of war.

The Houthi incident

Cursory examination of the global undersea cable network shows one of the pinch points lies where the Red Sea meets the Gulf of Aden, with some sixteen cables lying in water that in places is only 100 metres deep (see Figure 2). A rebel force in Yemen threatened to cut some of the cables, publishing a map of their routes and announcing its intention to attack any ship sent to make repairs. The strait, sometimes known as the Gate of Tears, lies within the territorial waters of Djibouti, Eritrea and Yemen.

Figure 2 ***Undersea cables in the Gulf of Aden*** (TeleGeography, 2024)



Repeated attacks on merchant vessels are part of a long running civil war being fought in Yemen, between two groups linked to religious cults and backed by regional allies, reflecting many centuries of dispute. The so-called Houthi rebels have sought to widen their conflict and to engage regional and global powers by using drones and missiles to attack merchant shipping

exercising its right to free passage between Europe and Asia through the Suez Canal. The attacks risk the lives of crews and the safety of cargoes, plus raising insurance premiums. For ships transporting goods between Asia and Europe the alternative is to sail around Africa, adding significantly to the journey time, the fuel consumption and the total costs. While cables could be laid overland from the Mediterranean Sea across the Near East to the Persian Gulf or across Africa to the Indian Ocean, the geopolitical risks would be unacceptable. The attacks on ships have been condemned by the UN Security Council, though China and Russia both systematically abstain (UNSC, 2024; 2025). The United Nations publishes monthly reports detailing attacks on shipping. (Al Dosari & George, 2019; Al Dawsari *et al*., 2024; Notteboom *et al*., 2024; Keyani & Henley, 2024; Carboni, 2025)

The United States created the strangely named "Operation Prosperity Guardian" to counter the attacks on commercial shipping in the Red Sea (Austin, 2023). It stationed a US Navy force, together with some allies, though it proved able to offer only limited protection for merchant vessels, despite attacking launch and logistics sites in Yemen.[7] The cost of deploying a US Navy group, led by an aircraft carrier, is vastly greater than the comparatively cheap weapons being used by the Houthi rebels, a problem not dissimilar to that faced by the Russian Navy in the Black Sea.

The European Union created Operation Aspides, operated by the European Union Naval Force (EUNAVFOR); a defensive maritime security operation under the Common Security and Defence Policy (CSDP) (EEAS, 2025). Aspides has a defensive mandate to provide:

- Situational awareness;
- Accompany vessels; and
- Protect them against attacks.

On 24th February 2024 reports began to emerge that four undersea cables had been cut:

- Asia-Africa-Europe 1 (AAE-1);
- Europe India Gateway (EIG);
- Seacom; and
- TGN-Gulf.

A telecommunications operator in Hong Kong, China, announced it had diverted its traffic, using other cables through the Red Sea, an overland route to Europe and transpacific cables to the United States. Seacom reported it had diverted its traffic via Southern and West Africa, i.e. going around the Cape of Good Hope. All four cable operators reported potentially long delays in restoring services, given the lack of safety for repair vessels, and the additional costs or impossibility of insuring repair ships in a war zone. (Gambrell, 2024; HGC, 2024; Tolba, 2024)

The Houthi rebels denied any responsibility for the cable breaks and blamed the US-led naval task force. The consensus view emerged that the breaks were caused by a Houthi rebel missile

[7] USS Truman 'lost' three of its fighter aircraft, one was shot down by 'friendly fire' and two were lost overboard, at a cost of over US$150 million.

attack on 18th February 2024 on the *MV Rubymar*. This bulk carrier was then abandoned by its crew, but before it sank the *MV Rubymar* is believed to have drifted and dragged its anchor along the seabed, cutting the four cables.

For the present, the attacks on shipping at the entrance to the Red Sea are thought likely to continue (Commons Library, 2025). The incident draws attention to similar risks in locations such as the Strait of Hormuz and the Strait of Malacca. Attacks on large merchant vessels have become much easier with the availability of cheap autonomous aerial and waterborne drones, which can be used to destroy or discourage shipping and thus to draw attention to a local dispute. While cutting cables is more complex, it is feasible in shallow waters, and as this incident shows, may occur as collateral damage, compounded by the difficulty or impossibility of making the necessary repairs. Unlike the subsequent examples, the reporting and repair obligations on cable operators were commercial, rather than statutory.

The *Yi Peng 3* incident

The case of the bulk carrier *Yi Peng 3* (伊鹏3) in November 2024 illustrates some of the challenges in dealing with sabotage to undersea cables, given it cut two telecommunications cables in the Baltic Sea, and tried to cut others, including an electricity interconnector. The issues include the determination of the motivation and reasons for cutting, the clouding of those issues by attempts at denial, the benefits and costs of rapid notifications between agencies, military responses to the cutting, the pursuit of vessels fleeing the scene under the right of innocent passage, legal investigations, and the use of open source intelligence (OSINT).

There had been three prior incidents, which had heightened tensions in the Baltic Sea. The first was the severing of both Nord Stream 1 and 2 gas pipelines on 26th September 2022 by the use of explosives, apparently necessary as the steel pipes had been reinforced by substantial layers of concrete (Shen *et al*., 2023; Hernández-Benito, 2024).[8] The Russians reported a break in their Baltika cable, operated by Rostelecom between St. Petersburg and Kaliningrad, which was repaired by the *CS Spasatel Karev* (Yle, 2023). The next incident was the cutting of cables and a pipeline by the Chinese flagged vessel *NewNew Polar Bear* (see Table 1). This occurred in a narrow stretch of international waters between the territorial waters of Estonia and Finland, bu part of the Finnish EEZ.

Table 1 ***Cables and pipelines cut by the NewNew Polar Bear on 7-8th October 2023***

Cable	*Landing stations*		*Carrying*	*Owner*
Baltic Connector	Paldiski, Estonia	Ingå, Finland	Gas	Gasgrid Finland and Elering (Estonia)
-	Estonia	Finland	Telecoms	Elisa Oyj (Finland)
EE-S 1	Estonia	Sweden	Telecoms	Arelion, GN Great Nordic & Telia Eesti

[8] It resulted in the release of a considerable amount of natural gas, contributing to climate change.

The incidents were quickly attributed to the *NewNew Polar Bear* (新新北極熊), owned by a small Chinese firm and registered in Hong Kong, China. Photographs of the vessel showed that one of the two anchors was missing and the remaining anchor matched another found at the site of a break (Hujanen & Lehto, 2023). The local investigation was conducted by the Finnish National Bureau of Investigation (NBI), Finnish Navy and Finnish Border Guard. It took almost six months to restore the damage to the Balticconnector gas pipeline (see Figure 3). After ten months the government of China made a rather terse announcement of the results of its investigation, accepting that the ship had been responsible for the damage. However, it claimed this was accidental, due to the prevailing weather conditions that had resulted in the vessel dragging its anchor across the Baltic Connector pipeline (SCMP, 2024). Nonetheless, the master of the *NewNew Polar Bear*, Wan Wenguo, was later remanded in custody in Hong Kong on one count of criminal damage and two charges of violating marine by-laws (Wong, 2025).

Figure 3 ***The damaged Balticconector pipeline*** (Rajavartiolaitos, 2023)

The *Yi Peng 3* incident occurred in November 2024, with reports of breaks in cables in the Baltic Sea (see Table 2). The locations of the breaks were rapidly identified, east of the Island of Gotland, beyond Swedish territorial waters, but inside the Swedish EEZ. Ships in the vicinity were soon identified, with the *Yi Peng 3* being much the most likely culprit, a bulk carrier built in 2001 by HD Hyundai Samho in South Korea. It had been acquired in 2016 by the Ningbo Yipeng Shipping Company, renamed as the *Yi Peng 3* and registered under that name in Ningbo, carrying the flag of and subject to the jurisdiction of China. The captain was a Russian national.

Table 2 ***Cables cut by the Yi Peng 3 in November 2024***

Cable	*Landing stations*		*Owner*	*Break detected*	*Restored*
BCS East-West Interlink	Sventoji, Lithuania	Katthammarsvik, Sweden	Arelion	21:00 17 November	28 November
C-Lion1	Helsinki, Finland	Rostock, Germany	Cinia Oy	03:00 18 November	28 November

The *Yi Peng 3* had sailed from the Russian port of Ust-Luga towards the Atlantic Ocean. It was later seen to have navigated in a peculiar pattern over the cables that had been found to be broken, before it resumed sailing towards the North Sea. The vessel was challenged by *HDMS Niels Juel* of the Royal Danish Navy while still in the Danish Straits, but it stopped only after leaving Danish territorial waters, though within its EEZ. The *Yi Peng 3* was subsequently held by circling vessels of the Royal Danish Navy and the German *Bundespolizei* (see Figure 4), with Swedish coast guard vessels monitoring from close by. One of the *Bundespolizei* vessels was armed with a 57mm naval cannon.

Figure 4 ***Bundespolizei Potsdam (BP84)***

On 22nd November, the Finnish President and the Ministerial Committee on Foreign and Security Policy discussed the damage to undersea cables, advised by the National Bureau of Investigation (NBI) and the *Suojelupoliisi Skyddspolisen* (Finnish Security and Intelligence Service) (Tasavallan Presidentti, 2024). Lithuania, Finland and Sweden established a joint investigative group on 26th November, its work coordinated by the EU Agency for Criminal Justice Cooperation (Eurojust) (BBC, 2024). The investigators considered charges of sabotage and terrorism. Given the ownership, the governments of the Baltic States had to seek mutual

legal assistance (MLA) from China by means of letters rogatory. Sweden made a formal request to China, which agreed to some cooperation in the investigation, but denied the request for the *Yi Peng 3* to sail into Swedish waters. The Royal Swedish Navy used remote-controlled submarines to investigate the sites of the two cables, to assist Swedish Police and prosecutors. (Bryant & Sauer, 2024; Milne & Telling, 2024)

The Government of Sweden (2024) hosted a meeting of the heads of government of the Nordic and Baltic countries (NB8), together with Poland, on 27-28th November 2024.[9] They urged European nations to take greater responsibility for their own security. They condemned the illegal war of aggression by the Russian Federation against Ukraine and its increasing use of hybrid warfare that had shattered peace and stability in the Euro-Atlantic area and gravely undermined global security. The leaders made a specific call for naval patrols of the Baltic Sea by NATO countries.

