

HENRY M. JACKSON SCHOOL OF INTERNATIONAL STUDIES



UNIVERSITY *of* WASHINGTON



Hidden Highways of the Internet: Global Subsea Cable Security

Task Force

The Donald C. Hellmann
Task Force Program

2025

This report is a product of the Henry M. Jackson School of International Studies' Donald C. Hellmann Task Force Program. For more information about the Donald C. Hellmann Task Force Program, please visit: <https://jsis.washington.edu/task-force/>

Cover image credit: Safaa Turner-Rahman, 2025.

*Henry M. Jackson School of International Studies
University of Washington, Seattle
Task Force Report Winter 2025*

Hidden Highways of the Internet: *Global Subsea Cable Security*

Faculty Advisor

Dr. Jessica L. Beyer

Evaluator

Major General Duke A. Pirak
Acting Director,
Air National Guard,
The Pentagon

Editors

Fern Hinrix
Georgia C. Brown
Max S. Zuber

Project Manager

Vaishnavi Pankaj

Researchers

Chloe Yi
Jaiden Shoel
Joaquin Ulloa
Marisa Wickline
Paige R. Foster
Ryan Gunnarson
Safaa Turner-Rahman
Sara Yohanes
Selena Nguyen
Sophie Himka
Zhiting Xiao

TABLE OF CONTENTS

EXECUTIVE SUMMARY	1
POLICY RECOMMENDATIONS	2
CREATE A DEPARTMENT OF HOMELAND SECURITY CRITICAL INFRASTRUCTURE SUB-SECTOR FOR SUBSEA CABLES UNDER THE COMMUNICATIONS SECTOR	3
ESTABLISH A COMPREHENSIVE AND COORDINATED STRATEGY TO INCREASE U.S. INVESTMENT IN SUBSEA CABLE PROJECTS	4
LEVERAGE EXISTING PARTNERSHIPS AND FRAMEWORKS WITH U.S. PARTNERS AND ALLIES IN KEY GEOGRAPHIC REGIONS	5
MONITOR RUSSIA’S NAVAL ACTIVITY, SPECIFICALLY THE INTELLIGENCE VESSEL <i>YANTAR</i>	6
RATIFY THE UNITED NATIONS CONVENTION ON THE LAW OF THE SEA	7
INTRODUCE AND ENFORCE MORE STRINGENT REGULATIONS AND REQUIREMENTS FOR VESSEL FLAGGING THROUGH THE UNITED NATIONS CONVENTION ON THE LAW OF THE SEA	8
EXPAND THE UNITED NATIONS CONVENTION ON THE LAW OF THE SEA TO INCLUDE THE RIGHT TO VISIT IN THE EXCLUSIVE ECONOMIC ZONE	9
TECHNICAL ANALYSIS OF SUBSEA CABLE INFRASTRUCTURE	11
MAJOR ATTACKS ON SUBSEA CABLE INFRASTRUCTURE	13
ATTRIBUTION OF SUBSEA CABLE ATTACKS	25
MAJOR PERPETRATORS OF SUBSEA CABLE ATTACKS	25
FLAG OF CONVENIENCE SHIPS AND SUBSEA CABLE INCIDENTS	27
RUSSIA’S ROLE IN SUBSEA CABLE INCIDENTS	28
CHINA’S ROLE IN SUBSEA CABLE INCIDENTS	29
LOCATIONS OF MAJOR SUBSEA CABLE INCIDENTS	30
IMPACT OF SUBSEA CABLE DISRUPTION	31
RESPONSES TO SUBSEA CABLE DISRUPTIONS	32
RISKS AND THREATS TO GLOBAL SUBSEA CABLE INFRASTRUCTURE	34
ACCIDENTAL AND ENVIRONMENTAL RISKS	34
STRATEGIC AND GEOGRAPHIC VULNERABILITIES	36
DELIBERATE SABOTAGE AND STATE-SPONSORED THREATS	37
ESPIONAGE AND CYBERSECURITY THREATS	38
IMPLICATIONS	40
INTERNATIONAL AGREEMENTS AND FORUMS	42
INTERNATIONAL AGREEMENTS	42
INTERNATIONAL FORUMS	46
KEY CASE STUDIES: BALTIC SEA, SOUTH CHINA SEA, RED SEA	49
BALTIC SEA	49
SOUTH CHINA SEA	56
RED SEA	62
KEY STATE ACTORS: U.S., CHINA, AND RUSSIA	70
UNITED STATES OF AMERICA	70
PEOPLE’S REPUBLIC OF CHINA	75
RUSSIAN FEDERATION	79
THE PRIVATE SECTOR AND SUBSEA CABLE INFRASTRUCTURE	84

THE “BIG FOUR”	84
NEW OWNERSHIP	85
MAINTENANCE AND REPAIR	86
PUBLIC-PRIVATE PARTNERSHIPS	87
ADVANCEMENTS IN CABLE TECHNOLOGY	88
IMPLICATIONS	89
REFERENCES	90

Executive Summary

Subsea cables are the backbone of global communications infrastructure, carrying approximately 99% of intercontinental data traffic and enabling trillions of dollars in daily financial transactions (Mauldin, 2023). These fiber-optic networks span 1.39 million kilometers of the ocean floor, transmitting private communications, commercial data, and government intelligence (KV Cable, 2023). Despite their importance, they remain vulnerable—they are often no thicker than a garden hose, exposed on the seabed, and concentrated at choke points in global shipping routes.

The object of this report is to provide a comprehensive examination of the current landscape of global subsea internet cable infrastructure security. To do this, we conducted a comprehensive analysis of 22 suspicious subsea cable break incidents from 2005 to 2025, highlighting key trends and patterns. We identified four key risks and threats to subsea cables: (1) accidental and environmental risks, (2) vulnerable choke points (3) deliberate sabotage by state actors, and (4) espionage and other cybersecurity threats. Additionally, we reviewed major relevant international agreements governing this infrastructure, and found that the Paris Convention of 1884, the Geneva Conventions of 1958, the United Nations Convention on the Law of the Sea are all key agreements which define the current landscape of subsea cable protection. We identified gaps that exist in those agreements and opportunities to strengthen them further. We analyzed three regional case studies: the Baltic Sea, the South China Sea, and the Red Sea, and found that conflict over internet infrastructure largely reflects the greater geopolitical conflicts in each region as well as competition between the U.S., China, and Russia. We then researched each of these three countries and found that while the U.S. and China view subsea cables as a matter of national security and engage in competition over control of this infrastructure, Russia is more concerned with developing offensive capabilities to engage in attacks on it. Finally, we explored the private companies that own, manufacture, and maintain the majority of the world's cables, and the central role that the private sector plays in this rapidly changing industry.

Given the research done and the conclusions made throughout this report, we make the following seven policy recommendations to the Federal Government of the United States.

1. Create a Department of Homeland Security critical infrastructure sub-sector for subsea cables under the Communications Sector.
2. Establish a comprehensive and coordinated strategy to increase U.S. investment in subsea cable projects.
3. Leverage existing partnerships and frameworks with U.S. partners and allies in key geographic regions.
4. Monitor Russia's naval activity, specifically the intelligence vessel *Yantar*.
5. Ratify the United Nations Convention on the Law of the Sea.
6. Introduce and enforce more stringent regulations and requirements for vessel flagging through the United Nations Convention on the Law of the Sea.
7. Expand the United Nations Convention on the Law of the Sea to include the right to visit in the exclusive economic zone.

Policy Recommendations

The global subsea cable infrastructure is vulnerable to attacks, accidents, and, to a lesser extent, espionage. This essential infrastructure has a long history of accidental cable breaks, but in the past 17 years there has been a rise in deliberate nation-state attacks on subsea cables. Complicating the picture, many of these attacks are made to look like accidents. Because this infrastructure is now so central to human wellbeing, the steady increase in targeting and damage to it is a pressing policy issue for every country in the world—and particularly the U.S., whose companies have traditionally dominated the subsea cable market.

There are several key factors causing this problem. First, there is insufficient collaboration between public and private stakeholders within the U.S. Second, geopolitical competition between the U.S. and China and the U.S. and Russia impacts subsea cable security. Third, it is difficult to accurately and confidently attribute attacks on subsea cables, allowing attacks to occur with few consequences. Finally, international agreements relating to this infrastructure need greater specification and there is a lack of enforcement mechanisms for agreements that do exist to protect this vital infrastructure.

We make our recommendations with the following underlying understanding: we cannot eliminate the geopolitical and market competition between the U.S. and China and the U.S. and Russia. Operating within this framework, our recommendations are not aimed at reducing this competition, but rather at advancing the U.S.'s interests, which we have identified as follows: (1) protect global subsea cables and infrastructure, (2) expand U.S. advantages in the competition for market dominance of global internet infrastructure, (3) project U.S. power and influence globally, and (4) do all this while not escalating tensions and risking war with China or Russia.

With all these considerations in mind, we make the following seven policy recommendations to the Federal Government of The United States:

1. Create a Department of Homeland Security critical infrastructure sub-sector for subsea cables under the Communications Sector.
2. Establish a comprehensive and coordinated strategy to increase U.S. investment in subsea cable projects.
3. Leverage existing partnerships and frameworks with U.S. partners and allies in key geographic regions.
4. Monitor Russia's naval activity, specifically the intelligence vessel *Yantar*.
5. Ratify the United Nations Convention on the Law of the Sea.
6. Introduce and enforce more stringent regulations and requirements for vessel flagging through the United Nations Convention on the Law of the Sea.
7. Expand the United Nations Convention on the Law of the Sea to include the right to visit in the exclusive economic zone.

Recommendation 1: Create a Department of Homeland Security critical infrastructure sub-sector for subsea cables under the Communications Sector

There is no existing forum to facilitate interaction between the domestic subsea cable industry and the U.S. government to identify and address challenges facing this infrastructure. While the Federal Communications Commission (FCC) has the Assessment of Foreign Participation in the U.S. Telecommunications Services Sector oversight body, or Team Telecom, its purpose is only to review applications and licenses for subsea cables that touch a U.S. territory and evaluate the security risks, rather than facilitate cross-sector coordination (Department of Justice, 2023). The lack of such a forum has made collaboration between the public and private sectors regarding subsea cable infrastructure difficult. To capture the entirety of the subsea cable network, we propose that the U.S. government designate a sub-sector: subsea internet cables and associated infrastructure, which should fall under the Communications Sector. The Communications Sector is responsible for the physical transmission systems of communication and recognizes the private sector as the primary entity that owns and operates communications infrastructure (DHS, 2015). The subsea cable infrastructure fits nicely into this, allowing collaboration between the public and private sectors to address the totality of the subsea cable industry.

The Critical Infrastructure Partnership Advisory Council (CIPAC) exists within the Cyber and Infrastructure Security Agency (CISA)—created to facilitate interaction between government and private entities that are involved in the same type of critical infrastructure (*Critical Infrastructure Security and Resilience*, n.d.). However, because the subsea cable network fits between two Department of Homeland Security (DHS) critical infrastructure sectors—the Communications and Information Technology Sectors—there is no set mechanism for the U.S. government to address subsea cables as critical infrastructure. Existing U.S. government mechanisms for engaging critical infrastructure owners and operators include Sector Coordinating Councils (SCC) and Government Coordinating Councils (GCC).

In December of 2024, the DHS released a white paper on the engagement of subsea cable security and resilience (Department of Homeland Security [DHS], 2024). The paper underscores the importance of public-private coordination of the subsea cable critical infrastructure that addresses international security and communications (DHS, 2024), while also recognizing that under the current framework, the DHS is limited in what it can accomplish in terms of cooperation. It recommends leveraging existing critical infrastructure collaborative bodies, particularly Government Coordinating Councils and Sector Coordinating Councils, and exploring new ways to address the industry. But the paper fails to go into further detail, and the recommendations made do not address the core issue—subsea cable infrastructure does not fit cleanly into any of the existing mechanisms.

In April of 2024, the federal government released the National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22). NSM-22 is an updated framework

outlining the roles and responsibilities of federal agencies within the national critical infrastructure risk management landscape (Humphreys, 2024). It offers comprehensive guidance for federal agencies to engage in public-private partnerships but, unfortunately, is relatively restrained in its scope. The memorandum does not introduce any new sectors or sub-sectors to the 16 existing critical infrastructure sectors, meaning that subsea cable infrastructure is still left without its own designated sector or sub-sector within the DHS.

We recommend that the U.S. designate a sub-sector: subsea internet cables and the associated infrastructure. This designation would allow the federal government to collaborate with the private sector more closely and engage in public-private partnerships under the framework of documents like NSM-22. Such a move would simplify the way that the federal government approaches collaboration with the private sector on subsea cables by fitting it into a pre-existing framework that the public sector is already comfortable with through its collaboration in other critical infrastructure sectors.

Recommendation 2: Establish a comprehensive and coordinated strategy to increase U.S. investment in subsea cable projects

China's increasing market share in the subsea cable industry because of Belt and Road Initiative's Digital Silk Road project poses a threat to the security of U.S. communications and data. As a response, the U.S. has used diplomatic leverage and market incentives to block Chinese companies from subsea cable projects. Additionally, the U.S.—in partnership with allies including Japan and Australia—is investing in cable projects in areas such as the Pacific Islands using U.S. suppliers (The White House, 2023). However, the piecemeal nature of the U.S.'s approach to investment in subsea cable projects hinders its efforts to counter the expansion of Chinese firms and secure cable infrastructure with trusted providers. We propose that the U.S. establish a comprehensive and coordinated strategy to invest in cable infrastructure in key geopolitical areas.

Other countries and regional organizations have taken a more comprehensive and robust approach to investment in cable projects. The EU has invested heavily in cables through the Global Gateway Strategy, which so far has mobilized 962 million Euros for investment in backbone connectivity projects including subsea cables (European Commission, 2024). The Global Gateway Strategy has been presented as an attractive alternative for infrastructure development in the Global South to China's Belt and Road Initiative (Tagliapietra, 2024). Australia's Department of Foreign Affairs and Trade has also announced a new Australian Infrastructure Financing Facility for the Pacific, which will support three cable projects connecting Pacific Island nations (Channer, 2024). These strategies from U.S. partners and allies offer examples of concrete and coordinated approaches to strategically funding cable infrastructure.

The U.S. lacks a similarly comprehensive strategy for financing and investing in subsea cable projects. In 2019, the U.S., Japan, and Australia announced the Blue Dot Network (BDN), a multilateral infrastructure certification organization, which is designed to encourage private investment in sustainable projects (Goodman et. al., 2020). However, while the Blue Dot Network provides effective rhetorical opposition to China’s Belt and Road Initiative, it does not include any kind of lending capacity for the projects it certifies. Separately, the U.S. is providing five million dollars in funding through the CABLES program to provide technical assistance and capacity building on subsea cables but has not committed significant funding for cable development projects (Department of State, 2024).

We recommend the U.S. to create a comprehensive and systematic strategy for U.S. investment in subsea cables, leveraging the International Development Finance Corporation and U.S. Trade and Development Agency, as well as other relevant agencies. Investment should focus on key geopolitical areas where the U.S. seeks to mitigate the increasing presence of Chinese firms and expand its influence—such as in Southeast Asia and the South Pacific. The private sector should play an instrumental role in this strategy, as government investment alone will not be sufficient to support the financial requirements of large-scale cable projects. Additionally, the U.S. should continue to work in coordination with country partners such as Japan and Australia, as well as multilateral organizations such as the G7, the EU, and the Quad to co-finance secure cable projects.

Recommendation 3: Leverage existing partnerships and frameworks with U.S. partners and allies in key geographic regions

While subsea cables are a global infrastructure, certain regions are hotspots for attacks on this infrastructure—often those with high concentrations of cables. The distinct geopolitical dynamics in each region pose unique challenges to protecting subsea cables and shape the type of measures that are most effective for advancing U.S. interests. However, each region also features partnerships the U.S. can leverage to address threats to subsea cables. We propose that the U.S. leverage existing partnerships with relevant partners and allies in key geographic regions to address threats to subsea cable infrastructure.

In the Baltic Sea, North Atlantic Treaty Organization’s (NATO) Baltic Sentry operation has utilized the alliance to mitigate the threats to subsea cables. Through increased military presence and monitoring in the Baltic Sea, Baltic Sentry aims to decrease the plausible deniability of attacks and deter further attempts to damage or sever cables (SHAPE Public Affairs Office, 2025). It is important to note that while NATO’s unique military capabilities and the robust regional backing from nine out of ten of the countries bordering the Baltic Sea means something like Baltic Sentry is effective in the Baltic Sea region, it not necessarily a blueprint for collaborative measures elsewhere. However, other partnerships and initiatives can also be measures mitigating threats.

In the Indo-Pacific, the Quadrilateral Security Dialogue (the Quad) and the trilateral Australia-United Kingdom-United States security partnership (AUKUS) have also proven to be effective venues for collaboration. In 2023, the Quad announced the Quad Partnership for Cable Connectivity and Resilience, which provides technical assistance and capacity building for Indo-Pacific governments expanding subsea cable infrastructure (Quad Leaders' Summit Fact Sheet, 2023). In contrast, AUKUS, as a security partnership, offers a distinct forum for addressing threats to subsea cables using military technology. Under AUKUS Pillar II, the U.S., the U.K., and Australia are improving and testing uncrewed undersea vessels for monitoring of underwater critical infrastructure including cables (U.S. Department of Defense, 2023). These initiatives, rather than taking overly provocative measures in the South China Sea, prioritize sharing information and building monitoring capabilities—actions appropriate to advancing U.S. interests while balancing the heightened geopolitical tensions in the region.

We recommend that the U.S. leverage existing partnerships and frameworks to build collaborative measures to address threats to subsea cables in key geopolitical areas including, but not limited to, the Indo-Pacific and the Baltics. Key to this recommendation is that initiatives must be tailored to be appropriate for U.S. assets and other actors in the region in which they operate in order to best advance U.S. interests. NATO, the Quad, and AUKUS all provide strong multilateral frameworks on which to build and expand. Additional measures may include increasing monitoring, facilitating information sharing among U.S. partners and allies, and developing capacity building initiatives.