The BCS East-West Interlink cable had initially been laid for and owned by Telia Carrier, until the latter and TeliaSonera International Carrier (TSIC) were sold for US$1 billion in 2021. The two firms were purchased by Polhem Infra, which invests funds from three Swedish pension funds in critical national infrastructure (CNI). On 19th January 2022, Telia Carrier was rebranded as 'Arelion'.

C-Lion1 is owned and operated by the Finnish company Cinia Oy, an ICT company specialising in high reliability networks and cybersecurity. The C-Lion1 was reported as broken on 18th November and repaired on 28th November, the work undertaken by the *CS Cable Vigilance* (see Figure 5), which had sailed from France to the Baltic Sea (Cinia, 2024; Tagesschau, 2024).

Figure 5 ***CS Cable Vigilance*** (Britz, 2024)

[9] All of these are members of NATO.

OSINT provided useful information about the incident, especially when the authorities were being unduly reticent. Using AIS (2024), which displays data from the transponders on vessels, the peculiar route of the *Yi Peng 3* was made public, together with details of the various vessels in its vicinity when it was allegedly cutting the cables, being chased and then detained.[10] The information was matched to photographs of the vessel and to details of its registration and ownership. The route taken by the *Yi Peng 3* was inexplicable and neither matched those of other vessels in the area nor did it appear to be a response to the weather, rather the vessel was doing something odd.

Evidence later emerged that the *Yi Peng 3* had tried to cut other cables while sailing through the Kattegat on its way to a Russian port in the Baltic Sea.

The legal status of the *Yi Peng 3* was complicated. Although China is not a signatory to the Copenhagen Convention the ship had the right of 'innocent passage' through the Danish straits, always provided it had not violated Danish law or committed acts of piracy or slavery, and similarly it could sail in Swedish territorial waters. This raised the question of whether or not it was truly innocent (Lloyd's List, 2022). Accepting it had cut the cables, then it should have been in violation of Chinese law, but had not violated international law nor the laws of the three countries affected. A further complication is that the waters are treated as national, rather than being unitary EU waters.

Boris Pistorius, the German Minister of Defence, called the cable cuts acts of "sabotage", but that is not a term used in UNCLOS (Astier & Kirby, 2024). He said:

> No one believes that these cables were cut accidentally . . . Therefore, we have to state, without knowing specifically who it came from, that it is a 'hybrid' action. And we also have to assume, without knowing it yet, that it is sabotage. (Milne & Telling, 2024)

The *Yi Peng 3* was held off the Danish coast. That it was stopped promptly indicates the existence of a plan for vessels suspected of cutting cables, necessarily including a legal analysis. It also suggests its captain and owners understood that some or all of the Danish, German and Swedish authorities had rights in the matter, otherwise it could have tried to sail into the Atlantic Ocean. The *Yi Peng 3* was finally boarded by Chinese officials on 19th December 2024, accompanied by Danish, German, Finnish, and Swedish officials, though merely as observers, explicitly excluding Henrik Söderman, the Swedish public prosecutor in charge of the investigation. The Swedish police opined that:

> The investigations taking place on the vessel on Thursday are not part of the police investigation (Polisen, 2024).

The Swedish foreign minister Maria Malmer Stenergard complained:

> It is something the government inherently takes seriously. It is remarkable that the ship leaves without the prosecutor being given the opportunity to inspect the vessel and question the crew within the framework of a Swedish criminal investigation (Milne, 2024).

[10] While mandatory for most vessels, transponders are not required in the Russian Federation.

The China Maritime Safety Administration (中华人民共和国海事局) had approached the *Statens haverikommission* (Swedish Accident Investigation Authority) to participate in the investigation into the Yi Peng 3.[11] Initial talks were held in Copenhagen on 16th and 17th December 2024, involving Chinese, Danish, Finnish, German and Swedish officials, followed by investigations on the vessel on the following day, controlled by the Chinese. The ship was anchored south of Anholt in international waters, where it had stopped on the orders of the Chinese authorities. It carried a crew of 22, all Chinese citizens, who had come aboard in Port Said, before it sailed to Ust-Luga, and this was their first time on this vessel. (SHK, 2024; 2025)

Evidence from examination of the seabed showed the anchor must have run out rapidly. The crew claimed that the port anchor had come loose from its winch, running out its entire length of 330 metres, with one of its anchor sheets seen to have been damaged. This was only discovered on the morning of 18th November, when the ship was in Hanö Bay and the weather had improved sufficiently to inspect the ship.

The ship was equipped with a Simplified Voyage Data Recorder (S-VDR), which continuously records conversations on the bridge, course, speed, and position, together with a number of cameras. However, data are stored only for a limited period and had been overwritten before the investigation. The crew were interviewed, but these were not allowed to be recorded.

The Swedes concluded there were two alternative scenarios. The ship might have deliberately released the anchor to damage cables and pipelines, with a significant risk in doing so to the vessel and the individuals operating the anchor windlass. Otherwise, the anchor came loose because it had been improperly secured, but this should have damaged the chain box and the windlass. Moreover, the *Yi Peng 3* had been dragging its anchor along the bottom for 1½ days over 180 nautical miles (just over 330 km) apparently without being discovered. Importantly, there was no proof of intentional damage.

The view of the Lithuanian foreign minister Kestutis Budrys was that:

> China's unwillingness to co-operate on the undersea incident investigations in the Baltic Sea cannot be allowed to set a precedent in Europe - or anywhere else (Milne, 2024).

Finally, the *Yi Peng 3* sailed away on 21th December 2024, apparently for Port Said.

The lessons from the incident were that the non-Russian nations of the Baltic Sea had made some preparation for the cutting of cables and pipelines. Clearly there was coordination between cable operators, regulators, and with military authorities. On the one hand they stopped the vessel that they believed had cut the cables and gathered evidence from the seafloor about actual and attempted breaks. On the other hand they repaired the broken cables very efficiently. Nonetheless, the only costs to the owners of the *Yi Peng 3* was the loss of almost a month of its use and the possibility of civil action for damages to the cables.

[11] SHK normally investigates accidents, rather than cases of intentional damage.

The *Eagle S* incident

On 25th December 2024 breaks were reported in five undersea cables (see Table 3).[12] The effect on the flow of electricity was immediate and significant, with the loss of about 385 MW of transmission capacity between Finland and Estonia, greatly reducing onward transmission to Latvia and switching Estonia from exporting electricity to Russia to importing (see Figure 6). Within an hour the breakages of the telecommunications cables were reported to the Cyber Security Center of the Finnish Transport and Communications Agency (TRAFICOM, 2024), which informed the Finnish Defence Forces, Border Guard, Police and prosecutors.

Table 3 ***Cables cut by the Eagle S on 25th December 2024***

Name	*Type*	*Landing stations*		*Owner*
Estlink 2	Electricity	Estonia	Finland	-
C-Lion1	Telecoms	Finland	Germany	Cinia Oy
-	Telecoms	Estonia	Finland	Elisa Oyj
-	Telecoms	Estonia	Finland	Elisa Oyl
-	Telecoms	Estonia	Finland	CITIC

The vessel suspected of cutting the five cables was identified as the *Eagle S*, an oil tanker sailing from Ust-Lugu (Усть-Луга), a harbour west of St Petersburg, destined for Port Said (Vessel Finder, 2024).[13]

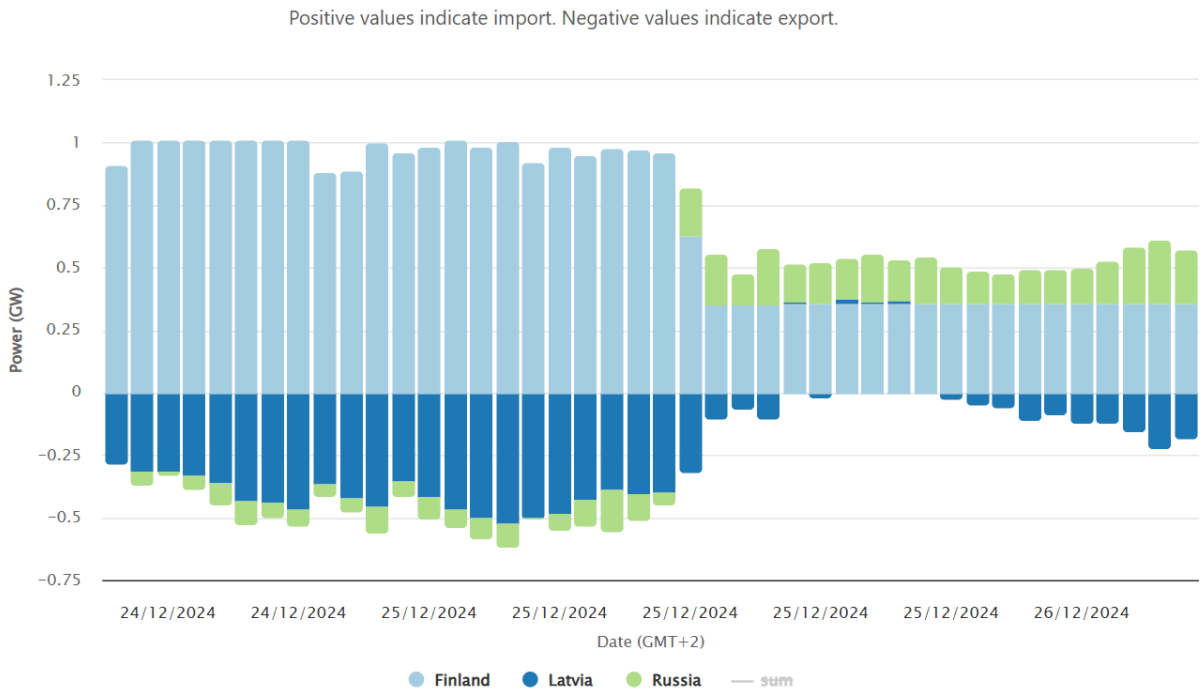
President Stubb noted:

> I have to say it was rather hectic Christmas Day or afternoon for the Finnish political leadership and our authorities (Rachman, 2025).

[12] Christmas Day in Russia comes later than in Europe.

[13] Another vessel, *Xin Xin Tian 2*, registered in Hong Kong, China, was reportedly in the area. It is owned by Hainan Yangpu, part of the Torgmol group.

Figure 6 ***Cross border physical flows of Estonia in week 52*** (Energy-Charts, 2024)



Very early in the morning of the 26th, the *Eagle S* was ordered into Finnish territorial waters, where two helicopters, one each from the Defence Forces and the Border Guard, abseiled special operations troops onto its deck and took control. The helicopters were supported by the Border Guard Patrol Ship *Turva*, which initially guarded the *Eagle S*, anchored off Porkkala, inside a 3km radius aircraft exclusion zone. It was later moved to an anchorage off Porvoo. The *Eagle S* had been stopped some 12 minutes before it would have reached the second electricity interconnector across the Gulf of Finland. On trying to raise its anchor, there had been only the chain, the anchor was presumed to have been snagged on a cable or on the seabed, which the authorities found after a long search. The cargo was contraband Russian unleaded petrol, in violation of EU sanctions. The *CS Cable Vigilance* was reported to have left France immediately to repair the Cinia cable, while the Finnish *CS Telepaatti* sailed from Turku to repair the two cables belonging to Elisa. There was no news of the repair to the CITIC Telecom CPC (2024) cable, which could immediately redirect traffic via Stockholm. While three of the telecommunication cables were repaired within days, the electricity interconnector was to take very much longer. (ERR, 2024; Sajari, 2024; Sajari *et al*., 2024)

The *Eagle S* is registered in and flies the flag of the Cook Islands, which is a self-governing state in free association with New Zealand. It has a population of only fifteen thousand people across fifteen islands with a land area of 237 km^2, scattered across 2 million km^2 of the Pacific Ocean, between New Zealand and Hawaii (USA). It claims to operate a "world class" register of ships, with more than 800 vessels. The Cook Islands are not a signatory to the 1884 Convention, but have ratified UNCLOS. The vessel had a Georgian captain and a Georgian and Indian crew.

Its government is engaged in litigation at the International Court of Justice (ICJ), seeking an advisory opinion on the obligations of states in relation to climate change (MFAI, 2024). It is thus grossly hypocritical of the Cook Islands to run a register for elderly and poorly maintained oil tankers that belong to the 'shadow fleet' of Russia, used to break sanctions imposed because of its second invasion of Ukraine (Bockmann, 2024). Following an inspection off Skagen, the *Eagle S* had been found to have a string of deficiencies compromising both crew and environmental safety, about which the owners and the Cook Islands did nothing (Bockmann, 2024a). It is unclear whether the actions of the Cook Islands government were merely hypocritical or whether there is also corruption.

Lloyd's List reported the *Eagle S* as being the only vessel belonging to Caravella LLC-FZ, a company based in the United Arab Emirates (UAE), with an address in an hotel! Technical management of the vessel is apparently by Peninsular Maritime India Private Limited (IN CIN U74999MH2017PTC302046), based in Mumbai.[14] The ship had been built in 2006 by the New Century Shipyard Ltd., Jingjiang, China, for the Singapore company FR8 Holdings PTE Ltd.

On 26th December, the Prime Minister of Finland, Petteri Orpo, led a press conference, thanking the Finnish authorities for their prompt and exemplary action. He explained that an investigation was underway. He noted there was coordination with neighbouring countries, especially Estonia, but not Russia, and discussions with the EU and NATO concerning improved security for infrastructure. He expressed concern over the environmental dangers from the Russian shadow fleet. (Typpö, 2024).

The Finnish authorities were investigating charges of :

- Aggravated sabotage; and
- Aggravated sanctions violation (carrying a full cargo of lead-free gasoline).

The aggravation being the damage to important economic and social functions. A further consideration was whether the charges should include terrorism. The vessel may not have had a valid insurance certificate.

Despite the beneficial owners of the *Eagle S* being unknown, someone engaged a Finnish lawyer, Herman Ljungberg, to act on their behalf. Rather dramatically, he accused the government of "hijacking" the tanker in international waters in contravention of the law of the seas. He claimed Finnish authorities had no jurisdiction over the vessel or to conduct investigations, and no basis for suggesting links to Russia, going on to deny there was a shadow fleet.

Later on the 26th, the government of Estonia held a press conference. It reported it was coordinating with neighbouring countries, including cooperation with Finnish prosecutors, and also with the EU and NATO. The country could continue to use other cables and other energy sources, but argued that cable cutting had become systemic and required closer monitoring of critical national infrastructure (CNI). Estonia would look at increasing deterrents, reviewing

[14] Confusingly there is a web site for a Peninsular Maritime registered in the United Kingdom.

both domestic laws and international conventions. The interconnector would take several months to repair, though the telecommunication cables were expected to be restored quite quickly. Estonia was due to disconnect from the Russian electricity grid on 9th February 2025, which proceeded as scheduled and was successful. There was increased environmental risk from the shadow fleet, with authorities intensifying checks of documents. Naval patrols had been initiated on the route of the remaining electric interconnector. (Valitsuse Uudised, 2024)

The European Commission responded to the attack on the 26th: "standing in solidarity with Finland, Estonia, and Germany". The Russian shadow fleet was seen as threatening security and the environment, while contributing to its funding of a war of aggression. The EC would propose further measures, including sanctions, to target the fleet, and to strengthen efforts to protect undersea cables, including enhanced information exchange and new detection technologies. It would also look at undersea repair capabilities and increased international cooperation. The EC remained committed to ensuring the resilience and security of its critical infrastructure. (EC, 2024b)

It subsequently emerged that the *Eagle S* had been involved in an incident off the coast of the Netherlands. It had allegedly been observed sailing back and forth over Atlantic Crossing 1, a telecommunications cable linking Germany, the Netherlands, United Kingdom, and the United States.

It was later disclosed that the oil tanker had previously carried special transmitting and receiving devices that were used to monitor naval activity, being a Russian spy ship. It was alleged to have had Russian, Turkish, and Indian radio officers to operate the equipment and that the *Eagle S* had dropped sensors when sailing through the English Channel. However, the Finnish authorities found no evidence of such equipment or activities on the *Eagle S*. (Bockmann, 2024c)

The 11-tonne anchor of the Eagle S was later found on the seabed (see Figure 7). Investigators estimate it had been dragged about 90km. They also established that the Federal Security Service of the Russian Federation (FSB), had held the ship for two days after it was loaded, though they could not identify the cause of the delay, and the FSB had declined to comment or explain.[15] (Pancevski & Michaels, 2025)

While the *Eagle S* was released on 2nd March 2025, three members of the crew were detained for trial.

Repairs to Estlink 2 were made by Nexans, a specialist electricity infrastructure firm, but did not begin until May 2025 and were not expected to be completed until July (Skopljak, 2025). However, Estlink 2 was restored on 20th June 2025 (Fingrid, 2025).

[15] The FSB was formerly the KGB, before which the NKVD and Cheka.

Figure 7 ***The anchor of the Eagle S recovered from the Gulf of Finland*** (Murday, 2025)

The coordination within Finland appears to have involve:

- Prime Minister's Office
- Prosecutor General of Finland
- Ministry of Justice
- Ministry of Defence
    - Finnish Special Operations Forces (FINSOFs)
- Ministry of the Interior
    - Finnish Border Guard
    - Police of Finland
- Ministry of Economic Affairs and Employment
    - Finnish Transport and Communications Agency (Traficom):
        - National Cyber Security Centre Finland
- Courts

Following so closely after the *Yi Peng 3*, the *Eagle S* incident shows that the Putin regime is intent on destabilising the Baltic Sea region. The other Baltic Sea states are not taking the issue lightly, having moved expeditiously to seize the *Eagle S* in international waters.

Passage through the Baltic Sea and Danish straits

The free passage of vessels through closed and shallow seas and the associated straits present a series of problems. Most, though not all of the waters are territorial. The relatively shallow nature of the Baltic and the slow exchange of water with the Atlantic Ocean means it is especially at risk from pollution. The shallow nature of the waters means that cables,

interconnectors and pipelines are at risk from ships, whether accidental or malicious damage. Moreover, the political aspirations of Russia to control the waters and its practice of hybrid warfare add to the complexities and the risks.

The long standing desire of commercial and naval maritime powers to ensure unrestricted transit through straits has to be reconciled with the growing concern of coastal states about the dangers from pollution, leaks of oil, and vessels sinking. In the Baltic Sea there is the Helsinki Convention addressing environmental concerns. The Russian 'shadow fleet' of poorly maintained, uninsured and badly crewed vessels presents heightened environmental risks.

Innocent passage is defined as being "not prejudicial to the peace, good order, or security of the coastal State." Article 19 of UNCLOS includes a non-exhaustive list of acts that would be considered to be non-innocent and thus permit a coastal state to interfere with the passage of the ships, but omits cable cutting.

The transit passage regime is defined under Article 37 of UNCLOS. Where a ship has the right of innocent passage it is hard for another nation to justify stopping, boarding or searching the vessel. This is further complicated by the willingness of the Russian Federation to deploy its warships near vessels from the shadow fleet.

The International Court of Justice (ICJ) ruled on the passage of ships through the Corfu Channel in 1949. The incident had involved damage to two Royal Navy destroyers, *HMS Saumarez* and *HMS Volage*, with the loss of forty-four lives and a comparable number of injuries, caused by mines placed in the Channel. The Court found Albania liable for having allowed mines to be placed in a strait in which there was a right of passage.

The Baltic Sea is accessed from the North Sea by the Skagerak (between Norway and Denmark) and the Kattegat (between Denmark and Sweden), with three principal routes around the Danish islands of Funen and Zeeland, namely the Little Belt, Great Belt and the Øresund, between Denmark and Sweden. These bodies of water have complex legal histories, reflecting concerns of the coastal states and great powers, notably the Russian Empire, the United Kingdom and the United States. Indeed the United Kingdom fought two battles of Copenhagen in 1801 and 1807 to ensure the rights of passage of its vessels, while Germany opened the Kiel Canal in 1895 to ensure its own access to the North Sea. (Miljan, 1974; Oral, 2019)

Access to the Baltic Sea was an historic problem, with the Danes having collected revenues from passing vessels for centuries. In return for fixed cash payments, the Kingdom of Denmark agreed to the innocent passage of vessels. Article 1 (1) of the 1857 Copenhagen Convention states, *inter alia*:[16]

> Aucun navire quelconque ne pourra désormais, sous quelque prétexte que ce soit, être assujeti, au passage du Sund ou des Belts, à une dctention ou entrave quelconque; mais Sa Majesté le Roi de Danemark se réserve expressément le droit de régler, par accords particuliers, n'impliquant ni

[16] The US refused to sign the 1857 Convention, insisting on a broadly similar Convention of its own.