Additionally, the U.S. should continue to engage with and utilize the International Cable Protection Committee and the International Advisory Body for Submarine Cable Resilience (SCR). While not tailored to a specific region, these forums provide an opportunity to share information and capacity building measures with international partners in a forum which recognizes the global nature of this infrastructure (International Cable Protection Committee, 2025; The International Telecommunications Union, n.d.).

Recommendation 4: Monitor Russia's naval activity, specifically the intelligence vessel *Yantar*

Russia poses a major threat to the global subsea cable infrastructure, usually involving sabotage against cables in areas of key geopolitical importance to Russia. Most notably, Russia is likely behind incidents targeting subsea cables in the Baltic Sea, although these breakages have not been officially attributed to Russia. Amongst Russia's offensive tools, Russia has a vessel called the *Yantar*, which is an advanced intelligence gathering vessel equipped with two submarines that can submerge to great depths of up to 20,000 feet (Peter, 2018). The *Yantar* also has the capability to cut underwater cables (Peter, 2018). The *Yantar* has been caught on multiple occasions loitering in waters near critical subsea cables, such as off the coast of the U.S. near a submarine base in Georgia, in U.K. territorial waters, and other spots around the globe.

Russia's *Parlamentskaya Gazeta* (parliamentary newspaper) claims that the *Yantar* has the capability to tap into subsea cable traffic and spy on the information flowing through cables, along with its capacity to physically damage the infrastructure (Andreev, 2017). We propose that the U.S. government engage in active monitoring of the *Yantar* to keep tabs on its activities and prevent it from engaging in direct offensive action.

In November of 2024, the United Kingdom sent its intelligence vessel the *RFA Proteus* to monitor the whereabouts of the *Yantar*. The *Proteus* and the *Yantar* faced off in early 2025, as the U.K. vessel has been tailing the *Yantar* since 2024. This style of monitoring has allowed the U.K. to stay ahead of any potential risks the *Yantar* poses and is responsible for how quickly the U.K. was able to identify that the *Yantar* was sailing in its territorial waters in early 2025.

Although the U.S. and its NATO allies are aware of the *Yantar's* presence when it shows up in different parts of the world, we recommend that the U.S. follow the U.K.'s more direct approach. By more openly monitoring the *Yantar*, and making it known that the boat is being watched, the U.S. gains two key strategic advantages. First, it is less likely to be caught off guard if the *Yantar* moves into a sensitive part of the world, as it will already be aware of the ship's whereabouts. Second, if the *Yantar* is aware it is being monitored as closely as we recommend, it is less likely to actively engage in sabotage of critical subsea cables.

Recommendation 5: Ratify the United Nations Convention on the Law of the Sea

As subsea cable incidents continue to grow around the world, the United States remains one of the few countries that lack the internationally sanctioned authority to confront the two main perpetrators: Russia and China. To gain that authority, we propose that the United States ratify the United Nations Convention on the Law of the Sea (UNCLOS), which would expand U.S. diplomatic power to address illicit behavior surrounding subsea cables. Ratifying UNCLOS would send a strong message of support to our allies who have already ratified the convention, signaling that the U.S. is a reliable ally.

UNCLOS grants a party state legal certainties that could assist the U.S.' presence in international protected waters. For instance, UNCLOS makes a distinction between the exclusive economic zone (EEZ) and the high seas, which allows for states to retain control over resources along their coastlines (Office of the Staff Judge Advocate, 2021a). The convention also details subsea cable protections and grants jurisdiction to party states for damaged subsea cables. Regarding security, UNCLOS codifies innocent passage of vessels in coastal territorial waters and also allows immunity for warships on the high seas (Office of the Staff Judge Advocate, 2021b).

Because the U.S. has not ratified UNCLOS it has not been able to participate in negotiations related to the high seas—such as in the Permanent Court of Arbitration at the Hague when it is dealing with subsea cable issues in the South China Sea and Russia's actions in the Black and Baltic Seas (A resolution calling upon the United States Senate to give its advice

and consent to ratification of the United Nations Convention on the Law of the Sea, 2023). During the 2016 Matter of the South China Sea Arbitration, the U.S. asked to be admitted as an observer, but was rejected since it was not a signatory to UNCLOS (A resolution calling upon the United States Senate to give its advice and consent to ratification of the United Nations Convention on the Law of the Sea, 2023). The arbitration in that case concerned China’s activities in the South China Sea and the issue of the nine-dash line—China’s claim to 90% of the South China Sea (Campbell and Salidjanova, 2016). China’s unlawful claim would mean that China could implement levies on non-Chinese subsea cables and could possibly withhold internet access from surrounding countries.

The failure to ratify UNCLOS means the U.S. cannot bring any complaints, either for general violations or for expanding jurisdiction, against Russia. Russia has repeatedly mocked the U.S. for this failure and also has used the U.S.’ selective interpretation of international law as justification for their war in Ukraine. (Wahden, 2024) Russia’s history of compliance with UNCLOS has been irregular, yet it benefits from jurisdictional advantages from the convention in regard to the Arctic Shelf (Wahden, 2024). If the U.S. were to ratify the convention, it would allow for the U.S. to confront Russia’s predatory behavior in the Baltic Sea and beyond.

Ratifying UNCLOS would provide a forum for the U.S. to expand its diplomatic power in the struggle for subsea cable security against potential adversaries such as Russia and China. The U.S.’s reliability as a partner to the EU, whose countries have all ratified the convention, would increase and would also allow for the U.S. Navy and Coast Guard to operate with greater legal certainty. Above all else, UNCLOS would help provide a framework for addressing damage to subsea cables.

Recommendation 6: Introduce and enforce more stringent regulations and requirements for vessel flagging through the United Nations Convention on the Law of the Sea

One of the central issues concerning subsea cable attacks is the difficulty in attributing such attacks. The current vessel flagging regulations, established in Article 91 of UNCLOS, allow for party states to create their own conditions for granting nationality and flag rights to vessels (United Nations Convention on the Law of the Sea [UNCLOS], 1982). UNCLOS only specifies that there must be a “genuine link” between a ship and its flag, but no definition is provided for what is considered a “genuine link” (International Maritime Organization [IMO], n.d.). We believe that revising UNCLOS’s “genuine link” provision to define stringent conditions for a “genuine link” between a vessel’s owner, crew and flag state will aide in overall attribution efforts for ships engaged in illicit operations, particularly subsea cable breaks.

As seen in the Baltic Sea and Major Attacks sections of this report, there is a pattern of recent attacks on subsea cables from boats that are flagged with one country’s flag but crewed with another country’s citizens. The growing phenomenon of mismatched flagged and crewed vessels is in large part due to varying conditions surrounding flagging due to “open registry.”

Open registry is a vessel registration system which does not have nationality or residency requirements—it is this system that allows foreign owned companies to register vessels with crews and owners that are neither nationals of or domiciled in the flag state (Ford & Wilcox, 2019; Watterson et al, 2020; Windward, n.d.; IMO, n.d.). Countries such as Russia and China are believed to utilize these open registries to flag ships under nations with relaxed jurisdiction—known as flag of convenience ships (Brennan, 2025; Staff Writer with AFP, 2025). Flags of convenience are usually used for economic purposes, such as when another country has more relaxed regulations including conditions for flagging, wages, and lack of infrastructure in vessel monitoring, control, and surveillance capacity (Kuznietsov, 2021). However, flags of convenience are increasingly being used to disguise illicit activities. China is suspected to have 52 vessels utilizing open registries, while Russia’s shadow fleet has over 1,000 vessels (Windward, n.d.; Kirby, 2024; Staff Writer with AFP, 2025). Many vessels believed to be members of the Russian shadow fleet are also those believed responsible for suspicious cable accidents, particularly in the Baltic Sea (Grylls, 2025). As ships continue to register and flag their vessels under unassociated states, the capacity to get away with further illicit activities grows while the ability to definitively attribute and combat this lessens, leaving affected states unable to mitigate detrimental breaks.

For combatting differing ownership and crewing of vessels under flags of an unassociated state, we recommend that the U.S. propose a revision to UNCLOS Article 91 in relation to the “genuine link” provision. We urge the U.S. adopt language from the UN Convention on Conditions for Registration of Ships Articles 7–10, stipulating that: (1) a satisfactory share of the ship’s crew must be nationals of, domiciled in, or lawfully permanently in residence in the flag state/state of registration and (2) the ship-owning company or a subsidiary company is established in or has their main place of business in the flag state (United Nations Convention on Conditions for Registration of Ships, 1986). Where this cannot be the case, the state of registration should ensure that there is a representative or management persons that is a national of or domiciled in its territory (United Nations Convention on Conditions for Registration of Ships, 1986).

Recommendation 7: Expand the United Nations Convention on the Law of the Sea to include the right to visit in the exclusive economic zone

Within the high seas and exclusive economic zone (EEZ), it is difficult for UNCLOS party states to investigate suspicious behavior which can result in such behavior going unpunished. To address these issues, it is pertinent to amend UNCLOS to include a version of the right to visit—as outlined in the Paris Convention of 1884—to allow for cross-national investigation of suspicious activity that threatens subsea cables in the EEZ.

As it stands, UNCLOS fails to protect subsea cables within internationally protected waters. UNCLOS stipulates that a ship suspected of a crime can only be visited or boarded by a

ship of the same flag state (Guilfoyle et al, 2022). Article 113 provides ships with flag state jurisdiction on the high sea, meaning that the laws of the flag state preside over the ship as if it were an extension of its territory. The issue of jurisdiction is extended into the EEZ by Articles 58 and 87 which protects foreign ships from investigation as they are entitled to due to the freedoms granted under UNCLOS.

While most of the cable incidents occur in the economic exclusive zone, the coastal states, which have legal jurisdiction over the EEZ, cannot investigate due to UNCLOS protecting other states and their rights to resources in that zone. Article 58 grants the flag state legal immunity with regard to the freedoms established in Article 87. These two articles protect a flag state's right to resources such as subsea cables within the EEZ, which extends 200 nautical miles from the territorial sea. This means when interference to subsea cables occur, neither the coastal state nor any state other than the flag state can investigate or board the vessel that is suspected of perpetrating the incident (United Nations Convention on the Law of the Sea, 1982).

The limitation of flag state jurisdiction on the high seas and EEZ results in a lack of accountability and fidelity in these international protected spaces, including the EEZ. The November 2024 Baltic Sea incident with a Chinese vessel led to a month-long diplomatic standoff which took place between European and Chinese officials before investigators were allowed to board, preventing investigations of the incident from occurring (Ahlander et al., 2024). Out of 22 total incidents identified in this report, only 11 were either confirmed or assumed to have taken place in a country's EEZ. The significant frequency of events in EEZs emphasizes the necessity for investigational rights in the EEZ.

We propose that UNCLOS prescribes the right to visit to vessels who are serving on the behalf of the government of a party state within the EEZ. Adjusting the right of visitation by amending it into UNCLOS is the answer to the lapse in jurisdiction in the high seas and EEZ. The right of visit, as provided by Article X of the Paris Convention of 1884, permits any ship to board and investigate non-military ships on the high seas with due cause (Convention for the Protection of Submarine Telegraph Cables, 1884). The article is significant as it allows for investigation of suspicious activities on the high seas.

Technical Analysis of Subsea Cable Infrastructure

Modern global telecommunications infrastructure relies on a complex network of subsea fiber optic cables, with approximately 486 cable systems and 1,306 landing stations active or under construction worldwide in 2022 (Gallagher, 2022). These cables serve as the primary conduit for international data transmission, carrying approximately 99% of transoceanic digital communications and 95% of intercontinental internet traffic (Ruffino, 2024).

The physical architecture of these cables consists of multiple protective layers surrounding a core of optical fibers. The central fibers, made of ultra-pure silica glass no thicker than human hair, are encased in successive layers including petroleum jelly, copper or aluminum tubing for power transmission, polycarbonate housing, aluminum water barriers, steel wire reinforcement, and polyethylene outer sheathing (Swinhoe, 2021). This design ensures both data transmission capability and physical resilience in harsh oceanic environments.

Two primary system types exist in current deployments: unrepeated and repeated systems. Unrepeated systems, typically used for shorter regional connections, operate without internal power sources and rely on shore-based power facilities (Ruffino, 2024). These systems are determined primarily by geography but also provide additional route redundancy, increasing the overall resilience of the network (Ruffino, 2024). Repeated systems, essential for transoceanic routes, incorporate signal boosters approximately every 70 kilometers and require 20kV power supplies from both termination points (Gervasi, 2023). Modern cable capacity has reached unprecedented levels, with recent installations like the Dunant cable achieving 250 terabits per second through space-division multiplexing (SDM) technology that increases capacity by using additional fiber pairs and power-optimized repeater designs (Gallagher, 2022).

The terrestrial infrastructure, known as the "dry plant," consists of cable landing stations housing terminal equipment, power feed systems, and network operations centers, along with beach manholes that serve as the interface between land and sea segments (Network Encyclopedia, 2024). These facilities connect to broader terrestrial networks through points of presence (POPs) that integrate the subsea infrastructure with national telecommunications systems.

Maintenance operations utilize approximately 60 specialized cable ships stationed strategically worldwide, equipped with remotely operated vehicles and specialized repair equipment (Ruffino, 2024). The industry employs sophisticated monitoring systems including automated fault detection, continuous network operations center oversight, and remote management systems that provide real-time status updates on cable performance and integrity (Data Center Dynamics, 2021).

Modern subsea cables employ Dense Wavelength Division Multiplexing (DWDM) technology, enabling multiple data streams to be transmitted simultaneously over single fibers using different light wavelengths. The fiber optic cores are specifically engineered for undersea

use, utilizing G.654 subset fiber that achieves remarkably low attenuation rates of 0.15-0.17dB/km (Linden Photonics, 2023).

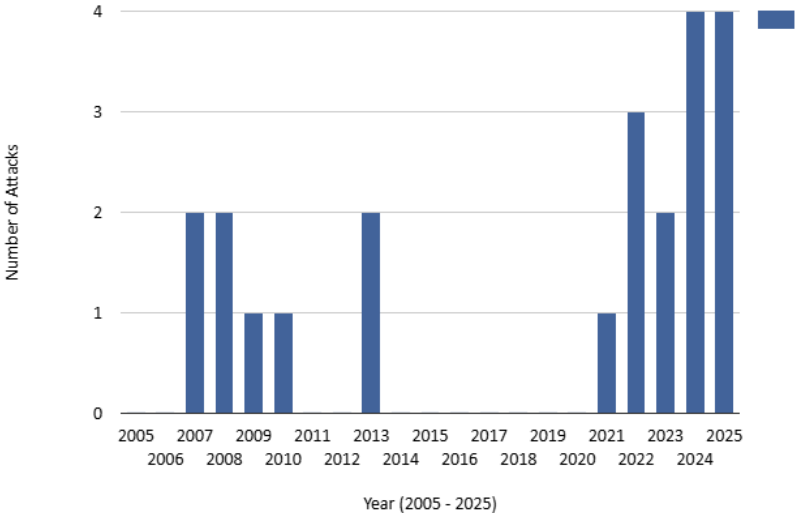
Historically, subsea cables were laid by consortiums of telecommunications companies and others, but increasingly single companies known as hyperscalers are laying cables. Hyperscale computing enables system scalability through computational resources, memory, networking, and storage solutions across environments (GeeksforGeeks, 2024). This architecture powers cloud systems and big data operations, with technologies like MapReduce optimizing large-scale data workflows through parallel processing (Orange Matter, 2023). Hyperscalers—predominantly Amazon, Google, Meta, and Microsoft in the U.S.—operate at massive scale with rapid infrastructure expansion capabilities. These organizations are distinguished by their extensive data center infrastructure, global network presence, and proprietary software/hardware solutions (Red Hat, 2022). Their operations are supported by specialized hardware manufacturers like Ericsson, AMD, and Intel, who provide critical infrastructure components (Inven AI, 2024). The success of hyperscalers stems from their ability to vertically integrate operations, as exemplified by Amazon Web Services' global network of data centers delivering cloud infrastructure services (IBM, 2024). This integration enables rapid scalability and operational efficiency (Red Hat, 2022).

Major Attacks on Subsea Cable Infrastructure

This section provides a comprehensive analysis of suspicious subsea cable break incidents from 2005 to February 2025, highlighting key trends, patterns, and distinctions between the periods 2005-2021 and 2022-2025. Given that between 100 and 200 cable breaks occur annually, this section focuses solely on cases where the cause was deemed suspicious or has been labeled intentional. We have identified 22 suspicious cable break incidents that occurred from 2005 to February 2025.

Suspicious subsea cable breaks are not a recent phenomenon and can be traced back to the time of telegraph cables (Hinck, 2017). However, suspicious breakages have continued in the time of subsea internet cables with one of the first notable incidents occurring in Bangladesh in 2007 (The Daily Star, 2007). As Figure 1 illustrates, between 2005 and 2021, incidents suspected or classified as intentional/sabotage were relatively infrequent, with only nine suspicious attacks recorded over the 16-year period. Notably, six of these occurred within separate one-year periods—two in 2007, two in 2008, and two in 2013. In stark contrast, the three-year period from 2022 to 2025 has seen a dramatic surge in suspicious incidents, with a total of 13 cases. As Figure 1 illustrates, all 13 have occurred within single year clusters—three in 2022, two in 2023, four in 2024, and four in 2025.

Figure 1: The Volume of Suspicious Subsea Cable Incidents (2005–Present)¹



We have identified 22 overall suspicious cable break incidents from 2005 to February 2025. Table 1 details these incidents, articulating the volume, attribution, major perpetrators, major incident locations, impact, and responses to these attacks.

¹ Figure data from: LIRNEasia (2007), The Daily Star (2007), Webmaster (2011a), Radio Jamaica (2008), Preuitt (2009), Saffo (2013), Davenport (2015), Reuters (2013), Fredriksen et al. (2022), Nilsen (2022), King (2022), Martin (2022), Braw (2023), Pollard & Kauranen (2023), Gambrell (2024), Burgess (2024), Al Jazeera (2024), Porter (2024), Traficom (2024), Tobin et al. (2025), Bir (2025), Reuters (2025), and Chang (2025).