> visite ni détention, le traitement fiscal et douanier des navires appartenant aux Puissances qui n'ont point pns part au présent Traité;

The ICJ heard a case on passage of ships through the Great Belt, brought by Finland against Denmark. However, it was settled out of court, so that no ruling was made.

During the First World War the Danish Navy mined the routes at the insistence of the German Empire.

Oude Elferink (2000) concluded that the 1857 Copenhagen Convention and Article 35(c) of the Law of the Sea Convention meant that Part III of UNCLOS did not apply to the Danish straits:

> … the legal regime in straits in which passage is regulated in whole or in part by long-standing international conventions in force specifically relating to such straits.

The 1857 Convention precludes Denmark from establishing a system of compulsory pilotage in the Danish Straits.

As a Eurasian power the Russian Empire sought access to warm water ports from which it might trade freely and develop a deep water navy. Its northern ports of Archangel and Murmansk were frozen in winter. St Petersburg had access to the Baltic Sea with a potential connection to the North Sea and Atlantic Ocean, but this was effectively controlled by Denmark until the 1857 Copenhagen Convention. Although Russia had annexed Crimea from the Ottoman Empire in 1783, the Sublime Porte retained control over the Bosphorus and thus access to the Mediterranean Sea, which Turkey currently controls under the 1923 Treaty of Lausanne. Following the Second World War, the Union of Soviet Socialist Republics (USSR) tried, unsuccessfully, to take control of the Baltic Sea, aided by its allies in the Warsaw Pact. As part of its plan it had seized from Germany the city of Königsberg, formerly in Ostpreussen, to create the Kaliningrad exclave.[17] Today the Baltic Sea is sometimes termed a NATO 'lake', given that all the coastal countries are members. The sole exception is Russia that is working to undermine and increase the cost of any control exercised by NATO.

The states parties to the 1884 Convention on Submarine Cables include Denmark, Germany, Norway, Russia, Sweden, United Kingdom, and the USA, but not China or the Cook Islands. While Estonia, Latvia, and Lithuania could have inherited accession to the Convention from Russia and the USSR, they did not do so when they became independent.

Even after the *NewNew Polar Bear*, *Yi Peng 3* and *Eagle S* incidents, there were further problems (see Table 4). There will be some respite in 2029 with the opening of the Fehmarnbelt Tunnel, linking the Danish island of Lolland with the German island of Fehmarn, which together with the Øresund Tunnel provide comparatively secure capacity for cables.

In January, a Bulgarian bulk carrier that had departed the Russian port Ust-Luga was detained and boarded by the Swedish Coast Guard as part of the NATO Baltic Sentry exercise. It was

[17] Russia broadcasts radio signals from Kaliningrad to jam GPS or to make it inaccurate, endangering aircraft and shipping.

later released by Swedish prosecutors, led by Mats Ljungqvist, senior prosecutor at the Swedish National Security Unit.

Table 4 ***Further cable incidents in the Baltic Sea***

Ship	*Date*	*Landing stations*	*Cable affected*
Vezhen	26 January 2025	Ventspils, Latvia to Fårösund on Gotland (Sweden)	Latvian State Radio and Television Centre (LVRTC) (Milne, 2025b)

The Baltic sea is a mixture of the territorial waters of the coastal states, with some areas of EEZs, and areas of international waters to facilitate transit of vessels. States parties to UNCLOS have been reluctant to restrict freedom of navigation because they want the same rights in other parts of the world. Telecommunication cables were first laid in the Danish Straits in the 1850s, gradually extended over the subsequent decades, with a surge in recent years to support broadband digital services. A number of electricity interconnectors were added to provide greater resilience for electricity supply within the EU single market. The presumption had been that, at least in peacetime, these would be subject only to natural risks and fishing nets, but this changed with the Russian adoption of very aggressive tactics, sometimes termed hybrid warfare. A set of problems has presented itself, with a lack of protection in international law for the cables, interconnectors and pipelines, and limited powers to intervene over the actions of vessels that are protected by the states whose flags they fly. However, flags of convenience are much less able to resist demands than great powers.

Legal and policy frameworks

The international conventions are obviously deficient for undersea cables. There is remarkably little protection offered, despite the considerable investments, the high costs of repairing malicious damage, and the economic and social significance of the cables. A vessel cutting a cable is treated as part of the territory of the country where it is registered and therefore cannot readily be stopped or boarded, even if it is suspected or known to have cut cables, interconnectors or pipelines. The Russian Federation, as would be expected, denied any involvement in the *NewNew Polar Bear*, *Yi Peng 3* and *Eagle S* incidents, brushing aside such accusations as absurd. Two of those incidents were committed by vessels from its close ally China, which blocked thorough inspections and denied any intentionality on their part, obfuscating blame. The *Eagle S* voluntarily entered Finnish waters, having been caught in the act of cutting cables over a distance of 100 kilometres and a period of twelve hours, while carrying contraband and lacking insurance, in violation of international law.

The European Union has addressed threats to undersea cables from two perspectives, through its 'Digital Decade' it promoted the adoption of technologies within its single market, and through its Security Strategy it has sought to protect them. These are typical multi-level

governance (MLG) systems, at EU and member state levels, with agencies linked by European regulatory networks (ERNs) and individually engaging with market players. The resulting structures are thus both multi-layered and polycentric. The EU has enacted legislation in which member states have bound themselves and operators to protect CNI, including CUI, notably:

- Directive (EU) 2018/1972 (European Electronic Communication Code);
- Directive (EU) 2022/2555 (Network and Information Security (NIS 2) Directive); and
- Directive (EU) 2022/2557 (Critical Entities Resilience (CER) Directive).

At Nevers in March 2022, an informal council of telecommunications ministers unanimously recognised the strategic importance of networks (EU, 2022). The issues of both cyber and physical security were to be taken up by the NIS Cooperation Group, ENISA and BEREC, to provide a general risk assessment. The NIS Cooperation Group (2024) report was published two years later.

The Council (2023) invited the European Commission to conduct a comprehensive study of undersea infrastructure, both interconnecting Member States and connecting them to the rest of the world. It also encouraged the use of EU surveillance assets, such as Copernicus, Galileo and the European Geostationary Navigation Overlay Service (EGNOS), to monitor CNI and their immediate vicinities.

The EU noted the increased risk that "malicious actors" would attack CNI, including undersea cables, and proposed actions to enhance their resilience and protection (Consilium, 2024).

The EC (2024a) adopted a Recommendation calling on member states to:[18]

- Assess regularly and improve the security and resilience of existing and new submarine cable infrastructure; and
- Support deployment of Cable Projects of European Interest (CPEI).

MSs were encouraged to take into account defence-level security standards. They should also conduct national risk assessments of the cybersecurity and physical security of submarine cable infrastructure, plus the security of the associated supply chains (i.e., cable operators, cable repair ships and cable manufacturers). There were to be mapping exercises at MS and EU levels, identifying the ownership and capacity of the cables. There were also to be assessments of risks, vulnerabilities of and dependencies on submarine cable infrastructure, in particular concerning high-risk suppliers and critical supply chains. One aim was the creation of a 'Cable Security Toolbox'. MSs were to discuss the potential for innovative solutions for the detection and deterrence of threats against undersea cables, including incorporating the results of EU-funded projects. The construction of CPEIs was intended to diminish risks by improving resilience. The Recommendation is to be reviewed by the end of 2025.

The EU Action Plan on Cable Security aims to increase the resilience and security of submarine cables, both communications and electricity, possibly offshore wind farms. It seeks to

[18] Somewhat eccentrically, the EC repeatedly "incited" MSs to act.

- Prevent "disruptive incidents";
- Increase detection capacity;
- Coordinate responses; and
- Enhance its deterrence posture.

The work is designed to be complementary with NATO. (EC & High Representative, 2025)

Another approach is through support for technological innovation. For example, Thales coordinates the work on the SEACURE project, an acronym for SEabed and Anti-submarine warfare Capability through Unmanned featuRe for Europe (SEACURE). The other firms being:

- Fincantieri SPA;
- Kongsberg Discovery AS;
- Leonardo;
- Naval Group;
- Navantia; and
- Saab Cockums Aktiebolag.

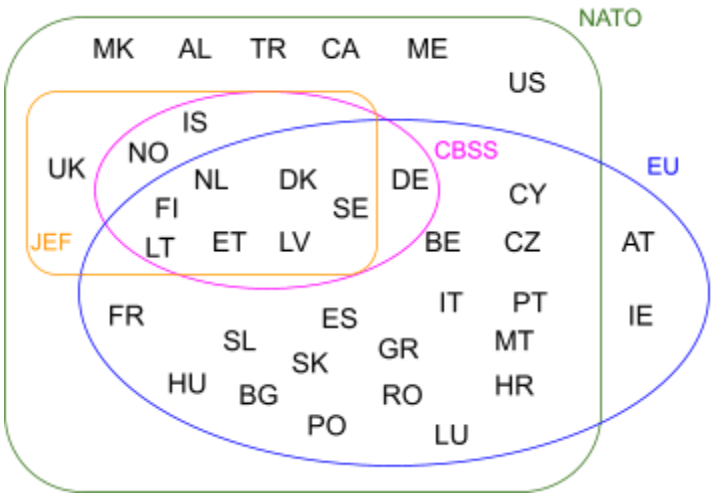
This received €45 million from the European Defence Fund to deliver more effective anti-submarine and seabed warfare through autonomous systems. SEACURE aims to find effective ways of tackling the evolving threat landscape in the sea.

EU legislation directly covers the land areas of its twenty-seven MSs states, plus Iceland and Norway as members of the European Economic Area (EEA), extending to their territorial waters, which in most cases is 12 nautical miles or 22 kilometres. Beyond the territorial waters, in EEZs, any legislation has to be read alongside UNCLOS and, in the case of the Danish straits, the Copenhagen Convention, giving ships freedom or innocent passage, which greatly diminishes the protections.

Under the umbrella of the Common Security and Defence Policy (CSDP), the European Defence Agency (EDA) promotes and facilitates integration between member states.

Nearly all EU member states are also Allies in NATO, with the notable recent admission of Finland and Sweden (see Figure 8). The exceptions are Austria and Ireland, despite the latter having a very important EEZ with many cables running across its continental shelf, though it possesses minimal naval resources. On 16th December 2002, the Berlin Plus package of agreements was struck between the EU and NATO, including the NATO-EU Security Agreement. The use of NATO assets by the EU is subject to a 'right of first refusal'; NATO must have declined to intervene in a particular crisis.

Figure 8 ***CBSS, EU, NATO and the JEF***



The North Atlantic Treaty Organization (NATO) has complex origins in the aftermath of the Second World War and the Cold War, being a defensive military alliance of democratic states, which it terms 'Allies' rather than member states or states parties. In 2020, NATO approved the concept of the Deterrence and Defence of the Euro-Atlantic Area (DDA), providing a framework for NATO Allies against its principal threats. This is used to strengthen preparedness through advance planning for potential crisis and conflict scenarios. Other groups include the Council of the Baltic Sea States (CBSS, 2025), and the Joint Expeditionary Force (JEF).

At a summit in Vilnius, NATO leaders agreed that:

> The threat to critical undersea infrastructure is real and it is developing. We are committed to identifying and mitigating strategic vulnerabilities and dependencies with respect to our critical infrastructure, and to prepare for, deter and defend against the coercive use of energy and other hybrid tactics by state and non-state actors. Any deliberate attack against Allies' critical infrastructure will be met with a united and determined response; this applies also to critical undersea infrastructure. (NATO, 2023)

To address these issues NATO created the Maritime Centre for the Security of Critical Undersea Infrastructure (NMCSCUI), within its existing Maritime Command (MARCOM, 2024; NATO, 2024). NMCSCUI supports Allies in their national responsibilities to secure their respective critical undersea infrastructure (CUI). It also serves as a platform for operational-level information exchange amongst the "community of trust", helping to deter, defend, and optimize responses to the coercive use of hybrid warfare tactics by state and non-state actors.

A summit of Baltic Sea NATO Allies was held on 14th January 2025 in Helsinki, at a very high level with:

- Finnish President Alexander Stubb;

- Estonian Prime Minister Kristen Michal;
- Danish Prime Minister Mette Frederiksen;
- German Chancellor Olaf Scholz;
- Latvian President Edgars Rinkevics;
- Lithuanian President Gitanas Nauseda;
- Polish Prime Minister Donald Tusk;
- Swedish Prime Minister Ulf Kristersson;
- NATO Secretary General Mark Rutte; and
- EC Vice-President Henna Virkkunen.

It proposed the creation of an open-ended Operation Baltic Sentry, under the Maritime Operational Warfighting Headquarters. This was to improve vigilance, in particular in monitoring the Russian 'shadow fleet' of ageing and poorly maintained vessels sometimes used to cut cables and which posed serious environmental and pollution risks. The aim of the move was to deter future saboteurs and increase the likelihood of catching them, after Russia had been accused of cutting undersea cables. (Milne, 2025a)

Operation Baltic Sentry deployed a range of assets from NATO Allies, including frigates, minesweepers, drones and maritime patrol aircraft (e.g., P8 Poseidon and Rivet Joint maritime patrol aircraft from the United Kingdom). NATO Secretary General Rutte said:

> What matters is that we employ the right military assets in the right places at the right time to deter future destabilising acts.

A decade before, some Allies had agreed to create the Joint Expeditionary Force (JEF), formally outside NATO but available to it, currently comprising: Denmark, Estonia, Finland, Iceland, Latvia, Lithuania, the Netherlands, Norway, Sweden, and the United Kingdom (Knighton, 2024). Following the cable incidents in the Baltic Sea, the JEF initiated an exercise known as 'Nordic Warden' (JEF, 2025; MoD, 2025). This uses an artificial intelligence system to assist in monitoring the Russian 'shadow fleet' and in protecting CUI, being run from Northwood in London. (Healey, 2025)

The Lithuanian Armed Forces signed an agreement on 13th January with Litgrid, the operator of the national electricity transmission system, to strengthen the security of CUI in the Baltic Sea. This involves the exchange of information on any infringements, unusual activities and updating safeguards. (Lietuvos kariuomenė, 2025)

On the borders of the 79th annual United Nations General Assembly, a group of nations issued the New York Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World (Dept of State, 2024).[19]

[19] United States of America, Australia, Canada, the European Union, the Federated States of Micronesia, Finland, France, Japan, the Marshall Islands, the Netherlands, New Zealand, Portugal, Republic of Korea, Singapore, Tonga, Tuvalu, and the United Kingdom.

In the US House of Representatives, August Pfluger (R-Texas) introduced a bill (HR 9766) to establish an interagency working group including the Department of Homeland Security (DHS), Federal Communications Commission (FCC), Coast Guard, Cybersecurity and Infrastructure Security Agency (CISA) and others, with the intention of improving the security, resiliency, and integrity of undersea cables (Pfluger, 2024).[20] This made little progress and seemed only intended to address territorial waters.

A hearing of the Subcommittee on Communications, Media and Broadband (2024) addressed communications networks safety and security. Given it came shortly after disclosure of the Salt Typhoon cyber attack on all the major US carriers, that took up much of the time. It also reflected an earlier hearing by the Subcommittee on Communications and Technology (2024), which principally addressed issues concerning the perceived dangers of China and Chinese equipment. A further issue was the increased funding of the rip and replace policy for Chinese network equipment, for which US$3 billion was included in the National Defense Authorization Act for Fiscal Year 2025. Justin Sherman addressed the issue of cable security, with a strongly anti-Chinese message, calling for the exclusion of cables landing in China, laid by Chinese companies or made by Chinese manufacturers. He believed they would install monitoring or wiretapping equipment, which would be a threat to US national security. Sherman proposed a commission to study the Chinese threats to undersea cables, since the operators and manufacturers had not always understood the national security risks in breakages. Many of these issues had been dealt with over recent years by the Committee on Foreign Investments in the United States (CFIUS) (Sutherland, 2021).

Sherman noted a major change in the global undersea cable market, with the decline of traditional network operators and their replacement by:

- Alphabet (Google);
- Amazon;
- Meta (Facebook); and
- Microsoft.

In a mere decade these platform operators had gone from 6 to 69 per cent of total international cable capacity and were investing heavily in additional undersea cables.[21] These appear to have very limited resilience and thus are exposed to considerable risk, being undefended and easily cut.

The US Department of Homeland Security announced its priorities for subsea cable security and resilience (DHS, 2024), for which the legal basis is the Critical Infrastructures Protection Act of 2001 (42 USC § 5195c).[22] While it insists the US is a leader in undersea cables, its own supply chain analysis tells a different story. The DHS reported 22 ships globally for the repair of subsea cables, of which only two are registered in the USA, pointing to the apparent reluctance of

[20] Pfluger did not include the Department of Defense.

[21] The data on these cables are presumed to be available to the National Security Agency (NSA).

[22] Aided by Critical Infrastructure Partnership Advisory Council (CIPAC).

operators to invest in new vessels. Only four companies provide 'turnkey' cable systems, from conception, engineering, and manufacturing to construction, installation, and repair, of which only one is based in the USA:

- Alcatel Submarine Networks (France);
- HMNTech (China);
- NEC (Japan); and
- SubCom (USA).

Cable operators and consortia are required to engage with a number of silos of the US government, each looking at different issues:

> Regrettably, several industry representatives lamented that governmental authorities' shifting expectations and the increasingly unpredictable outcomes of these processes have made the United States, in their view, one of the most difficult countries in which to land subsea cable systems (DHS, 2024, p 5).

The DHS promised to conduct a comprehensive assessment of cable permitting and licensing.

More seriously, the DHS admitted to deficiencies in the responsibilities across multiple departments and agencies for:

- Cable protection;
- Outage reporting;
- Threat intelligence sharing;
- Direct cable operations; and
- Crisis response.

Given rising threats this presents serious problems.

A possible approach would be to use Article 51 of the UN Charter:

> Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

The obvious question is whether using a civilian vessel to cut a cable could be construed as an "armed attack", it would seem more applicable to the greater and more prolonged damage from cutting a gas pipeline or electricity interconnector. It leaves open questions of attribution of the attacking belligerent power, which is often very difficult, and the proportionality of any response. In the absence of identification, an attack can be treated as terrorism, which opens some options in international law.

By improved coordination between operators and the military, through CERTs, it has become possible to accelerate responses enabling 'hot pursuit' of cable cutting vessels. This can be further improved with more accurate locations of breaks and better systems for passing information. The speed of the repairs to telecommunication cables in the *Yi Peng 3* and *Eagle S* cases was commendable, though further investments in repair ships would help. However, action is required to accelerate repairs to interconnectors and gas pipelines from months to days.

Conclusion

The *Yi Peng 3* incident, followed so quickly by the *Eagle S* incident, demonstrated the intensity of the threat by Russia to countries around the Baltic Sea and raised questions about further attacks. Given the prompt action by Finland, Russia ought to have found it more difficult to persuade captains to cut cables, whether having to pay them more or to coerce them more severely. Its shadow fleet of ageing and dangerous oil tankers risk an environmental disaster in the confined waters of the Baltic Sea, in addition to any efforts those vessels make at cable cutting. Since Russia has mapped underwater cables in far more detail than required for the dragging of anchors, it wishes to appear prepared to deploy more advanced technologies. Its General Staff Main Directorate for Deep Sea Research (GUGI) already operates the 'research vessel' *Yantar*, which has specialist submarines and autonomous underwater vehicles. Having gone so far and suffered so few consequences, Russia seems willing to push further.

European states have improved their coordination through both the EU and NATO, with greater monitoring, better coordination, accelerated responses and the development of a limited willingness to board and seize vessels. Nonetheless, more work is required to reduce the complexity of the governance arrangements and to improve resilience and responses. Breaks in cables are reported rapidly by commercial operators to the authorities, which now have plans to respond. Operators have made speedy repairs to damaged telecommunications cables, though a strong case can be made for significant investments in laying more cables and purchasing additional specialist repair ships. Further preventive measures could include laying dummy cables as decoys for attackers. A more sophisticated approach would be to deploy more detectors, part of the Internet of Underwater Things, so that breaks and anchor dragging are more immediately located and thus facilitate rapid military responses. Underwater drones are apparently being deployed to monitor cables, interconnectors and pipelines, though with potentially significant costs.