Table 1: Major Suspicious Cable Break Incidents (2005–2025)²

Location	Date	Background	Impact	Cause	Suspected Perpetrator	Attributed?
Vietnam	3/2007	Local fisherman accidentally cut and stole at least 11km of the Vietnamese portion (The TVH cable system) of the Sea-Me-We-3 cable. ^a One incident in many surrounding stolen internet cables in Vietnam in 2007 by 5 different rings of cable stealing pirates. ^a The cuts occurred in the Ca Mau Sea, likely in Vietnam’s exclusive economic zone. ^a	Internet speeds slowed down considerably. ^a Vietnam’s communications with Hong Kong and Thailand were disrupted for nearly three months. ^b It cost Vietnam Telecom International over \$4 million in revenue and an additional \$2.6 million to fix underwater missing link. ^a	Intentional or accidental break. ^{bn}	Local fisherman. ^c	Yes. ^c

² Table data from ^aLIRNEasia (2007), ^bInternational Cable Protection Committee (n.d.), ^cSingel (2007), ^dThe Daily Star (2007), ^eDavenport (2015), ^fHinck (2017), ^gWebmaster (2011a), ^hHantover (2014), ⁱStarosielski (2015), ^jFrance24 (2008), ^kRadio Jamaica (2008), ^lPreuitt (2009), ^mWollan (2009), ⁿSaffo (2013), ^oCahyafitri & Cahyafitri (2013), ^pReuters (2013), ^qArthur (2013), ^rFredriksen et al. (2022), ^sNilsen (2022), ^tStaalesen (2022), ^uKing (2022), ^vMartin (2022), ^wBritish Broadcasting Corporation (2022), ^xBraw (2023), ^yRunde et al. (2024), ^zTobin & Chiang (2023), ^{aa}Pollard & Kauranen (2023), ^{ab}Ministry of Defence (2023), ^{ac}Gambrell (2024), ^{ad}Burgess (2024a), ^{ae}Clark (2024), ^{af}HGC Global Communications (2024), ^{ag}Al Jazeera (2024), ^{ah}AFP (2024), ^{ai}Kottasova (2024), ^{aj}Schwartz et al. (2024), ^{ak}Astier & Kirby (2024), ^{al}Porter (2024), ^{am}Moss (2024), ^{an}Traficom (2024), ^{ao}Lott (2024), ^{ap}Rosman (2024), ^{aq}Tobin et al. (2025), ^{ar}Sharwood (2025), ^{as}Aggarwal (2025), ^{at}Bir (2025), ^{au}Associated Press (2025), ^{av}Libel & Chutel (2025), ^{aw}Aikman (2025), ^{ax}News Wires (2025), ^{ay}Reuters (2025), ^{az}Al Jazeera (2025), ^{ba}Cinia (2025), ^{bb}AFP (2025), ^{bc}Chang (2025), ^{bd}McCartney (2025), ^{be}The Financial Express (2007), ^{bf}Smith (2008), ^{bg}Gulldahl & Eriksen (2024), ^{bh}Moss (2022), ^{bi}Weissberger (2022), ^{bj}“Cable Theft Costs Vietnam \$6M” (2007), ^{bk}Webmaster (2011b), ^{bl}Kulha (2021), ^{bm}Humpbert (2022), ^{bn}Brennan (2025), ^{bo}Lemola & Chutel (2024), ^{bp}Ahlander & Jacobsen (2025), and ^{bq}Kwai et al. (2025).

Bangladesh	11/2007	Criminals snapped fiber optic cable (likely SeaMeWe-4) at three points near Cox's Bazar and Feni. ^d On land in Joaria Nala, another part of the cable, surrounded in brick casing, was damaged using a crowbar. ^d It was the 7th incident on the cable occurring in 2007. ^d The cuts occurred on land near the coast. ^d	Overseas calls and internet connection was affected, total loss of communications for at least a week. ^e It cost Bangladesh Telegraph and Telephone Board over \$1 million in repairs and lost revenue. ^f	Likely an intentional attack. ^d	Vandals or criminals. ^{be}	No.
Egypt, Dubai	1/2008-2/2008	Two cables—Sea-Me-We-4 and Flag Europe-Asia (FEA)—cut off the coast of Alexandria, Egypt. Sea-Me-We-4 is cut twice. ^g A day later, the FALCON cable was cut off the coast of Dubai, as well as near the Suez and Sri Lanka, and outside Bandar Abbas, Iran. ^g The cut in Egypt likely occurred in Egypt's EEZ, while the cut in Dubai occurred 56 km from shore, in the UAE's EEZ. ^g	At least fourteen countries reported problems with connectivity and lose significant amount of data traffic. ^h Affected at least 60 million users in India, 12 million in Pakistan, six million in Egypt and 4.7 million in Saudi Arabia. ^g The Maldives were entirely disconnected. ^h Egypt experienced disruptions of 70% and massive internet outage. ⁱ India experienced disruptions of 60%. ^j	Unknown whether all intentional or due to maritime traffic and weather conditions. ^{bk}	Likely a ship dragging anchor; intentional attack by vandals or terrorists suspected. ^{bf}	No.

Jamaica	2008	<p>Throughout the year of 2008, numerous incidents of cable theft and vandalism occurred throughout Jamaica.^k Segments of cables throughout the Parish of St. Catherine (in the towns of Mount Rosser, Ewarton, Linstead, and the communities of McCook's Pen and Succaba Gardens) were repeatedly stolen, many after being replaced.^k Particularly, several hundred feet of optical fiber closures which were used to connect to phone lines outside of the parish.^k Information on where exactly the cut occurred is inconclusive.</p>	<p>Hundreds of customers in sections of St. Catherine's Parish were left without land-line telephone service.^k Cable and Wireless Jamaica lost 1.5 million dollars.^k Phone lines outside of St. Catherine's Parish disabled.^k</p>	<p>Likely an intentional attack.^k</p>	<p>Vandals or criminals.^e</p>	<p>No.</p>
U.S.	4/2009	<p>Four cables belonging to AT&T cut in San Jose, CA via open manhole covers.^l Another four cables cut in San Carlos, and another two in South San Jose.^l The cuts occurred on land.^l</p>	<p>52,000 Verizon landline and wireless customers left without service.^m Over 10,000 Silicon Valley residents left without internet access or landline or mobile phone service.^m Emergency 911 services unavailable on landline and mobile phone.^l</p>	<p>Intentional attack.^m</p>	<p>Vandals or criminals.^m</p>	<p>No.</p>

Philippines	6/2010	International cable linking the Philippines and Japan is cut near Cagayan de Oro via beach manhole connection. ⁿ The cuts occurred on land near the coast. ⁿ	Internet access disrupted in the Philippines. ^e	Likely an intentional attack. ^e	Separatists/terrorists group. ⁿ	No.
Indonesia	3/2013	16 tons and 31.7km of subsea cables between Banka Island and Riau Island of Indonesia were stolen. ^e Information on where exactly the cut occurred is inconclusive, likely occurred in Indonesia's territorial waters.	Voice and Data service were disrupted for more than a month. ^o Cost PT Indosat \$1 million to replace cable and more money for other stolen material. ^o	Intentional break. ^o	Cable stealing criminals. ^o	Yes. ^o
Egypt	3/2013	Egyptian Coast Guard caught 3 divers trying to cut the Sea-Me-We-4 cable 750m off the coast of Alexandria ^p Speculation on relation to the cuts to the I-ME-WE, TE North, EIG and Sea-Me-We-3 cables a week earlier initially attributed to a dragging anchor. ⁿ Divers in the waters near Egypt are arrested attempting to cut a fourth cable. ^p The cuts occurred 750m (820 yards) north of Alexandria, in Egypt's territorial waters. ^p	Damaged cable caused a drop in internet speed in Egypt and a couple other countries. ^q	Intentional break. ^p	Vandals or criminals. ^p	Partially. ^p

Norway	4/2021	More than 4.3km of cable connecting the Lofoten-Vesteralen (LoVe) marine observatory to its inland IMR station in Hovden severed and removed during the Easter Break. ^r Information on where exactly the cut occurred is inconclusive, likely occurred in Norway's exclusive economic zone	LoVe observatory completely dead, with no connection. ^r Researchers put vital work and projects on hold. ^r Monitoring data couldn't be delivered to the Norwegian Armed Forces. ^r	Suspected intentional attack; lacking conclusive evidence of an attack. ^{bi}	No suspects identified, Russia suspected. ^r	No. ^r
Norway	1/2022	Damage to one of the cables in the Svalbard Undersea Cable. System connecting Svalbard to Norway damaged between 130 to 230 km from Longyearbyen. ⁵ Information on where exactly the cut occurred is inconclusive, likely occurred in Norway's EEZ.	Communications to and from Svalbard were still running as normal. ⁵ No negative effect on ability to communicate effectively to and from Mainland Norway with Svalbard. ⁵ Temporary lack of redundancy. [‡]	Suspected intentional attack; attributed to trawling activity. ^{bg}	No suspects identified, Russia suspected. ^{bg}	No. ^{bg}
France	10/2022	Subsea cable in the South of France near Marseille simultaneously cut to three links connecting Marseille to Milan, Marseille to Lyon, and Marseille to Barcelona. ^u Information on where exactly the cut occurred is inconclusive. ^u	Widespread connectivity issues. ^u Internet access for users in Europe, Asia, and the U.S. slowed. ^u One connection quickly fixed ^u	Likely an Intentional break. ^{bi}	Vandals or criminals. ^{bh}	No.

Scotland	10/2022	On October 15th, the North Section of the SHEFA-2 cable connecting the Shetland Islands to the Faroe Islands was cut. ^v 5 days later on October 20th, the South portion of the cable connecting the Islands to Mainland Britain got cut. ^v Information on where exactly the cut occurred is inconclusive, likely occurred in the Scotland's EEZ.	Widespread broadband internet outages. ^w Mobile phone service somewhat compromised. ^w Some landline and mobile working. ^w Connectivity for some restored mid-afternoon. ^w Transport services (Airport and Ferry) operating normally. ^w	Suspected intentional attack; likely an unintentional break. ^{bi, v}	No suspects identified, Russia suspected. ^{bi}	No.
Taiwan	2/2023	Taima No. 2 cable near Dongyin in the Matsu Islands damaged on February 2nd by a Chinese fishing ship. ^x Six days later, the Taima No. 3 cable near Juguang damaged by a Chinese cargo freighter. ^x The cuts occurred 10 nautical miles off China's coast. ^x	Six week internet blackout and digital isolation for Matsu Island. ^y Island switches to a microwave internet system. ^x Citizens left with only rudimentary internet access, with slow connectivity. ^x Local businesses slowed due to blackout. ^z Fixing the cable costs Chunghwa Telecom between \$660,000 and \$1.3 million. ^x	Suspected intentional attack; lacking conclusive evidence of an attack. ^z	China registered vessels. ^x	Yes. ^x

Baltic Sea: Finland, Sweden, Estonia	10/2023	The Chinese vessel, <i>Newnew Polar Bear</i> , damaged both an subsea cable. Internet cable connecting Finland to Estonia along with the Baltconnector pipeline. ^{aa} Damage was also inflicted onto the EE-S1 cable connecting Sweden to Estonia. ^{aa} Vessel is later identified as the <i>Newnew Polar Bear</i> . The cuts to the cable connecting Estonia to Finland occurred in Finland’s EEZ, while the cuts to the EE-S1 occurred some 50 km (30 miles) west of Hiiumaa Island, in Estonia’s EEZ. ^{aa}	Ability to communicate and overall function of the cable not affected. ^{ab}	Suspected intentional attack ^{ap} ; attributed to an accidental dragging anchor due to a storm. ^{bn}	China registered vessel, but Russia suspected. ^{aa}	Yes. ^{aa}
Red Sea: Yemen	2/2024	Three cables: Seacom—TGN-gulf, Asia Africa Europe-1 (AAE-1), and Europe-India Gateway cut in the Red Sea off the coast of Djibouti in the Bab el Mandeb strait due to dragging anchor. ^{ac} The cut occurred 18 miles from cable landing spot in Djibouti, in Djibouti’s contiguous zone and EEZ as well as in Yemen’s maritime jurisdiction. ^{ad}	Drop in connectivity from Europe to Asia. ^{ad} Outages in East Africa (Tanzania, Kenya, Uganda, and Mozambique) and Southeast Asia (Vietnam, Thailand, and Singapore). ^{ae} 25% of global internet traffic impacted. ^{af} At least a dozen operators affected. ^{ae} Service quickly rerouted but countries including Bahrain and Djibouti still facing interruptions. ^{ac}	Suspected intentional attack; likely an unintentional break. ^{ad}	Belize flagged British registered carrier vessel; Houthis suspected. ^{ad}	Partially. ^{ad}

Baltic Sea: Sweden, Lithuania, Germany, Finland	11/2024	On November 17th, the BCS East-West Interlink cable connecting Sweden to Lithuania was cut. ^{ag} Less than 24 hrs later, on November 18th, the C-Lion 1 cable connecting Finland and Germany was cut. ^{ag} Vessel is later identified as the <i>Yi Peng 3</i> and is held in port in Denmark with ongoing investigations. ^{ah} Both of the cuts occurred in Sweden's EEZ. ^{ag}	The BCS East-West Interlink cable sustained full damage. ^{ai} Data transfers were disrupted but internet connections not cut off. ^{aj} Finland International Telecoms rerouted connections. ^{ai} ~1/5 of Lithuania's internet capacity disrupted, although consumers not too affected. ^{ak} Traffic eventually restored. ^{ai}	Suspected intentional attack; partially attributed to an accidental dragging anchor. ^{aj}	China registered vessel, but Russia suspected. ^{ah}	Partially. ^{ah}
Finland	12/2024	On December 3rd, a cable connecting Sweden and Finland was cut in two separate locations in Vista and Espoo. ^{al} The cuts occurred on land. ^{al}	Widespread outages in Finland, with thousands of households affected. ^{al} 6,000 private customers and ~100 business customers of Traficom telecom company affected. ^{am} Cables quickly repaired and services restored. ^{ah}	Suspected intentional attack; unintentional accident due to construction work. ^{al}	Construction workers. ^{al}	Yes. ^{al}

Baltic Sea: Finland, Estonia	12/2024	<p>On December 25th, the Estlink 2 power cable and the Finland Estonia Connection 1 (FEC-1) and Finland Estonia Connection 2 (FEC-2) internet cables were cut.^{an} Vessel is quickly identified as the <i>Eagle S</i> and is apprehended by the Finnish Patrol Ship <i>Turva</i>.^{ao} Information on where exactly the cut occurred is inconclusive, likely occurred in Finland and Estonia's EEZ.</p>	<p>Little immediate impact on services.^{ap} Traffic quickly rerouted to backup cables.^{ap} Traffic between Finland to Europe and the rest of the world still operational.^{an} May have caused some delays in customers' communication services.^{an}</p>	<p>Suspected intentional attack; partially attributed to an accidental dragging anchor.^{bs}</p>	<p>Emirati registered, Cook Islands flagged tanker, but Russia suspected.^{at,bo}</p>	Partially. ^{ap,bo}
Taiwan	1/2025	<p>On January 3rd, the Trans Pacific Express (TPE) cable is damaged off the coast of Keelung.^{aq} Vessel is quickly identified as the <i>Shunxing 39</i>.^{aq} Information on where exactly the cut occurred is inconclusive.^{aq}</p>	<p>Only four fibers impacted.^{ar} Connectivity was not disturbed and data quickly rerouted to other cables after damage is detected.^{aq,as}</p>	<p>Suspected intentional attack, lacking conclusive evidence of an attack.^{aq, as}</p>	<p>Hong Kong owned, Tanzanian and/or Cameroonian flagged and registered, Chinese crewed freighter, but China suspected.^{aq}</p>	Partially. ^{aq}

Baltic Sea: Sweden, Latvia	1/2025	<p>On January 26th, the Sweden-Latvia fiber optic cable connecting the Swedish Island of Gotland to Latvia was significantly damaged.^{at} A vessel is quickly detained and by Swedish forces and identified as the <i>Vezhen</i>.^{au} On January 31st, Norwegian forces, working on request from Latvian authorities, identified and detained the Russian crewed Cargo vessel.^{av} The vessel is identified as the <i>Silver Dania</i>.^{av} Information on where exactly the cut occurred is inconclusive, likely occurred in Sweden's EEZ.</p>	<p>Disruptions in data services are reported.^{aw} Cable operator warned there may be delays in data transmission speeds.^{ax} Cable operator, Latvian State Radio and Television Center (LVRTC) was able to operate using other transmission routes.^{aw} Users mostly unaffected.^{aw}</p>	<p>Suspected intentional attack; deemed accidental and attributed to weather conditions and deficiencies in equipment and seamanship.^{aw, bp}</p>	<p>Bulgarian owned, Malta flagged Bulk Carrier, but Russia suspected.^{au, aw}</p> <p>OR</p> <p>Norwegian flagged, owned, and registered, Russian crewed cargo ship, Russia still suspected.^{av, aw}</p>	Partially. ^{au, av, aw}
Baltic Sea: Sweden, Finland	2/2025	<p>On February 19th, minor damage to the C-Lion1 Cable was identified.^{av} Preliminary investigations on February 21st confirmed the cable was damaged.^{av} Investigations by Sweden and Finnish police are currently ongoing.^{az} No suspect has been identified.^{az} The cuts occurred in Sweden's EEZ.^{av}</p>	<p>Minor cable damage.^{ba} Functionality of telecommunications connections and data traffic running normally.^{bb} No apparent disruptions to connections.^{bb}</p>	<p>Suspected intentional attack.^{bq}</p>	<p>No suspects identified yet; investigation ongoing.</p>	No.

Taiwan	2/2025	<p>On February 25th, at after 3 am, Chunghwa Telecom detected a cable linking Taiwan's mainland and the outlying Penghu Islands had been severed.^{bc} Chunghwa Telecoms contacted the Taiwanese Coast Guard, who at around 2:30 am had been tracking the freighter vessel <i>Hong Tai</i> – (originally registered as the <i>Hong Tai 58</i> but the hull of the ship reading <i>Hong Tai 168</i>).^{bd} The vessel is believed to have Chinese ownership, while all members of the crew are identified as Chinese nationals.^{bd, bc} The <i>Hong Tai</i> is guided back to Anping Port and comes to anchor in Tainan where it its crew is detained and the vessel boarded by the Coast Guard.^{bd} An investigation is now ongoing.^{bc} Information on where exactly the cut occurred is inconclusive.^{bg}</p>	<p>Chunghwa Telecom activated redundant backup cable.^{bd} No communications disrupted between Taiwan mainland and the Penghu Islands.^{bd}</p>	<p>Suspected intentional attack.^{bc}</p>	<p>Togolese flagged, possibly Chinese owned, Chinese crewed freighter, but China suspected.^{bc}</p>	<p>Partially.^{bc}</p>
--------	--------	---	---	---	--	--------------------------------

The rise in suspected intentional sabotage attacks corresponds with increasing geopolitical tensions, particularly following the 2022 Nord Stream pipeline attacks and Russia's invasion of Ukraine (Desmarais, 2024a). This pattern suggests that cable sabotage may have become a strategic tool in hybrid warfare, with certain state actors prompted to target subsea cables as a means of intimidation or disruption.

Attribution of Subsea Cable Attacks

Along with volume, the attribution of subsea cable attacks has shifted significantly between the periods of 2005–2021 and 2022–2025. Between 2005–2021, most intentional attacks were attributed to low level criminals, vandals, or terrorists. For instance, cable breaks in Jamaica (2008) and Egypt (2013) were linked to criminal activity, while incidents in Bangladesh (2007) and the United States (2009) were classified as vandalism (Radio Jamaica News, 2008; Reuters, 2013; The Financial Express, 2007; Wollan, 2009). Although rare, some cases were at one point linked to terrorism, including the 2008 breaks in Egypt and Dubai and the 2010 attack in the Philippines (Smith, 2008; Davenport, 2015). These incidents fueled growing concerns in the 2010s that subsea cables, vital to global communications, were increasingly vulnerable and could become prime targets for terrorist groups (Saffo, 2013).

Since 2022, attribution has increasingly shifted towards state actors, particularly after the Nord Stream incident and the start of the 2022 Ukraine War. Suspicion of Russian involvement in incidents in Norway (2021), Norway's Svalbard (2022), and Scotland's Shetland Islands (2022) further fueled concerns over state threats, despite later findings that the breaks were likely accidental (Fredriksen et al., 2022; Gulldahl & Eriksen, 2024; Martin 2022). This trend has fueled growing suspicion that any damaged cable is the result of state action. European officials, in particular, increasingly classify even mildly suspicious incidents as probable sabotage (Rintakumpu et al., 2025).

The shift in attribution from low level malicious actors to state actors has also influenced overall attribution of more routine disruptions. In February 2024, a cable disruption in the Red Sea was at first quickly attributed to intentional Houthi sabotage. However, upon closer investigation, experts later identified a disabled British carrier ship as the likely cause (Young, 2024; Gambrell, 2024). These incidents reflect a growing tendency to quickly attribute damage to states, often prioritizing geopolitical tensions in attribution before fully investigating incidents.

Major Perpetrators of Subsea Cable Attacks

Despite growing concerns since 2022 about state involvement in suspicious subsea cable breaks, official attribution—which includes definitive identification, verification, and, in some cases, subsequent action against a perpetrator—remains rare due to challenges in gathering

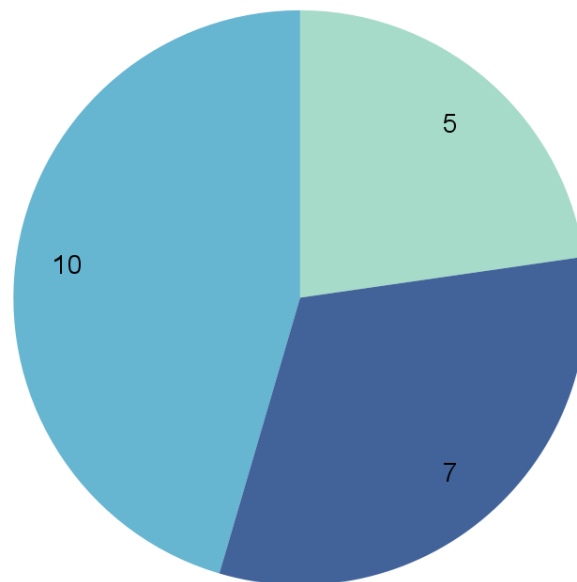
evidence that unequivocally verifies intent. The high vulnerability of subsea cables and the ambiguous nature of cable breaks make it difficult to gather concrete evidence of perpetrator identity and purpose. As a result, many suspected sabotage incidents go unattributed or are later classified as caused by accidental human or maritime activity.

As Figure 2 illustrates, of the 22 incidents since 2005, only five have been officially attributed. These cases are: Vietnam (2007), Indonesia (2013), the Baltic Sea (2023), Taiwan (2023), and Finland (December 2024) (Singel, 2007; Cahyafitri & Cahyafitri, 2013; Rosman, 2024; Braw, 2023; Agence France Presse [AFP], 2024). Only one of these, the 2023 Baltic Sea incident, was attributed to a state actor: China (Rosman, 2024). China has acknowledged their responsibility in this case. The Chinese government recognized that damage was caused by the culprit, a Chinese ship the *Newnew Polar Bear*, although it insists the breaks were accidental (Brennan, 2025). As Figure 2 also illustrates, seven incidents between 2005 and 2025 have been partially attributed, meaning evidence points to a specific cause or party; however, official attribution remains elusive due to ongoing investigations or conflicting statements. Six of these partially attributed incidents occurred between 2022 and 2025.

Figure 2: The Attribution of Suspicious Subsea Cable Breaks (2005–Present)³

The Attribution of Suspicious Subsea Cable Breaks

- Officially Attributed
- Partially Attributed
- Not Attributed



³ Figure data From: Singel (2007), Cahyafitri & Cahyafitri (2013), Rosman (2024); Braw (2023), Agence France Presse [AFP] (2024), Porter (2024), Pollard & Kauranen (2023), Reuters (2013), Burgess (2024), Lemola & Chutel (2024), Tobin et al. (2025), Associated Press (2025), Aikman (2025), Libel & Chutel (2025), Chang (2025), The Financial Express (2007), Smith (2008), Davenport (2015), Wollan (2009), Saffo (2013), Fredriksen et al. (2022), Moss (2022), Weissberger (2022), and Al Jazeera (2025).

Some of the major challenges in attributing cable breaks lie in limitations in vessel tracking capabilities. The Automatic Identification System (AIS) is a crucial tool for monitoring ship activity—including suspicious erratic behavior—but has significant limitations. Mainly, routine fishing operations can resemble suspicious behavior, while many ships disable their AIS when engaging in illicit activities (Burdette, 2024; Fredriksen et al., 2022; Desmarais, 2024a). These gaps complicate attribution and expose vulnerabilities in protecting essential cable infrastructure.

Flag of Convenience Ships and Subsea Cable Incidents

Although certain key states like Russia and China are suspected of deliberately breaking subsea cables, most of these incidents are linked to ships registered under seemingly random national flags. International regulations on vessel registration and flagging are lax, with few restrictions linking ships to specific states. The United Nations Convention on the Law of the Sea (UNCLOS) merely specifies there must be a “genuine link” between a ship and its flag state but fails to define what that entails (International Maritime Organization [IMO], n.d.). Moreover, Article 91 of the convention further allows states to set their own conditions for granting nationality and flag rights, leading many to adopt lenient regulations (United Nations Convention on the Law of the Sea [UNCLOS], 1982). On top of this, in the high seas, UNCLOS grants flag states jurisdiction over vessels flying their flags (UNCLOS, 1982). As such, countries often evade blame for subsea cable breaks and other illicit activities by exploiting this loophole through the use of flag of convenience (FOC) ships, which are typically flagged under nations with more relaxed jurisdiction. Russia and China, in particular, are suspected of employing this tactic. Russia is believed to operate a shadow fleet of over 1,000 vessels with opaque ownership structures in order to evade sanctions, while China is suspected of maintaining a similar flag of convenience fleet with up to 52 vessels (Windward, n.d.; Kirby, 2024; Staff Writer with AFP, 2025). Both countries have been suspected of using these fleets to intentionally break subsea cables.

Of the six vessels identified in the six partially attributed cases since 2022, as Table 1 illustrates, two (from the Baltic Sea incidents in November and December 2024) were conducted by ships flagged under China and the Cook Islands respectively but are suspected of being part of Russia’s fleet (Rosman, 2024). Additionally, the Malta flagged *Vezhen*, linked to Baltic Sea cable cuts in January 2025, displayed similar behavior to suspected Russian vessels (O’Sullivan, 2025). However, the owner—a Bulgarian company—has denied any connection to Russia (O’Sullivan, 2025). Two vessels involved in the Taiwan January and February 2025 breaks were flagged under Tanzania and Togo respectively but are suspected of having Chinese ties. This is due in part to the fact that both had all Chinese crews (Reuters, 2025b; Forum Staff, 2025; Chang, 2025). Taiwan has accused China of operating 52 such vessels, 15 of which were

flagged as threats due to suspicious behavior (Staff Writer with AFP, 2025). Notably, the vessel suspected in the February 2025 incident was one of these 52 vessels (McCartney, 2025). These 2025 incidents, in particular, have fueled concerns over China's use of flag of convenience ships to damage critical infrastructure. Overall, the use of flags of convenience ships complicates attribution, as the responsibility falls to the flag state, allowing perpetrator states—like Russia and China— to deny involvement and obscure as well as avoid accountability (Tobin et al., 2025).

Russia's Role in Subsea Cable Incidents

Russia is a major suspected perpetrator in subsea cable breaks, particularly after 2022, although no official attributions have been made. Suspicion of Russia's interest in subsea infrastructure dates back to 2015 and grew in 2017 when NATO reported increased Russian subsea activity (Hinck, 2017; Newdick, 2021). While none of the 22 suspicious incidents since 2005 have been officially linked to Russia, it has been suspected in seven incidents (Fredriksen et al., 2022; Newdick, 2022; Gulldahl & Eriksen, 2024; Weissberger, 2022; Pollard & Kauranen, 2023; Kottasová, 2024; Rosman, 2024; Libell & Chutel, 2025). Notably, six of these incidents occurred in the period of 2022–2025, particularly after the invasion of Ukraine. Experts believe Russia has the capability to damage cables and may have already targeted Atlantic infrastructure (Hendriks & Halem, 2024). Despite these concerns, formal investigations regarding Russian involvement in subsea cable breaks have been widely inconclusive. While vessels linked to these incidents have been identified, none are flagged under Russia. In all seven cases where it was suspected, Russia has maintained plausible deniability due to the lack of concrete evidence despite the frequent pattern of incidents (Kottasova, 2024; Desmarais, 2024b).

While concerns over Russian sabotage persist, particularly among European and NATO members, many U.S. and European security officials and naval experts caution against quick attribution, especially in the Baltic Sea. These intelligence officials now suggest these incidents are more likely due to maritime accidents or poorly maintained vessels, a view that has become the prevailing consensus among U.S. and NATO countries' security services (Miller et al., 2025). Nevertheless, Russia has reportedly signaled its readiness to target subsea infrastructure, with officials stating it has “no constraints, even moral, left” (Desmarais, 2024a). The lack of official attribution complicates responses, as the affected states—particularly in the Baltic area— cannot formally accuse or retaliate, leaving Russia emboldened. This uncertainty weakens the ability of European and NATO countries to address hybrid warfare threats to their critical internet infrastructure effectively.

China's Role in Subsea Cable Incidents

China is considered a major perpetrator of suspicious subsea cable breaks, particularly given their historic relationship with and repeated aggressive actions towards Taiwan (Lee, 2021). China has been officially linked to two cases—the 2023 Baltic Sea break and the 2023 Taiwan breaks—and has overall been suspected in three incidents from 2005 to the present (Aggarwal, 2025; Chang, 2025). While China took responsibility for the 2023 Baltic Sea cable break, many suspected Russian involvement (Braw, 2024). Similarly, the November 2024 Baltic Sea break involved a Hong Kong flagged vessel, *Yi Peng 3*, which was crewed by a Chinese captain and one Russian sailor (Brovko, 2024). Similarities in the ship's movement to vessels suspected to be part of Russia's shadow fleet has led to investigations into whether the Chinese captain was recruited by Russian Intelligence (The Maritime Executive, 2024; Brovko, 2024). Moreover, China's foreign ministry denied any responsibility, further fueling beliefs of Russian led sabotage (AFP, 2024).

China has been suspected of perpetrating a further two of the overall 22 incidents: the January and February 2025 Taiwan cable breaks. Both January and February 2025 breaks, although suspected to involve China, were carried out by vessels flagged under Tanzania (possibly Cameroon) and Togo respectively (Sharwood, 2025; Chang, 2025). Notably the vessel identified in the January 2025 Taiwan incident, the *Shunxing 39*, while flagged under Tanzania (possibly Cameroon), originally carried a Chinese flag before changing registration in 2024 (Forum Staff, 2025; Addis, 2025). China has not taken responsibility for either of the 2025 incidents (Hunter, 2023; Aggarwal, 2025). Moreover, in the aftermath of the February 2025 break, China accused Taiwan of manipulating the incident for political purposes (Chang, 2025).

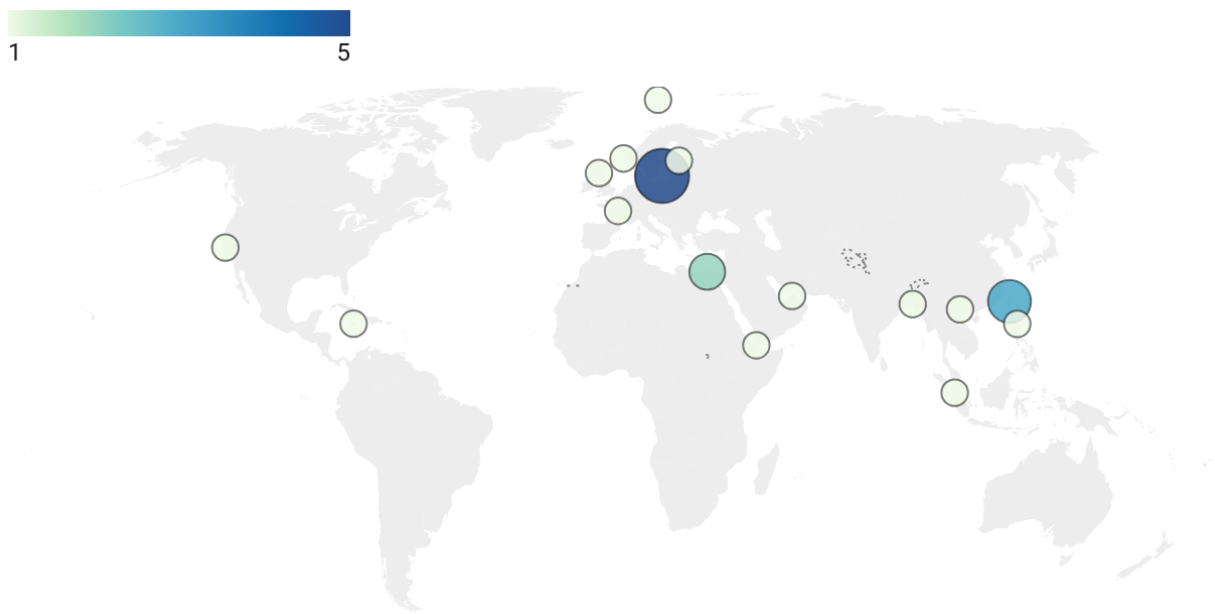
Like Russia, China has the capability and motive for subsea cable sabotage. Its engineers have spent 15 years developing cable cutting tools, officially for removing illegal cables (Forum Staff, 2025; Tatlow, 2025). However, many suspect China uses these tools for strategic offensive purposes instead (Tatlow, 2025). Taiwanese officials have accused China of routinely pressuring Taiwan with fishing and shipping vessels in its waters, often causing cable damage (Lii, 2023). Additionally, these vessels have been repeatedly spotted disabling their tracking systems while operating near critical cables, raising suspicions of covert mapping or sabotage activities (Runde et al., 2024).

China's intimidation of Taiwan predates the 2023 and 2025 incidents, with around 30 cable breaks since 2017 (Lii, 2023). These 30 are excluded from the overall 22 incidents recorded here as they were deemed accidental or inconsequential at the time (Lii, 2023). Taiwan and its allies fear escalation, viewing these as tests for a larger operation to sever Taiwan's communications ahead of an invasion (Lee, 2021). China dismisses such concerns as baseless, but its growing link to cable disruptions continues to raise alarms (Aggarwal, 2025). As with Russia, the lack of definitive attribution limits Taiwan and its allies' ability to respond, forcing a focus on building alternative systems and increasing redundancy instead.

Locations of Major Subsea Cable Incidents

The geographical distribution of major cable break incidents, illustrated in Figure 3, has shifted dramatically from 2005–2021 to 2022–2025, mirroring the growing link between these attacks and geopolitical tensions. Between 2005 and 2021, suspicious cable breaks appeared to be random, mainly unrelated to geopolitical tensions or strategic choke points, instead coinciding with domestic incidents.

Figure 3: The Density and Location of Suspicious Cable Breaks (2005–Present)⁴



As Figure 3 illustrates, the nine recorded breaks prior to 2022 were scattered across six regions—Southeast Asia, South Asia, North Africa, Europe, the Caribbean, and North America—affecting eight countries: the Philippines, Indonesia, Vietnam, Bangladesh, Egypt, Norway, Jamaica, and the United States (Davenport, 2015; Cahyafitri & Cahyafitri, 2013; Singel, 2007; The Daily Star, 2007; Reuters, 2013; Fredriksen et al., 2022; Radio Jamaica News, 2008; Wollan, 2009). Only Egypt (2008, 2013) and Southeast Asia (Vietnam 2007, the Philippines 2010, Indonesia 2013) saw multiple incidents (Reuters, 2013; Singel, 2007; Davenport, 2015; Cahyafitri & Cahyafitri, 2013). Egypt’s 2013 incident is the only break that appeared strategically motivated due to its location in a geographic choke point (Arthur, 2013). All other incidents

⁴ Note. From LIRNEasia (2007), The Daily Star (2007), Webmaster (2011a), Radio Jamaica (2008), Preuitt (2009), Saffo (2013), Davenport (2015), Reuters (2013), Fredriksen et al. (2022), Nilsen (2022), King (2022), Martin (2022), Braw (2023), Pollard & Kauranen (2023), Gambrell (2024), Burgess (2024), Al Jazeera (2024), Porter (2024), Traficom (2024), Tobin et al. (2025), Bir (2025), Reuters (2025), and Chang (2025).

appeared tied to domestic events rather than geopolitical motives, such as the 2013 Indonesia and 2007 Vietnam breaks, which were linked to ongoing cable smuggling operations (“Cable Theft Costs Vietnam \$6M,” 2007; Cahyafitri & Cahyafitri, 2013).