Cable cutting has been called sabotage and vandalism, but not yet an act of war. Historically, it has been conducted as a military action in wartime, but has yet to trigger a war. Russia must have crossed or be very close to having crossed the line that requires retaliation, whether kinetic warfare or sanctions banning specific vessels or, even, closing the Baltic Sea to vessels sailing to Russian ports.

One option would be to designate cable cutting an act of piracy, which would circumvent most of the restrictions in UNCLOS, removing 'innocence' from the passage of vessels. Ordinarily piracy should be a commercial or private matter, not normally including state-on-state actions, which in any event the Russians always deny. An alternative would be to designate cable cutting as terrorism, again overcoming some of the constraints of UNCLOS. Whereas, there seems little purpose in trying to amend UNCLOS or the 1884 Convention, since it could take years or decades, and might well be blocked by Russia and its allies or they might not sign the relevant provisions. An alternative approach would be to take up the issue of protection of infrastructure in the United Nations talks on digital sovereignty.

Any measures to limit freedom of navigation could be used against European nations in other waters, notably in the Arctic Ocean and South China Sea.

One insuperable problem is convicting the master and crew of a vessel, given the need to prove beyond reasonable doubt. Without evidence of instructions to cut a cable, then a plea of ignorance, incompetence or stupidity is hard to refute. That leaves only the issue of damages, with the lower level of the balance of probabilities, which might be achieved. Even then it requires identification of the beneficial owner of the vessel, which may not be known.

There is a significant difference between electricity interconnectors and telecommunications cables, with the latter more easily duplicated and built into diverse and thus more resilient networks. Electricity interconnectors now require much greater protection and work to achieve more rapid repairs, with the present delays unnecessarily reducing resilience. The laying of more interconnectors seems unavoidable, and they would be better protected legally in territorial waters, and elsewhere by being buried, reinforced or even placed in tunnels.

Russia denies responsibility for the three incidents, which is implausible and unconvincing. In the case of the *NewNew Bear* and *Yi Peng 3* it noted that the vessels flew the flag of China, its very close ally, and whose government has not permitted its vessels to be investigated by officials of the countries affected by the breaks. The government of China shows no indication it would ever make a public admission that breaks were other than accidental.

The position of the Cook Islands is one of unsupportable stupidity. On the one hand it poses as a victim of climate change and rising sea level, while on the other it profits from a register with dozens of defective and dangerous oil tankers whose operations help to pay for a war of aggression. Moreover, the Cook Islands are dependent on tenuous international connections, with a single undersea cable.[23] It is extremely doubtful that the Cook Islands registrar knew or yet knows who was the beneficial owner of the *Eagle S*, having failed to perform due diligence. The hypocrisy is, to use its own terminology, "world class". The sensible response of the EU would be to ban all ships flying the debased flag of the Cook Islands from its ports and waters and to place its government under sanctions, though cutting its single undersea cable might be thought excessive.

[23] https://www.submarinecablemap.com/submarine-cable/manatua

Further research could usefully examine the issues around the cutting of undersea cables in the Sea of Japan and the South China Sea, together with the measures necessary to protect them (土屋, 2025). The impending deployment of AUVs requires further analysis. Issues of piracy and terrorism.

Acknowledgements

To the pseudonymous OSINT source @auonsson.bsky.social. For very useful discussions with Motohiro Tsuchiya of Keio University.

Vessels

Name	*Type*	*IMO*	*MMSI*	*Owner*	*Flag*
Cable Vigilance	Cable ship	9329930	228416900	Optic Marine Maintenance Ltd (France)	France
Eagle S	Oil tanker	9329760	518998865	Caravella LLC-FZ* (UAE)	Cook Islands
NewNew Polar Bear	Container Ship	9313204	477893800	Hainan Xin Xin Yang Shipping (China)	Panama
Niels Juel	Frigate	-	219105000	Royal Danish Navy	Denmark
Potsdam	Patrol vessel	9830018	211815660	Bundespolizei (Germany)	Germany
Rubymar	Bulk carrier	9138898	312168000	Golden Adventure Shipping SA (Marshall Islands)	Belize
Spasatel Karev	Salvage ship	9497531	273357360	Russian Federation	Russia
Telepaatti	Cable ship	7636341	230234000	Relacom Finland Oy	Finland
Turva	Patrol Ship	9650377	230018000	Finnish Border Guard	Finland
Vezhen	Bulk carrier	9937270	229659000	Navigation Maritime Bulgare JSC (Bulgaria)	Malta
Xin Xin Tian 2	Container ship	9359715	477150700	Hainan Yangpu, part of the Torgmol group (China)	China
Yantar	Research vessel	7524419	273546520	Russian Federation Navy	Russia
Yi Peng 3	Bulk carrier	9224984	414270000	Ningbo Yipeng Shipping (China)	China

* This firm is not considered to be the beneficial owner.

Legal cases

Corfu Channel (United Kingdom v. Albania), International Court of Justice. https://www.icj-cij.org/case/1

Passage through the Great Belt (Finland v. Denmark), International Court of Justice. https://www.icj-cij.org/case/86

The cases concerning the Spanish American war were reported by Fromageot (1924a & 1924b).

References

土屋, 大. (2025). 海底の覇権争奪: 知られざる海底ケーブルの地政学 *(The Battle for Undersea Dominance: The hidden geopolitics of undersea)*. 日経BPマーケティング.

AIS. (2024, December 21). *Automatic Identification System*. Marine Traffic. Retrieved December 21, 2024, from https://www.marinetraffic.com/en/ais/home/centerx:10.3/centery:56.3/zoom:7

Al Dawsari, N., Coombs, C., Jalal, I., Pollack, K. M., Shiban, B., & Zimmerman, K. (2024). *Ending the Houthi threat to Red Sea shipping*. American Enterprise Institute. https://www.jstor.org/stable/resrep58032

Al Dosari, A., & George, M. (2019). Yemen War: an overview of the armed conflict and role of belligerents. *Journal of Politics and Law*, *13*(1), 53-65. 10.5539/jpl.v13n1p53

Astier, H., & Kirby, P. (2024, November 18). *Germany suspects sabotage over severed undersea cables in Baltic*. BBC. Retrieved December 31, 2024, from https://www.bbc.co.uk/news/articles/c9dl4vxw501o

Austin, L. J. (2023, December 18). *Statement from Secretary of Defense Lloyd J. Austin III on Ensuring Freedom of Navigation*. Department of Defense. Retrieved May 15, 2025, from https://www.defense.gov/News/Releases/Release/Article/3621110/statement-from-secretary-of-defense-lloyd-j-austin-iii-on-ensuring-freedom-of-n/

Azaria, D. (2025, March 17). *Expert report: Security of submarine cables and pipelines under public international law: use of force and the law of the sea*. University College London. Retrieved May 1, 2025, from https://discovery.ucl.ac.uk/id/eprint/10207074/1/Expert%20Report_Presentation_Azaria_CAHDI_17.3.2025.pdf

BBC. (2024, November 28). *Lithuania, Finland, Sweden to jointly probe undersea cable damage.* BBC Monitoring International Reports.

Bockmann, M. W. (2024a, July 11). Tanker vetting report reveals dark fleet safety concerns. *Lloyd's List*. https://www.lloydslist.com/LL1149872/Tanker-vetting-report-reveals-dark-fleet-safety-concerns

Bockmann, M. W. (2024b, July 25). Cook Islands flags more tanker tonnage than registries 30 times larger as it embraces 'dark fleet' niche. *Lloyd's List*.

https://www.lloydslist.com/LL1150022/Cook-Islands-flags-more-tanker-tonnage-than-registries-30-times-larger-as-it-embraces-dark-fleet-niche

Bockmann, M. W. (2024c, December 27). *Russia-linked cable-cutting tanker seized by Finland 'was loaded with spying equipment'*. Lloyd's List. Retrieved December 27, 2024, from https://www.lloydslist.com/LL1151955/Russia-linked-cable-cutting-tanker-seized-by-Finland-was-loaded-with-spying-equipment

Britz, C. (2024, November 22). *Le Cable Vigilance a quitté Calais pour réparer un des câbles endommagés en Baltique*. Mer et Marine. Retrieved May 1, 2025, from https://www.meretmarine.com/fr/marine-marchande/le-cable-vigilance-a-quitte-calais-pour-reparer-un-des-cables-endommages-en-baltique

Bryant, M., & Sauer, P. (2024, November 20). Swedish police focus on Chinese ship after suspected undersea cable sabotage - Investigators gather evidence at two Baltic sites while Danish navy is shadowing Chinese cargo ship. *The Guardian*. https://www.theguardian.com/world/2024/nov/20/sweden-denmark-undersea-cable-sabotage-navy-investigation

Carboni, A. (2025). The Houthi movement and the management of instability in wartime Yemen. *Civil wars*, *in print*, 1-25. 10.1080/13698249.2024.2347144

CBSS. (2025). *CBSS*. Council of the Baltic Sea States – Building Collaboration and Trust. Retrieved May 1, 2025, from https://cbss.org/

Cinia. (2024, November 29). *Cinia's C-Lion1 submarine cable has [been] fully restored*. Cinia Oy. Retrieved December 22, 2024, from https://www.cinia.fi/en/news/cinias-c-lion1-submarine-cable-has-fully-restored

CITIC Telecom CPC. (2024, December 25). *Your trusted ICT solution partner*. CITIC Telecom CPC. Retrieved December 25, 2024, from https://www.citictel-cpc.com/en-eu/product-services/baltic-sea-cable

Clark, M. (2020). *Russian hybrid warfare*. Institute for the Study of War. https://www.understandingwar.org/report/russian-hybrid-warfare

Commons Library. (2025). *UK and international response to Houthis in the Red Sea 2024/25. CBP 9930*. House of Commons. https://commonslibrary.parliament.uk/research-briefings/cbp-9930/