Since 2022, cable breaks have become more concentrated in geopolitical hotspots, particularly the Baltic Sea, South China Sea, and the Red Sea. Of the 13 recorded incidents, eight occurred in previously targeted regions, including, notably, five in the Baltic Sea and three near Taiwan (Kauranen et al., 2025; Aggarwal, 2025). The Baltic Sea incidents, which occurred in the wake of the Nord Stream sabotage and Russia’s invasion of Ukraine, suggest a deliberate campaign against NATO and EU states supporting Ukraine (Kwai et al., 2025)—raising concerns over Russian hybrid warfare tactics (Desmarais, 2024b). Additional attacks on cables serving Norway’s Svalbard and Scotland’s Shetland Islands further point to this broader strategy. Meanwhile, Taiwan’s recent breaks (2023, January and February 2025) coincide with China’s increasing maritime pressure and malicious activities in the South China Sea, raising fears of preemptive efforts to disrupt the island’s communications (Lee, 2021). Although only one suspicious break has been recorded in the Red Sea since 2022, the break was partly a result of the geopolitical tensions in the region: the Israel-Hamas conflict (Reed, 2024). The vessel responsible for the break was disabled by a Houthi attack, because the organization was targeting ships from countries supporting Israel (Gambrell, 2024). All of these locations have gained significant geopolitical importance since 2022, with the surge in attacks appearing closely tied to their strategic value.

Since 2022, suspicious cable break incidents have shifted from a geographically dispersed and seemingly random distribution, comparable to their attribution to unrelated gangs, vandals, or criminals. These incidents are now increasingly concentrated in strategic geopolitical hotspots, including the Baltic Sea, South China Sea, and the Red Sea. This shift aligns with changing attribution trends, which suggests that states are increasingly targeting subsea cables as part of hybrid warfare strategies driven by geopolitical tensions and conflicts.

Impact of Subsea Cable Disruption

Along with changes in subsea cable incident patterns, there are clear shifts in impact trends between the periods of 2005–2021 and 2022–2025 with cable disruptions becoming far more costly. Prior to 2022, the primary impact of subsea cable disruptions was regional connectivity loss, financial damage to telecommunications companies, and temporary slowdowns in internet speed. Incidents were usually localized outages, such as in Vietnam’s internet slowdown in 2007 (LIRNEasia, 2007) or Egypt’s connectivity drop in 2008 (Hantover, 2013). These incidents typically only affected one country or a small group of countries. Additionally, the economic consequences were significant but contained, often limited to repair costs and revenue losses for telecommunication providers. These costs ranged from \$1 to \$2

million on average, as evidenced by incidents like the 2007 Bangladesh cable break and the 2013 Indonesia theft, shown in Table 1.

Since 2022, the scale and severity of impacts have escalated. Attacks now frequently disrupt cross-border communication, threaten national security operations, and target specific areas and choke points to create constant vulnerabilities. There has been a notable shift in the increase in multi-country and transcontinental disruptions. For example, the 2024 Red Sea cable cuts impacted the internet traffic between Europe, Africa, and Asia. While the Baltic Sea incidents disrupted internet traffic between Sweden, Finland, Estonia, and Germany. Unlike earlier cases where incidents were relatively isolated, recent attacks have demonstrated a sustained pattern of strategic disruption, affecting entire regions rather than single nations.

Altogether, impact trends have evolved from isolated economic and service disruptions to large scale, multinational connectivity threats that carry severe geopolitical and security implications. The increasing weaponization of subsea infrastructure has made these attacks a critical vulnerability in global communications networks, reinforcing the urgency for stronger international cooperation and preventive security measures.

Responses to Subsea Cable Disruptions

Responses to subsea cable disruptions have evolved significantly over time, reflecting broader changes globally in technological capabilities, geopolitical tensions, and international coordination. Prior to 2022, responses were largely reactive, localized, and telecommunication company led, with affected providers focusing on damage assessment and repairs rather than proactive mitigation. Restoration efforts were often slow, with limited government involvement and a lack of redundancy, leading to prolonged outages, such as the total disconnection of the Maldives in 2008 (Hantover, 2013). Investigations into these early incidents were often inconclusive, with many cases remaining unattributed or dismissed as accidents due to insufficient monitoring technology and limited investigative capabilities.

Since 2022, a notable shift toward faster, more coordinated, and security-driven responses has emerged. Mitigation strategies have notably improved, as demonstrated during the Baltic Sea (2023–2025) incidents. In the Baltic Sea, rapid identification of damaged cables allowed for swift rerouting of internet traffic through alternative routes, minimizing disruptions across Finland, Sweden, and Estonia (Desmarais, 2024b; Rintakumpu et al., 2025). Cross-border coordination among countries further accelerated repair efforts and enhanced situational awareness by sharing real-time data on vessel movements (Shephard News Team, 2025). In response to the ongoing threats, the European Union recently announced new measures to strengthen Baltic Sea security, aiming to improve prevention, detection, and response to subsea cable sabotage over the next two years (Kwai et al., 2025). These efforts prioritize threat

detection, expand funding for new cables, and bolster enforcement against hostile actors—highlighting the EU’s growing recognition of the strategic importance of subsea infrastructure.

The growing frequency of suspected sabotage has increased military and government involvement, particularly in Europe and East Asia, where subsea cables are now recognized as critical national security assets (Runde et al., 2024). The increase in suspected sabotage has also amplified attention from leading policy research organizations. For example, the Center for Strategic and International Studies (CSIS) has emphasized the critical role subsea cables play in supporting global economic activities, military operations, and internet infrastructure (Runde et al., 2024). Although not a policymaking body, CSIS’s focus on these vulnerabilities reflects the broader strategic concern that has influenced government and private sector responses since 2022. The U.S. Department of Homeland Security (DHS) explicitly identifies subsea cables as vital to U.S. national security and economic stability within their white paper released in December 2024, emphasizing throughout that their disruption could compromise defense operations, financial systems, and global communications (United States Department of Homeland Security [DHS], 2024). With growing threats from geopolitical rivals like Russia and China, the U.S. sees these cables as a critical national security asset, recognizing that any disruption could cripple defense operations, disrupt markets, and weaken strategic alliances.

Through all of this, response patterns have transitioned from slow, reactive measures to proactive, security driven strategies that emphasize mitigation and rapid restoration. This shift further reflects how subsea cables are now seen as essential infrastructure, tightly linked to both global security and economic stability.

Risks and Threats to Global Subsea Cable Infrastructure

Subsea cables face multiple threats, from accidental damage and natural disasters to deliberate sabotage and espionage. This section examines four primary categories of threats to global subsea cable infrastructure. First, we examine the accidental and environmental risks—maritime activity, natural disasters, and system failures—that remain the most frequent causes of disruptions. Second, narrow maritime corridors connecting larger bodies of water serve as critical strategic choke points where strategic and geographic vulnerabilities increase the likelihood of cascading failures and delays in restoration. Third, deliberate sabotage by state actors, including covert or disguised attacks, presents a growing threat in the context of rising geopolitical tensions. Finally, espionage and cybersecurity threats, such as data interception at sea and cable landing stations, pose significant risks to global communications security and U.S. national security, particularly regarding the protection of sensitive information, military communications, and intelligence-sharing networks.

Accidental and Environmental Risks

Subsea cables are highly vulnerable to accidental damage and natural disasters, which account for the majority of disruptions. Maritime activities, such as fishing and anchor damage, frequently sever cables, while earthquakes, submarine landslides, and extreme weather also pose risks (International Cable Protection Committee [ICPC], 2021). Additionally, aging infrastructure and system failures contribute to outages, often requiring complex and time-consuming repairs (Runde et al., 2024). These threats are most severe in high-traffic shipping lanes and seismically active regions, where disruptions can cause widespread connectivity losses and economic impact (Integral Consulting, 2024; Veverka, 2011).

Human-Induced Maritime and Fishing Damage

The most frequent cause of subsea cable disruptions is accidental damage from maritime activities, accounting for 60-75% of cable faults annually (Bafoutsou et al., 2023; Crisis24, 2024). Fishing trawlers and ship anchors are the most common causes of damage, particularly in shallow waters near coastlines and busy shipping lanes. Due to the density of global trade routes, areas such as the South China Sea, the Mediterranean, and the North Atlantic see a disproportionately high number of these incidents.

The overlap between busy shipping lanes and areas of high cable density creates persistent vulnerabilities in global telecommunications networks. While international regulations require vessels to avoid damaging subsea cables, enforcement remains challenging, particularly because many commercial ships lack accurate information about cable locations or operate without proper awareness of cable routes in their vicinity (Runde et al., 2024).

Natural Disasters and Environmental Factors

While less common than human-induced disruptions, natural phenomena also pose significant risks to subsea cables, particularly in regions with high seismic activity. Earthquakes, mudslides, volcanic eruptions, tsunamis, and extreme ocean currents account for approximately 5% of cable incidents (Bafoutsou et al., 2023). These events often damage multiple cables simultaneously, amplifying the scale of internet disruptions and complicating repair efforts (Congressional Research Service [CRS], 2023).

One of the most well-documented cases of natural disaster-related cable damage occurred during the 2006 Hengchun earthquake near Taiwan, which severed multiple trans-Pacific cables and disrupted 90% of internet traffic across Asia (Qiu, 2011). The incident required weeks of complex repairs, underscoring the vulnerability of the global internet infrastructure to seismic events (Starosielski, 2015). Similarly, the 2011 Tōhoku earthquake in Japan damaged several subsea cables, slowing financial transactions and emergency communications across the Pacific (European Parliament, 2022). More recently, in 2022, a massive volcanic eruption in Tonga severed the nation's only international subsea cable, cutting the island country off from the rest of the world for several weeks (United Nations Office for Disaster Risk Reduction, 2022).

Beyond earthquakes and volcanic activity, extreme weather events linked to climate change are increasing the risk of cable damage. Powerful hurricanes and typhoons generate submarine landslides, particularly in continental shelf regions where cables are buried at shallow depths. As climate change intensifies, the likelihood of such events disrupting telecommunications infrastructure is expected to rise (Internet Society, 2023; Network Computing, 2023).

Systemic Infrastructure Weaknesses

Subsea cables have inherent physical vulnerabilities due to their construction and placement. While modern cables feature multiple layers of protective sheathing, they remain susceptible to manufacturing defects, aging infrastructure, and weak cable junction boxes (Tagliapietra, 2024; Runde et al., 2024). However, only about 4% of total subsea cable failures are full system failures and this number has been steadily reducing over time (Bafoutsou et al., 2023).

Aging infrastructure also poses long-term risks. Many active cables today were installed over 20 years ago, meaning they are approaching or surpassing their intended operational lifespan (Runde et al., 2024). While some regions have invested in new cable systems, others— notably in lower resources countries and areas and geographically isolated island states— remain heavily reliant on outdated infrastructure (Farge, 2024; Guarascio, Nguyen, & Brock, 2024; Submarine Networks, 2011).

Strategic and Geographic Vulnerabilities

Strategic choke points in the global subsea cable network create significant vulnerabilities where multiple high-capacity cables converge in specific geographic regions (Bafoutsou et al., 2023; Thompson, 2025). While physical route redundancy provides some protection, many regions rely on a small number of high-capacity subsea cables, making them vulnerable to both accidental and intentional disruptions (ICPC, 2022). Additionally, the lack of repair capabilities poses additional complications and vulnerabilities, particularly in geographically remote areas and in the event of multiple cable outages (Crisis24, 2024).

Geographical Choke Points

Certain maritime regions serve as key choke points in the global subsea cable network. Among the most vulnerable are the Red Sea and the Strait of Malacca, where multiple cables cross in close proximity (Runde et al., 2024; Crisis24, 2024).

The Red Sea and Suez Canal region is particularly vulnerable due to its role as a hub for 16 high-capacity cables, linking Europe, Africa, and Asia. In June 2023, an accidental cut to the Asia-Africa-Europe-1 (AAE-1) cable in Egypt led to severe outages, causing Ethiopia to lose 90% of its connectivity and Somalia to experience an 85% reduction in internet access (Burgess, 2022). Given the high concentration of international cables in this route, a coordinated attack on multiple cables could cause cascading failures across multiple continents.

Similarly, the Strait of Malacca, one of the world's busiest shipping lanes, serves as a key transit point for subsea cables linking the Indo-Pacific to Europe and North America. Approximately 90,000 ships pass through this narrow sea lane annually, facilitating about 40% of global trade (Hellenic Shipping News, 2024). Given the volume of maritime traffic, accidental damage from anchors and fishing activities is a persistent concern. However, regional security analysts and government officials, particularly in the United States and Southeast Asia, have raised growing concerns about the potential for hostile state and non-state actors to exploit this choke point (Indo-Pacific Affairs, 2024). Such disruptions could target critical infrastructure, sever key cables, or interfere with data transmissions, potentially affecting military communications, financial markets, and internet connectivity for millions across Asia (Indo-Pacific Affairs, 2024).

Limited Repair and Recovery Capacity

The limited capacity to quickly repair subsea cables is one of the weakest links in global telecommunications security. The process of fixing a damaged cable involves specialized repair vessels that must locate, retrieve, and splice the affected segment (Monaghan & Darrah, 2024). However, the number of such vessels is extremely limited, and they are often stationed far from the location of the disruption (European Union Institute for Security Studies, 2024). In the case of multiple simultaneous disruptions, as seen in Taiwan in 2023, the limited number of repair

ships globally can result in prolonged downtime and economic losses (Runde et al., 2024; Sze, 2023).

Currently, there are only a few dozen cable repair ships worldwide, and many are concentrated in Europe and North America. This lack of availability means that repairs in remote regions—such as the Pacific Islands or Arctic waters—can take weeks or even months (Bafoutsou et al., 2023). For instance, after the 2022 volcanic eruption in Tonga severed the country’s only submarine cable, the nation was without internet access for five weeks while waiting for a repair ship to arrive from Fiji (UNDRR, 2022).

In the event of an international conflict involving the severing of subsea cables, nations would face significant challenges due to the limited availability of specialized repair ships. With only about 60 such vessels worldwide, primarily concentrated in Europe and North America, demand for these ships would surge, leading to potential competition among countries for their services (Runde et al., 2024). This scarcity is further exacerbated by the fact that repairs can take several weeks, depending on the location and severity of the damage (Jackson, 2024). For instance, repairing damaged cables in the Red Sea can take at least eight weeks due to permitting requirements and logistical challenges (Monaghan & Darrah, 2024). The U.S. Navy only operates one specialized repair ship, the *USNS Zeus* (Cable Laying/Repair Ship -T-ARC, 2021). As such, the U.S. largely relies on private operators whose fleets are aging and may be ill-equipped to handle extensive damage during wartime (Caro, 2024).

Beyond logistical challenges, international regulatory hurdles further slow the repair process. Many subsea cables cross multiple jurisdictions, requiring approval from multiple governments before repairs can begin (CRS, 2023). In contested areas such as the South China Sea or the Eastern Mediterranean, political disputes can delay or even block repair efforts (Caro, 2024). A critical concern for the U.S. is China’s control over repair fleets, concentrated particularly in the South and East China Seas, some of which are owned by state owned enterprises. This gives China potential advantages that could be leveraged for intelligence gathering during the repair process (Caro, 2024).

Deliberate Sabotage and State-Sponsored Threats

While most disruptions to subsea cables result from accidental damage, as demonstrated in our analysis of major attacks, there is growing evidence that state-sponsored sabotage is an emerging threat (Cwalina, 2022). Nations with advanced deep-sea capabilities, such as Russia and China, have developed the ability to disrupt subsea cables in both peacetime and wartime scenarios (Cwalina, 2022; EUISS, 2024). Acts of sabotage can be disguised as routine maritime incidents, making it difficult to attribute attacks and respond accordingly (Bell, 2025; Runde et al., 2024).

Multiple incidents of cable damage in contested regions have raised concerns about deliberate sabotage as a form of geopolitical pressure. For example, Taiwan has experienced repeated cable disruptions, with authorities investigating a Chinese-crewed ship suspected of severing a subsea communications cable in the latest such incident, adding to mounting tensions between Taipei and Beijing (AP News, 2025).

Potential for Coordinated Attacks

The most concerning potential scenario for the U.S. and its allies is a coordinated, multi-cable sabotage event, where multiple subsea cables are cut simultaneously, overwhelming global repair capabilities. Given that the majority of global internet traffic passes through a limited number of high-capacity cables, a well-planned attack could disrupt financial markets, military communications, and global commerce (Burgess, 2022). Additionally, a coordinated attack on multiple cables could significantly degrade military response capabilities in a crisis for international alliances such as NATO (Nakamura, 2023).

One potential attack scenario could involve targeting multiple cables in a key choke point such as the Red Sea, effectively severing connectivity between Europe, Africa, and Asia. Another scenario could involve simultaneous attacks on transatlantic cables. These risks have prompted NATO and the European Union (EU) to begin developing contingency plans, including increased monitoring of subsea infrastructure and military protection of key cable routes (Leicester & Burrows 2025).

Threats to Cables Supporting U.S. Military and NATO Communication

The vulnerabilities of subsea cables have far-reaching consequences for U.S. and NATO security, as the majority of NATO's operational communications—including military command and control, intelligence-sharing, and encrypted diplomatic messaging—rely on subsea cables, making them a critical target for adversarial state actors (Runde et al., 2024). For decades, NATO has depended on commercially owned and operated subsea cables for secure data transmission. The most critical cables for NATO operations include those connecting North America to Europe, particularly the transatlantic cables that run between the U.S., the U.K., and mainland Europe (McNamara, 2024). These cables serve as the primary communication links for U.S. military forces stationed in Europe and for intelligence-sharing between NATO members (Wall & Morcos, 2021). A coordinated attack or disruption affecting multiple cables simultaneously has the potential to significantly degrade NATO's crisis response capabilities in the short term.

Espionage and Cybersecurity Threats

Beyond physical sabotage, subsea cables are prime targets for espionage, as they carry vast amounts of sensitive governmental, military, and financial data (Wall & Morcos, 2021).

Intelligence agencies and state actors have developed sophisticated methods to intercept or manipulate subsea cable traffic, ranging from deep-sea cable tapping to cyber infiltration at cable landing stations (Khazan, 2013). Unlike a direct attack, which risks provoking international retaliation, espionage and cyberattacks can be conducted more covertly, making these tactics an effective strategy for states to disrupt the transmission of data across subsea cable infrastructure.

Cable Tapping and Data Interception

One form of subsea surveillance involves cable tapping, where intelligence agencies capture data flowing through fiber-optic lines by creating a physical or electronic access point that diverts and copies the light signals without disrupting the original traffic (Khazan, 2013). This process typically uses 'intercept probes' that bounce the light through a prism, make a copy of it, and turn it into binary data without disrupting the flow of the original internet traffic (Khazan, 2013). Although deep-sea cable tapping is technically difficult, major state actors—particularly the United States, Russia, and China—possess the necessary technology to conduct such operations (Runde et al., 2024).

Historically, the United States National Security Agency (NSA) pioneered deep-sea tapping techniques under operations such as Ivy Bells, in which American submarines placed covert listening devices on Soviet subsea cables during the Cold War (Sontag et al., 1998). While encryption and security measures have improved since then, modern intelligence agencies continue to develop methods to intercept data as it travels across global networks.

Russia has also developed sophisticated capabilities for subsea surveillance and interception. Russia's Main Directorate of Deep-Sea Research (GUGI)-operated submarine *Losharik* and intelligence vessel *Yantar* are capable of deploying remote-operated vehicles (ROVs) to tap or manipulate fiber-optic cables (Runde et al., 2024). These operations remain difficult to detect, as they can be carried out thousands of meters below the ocean surface, where most surveillance systems are ineffective.

There have also been concerns, particularly in the U.S., that China's dominance in global cable manufacturing enables companies to potentially embed surveillance capabilities into newly installed infrastructure (Runde et al., 2024). In 2018, the Japanese government reportedly discovered a Chinese wiretapping device on a cable near Okinawa, confirming security risks associated with increased Chinese involvement in the global cable network (EUISS, 2024). With Chinese companies rapidly expanding their presence in the submarine cable construction and repair industry, some experts fear that Beijing could use its industry influence to monitor or manipulate international data flows (Financial Times, 2024).

Cable Landing Stations

Although much of the discussion on subsea cable security focuses on threats beneath the ocean, cable landing stations—the facilities where subsea cables connect to terrestrial

networks—represent equally critical vulnerabilities. Unlike cables on the seabed, which require advanced submersibles and specialized equipment to access, landing stations are fixed, physical locations that can be infiltrated through cyber or physical means (Bafoutsou et al., 2023).

One of the most concerning threats at landing stations is the potential for cyberattacks targeting network management systems (Sherman, 2021). Landing stations represent vulnerable points in the subsea cable network. The trend toward modernization has introduced new risks, as many operators have shifted from isolated management systems to internet-connected network management platforms, creating potential entry points for cybersecurity threats that previously did not exist (Bafoutsou et al., 2023). If an adversarial state gains access to software controlling data flow through a landing station, they could potentially reroute, manipulate, or even shut down global communications without needing to physically sever the cable (European Commission, 2024).

Additionally, physical security at landing stations is often minimal, making them vulnerable to covert sabotage or infiltration by intelligence operatives. In 2021, reports surfaced that suspected Russian operatives had mapped cable landing stations across Western Europe, raising concerns about potential future sabotage efforts (Burgess, 2022).

Emerging Cyber Threats to Cable Software

As global telecommunications infrastructure becomes increasingly digitized, new cybersecurity threats to subsea cables are emerging. Long-term state-sponsored cyber espionage operations now target the software controlling subsea cable networks, rather than just the physical infrastructure itself (Coker, 2024).

One growing concern is the potential for cyberattacks against submarine cable traffic management systems. Modern subsea cables are equipped with automated software that manages data flow, reroutes traffic, and detects anomalies (Patel, 2025). If hackers compromise these systems, they could disrupt global internet traffic without ever touching the cable itself (Sherman, 2021).

Additionally, nation-states are developing offensive cyber capabilities aimed at submarine optical transmission systems. In 2022, reports surfaced that Russian cyber units had attempted to access control systems of European submarine cable networks, potentially as a preliminary measure for future cyberattacks (Cwalina, 2022). Given the increasing reliance on cloud computing, artificial intelligence, and digital finance, the consequences of a cyberattack on global data traffic could be just as severe as a physical cable disruption.

Implications

Subsea cables remain highly vulnerable to accidental damage, natural disasters, sabotage, and espionage. Maritime activity is the leading cause of disruptions, but geopolitical tensions have increased concerns over state-sponsored attacks, particularly from Russia and

China. Strategic choke points like the Red Sea and the Malacca Strait are particularly at risk, where a single cable cut can have cascading global effects. The potential for multi-cable sabotage or cyber intrusions highlights the growing threat to global stability and security. As subsea cables become even more essential to the digital economy and military operations, their protection will remain a critical challenge.

International Agreements and Forums

The topic of subsea cables and their security is prevalent in discussions of maritime legislation and agreements because the cables primarily reside in international waters. The first convention addressing the issue was the 1884 Paris Convention, followed by the Geneva Conventions of the Continental Shelf and High Seas in 1958, and the United Nations Convention on Law of the Sea (UNCLOS) in 1982 (Convention for the Protection of Submarine Telegraph Cables, 1884; Geneva Conventions of the Continental Shelf and High Seas, 1958; United Nations Convention on the Law of the Sea, 1982). These conventions established several provisions of the sea responsible for shaping jurisdiction that protects the internet's hidden highway of subsea cables.

International Agreements

There are several major international agreements governing subsea cable. These include the Paris Convention of 1884, the Geneva Conventions of 1958, the United Nations Convention on the Law of the Sea, and the Law of Armed Conflict.

The Paris Convention of 1884

To understand how international forums and agreements can be used to protect and maintain the growing web of subsea cables, it is important to examine the development of international legislation regarding these cables. The Paris Convention of 1884 preceded the widely accepted United Nations Convention on Law of the Sea by 98 years, but the Paris Convention remains the basis for the modern maritime law that presides over the protection of subsea cables (Convention for the Protection of Submarine Telegraph Cables, 1884; United Nations Convention on the Law of the Sea, 1982).

The 1884 Paris Convention is specific to subsea telegraph cables, outside of territorial waters—which is defined as 12 nautical miles from the state's shore. The Paris Convention uses the term “high seas” to refer to the expanses of ocean that extend beyond the territorial waters as its provisions only apply to the sections of subsea cables that lie in international waters. The assumption is that party states would have domestic policy that protect subsea cables in territorial waters (Convention for the Protection of Submarine Telegraph Cables, 1884).

The Paris Convention introduced the provisions to international law that enabled prosecution for deliberate or culpable negligent damage to cables in the high seas as well as the liability for repairs and compensation in Articles II, IV, and VII (Convention for the Protection of Submarine Telegraph Cables, 1884). Under Article X, party states are responsible for trying officers of their nation with domestic institutions should they be indicated as liable for meaningful interference or culpable damage to cables in international waters (Convention for the Protection of Submarine Telegraph Cables, 1884). The same provision permits visitation

powers to other party states should investigation of other party states be warranted. While this power could lead to escalation of conflict, it provided a level of enforcement of subsea cable protection that is lacking in subsequent agreements even though it only pertains to incidents in the high seas (Convention for the Protection of Submarine Telegraph Cables, 1884).

The treaty was ratified by the United States, Russia, and 34 other signatories (Convention for the Protection of Submarine Telegraph Cables, 1884). The terminology introduced by the Paris Convention would be expanded upon and defined later in the more widely ratified Geneva Conventions of 1958.

The Geneva Conventions of 1958

The Geneva Conventions of 1958 were the first conventions to establish specific zones with varied levels of jurisdiction: the territorial sea, contiguous zone, and continental shelf. These different zones have different jurisdictions regarding the laying and protection of subsea cables. The first designated zone is the territorial sea, which is measured 12 nautical miles from the baseline of the coast at low tide and is considered part of the nation and subject to its jurisdiction (United Nations Convention on the Territorial Sea and the Contiguous Zone, 1964). The contiguous zone is introduced in Article 24 is a zone that extends an additional 12 nautical miles from the territorial sea within which the coastal state is limited to juridical control over “customs, fiscal, immigration or sanitary regulations” (United Nations Convention on the Territorial Sea and the Contiguous Zone, 1964). The Convention of the Continental Shelf describes the continental shelf as a zone outside of a nation’s territorial waters at 200 meters (United Nations Convention on the Territorial Sea and the Contiguous Zone, 1964). Coastal states are permitted to utilize resources from the continental shelf as long as it does not obstruct the freedoms outlined in the Geneva Conventions of 1958.

The Geneva Conventions of the Continental Shelf and High Seas of 1958 were a result of the United Nations expanding the protection of the 1884 Paris Convention to include non-telegraph cables like telephone and power cables as specified in Article 26 and 27 (Geneva Conventions of the Continental Shelf and High Seas, 1958). The conventions reiterate the provisions of the 1884 Paris Convention while adding further protections to rights of resources on the high seas for coastal and non-coastal states alike (Geneva Conventions of the Continental Shelf and High Seas, 1958). Article 2 establishes four freedoms as protected rights that are listed as follows: (1) Freedom of navigation; (2) Freedom of fishing; (3) Freedom to lay submarine cables and pipelines; (4) Freedom to fly over the high seas (Geneva Conventions of the Continental Shelf and High Seas, 1958, pg 81).

These freedoms of the international waters impose a need for enforceable jurisdiction on the high seas which is addressed by Articles 4 to 13 outlining any nation’s rights to a “Flag State” (Geneva Conventions of the Continental Shelf and High Seas, 1958). This terminology refers to the nationality of a ship as demonstrated by what flag it sails under. The principles of a

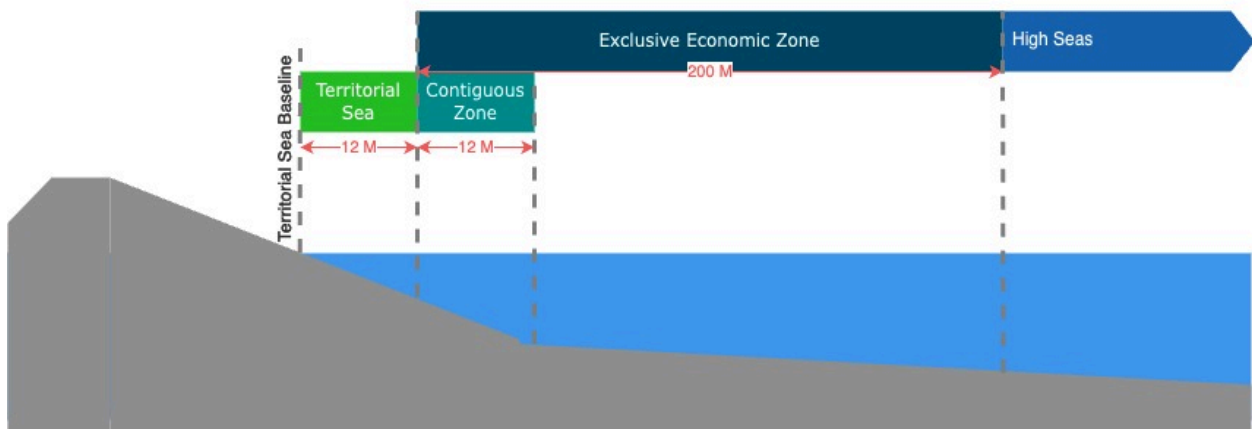
flag state were introduced in the 1884 Paris Convention; however, the Geneva Conventions of 1958 reinforced the conventions of flag states while omitting authority of other nations to incriminate and investigate other ships on the high seas as outlined in Article X of the Paris Convention (Convention for the Protection of Submarine Telegraph Cables, 1884).

The 1958 Geneva Conventions was ratified by 16 more countries with 41 signatories and 52 parties including Russia and the United States (United Nations Convention on the Territorial Sea and the Contiguous Zone, 1964). This convention established the laying of subsea cables as a right, outlined several zones of the ocean, and omitted the visitation rights of the 1884 Paris Convention without providing alternative means of enforcement in the high seas. This flaw would be reiterated in the United Nations Convention on the Law of the Sea 24 years later (United Nations Convention on the Law of the Sea, 1982).

The United Nations Convention on the Law of the Sea

In 1982, the United Nations held a Convention on the Law of the Sea which compiled many provisions of past treaties and either built upon or diverged from them (United Nations Convention on the Law of the Sea, 1982). The United Nations Conventions of the Law of the Sea (UNCLOS) reiterates the parameters and restrictions of the territorial and contiguous zone in addition to designating another zone. The exclusive economic zone, or the EEZ, extends 200 nautical miles from the territorial sea and is granted to the coastal state for access to its resources (United Nations Convention on the Law of the Sea, 1982). Figure 4 illustrates the zones reinforced by UNCLOS each with its own set of legislation marked by nautical miles (M) away from the territorial sea baseline (United Nations Convention on the Law of the Sea, 1982).

Figure 4: Zones of the Sea



In Article 58, the treaty includes a provision that protects the rights to lay subsea cables in the EEZ, stating:

In the exclusive economic zone, all States, whether coastal or land-locked, enjoy, subject to the provisions of this Convention, the freedoms referred to in Article 87 of navigation and overflight and of the laying of submarine cables and pipelines, and other internationally lawful uses of the sea related to these freedoms, such as those associated with the operation of ships, aircraft, and submarine cables and pipelines, and compatible with the other provisions of this Convention. (United Nations Convention on the Law of the Sea, 1982, pg 44)

There are several complex overlapping jurisdictions within the designation of the EEZ as it relates to subsea cables. Although UNCLOS distinguished the EEZ from the high seas, the second addendum to Article 58 calls for flag state jurisdiction within the EEZ pertaining to the subsea cables meaning that because subsea cables are considered resources, all nations have a right to lay them within the EEZ. Thus, all judicial responsibility is assigned to the flag state of the ship that lays or maintains the cables (United Nations Convention on the Law of the Sea, 1982). The laying of subsea cables is also permissible for any state in the continental shelf as long as the coastal state consents to any delineations as asserted in Article 79. However, as stated in Articles 2 and 33, the jurisdiction over subsea cables belongs to the coastal state within the contiguous and territorial zones as a state's sovereignty extends into its territorial waters and the state is responsible for regulation within the contiguous zone (United Nations Convention on the Law of the Sea, 1982).

Articles 112 through 115 are dedicated to the protection of subsea cables. The right for all states to lay cables in the high seas is repeated in Article 112 while Articles 113 through 115 address the repercussions for deliberate and negligent damage to subsea cables (United Nations Convention on the Law of the Sea, 1982). While under the jurisdiction of that nation's flag state on the high seas, Article 113 calls for party states to "adopt laws and regulations" that prosecute offenders responsible for damaged cables due to deliberate interference or "culpable negligence"—culpable negligence being recklessness or negligence that causes punishable harm (United Nations Convention on the Law of the Sea, 1982). The 114th and 115th Articles also require party states to assign the responsibility of reparations to owners of cables liable for damage to another cable when performing repairs on their own assets and also requires reimbursements for persons and vessels that lose anchors, or other assets, in an attempt to spare subsea cables (United Nations Convention on the Law of the Sea, 1982). These provisions grant prescriptive jurisdiction to party states, allowing for states to constitute their own laws and regulations regarding compensation for damaged subsea cables.

The Convention on the Law of the Sea was signed by 157 members and ratified by 170 parties including China and Russia (United Nations Convention on the Law of the Sea, 1982). Although it was not signed by the United States until the 1994 amendment and it has not been ratified by the Senate, the U.S. recognizes UNCLOS as customary international law due to its

widespread acceptance (Statement of Roger Rufe President, The Ocean Conservancy {PRIVATE} Before the Senate Committee on Foreign Relations, 2003).

UNCLOS is not without its criticisms and impotence. The visitation powers granted by Article X of the Paris Convention of 1884 are never reauthorized in subsequent conventions including UNCLOS, meaning that the only vessels permitted to investigate incriminating behavior on the high seas and within the EEZ are other vessels under the same flag state. Additionally, Article 113 of UNCLOS delegates the trust of legislating to individual party states. Article 114 of UNCLOS assigns fiscal responsibility to private actors who may damage cables for the purpose of funding repairs of those cables, the same fiscal responsibility is not applied to the case of state actors described in the preceding Article 113 (United Nations Convention on the Law of the Sea, 1982). While UNCLOS has reasserted that deliberate or negligent damage to subsea cables is a punishable offense, its provisions do little to inspire accountability amongst party states in the high seas and EEZs.

The Law of Armed Conflict

The Law of Armed Conflict (LOAC) consists of several conventions from 1863 to 2005 that provide international policies for conduct in active warfare (DOD, 2015). The Oxford Convention of 1913 specifies the neutrality of subsea cables and when it is permissible for “belligerent states” to cut them in war, the only immune cables being those between two neutral states (Oxford, 1913). The cutting of any cables during wartime is permitted because they are considered a military objective as long as economic, governmental, and military data are routed through subsea cables (DOD, 2015). However, cut cables impact more than military targets, the ramifications extend to the civilian population and the economy of the impacted state (Guilfoyle et al, 2022). The legislation that allows this was written following World War I when subsea cables were primarily telegraph cables connecting government officials to other international state officials (Hayes, 2008; Guilfoyle et al, 2022). In the 20th century the world was less interconnected than today, so permitting the cutting of cables would have been less impactful especially to civilians (Hayes, 2008). The reasons behind this legislation no longer fit our interconnected and interdependent world, where cable cuttings would have far-reaching ramifications for both civilians and military.