Consilium. (2024, October 24). *Council conclusions on the Revised EU Maritime Security Strategy (EUMSS) and its Action Plan*. Council of the European Union. Retrieved December 15, 2024, from https://www.consilium.europa.eu/media/67499/st14280-en23.pdf

Council of the EU. (2023, January 20). Council Recommendation of 8 December 2022 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure. 2023/C 20/01. *Official Journal of the European Union*, *C 20*, 1-11. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023H0120(01)

Dept of State. (2024, September 26). *Joint statement on the security and resilience of undersea cables in a globally digitalized world*. US Department of State. Retrieved December 25, 2025, from https://www.state.gov/joint-statement-on-the-security-and-resilience-of-undersea-cables-in-a-globally-digitalized-world/

DHS. (2024). *Priorities for DHS engagement on subsea cable security and resilience*. Department of Homeland Security.

https://www.dhs.gov/publication/priorities-dhs-engagement-subsea-cable-security-resilience

EC. (2024a, March 8). Commission Recommendation (EU) 2024/779 of 26 February 2024 on secure and resilient submarine cable infrastructures. C/2024/1181. *Official Journal of the European Union*, *L 779*, 1-13. http://data.europa.eu/eli/reco/2024/779/oj

EC. (2024b, December 26). *Joint statement by the European Commission and the High Representative on the investigation into damaged electricity and data cables in the Baltic Sea*. European Commission. Retrieved December 26, 2024, from https://ec.europa.eu/commission/presscorner/detail/en/statement_24_6582

EC & High Representative. (2025). *EU Action Plan on Cable Security. JOIN(2025) 9 final*. European Commission. https://digital-strategy.ec.europa.eu/en/library/joint-communication-strengthen-security-and-resilience-submarine-cables

EEAS. (2025). *EUNAVFOR Operation Aspides*. European External Action Service. Retrieved May 15, 2025, from https://www.eeas.europa.eu/eunavfor-aspides_en

Energy-Charts. (2024, December 26). *Cross border physical flows of Estonia in week 52 2024*. Energy-Charts. Retrieved December 26, 2024, from https://energy-charts.info/charts/power/chart.htm?l=en&c=EE&legendItems=0wcw4&source=cbpf_saldo&stacking=stacked_absolute&timeslider=0&min=38&max=79&year=2024

ERR. (2024b, December 26). *Eesti ja Soome vahelisi sidekaableid tabas rike, kuid sideteenused toimivad*. Eesti Rahvusringhääling. Retrieved December 26, 2024, from https://www.err.ee/1609560709/eesti-ja-soome-vahelisi-sidekaableid-tabas-rike-kuid-sideteenused-toimivad

EU. (2022, March 9). *Informal meeting of Telecommunications Ministers - March 2022*. Consilium. Retrieved May 1, 2025, from https://newsroom.consilium.europa.eu/events/20220309-informal-meeting-of-telecommunications-ministers-march-2022

Fingrid. (2025, June 18). *EstLink 2 electricity transmission link returns to commercial use*. Fingrid. Retrieved June 21, 2025, from https://www.fingrid.fi/en/news/news/2025/estlink-2-electricity-transmission-link-returns-to-commercial-use/

Fromageot, H. (1924b). American and British Claims Arbitration Tribunal: Case of the Cuba Submarine Telegraph Company, Limited (Claim No. 27). *he American Journal of International Law*, *18*(4), 842-844. 10.2307/2188863

Fromageot, H. (1924a). American and British Claims Arbitration Tribunal: Eastern Extension, Australasia and China Telegraph Company, Limited (Claim No. 36). *The American Journal of International Law*, *18*(4), 835-842. 10.2307/2188862

Gambrell, J. (2024, March 4). *3 Red Sea data cables cut as Houthis launch more attacks in the vital waterway*. AP News. Retrieved December 25, 2024, from https://apnews.com/article/red-sea-undersea-cables-yemen-houthi-rebels-attacks-b53051f61a41bd6b357860bbf0b0860a

Government of Sweden. (2024, November 29). *Nordic-Baltic Summit and new partnership with Poland*. Government.se. Retrieved May 15, 2025, from https://www.government.se/articles/2024/11/nordic-baltic-summit-and-new-partnership-with-poland/

Hansard. (1898, April 26). War and the cutting of cables. *Hansard - House of Commons*, *56*, 1213. https://api.parliament.uk/historic-hansard/commons/1898/apr/26/war-and-the-cutting-of-cables

Hansard. (1901, April 18). Cutting of submarine cables in time of war. *Hansard - House of Commons*, *92*, 604-605. https://api.parliament.uk/historic-hansard/commons/1901/apr/18/cutting-of-submarine-cables-in-time-of

Healey, J. (2025, January 22). Russian maritime activity and UK response. *Hansard - Commons*, *760*, 1016-1030. https://hansard.parliament.uk/Commons/2025-01-22/debates/7DB30945-1C23-48E1-A629-B113C53CD9E2/RussianMaritimeActivityAndUKResponse

HELCOM. (2025). *About us – HELCOM*. Helsinki Commission. Retrieved June 1, 2025, from https://helcom.fi/about-us/

Hernández-Benito, D. (2024). Damages to submarine cables and pipelines in times of peace and war: the Nord Stream sabotage. *Amsterdam Law Forum*, *16*(1), 1-18. https://amsterdamlawforum.org/articles/487/files/66a0a2b3c65d0.pdf

HGC. (2024, March 4). *Statement - Supplementary information of HGC Global Communications regarding submarine cable damage in the Red Sea to demonstrate Hong Kong as international telecommunication hub*. HGC Global Communications Limited. Retrieved December 15, 2024, from https://www.hgc.com.hk/press-releases/statement-supplementary-information-of-hgc-global-communications-regarding-submarine-cable-damage-in-the-red-sea-to-demonstrate-hong-kong-as-international-telecommunication-hub-to-demonstrate-hong-kong-as-international

Hujanen, M., & Lehto, M. (2023, October 24). *KRP: "Vierasesine" on ankkuri, josta puuttuu yksi piikki – kiinalaisalus vaikuttanut vastahankaiselta puhutteluun*. Ilta-Sanomat. Retrieved December 31, 2024, from https://www.is.fi/kotimaa/art-2000009944331.html

ICPC. (2024). *About the ICPC*. International Cable Protection Committee. Retrieved December 25, 2024, from https://www.iscpc.org/about-the-icpc/

ILA. (2024). *Submarine cables and pipelines under international law interim report*. International Law Association (ILA). https://www.ila-hq.org/en/documents/ilathi-1

ITU. (2024). *Submarine cable resilience*. International Telecommunication Union. Retrieved December 22, 2024, from https://www.itu.int/en/digital-resilience/submarine-cables/Pages/default.aspx

ITU. (2025). *International Submarine Cable Resilience Summit 2025*. International Telecommunication Union. Retrieved February 20, 2025, from https://www.itu.int/digital-resilience/submarine-cables/events/about-nigeria-summit/

JEF. (2025, January 6). *Public statement from the Joint Expeditionary Force following the recent damage to the Estlink-2 cables*. Joint Expeditionary Force. Retrieved May 1, 2025, from

https://jefnations.org/2025/01/06/public-statement-from-the-joint-expeditionary-force-following-the-recent-damage-to-the-estlink-2-cables/

Keyani, C., & Henley, C. (2024, July 18). *The Houthis, Operation Prosperity Guardian, and asymmetric threats to global commerce*. Center for Maritime Strategy. Retrieved May 1, 2025, from https://centerformaritimestrategy.org/publications/the-houthis-operation-prosperity-guardian-and-asymmetric-threats-to-global-commerce/

Knighton, R. (2024). *What is the Joint Expeditionary Force? CBP 10074*. House of Commons Library. https://commonslibrary.parliament.uk/research-briefings/cbp-10074/

Kuhn, T. S. (1962). *The structure of scientific revolutions*. University of Chicago Press.

Lietuvos kariuomenė. (2025, January 13). *Contract on undersea infrastructure security signed, an important step coincides with Lithuania's Freedom Defenders Day*. Lithuanian Armed Forces. Retrieved May 1, 2025, from https://kariuomene.lt/en/contract-on-undersea-infrastructure-security-signed-an-important-step-coincides-with-lithuanias-freedom-defenders-day/26301

Lloyd's List. (2022, November 22). Has Denmark challenged the right of innocent passage? Watch Yi Peng 3 to find out. *Lloyd's List*. https://www.lloydslist.com/LL1151566/Has-Denmark-challenged-the-right-of-innocent-passage-Watch-Yi-Peng-3-to-find-out

MARCOM. (2024). *Allied Maritime Command*. North Atlantic Treaty Organization. Retrieved December 31, 2024, from https://mc.nato.int/

MFAI. (2024, December 6). *Cook Islands delivers powerful message at the International Court of Justice*. Cook Islands: Ministry of Foreign Affairs and Immigration. Retrieved December 26, 2024, from https://mfai.gov.ck/news-updates/cook-islands-delivers-powerful-message-international-court-justice

Miljan, T. (1974). The Baltic Sea: mare clausum or mare liberum? *Cooperation and Conflict*, *9*(1), 19-28. 10.1177/001083677400900103

Milne, R. (2024, December 22). Sweden criticises China for refusing full access to vessel suspected of Baltic Sea cable sabotage. *Financial Times*. https://www.ft.com/content/9094dcc4-b0f8-4191-b6f6-d1196a5f2822

Milne, R. (2025a, January 14). Nato to build up defence against Baltic Sea sabotage. *Financial Times*. https://www.ft.com/content/3447d821-ea41-4c85-b403-e7cc7cc49b4c

Milne, R. (2025, January 26). Baltic Sea data cable damaged in latest case of potential sabotage. *Financial Times*. https://www.ft.com/content/b8765ad0-3e72-41b8-9915-da86b25de033

Milne, R., & Telling, O. (2024, November 19). Chinese vessel spotted where Baltic Sea cables were severed - Swedish investigators looking into movements of bulk carrier travelling from Russia to Egypt. *Financial Times*. https://www.ft.com/content/383516a5-02db-46cf-8caa-a7b26a0a1bb2

MoD. (2025, January 6). *Joint Expeditionary Force activates UK-led reaction system to track threats to undersea infrastructure and monitor Russian shadow fleet*. UK Government. Retrieved May 1, 2025, 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