International Forums

The dialogue on the protection of subsea cables is the subject of several international forums including the International Telecommunication Union, the International Cable Protection Committee, and their joint advisory body, the International Advisory Body for Submarine Cable Resilience. The collaboration of these congregations is essential for progress in securing subsea cables through international efforts.

The International Telecommunication Union

The International Telecommunication Union (ITU) was established in 1865. The ITU is part of the UN, and consists of 194 state members which includes China, Russia, and the U.S. as state members (International Telecommunication [ITU], n.d.b). The ITU plays the role of a broker for international telecommunication arrangements, including subsea cables, with the goal of providing telecommunication access to all states; however, only member states can participate in conventions (ITU, n.d.a, 1992). The lack of representation of sector members of the telecommunication industry has been a point of contention for parties in favor of multi-stakeholder governance of the internet. The ITU has a set of regulations adopted by members in the form of the International Telecommunication Regulations (ITR) agreement (ITU, 2012b). In 2012, the ITU broadened the scope of its ITR and its agreement of internet governance to regulate “authorized operating agencies” which includes subsea cable companies (ITU, 2012b). The United States responded with a rejection of the propositions: “The United States will oppose efforts to broaden the scope of the ITRs to empower any censorship of content or impede the free flow of information and ideas” (ITU, 2012a).

Per contra, China and Russia became signatories of the ITR proposed at the World Conference on International Telecommunications of 2012 (ITU, 2012b). The division between member states of ITU over internet governance undermines the organization’s ability to facilitate treaty-level agreements and policies in the international telecommunication space that could protect subsea cables.

The International Cable Protection Committee

In contrast to the ITU, the International Cable Protection Committee (ICPC) established in 1958 accepts “cable ship owners, operators, cable manufacturers and others involved in the industry,” as voting members. Governmental representatives are barred from voting and serving on the Executive Committee (International Cable Protection Committee [ICPC], 2023). However, subsea cable industry members can attend as representatives of their nation of origin; China has six corporations participating as members and the U.S. has 42 corporate representatives (ICPC, 2025b). The activities of the ICPC are stated as the following:

- Promote awareness of submarine cables as critical infrastructure to governments and other users of the seabed
- Establish internationally agreed recommendations for cable installation, protection and maintenance
- Monitor the evolution of international treaties and national legislation and help to ensure that submarine cable interests are fully protected
- Liaison with UN Bodies. (ICPC, 2025a)

The ICPC also published a best practices guide in 2020 for the protection and care of subsea cables that reiterates the applicable policies within UNCLOS with the addition of

industry-specific insights like the regulation of “fish aggregating devices (FADs),” the use of “automated identification systems (AIS),” and the establishing of “cable protection zones” (ICPC, n.d.). The distinction of these recommendations as enforceable international regulations would allow for higher-fidelity policies that protect subsea cables from intentional and unintentional damage but given that the ICPC has no international jurisdiction, there is no impetus for nations to abide by these recommendations.

The International Advisory Body for Submarine Cable Resilience

The International Advisory Body for Submarine Cable Resilience (SCR) was established November 2024 in a partnership between the ITU and ICPC with 40 leaders representing different regions of the world, including representatives from the United States and China (ITU, n.d.c). The SCR was established with the goal of “promoting dialogue and collaboration on potential ways and means to improve the resilience of this vital infrastructure that powers global communications and the digital economy.” However, in a press briefing from December 4, 2025, ITU Deputy Secretary General, Tomas Lamanauskas, reported that “the body is not set up to investigate specific incidents or attribute the causes of the incidents,” (ITU, n.d.c., 2025b) Regardless of the capabilities of the SCR, this new advisory body offers another opportunity between governmental and sectoral representatives to improve international legislation protecting subsea cables. In the first SCR Summit held on February 26th and 27th of 2025, many of the panels called attention to the same concerns—such as the previous lack of multi-stakeholder dialogue for subsea cable protections, incorporation of the ICPC Best Practices into UNCLOS, as well as a call for these cables to be classified and prioritized as critical infrastructure internationally (ITU, 2025a).

Key Case Studies: Baltic Sea, South China Sea, Red Sea

While subsea cables break all over the world, the subsea cables purposefully damaged are concentrated in three places globally. In order to understand the circumstances around these major attacks on subsea cable infrastructure, we chose to highlight three regional case studies: the Baltic Sea, the South China Sea, and the Red Sea. These three maritime regions were selected for their relatively high concentration of cables and incidents of damage to those cables—in each case driven by complex geopolitical dynamics involving actors in the region and often the U.S., China, or Russia. Each case study examines the subsea cable infrastructure in the region, geopolitical conflicts involving states and other actors with the potential to impact cables, major incidents causing damage to cables, and unilateral and multilateral responses to these incidents. Taken together, these case studies offer details of how international law and geopolitical dynamics appear in specific regions and incidents, and the global implications of threats to subsea cable infrastructure in the Baltic Sea, Red Sea, and South China Sea.

Baltic Sea

Spanning approximately 149,000 square miles, the Baltic Sea has shallow waters and narrow basins. It is only accessible via three narrow choke points: the Great Belt, the Little Belt, and Øresund—all located in the Danish Straits of Kattegat and Skagerrak (Pawlak, 2024; Encyclopædia Britannica, 2025). Since 2022, about ten subsea cables have been cut that connect the region, with seven of those cuts occurring between November 2024 and January 2025 (Buchholz, 2025). A majority of these incidents have raised suspicions of sabotage by state actors, specifically Russia and China, who have been particularly active in the region (Buchholz, 2025).

The increasing frequency of subsea cable incidents has propelled the Baltic Sea region to the forefront of international geopolitical discussions. As the Baltic Sea nations confront the vulnerabilities of their subsea cable infrastructure, addressing the region's resilience amidst a shifting security landscape has become increasingly paramount.

Infrastructure

The Baltic Sea hosts a significant subsea cable network, with over 35 cables connecting the countries bordering its waters (Dufetre, 2023). This network is crucial to the region's telecommunications and maritime infrastructure. Several telecommunications companies in the region have significant stakes in supporting this infrastructure. Arelion, a Swedish telecommunications company, owns about 17 regional cables, including the EE-S1 and the BCS East-West Interlink, both of which have sustained damage recently (Dufetre, 2023; Voltri & ERR News, 2023). Similar to Arelion is the Finnish Telecommunications and digital services company, Elisa Corporation. While Elisa has approximately three cables in the Baltic Sea, which is less than

Arelion, it is nonetheless one of the companies whose cables have been damaged, namely the FEC-1 and FEC-2 (Elisa, n.d.; Lott, 2024; Dufetre, 2023). Furthermore, the largest suppliers in the region are Ericsson, a Swedish telecommunications company, and the French company, Alcatel Submarine Networks (ASN), who is one of the largest manufacturers and installers of subsea cables (Ericsson, n.d.; & Alcatel Submarine Networks, n.d.).

The subsea cable Eastern Light Sweden-Finland II, built by the Swedish company Eastern Light, will become operational later this year (TeleGeography, n.d.). Eastern Light is also planning future subsea cable projects, including EL Baltic Sea East, EL Baltic Sea West, and EL Baltic Sea Crossing, although no conclusive launch dates have been set (Eastern Light, n.d.).

Table 2 displays data on the cables in the Baltic Sea that have been suspected of intentional damage. The data includes the date of incident, cable name, length in miles, owners, and supplier.

Table 2: Baltic Sea Cables Damaged in Suspected Attacks⁵

Date of Incident	Cable Name	Cable Length (Miles)	Cable Owners	Supplier
October 2023 ^a	Sweden-Estonia (EE-S1) ^c	149 ^a	Arelion (formerly Telia Carrier), GN Great Nordic, Telia Eesti (formerly Eesti Telekom, EMT, Elion) ^a	ASN ^a
November 2024 ^a	BCS East-West Interlink	135 ^a	Arelion (formerly Telia Carrier) ^a	Ericsson ^a
November 2024 ^a	C-Lion1	728 ^a	C-Lion1 ^a	ASN ^a
December 2024 ^a	Estlink 2	105 ^b	Fingrid, Elering ^b	--
December 2024 ^c	Finland Estonia Connection 1 (FEC-1) ^c	155 ^d	Elisa Corporation ^c	ASN ^c
December 2024 ^c	Finland Estonia Connection 2 (FEC-2) ^c	155 ^d	Elisa Corporation ^c	ASN ^c

Geopolitical Landscape

Russia’s 2022 invasion of Ukraine ushered in a new geopolitical reality for the Baltic Sea region, as it has forced the bordering countries to confront a rapidly shifting security landscape. In response, Sweden and Finland made the unprecedented decision to join the North Atlantic Treaty Organization (NATO), creating a “NATO Lake” as nine out of the ten countries in the

⁵ Table data from: ^aDufetre (2023). ^bFingrid (2017). ^cTelegeography (n.d.). ^dSouisa (2024).

region are NATO members (Kayali, 2023). With NATO's hold on the Baltic Sea nations strengthening and Moscow's persistent perception of NATO expansion as a strategic threat to its interests, tensions are being exacerbated within the region in an already inflamed security environment (Rahr, 2025).

The Baltic Sea, like the Red Sea's Gulf of Suez and the Bab el Mandeb Strait, is a shallow body of water, with an average depth of only about 180 feet (Brennan, 2025) The shallow depth makes the subsea cables more accessible because they lay closer to the surface. The Baltic Sea is also a central commercial trading hub, with as many as 4,000 ships passing through daily (Brennan, 2025). The combination of shallow depth and significant shipping traffic makes the Baltic Sea regions subsea cables more susceptible to intentional or unintentional damage. The accessibility of subsea cables to hostile actors, combined with rising tensions between Russia, the Baltic Sea nations and NATO has created a geopolitical hotspot.

Within the Baltic Sea region, the primary threat actor to subsea cable infrastructure is Russia. The region is known as the 'Achilles heel' of Europe, because it is particularly vulnerable to Russian attacks due to its proximity to the ports of St. Petersburg and the Kaliningrad enclave (Desmarais, 2024). A comprehensive report released in April 2023 by Sweden's Television et al. (2023) outlines Russia's decade-long large-scale activities mapping critical infrastructure in the North and Baltic Sea. The report specifically highlights the operation of 50 Russian ships in these waters, equipped with surveillance and advanced technology (Motrunych, 2023). Many of the ships were operating without their Automatic Identification System (AIS) enabled—a system crucial for ship crews to know their location and those of surrounding ships. The manipulation of this data, also known as AIS spoofing, creates potential for disorder and collisions, and undermines maritime order as it is difficult to take retaliatory measures against these vessels (Braw, 2024; Motrunych, 2023).

Coupled with Russia's persistent subsea mapping is its rapidly advancing naval capabilities. Stationed in Olenya Guba, off the coast of the Barents Sea, is Russia's military fleet of special-purpose vessels (Trakimavičius, 2021). These advanced vessels include intelligence ships, auxiliary submarines, and reconnaissance vessels that can hold deep-diving submersibles and drones for subsea engineering missions, all under the operations of Russia's General Staff Main Directorate for Deep Sea Research (GUGI) (Trakimavičius, 2021). Russia's increasingly confrontational nature and expansion of naval fleets and equipment are exacerbating the Baltic Sea countries' concerns about cable spying and sabotage.

While Russia is currently the primary threat in the region, China's expanding involvement is heightening apprehensions about the risks posed to subsea infrastructure. In 2020, the United States warned Europe about China's growing presence in the telecommunications industry, citing concerns over the usage of Chinese-made components in telecommunications infrastructure. However, Europe dismissed this warning, as at the time, it did not share the same threat assessment (Besch & Brown, 2024). But later, in January 2024,

the European Parliament passed a resolution highlighting the potential future implications of China's rising influence on European critical infrastructure (European Parliament, 2024). The report outlines the concerns about Chinese companies linked to the People's Liberation Army (PLA) acquiring European internet firms, China's HMN Technologies, and the high risk of cybersecurity and underwater surveillance (European Parliament, 2024). The report also calls on the European Commission to consider enacting new legislation to mitigate security risks related to subsea cables (European Parliament, 2024). Furthermore, allegations have been made that the Chinese vessel *Yi Peng 3*, involved in a recent subsea cable incident, was working on behalf of Russia. European officials also expressed suspicions over the vessel's crew, a Chinese captain and Russian sailor and the similarities of the AIS data to previous Russian shadow fleet vessels (Brovko, 2024; The Maritime Executive, 2024).

China and Russia's activity in the Baltic Sea have raised significant concerns about their intentions regarding subsea infrastructure. While Russia's maritime activities are not necessarily unusual, the intensification of its actions in a considerable weaponized capacity is raising questions. Coupled with this is the increasing assessment of China's activities relating to subsea infrastructure as a threat.

Major Incidents

In recent years, the frequency of subsea cable incidents in the Baltic Sea has increased significantly, highlighting the vulnerabilities of this infrastructure. On October 7th and 8th of 2023, the Baltconnector gas pipeline, two subsea cables connecting Finland and Estonia, and the EE-S1 subsea data cable connecting Sweden and Estonia were damaged (Chiappa & Ngendakumana, 2023). However, the overall functionality of the cables was not disrupted. The incident was attributed to the Chinese vessel *Newnew Polar Bear*, which had dragged its anchor for over 100 miles (Ministry of Defence, 2023; Tegler, 2023). Investigations revealed that the *Newnew Polar Bear*, and the Russia cargo vessel *Sevmorput* were present at the damage sites. The *Newnew Polar Bear* had also been found at the Russian port of Arkhangelsk with a missing anchor—the same anchor paint was discovered on the severed cable (Benner, 2025). Although Beijing initially denied the vessel's involvement, about ten months later, it admitted the Chinese flagged vessel was behind the incident, attributing it to “bad weather” (Benner, 2025).

Just over a year later, on November 17, 2024, the BCS East-West Interlink cable connecting Sweden and Lithuania was cut, resulting in about a fifth of Lithuania's internet capacity being reduced, although consumers were largely unaffected (Astier & Kirby, 2024). Less than 24 hours later, on November 18th, the C-Lion1 cable connecting Finland and Germany was also cut; however, consumers were not affected (Astier & Kirby, 2024). These incidents are believed to be related, with suspicions centering on the Chinese vessel *Yi Peng 3*. The vessel departed from the Russian port of Ust-Luga on November 15th, and maritime tracking data placed it at the exact time and place of breaches (Reuters, 2024). Following the cable cuts, the

Yi Peng 3 was held in the Kattegat Strait, with many Baltic leaders voicing concerns over suspected sabotage and the possibility that the captains or officers of the ship were bribed by Russian agents—no conclusive evidence has been found to corroborate these claims (Astier & Kirby, 2024; Pancevski, 2024). After tense negotiations with China, several officials from each of the affected countries were allowed to conduct inspections. A report has yet to be released and on December 21st, the *Yi Peng 3* was cleared to continue its journey (Benner, 2025; Swedish Coast Guard, 2024).

On December 25, 2024, just over a month after the severing of the BCS East-West Interlink and the C-Lion1 cables, the Estlink 2, the FEC-1, the FEC-2 connecting Finland and Estonia and C-Lion1 cables were cut by the Russian oil tanker *Eagle S* after it dragged its anchor for almost 62 miles (Lott, 2024). A unique vessel, the *Eagle S* bears a Cook Island flag, is registered with the United Arab Emirates, operated by an Indian company in Mumbai, and most of the crew is from India and Georgia (Benner, 2025). The ship is currently being detained in Finland, under the pretense of aggravated criminal mischief and interference with communications. Travel bans for nine of the crew members have also been put in place (Martin, 2025; Rintakumpu, Arts & Ondraskova, 2025). During the initial investigation, the *Eagle S* was found to have specific transmitting gear, laptops with Russian and Turkish language keyboards, and sensor-type devices; therefore, it is also suspected of being part of Russia's shadow fleet (Bockmann, 2024). Some European and U.S. intelligence analysts have suspected the incident to be accidental; however, the lead investigator and maritime experts argue otherwise, citing that the anchor weighs over 100 metric tons. Therefore, dragging that heavy of an anchor undoubtedly makes a significant amount of noise, and it would be impossible not to notice. Currently, investigations are ongoing and expected to continue over the next several months (Yadav, 2025; Martin, 2025).

International Response

In the wake of these incidents, the Baltic Sea countries are reassessing the vulnerabilities of their subsea infrastructure. This is coupled with a strong response from international organizations, which are initiating operations and action plans to protect subsea cable infrastructure and prevent future incidents.

Responses From States

As a response to these recent cable cuts, Finland, Sweden, and Lithuania have proactively initiated national measures to strengthen the resilience of their subsea networks. As a country that has been the victim of numerous attacks, Finland is diligently working with other Baltic Sea nations, including Sweden, Estonia and Germany, to conduct joint investigations (Bryant & Sauer, 2024). Additionally, Finland and Germany released a joint statement about how it is crucial to safeguard subsea infrastructure (Browne, 2024).

Finland's growing collaboration is due to its dedication to actively working with NATO—for instance, increasing the frequency of patrols around vital subsea cable areas. It is suspected that Russia's aggression is a result of Finland's accession to NATO (Braw, 2024; Wallace, 2024). Sweden also is showing strong support for inter-country collaboration and working towards Baltic Sea security. It has pledged to send up to three warships and a sea surveillance aircraft, the *ASC890*, from the Swedish Armed Forces to aid in monitoring subsea critical infrastructure and further investigate Russia's shadow fleet (Agence France-Presse, 2025). Lithuania is taking a unique approach to address subsea infrastructure vulnerabilities by fostering public and private partnerships. The Lithuanian Armed Forces have signed an agreement with Litgrid, the country's electricity transmission system operator, to enhance the security of critical subsea infrastructure in the Baltics (BBC, 2025).