Murday, H. (2025, January 9). *Finnish authorities search for revelations in anchor*. DCN. Retrieved May 1, 2025, from https://www.thedcn.com.au/news/finnish-authorities-search-for-revelations-in-anchor

NATO. (2023, July 11). *Vilnius Summit Communiqué*. North Atlantic Treaty Organization. Retrieved December 15, 2024, from https://www.nato.int/cps/ge/natohq/official_texts_217320.htm

NATO. (2024, May 28). *NATO officially launches new Maritime Centre for Security of Critical Undersea Infrastructure*. North Atlantic Treaty Organization. Retrieved December 31, 2024, from https://mc.nato.int/media-centre/news/2024/nato-officially-launches-new-nmcscui

Navy Dept. (1900). *United States War Code of 1900*. US Department of the Navy. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2653&context=ils

NIS Cooperation Group. (2024). *Cybersecurity and resiliency of Europe's communications infrastructures and networks*. European Commission. https://digital-strategy.ec.europa.eu/en/library/report-cybersecurity-and-resiliency-eu-communications-infrastructures-and-networks

Notteboom, T., Haralambides, H., & Cullinane, K. (2024). The Red Sea Crisis: ramifications for vessel operations, shipping networks, and maritime supply chains. *Maritime Economics & Logistics*, *26*(1), 1-20. 10.1057/s41278-024-00287-z

Oral, N. (2019). Navigating the oceans. *Ecology Law Quarterly*, *46*(1), 163-190. 10.15779/Z38BN9X35J

Oude Elferink, A. G. (2000). The regime of passage through the Danish Straits. *The International Journal of Marine and Coastal Law*, *15*(4), 555-566. 10.1163/157180800X00244

Pancevski, B., & Michaels, D. (2025, March 8). NATO hunts for sea-cable saboteurs but can't find proof; Prosecutions have been elusive since the military alliance began responding forcefully to suspected sabotage in the Baltic Sea. *The Wall Street Journal*. https://www.wsj.com/world/europe/nato-baltic-sea-suspected-sabotage-response-a4190a75

Person, R., Kulalic, I., & Mayle, J. (2024). Back to the future: the persistent problems of hybrid war. *International Affairs*, *100*(4), 1749-1761. 10.1093/ia/iiae131

Pfluger, A. (2024, October 1). *Pfluger introduces bill to combat threats to undersea cables*. US House of Representatives. Retrieved October 25, 2024, from https://pfluger.house.gov/news/documentsingle.aspx?DocumentID=2170

Pichon, X. L., Francheteau, J., & Bonnin, J. (2013). *Plate tectonics*. Elsevier.

Polisen. (2024, December 19). *Observer role for Police on Chinese vessel*. Polisen. Retrieved December 19, 2024, from https://polisen.se/aktuellt/nyheter/nationell/2024/december/observer-role-for-police-on-chinese-vessel/

Rachman, G. (2025, January 22). Transcript: Finland's president on Europe in a Trumpian world. *Financial Times*. https://www.ft.com/content/ae4987e4-3a58-4269-90f0-e98115a7bd0c

Rajavartiolaitos. (2023, October 31). Gasgrid: Damaged Balticconnector pipeline may be operational by April. *Yle*. https://yle.fi/a/74-20057930

Rossiter, A. (2025). Cable risk and resilience in the age of uncrewed undersea vehicles (UUVs). *Marine Policy*, *171*(106434), 1-6. 10.1016/j.marpol.2024.106434

Sajari, P. (2024, December 26). *HS:n tiedot: Aseistautuneet valmiusjoukot lähetettiin keskellä yötä Eagle S -alukselle, kun syyttäjä pohti vielä terrorismia*. Helsingin Sanomat. Retrieved December 26, 2024, from https://www.hs.fi/suomi/art-2000010927044.html

Sajari, P., Niemi, L., Aholainen, S., & Tuohinen, P. (2024, December 26). *Naton pääsihteeri kaapelirikosta: Olemme valmiita antamaan lisätukea – Viron pääministeri kehui Suomea "aivan uudenlaisesta reagoinnista"*. Helsingin Sanomat. Retrieved December 26, 2024, from https://www.hs.fi/talous/art-2000010926651.html

SCMP. (2024, August 12). Beijing admits Chinese ship destroyed key Baltic gas pipeline 'by accident'. *South China Morning Post*. https://www.scmp.com/news/china/diplomacy/article/3274120/china-admits-hong-hong-flagged-ship-destroyed-key-baltic-gas-pipeline-accident

7e Commission d'étude. (1879). Protection en temps de paix et en temps de guerre des câbles télégraphiques sous-marins qui ont une importance internationale. *Annuaire de l'Institut de droit international*, *3*(1), 351-394.

Shen, Y., Hu, X.-L., Wang, T.-D., Zhu, W., Guo, Q.-S., Yang, S., Lu, Q.-S., Zhang, D.-Z., & Xiao, W.-G. (2023). Analysis of Nord Stream explosions using seismic recordings. *Applied Geophysics*, *20*(3), 316-323. 10.1007/s11770-023-1070-7

Shepherd, B. (2020). Cutting submarine cables: the legality of the use of force in self-defense. *Duke Journal of Comparative & International Law*, *31*(1), 199-220. https://scholarship.law.duke.edu/djcil/vol31/iss1/4/

SHK. (2024, December 19). *Pressmeddelande - Undersökningar på det kinesiska fartyget Yi Peng 3*. Statens haverikommission. Retrieved May 1, 2025, from https://shk.se/aktuellt/nyhetsarkiv/2024-12-19-pressmeddelande

SHK. (2025). *SHK:s observationer ombord på det kinesiska lastfartyget YI PENG 3*. Statens haverikommission. https://shk.se/download/18.ffd11bf19626c638f3623/1744702687838/YP3-PM%202025-04-15%20-%20slutlig.docx.pdf

Skopljak, N. (2025, April 17). *Nexans to start repairing damaged Finland-Estonia subsea link next month*. Offshore-Energy.biz. Retrieved June 1, 2025, from https://www.offshore-energy.biz/nexans-to-start-repairing-damaged-finland-estonia-subsea-link-next-month/

Subcommittee on Communications and Technology. (2024, February 15). *Securing communications networks from foreign adversaries*. House Committee on Energy and Commerce. Retrieved January 2, 2025, from https://energycommerce.house.gov/events/communications-and-technology-subcommittee-hearing-securing-communications-networks-from-foreign-adversaries

Subcommittee on Communications, Media & Broadband. (2024, December 11). *Communications networks safety and security*. US Senate - Commerce Committee. Retrieved December 15, 2024, from

https://www.commerce.senate.gov/2024/12/communications-networks-safety-and-security

Sutherland, E. (2021). *CFIUS and Team Telecom: foreign interests and national security in telecommunications*. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2550469

SVT. (2025, June 15). Sjöfartsverket utökar varningen för GPS-störningar i Östersjön. *SVT Nyheter*. https://www.svt.se/nyheter/inrikes/sjofartsverket-utokar-varningen-for-gps-storningar-i-ostersjon

Tagesschau. (2024, November 29). Sabotage-Verdacht - Ostsee-Datenkabel repariert. *Tagesschau*. https://www.tagesschau.de/ausland/datenkabel-ostsee-102.html

Tasavallan Presidentti. (2024, November 22). *President and Ministerial Committee on Foreign and Security Policy discuss damage to telecommunications cables in Baltic Sea and Finland's participation in summit of NB8 and Polish leaders in Harpsund*. President of the Republic of Finland. Retrieved May 1, 2025, from https://www.presidentti.fi/en/president-and-ministerial-committee-on-foreign-and-security-policy-discuss-damage-to-telecommunications-cables-in-baltic-sea-and-finlands-participation-in-summit-of-nb8-and-polish-leaders-in/

TeleGeography. (2024). *Submarine Cable Map*. TeleGeography - Submarine Cable Map. Retrieved December 29, 2024, from https://www.submarinecablemap.com/

Tolba, A. (2024, March 2). *Yemen's Houthis blame UK and US for 'glitch' in Red Sea undersea cables*. Reuters. Retrieved December 25, 2023, from https://www.reuters.com/world/middle-east/yemens-houthis-blame-uk-us-glitch-red-sea-undersea-cables-2024-03-02/

Traficom. (2024, December 26). *Traficom mukana selvittämässä Suomenlahden kaapelivaurioita*. Traficom. Retrieved December 27, 2024, from https://www.traficom.fi/fi/ajankohtaista/traficom-mukana-selvittamassa-suomenlahden-kaapelivaurioita

Typpö, J. (2024, December 26). *Pääministeri Orpo: Varjolaivaston pysäyttämiseen tarvitaan lisää keinoja*. Helsingin Sanomat. Retrieved December 26, 2024, from https://www.hs.fi/suomi/art-2000010926873.html

UNSC. (2024, June 27). *Adopting Resolution 2739 (2024) on Yemen, Security Council demands Houthis immediately cease all attacks against merchant, commercial vessels*. United Nations Security Council. Retrieved May 1, 2025, from https://press.un.org/en/2024/sc15750.doc.htm

UNSC. (2025, January 15). *https://press.un.org/en/2025/sc15965.doc.htm*. United Nations Security Council. Retrieved May 1, 2025, from https://press.un.org/en/2025/sc15965.doc.htm

Valitsuse Uudised. (2024, December 26). *Press conference, December 26, 2024*. YouTube. Retrieved December 26, 2026, from https://www.youtube.com/watch?v=qLV4iyLe11Y

Vessel Finder. (2024, December 26). *EAGLES, Crude Oil Tanker - Details and current position - IMO 9329760*. Vessel Finder. Retrieved December 26, 2024, from https://www.vesselfinder.com/vessels/details/9329760

Wong, B. (2025, May 8). Ship captain remanded in custody in Hong Kong over damaging Baltic Sea pipeline. *South China Morning Post*.

https://www.scmp.com/news/hong-kong/law-and-crime/article/3309618/ship-captain-remanded-custody-hong-kong-over-damaging-baltic-sea-pipeline

Yle. (2023, November 6). *Venäläinen tietoliikennekaapeli rikki Suomenlahdella | Kotimaa*. Yle. Retrieved May 1, 2025, from https://yle.fi/a/74-20058825