Although the Baltic Sea nations are addressing subsea cable security issues individually, they also maintain strong regional collaboration and cooperation. On December 17, 2024, The Joint Expeditionary Force Leader summit in Tallinn between 12 countries yielded a strong response to Russia's growing shadow fleet—countries pledged to disrupt and deter this growing threat (Government Communication Unit, 2024). As part of a coordinated effort, maritime authorities are now requesting proof of insurance from suspected shadow vessels as they pass through the English Channel, Danish Straits of the Great Belt, which is the sound between Denmark and Sweden, and the Gulf of Finland (Government Communication Unit, 2024).

Furthermore, in early January 2025, the U.K. initiated a Joint Expeditionary Force (JEF), dubbed operation "Nordic Warden," which consists of the Baltic Sea nations, Iceland, Norway and the Netherlands to bolster security in the Baltic Sea, North Sea, English Channel, and Kattegat Strait (Ministry of Defense et al., 2025). Nordic Warden primarily utilizes artificial intelligence (AI) to analyze data from various sources and compile a system where shadow fleet vessels can be registered (Ministry of Defense et al., 2025). If a risk is detected, a widespread signal is spread to NATO and other allies. This JEF operation focuses on the protection of Critical Undersea Infrastructure, complementing NATO's actions to deepen military ties and interoperability between these countries (Ministry of Defense et al., 2025; & Moyer, 2024).

Responses From International Organizations

The threat to the Baltic Sea countries' subsea infrastructure has forced the European Union to evaluate how it can become more resilient against cable damage. On December 26, 2024, one day after the severing of the Estlink 2 cable between Finland and Estonia, the European Commission and the High Representative on the Investigation into the Damaged Electricity and Data Cables in the Baltic Sea released a joint statement (European External Action Service [EEAS], 2024). This statement not only commended Finland's rapid response to the incident but also reaffirmed the European Commission's strong and unwavering support for Finland, Estonia, and Germany (EEAS, 2024). It also proposed measures to protect Critical Undersea Infrastructure and address Russia's shadow fleet including enhanced information

sharing, developing repair capabilities, and creating new detection technologies to reinforce subsea safeguards (EEAS, 2024).

Then, on January 29, 2025, the European Commission, led by Equality Commissioner Helena Dalli, called for an EU-wide response to the mounting threats towards crucial subsea infrastructure in the Baltic Sea (CE Noticias Financieras: English, 2025). The European Commission, citing Russia's aggressive actions and China's increasing influence, stressed the need for a unified EU response (CE Noticias Financieras: English, 2025). Dalli reiterated the region's vulnerability to hybrid attacks and the EU's role in defending national critical infrastructure and bolstering European Security (CE Noticias Financieras: English, 2025).

Less than a month after this declaration, Henna Virkkunen, Executive Vice-President of the European Commission for Tech Sovereignty, Security and Democracy, presented the Joint Communication to strengthen the security and resilience of submarine cables (European Commission 2025). This EU-wide action plan, with its focus on prevention, detection, response, recovery, and deterrence, is designed with a long-term vision to ensure the security of subsea cables (European Commission, 2025). The primary actions included in this strategy are investing in cable resilience through new technology, increasing the ability to detect and respond to incidents before they occur, and enhancing surveillance capabilities and cooperation on intelligence data sharing. The goal of this new plan, which will take place between 2025 and 2026, is to expand the EU's subsea cable security in the face of a dynamic threat landscape (European Commission, 2025). The EU is taking the concrete steps needed to ensure Europe's subsea cable security, as the continued incidents in the Baltic Sea have displayed the vulnerabilities of subsea cables and the potential for destabilization through subsea cable destruction (European Commission, 2025).

In response to the recent string of subsea cable incidents in the Baltic Sea, NATO's Allied Command Operations (ACO) launched a new mission known as 'Baltic Sentry' on January 14, 2025. This mission aims to increase NATO military presence and build countries' resilience against future attempts at damage by an adversary (SHAPE Public Affairs Office, 2025). The Allied Joint Force Command Brunssum (JFCB) is leading the new mission and working closely with the Allied Maritime Command (MARCOM) and the NATO Maritime Centre for Security of Critical Underwater Infrastructure (NMCSCUI) (SHAPE Public Affairs Office, 2025). The strategy involves the deployment of a wide range of advanced assets, including frigates, maritime patrol aircraft, naval drones, and surveillance technology, all to counter the destabilizing actions posed by state and non-state actors (North Atlantic Treaty Organization, 2025). With the new mission underway, NATO is set to deploy uncrewed surface vessels (USVs), also known as drone boats, as part of the Baltic Sentry (Altman, 2025). The USVs will continuously monitor critical areas 24/7, delivering situational awareness via imagery and electromagnetic spectrums, generating it on various platforms (Altman, 2025).

Implications

In the midst of rising geopolitical tensions, the Baltic Sea region is confronting a new reality regarding threats and offensive actions against their subsea cable infrastructure. With Russia's expanding maritime activities, and China's increasingly assertive nature, the Baltic Sea nations and international organizations are realizing the very real threat to the subsea cables in the region. This realization is driving the urgency of collaborative efforts to implement more essential safeguards that ensure the safety and resilience of these cables.

South China Sea

The South China Sea spans 3.5 million square km wide across the western Pacific Ocean and lies south of China, west of the Philippines, east of Vietnam, and north of Malaysia, Brunei, Singapore, and Indonesia (Guo, 2018). The South China Sea holds valuable natural resources such as oil and gas and a fishing ground, functions as a high-volume shipping waterway, and is a central hub for subsea cables (Congressional Research Service [CRS], 2023; Guo, 2018; TeleGeography, n.d.). However, the sea is also a hot point of geopolitical contention. Overlapping territorial disputes, tense cross-strait relations between China and Taiwan, and increasing U.S.-China competition makes this region more and more challenging as an area to lay and maintain subsea cables.

The geopolitical conflicts over the South China Sea may have also led to increasing numbers of incidents involving cables. There have been three major instances of subsea cable damage that are suspected to be intentional state actions in the South China Sea, all involving cables connecting to Taiwan (Runde et. al, 2024). In 2023, two cables near Taiwan's outlying Matsu Islands were severed at the same time; in January of 2025, a cable was damaged off the northern coast of Taiwan; and in February of 2025, while this report was in progress, a cable linking Taiwan to its outlying Penghu islands was severed (Chang, 2025; Braw, 2023; Tobin et. al, 2025). It is difficult to infer if the cables were damaged accidentally or intentionally, but Taiwanese officials suspected the incidents were intentional efforts from China to pressure Taiwan politically (Chang, 2025; Braw, 2023; Tobin et. al, 2025).

Infrastructure

The South China Sea is a key area for subsea cables connecting Africa, Asia, Australia, Europe, and the Americas (Noor, 2024a). Many of these cables coalesce at landing points in Hong Kong and Singapore, the latter of which will be connected to over 40 subsea cables by 2028 (Noor, 2024b). Greater demand for internet connectivity and speed as well as investments in data centers in Southeast Asia have driven increased need for bandwidth, leading to more subsea cables in the region (Noor, 2024b).

Ownership of these cables varies. In Taiwan, as the largest telecommunications company, Chunghwa Telecom holds primary ownership of the subsea cables connecting to the

island (Wang. 2025). In contrast, the Trans-Pacific Express (TPE) cable—one of the cables damaged under suspicious circumstances—has multiple owners including AT&T, China Telecom, China Unicom, Chunghwa Telecom, KT, NTT, and Verizon; all of which share a joint investment of \$500 million (Submarine Cable Networks [SCN], n.d). They all have equal rights of vote and capacity ownership over the cable. TPE is also the subsea cable system that directly links the U.S. to China, Japan, and South Korea (SCN, n.d).

In terms of major suppliers, Japanese-based NEC is one of the main suppliers of subsea cables in the South China Sea, having built more than 400,000 km of cables (PR Release, 2024). NEC has also signed agreements with the Southeast Asia-Japan 2 consortium to build subsea cables that connect Singapore, Thailand, Cambodia, Vietnam, Hong Kong, Taiwan, China, Korea, and Japan (Qui, 2018). The company has also taken on various other projects in the South China Sea to manufacture and lay cables.

With the recent cable damages, there have been many delays on future subsea cable projects in the South China Sea due to tensions between China and the United States. Since 2020, the U.S. has been discouraging other nations to build or repair subsea cables by China because of concerns with sensitive communications passing through those cables and Chinese spying and sabotage (Lee, 2024). The U.S. is also concerned with China potentially collecting data and believes that Chinese firms would monitor data running through the cables (Runde et. al, 2024). However, after hearing this, China delayed projects without giving approval of permits for other companies to repair or build new cables (Lee, 2024).

Table 3 shows cables that have been suspected of being attacked or damaged by state actors in the South China Sea. The data table includes the cables’ length in miles, owners, suppliers, and the date of when the incident of the cable occurred.

Table 3: South China Sea Cables Damaged in Suspected Attacks⁶

Date of Incident	Cable Name	Cable Length (Miles)	Cable Owners	Supplier
February 2023 ^b	Taiwan Penghu Kinmen Matsu No.2 (TPKM2) ^a	290 ^a	Chunghwa Telecom ^a	NEC ^a
February 2023 ^b	Taiwan Penghu Kinmen Matsu No.3 (TPKM3) ^a	316 ^a	Chunghwa Telecom ^a	NEC ^a
January 2025 ^c	Trans-Pacific Express (TPE) ^a	11,164 ^a	AT&T, China Telecom, China Unicom, Chunghwa Telecom, KT, NTT, Verizon ^a	SubCom ^a
February 2025	Taiwan Penghu Kinmen Matsu (Number unknown)	Unknown	Chunghwa Telecom ^a	NEC ^a

⁶ Table data from: ^aTeleGeography (n.d.), ^bLipscombe (2025), ^cTobin et. al (2025)

Geopolitical Landscape

The South China Sea is a center for maritime economic activities and a major shipping route. Around 70% of all global trade is transported through the sea, and of this percentage 60% of maritime trade passes through Asia and the South China Sea (Schrag, 2021). The UN Conference on Trade and Development estimates that over 21% of global trade travelled through these waters in 2016, generating \$3.37 trillion (BBC, 2023). With heavy shipping traffic, subsea cables are already vulnerable to intentional or accidental damage from anchors. Additionally, as one of the world's top fishing grounds, cables are prone to accidents since anchors and nets are constantly dragged through the seabed (Tan, 2024). In addition to the economic importance of the South China Sea are complex geopolitical dynamics. There are several interconnected issues in the region—contested territorial claims in the South China Sea, cross-strait relations between China and Taiwan, and increasing U.S.-China competition and conflict.

Overlapping claims to the waters of the South China Sea, and subsequently increased control over the subsea cables along its seabed, have created a tense geopolitical environment in this key region. Brunei, China, Indonesia, Malaysia, the Philippines, Taiwan, and Vietnam have various territorial claims in the sea—with China making arguably the most assertive claims over its rights to the area (CRS, 2023). Many of these territorial claims center around the Parcel Islands, Scarborough Shoal, and Spratly Islands, because sovereignty over these small rocky land masses extends a country's exclusive economic zone (EEZ) under the UN Convention on the Law of the Sea (CRS, 2023; Desurmont, 2024). China's claims in the sea, including all three of these island and shoal clusters, is articulated by the Chinese government as a "nine-dash line," which extends into the 200-nautical-mile EEZs from the mainland coasts of Brunei, Indonesia, Malaysia, the Philippines, and Vietnam (CRS, 2023).

The Philippines, in particular, has had tense relations with China over disputed claims in the South China Sea. After a confrontation between Chinese and Philippine ships in 2013, the Philippines sought arbitration in an UNCLOS arbitral tribunal concerning maritime rights and entitlements in the South China Sea (Guo, 2018). Since the Philippines and China are both parties to UNCLOS, they were able to address the issues for settlement of the dispute. The tribunal ruled that China's claims to its right within the "nine-dash line" did not align with the entitlement permitted by UNCLOS and that China unlawfully interfered with Philippine vessels (CRS, 2023; Guo, 2018). The decision stated that the Philippines' arbitration was valid and China would face consequences if it refuses to abide by the ruling, but China declared the ruling "null and void" (CRS, 2023; Guo, 2018). More recently, there have been minor conflicts between the Coast Guards of the two countries (CRS, 2023). The Philippines' Coast Guard has been "actively challenging" the Chinese Coast Guard presence in the Philippine province Zambales (Baum et al, 2025). On January 24, Philippine President Marcos proposed dismantling a U.S. missile system in the Philippines if China agreed to cease its aggressive actions in the South China Sea

(Baum et. al, 2025). As the U.S. and the Philippines have a mutual defense treaty, an attack on Philippine forces in the South China Sea would invoke U.S. commitments, making the South China Sea a potential starting ground for a larger conflict (CRS, 2023).

The disputes over territorial claims and tensions between China and other claimants create an environment that hinders the ability of cable companies to operate in the South China Sea. Since UNCLOS gives countries sovereignty over cables in their EEZs, cable companies must receive permitting from each claimant—something that is complicated by the different interpretations of UNCLOS. Additionally, as geopolitical tensions heat up, companies are wary of sending personnel to the South China Sea, leading to a lack of maintenance ships able to navigate the region (Desurmont, 2024).

Another complex issue in the outskirts of the South China Sea is the relationship between China and Taiwan. While Taiwan is functionally independent, including having its own democratically elected government, China claims the island as part of its territory. Domestically, political leaders in Taiwan have differing views on its status and relationship with Beijing, but recently consecutive electoral wins by the Democratic Progressive Party (DPP), which do not view Taiwan as part of China, have ratcheted up tensions across the Strait. In terms of its international status, Taiwan is not a member of the UN and is therefore not a signatory to UNCLOS (Maizland & Fong, 2025). Additionally, the U.S. and Taiwan do not have official diplomatic relations but instead have a robust unofficial relationship including extensive economic ties and continuing U.S. arms sales to Taiwan. While the possibility of an invasion of Taiwan to forcefully reincorporate the island under China's control has loomed in international conversations for years, experts disagree on the likelihood and timing of such an event (Maizland & Fong, 2025). The U.S. has provided military support to Taiwan for decades, but it is important to note the U.S. and Taiwan do not have any sort of mutual defense treaty and the U.S. endeavors to maintain a certain level of ambiguity around whether it would come to Taiwan's aid in the event of an attack from China (Maizland & Fong, 2025).

Incidents regarding damage to Taiwan's subsea cables can be viewed in parallel with China's other actions in the Taiwan Strait and, therefore, have far-reaching implications in the event of a conflict. Beijing's history of sending military ships, fishing vessels, and sand dredgers into the waters around Taiwan have been described as pressure tactics intended to intimidate the Taiwanese government. In addition, Taiwan has been the victim of a barrage of cyberattacks from Chinese hackers targeting government agencies (Cheung et. al., 2021). The possibility of a deliberate severing of subsea cables as a precursor to an invasion has been discussed by the U.S. and its partners in the region, as such a tactic could isolate Taiwan diplomatically and hinder a coordinated military response (Hinrix, 2024). This possibility has been explored in a war game simulation held by the Japan Forum for Strategic Studies in Tokyo (Chin & Yun-yao, 2023).

Major Incidents

The three incidents in the South China Sea regarding suspected state sponsored attacks of cables all involved Taiwan. In 2023, two cables connecting Taiwan to Matsu, a series of outlying islands off the coast of China, but under Taiwan's jurisdiction, were severed within days by Chinese fishing and cargo vessels. The two cables, Taiwan Penghu Kinmen Matsu No.2 (TPKM2) and Taiwan Penghu Kinmen Matsu No.3 (TPKM3) were the only source of connection in Matsu, causing 13,000 residents to experience an internet blackout for weeks (Braw, 2023, SCM, n.d.). While there was no concrete evidence to point to state sponsored sabotage as the reason for the break, Taiwanese officials from the Democratic Progressive Party accused Beijing of intentionally causing damage to harass Taiwan (Chiang & Tobin, 2023; Shan, 2023).

Another incident involving Taiwan's subsea cables occurred more recently. On January 7, 2025, damage was detected on the Trans-Pacific Express, a cable linking Taiwan to the U.S., China, Japan, and South Korea. Communications were rerouted immediately, and there were no major disruptions of service (Tobin et al, 2025). Taiwan's Coast Guard intercepted a cargo ship, the *Xing Shun 39*, that was suspected of dragging its anchor to damage the cable. The ship was flagged under Tanzania and Cameroon but is owned by a Hong Kong company and crewed by seven Chinese nationals (Tobin et al, 2025). Taiwan officials said the ship appeared to use two sets of Automatic Identification System (AIS) equipment, which broadcasted two different names and locations, leading to suspicions that the incident was intentional (Tobin et al, 2025). In an interview, Harming Chiueh--the deputy head of Taiwan's Ministry of Digital Affairs--stated that cable-cutting accidents are unlikely to be accidental because, "you need to accidentally [drop your] anchor on the cable, and then you need to accidentally turn on your engine with the anchor down, and even [if] you realize your anchor is down, you need to keep the engine moving until you cut the cable" (Wang, 2025). The incident ended with the cargo ship departing towards South Korea, and Taiwanese authorities notifying their South Korean counterparts of the damage (Tobin et al, 2025).

Another instance of damage to subsea cables connecting to Taiwan occurred while this report was being developed. On February 25, 2025, Chunghwa Telecom detected that the cable linking Taiwan to its outlying Penghu islands had been disconnected. The damage was suspected to be from a Togo-flagged vessel crewed by eight Chinese nationals, which the Coast Guard intercepted and escorted back to the port of Tainan for investigation (Chang, 2025). The Taiwanese Coast Guard said the incident is now under investigation by prosecutors "in accordance with national security-level guidance" (Chang, 2025). In response to coverage of this incident, Beijing has accused Taiwan of manipulating the incident for political purposes (Chang, 2025). This statement is aligned with common narratives from Beijing on subsea cables, as China has not taken accountability for the attacks in the subsea cables near Taiwan and has claimed that they fall in line with other previous 'common maritime accidents' (Chang, 2025).

International Response

These attacks and the vulnerability of the cables have raised concerns for countries surrounding the South China Sea as well as for countries involved in future cable projects. Many countries have responded to the subsea cable incidents that have occurred in the South China Sea, including the U.S. and Taiwan. These incidents have also contributed to measures taken in multilateral organizations to address vulnerabilities in subsea cables.

Responses From States

Increased risks to cables in the South China Sea have led to several responses from the United States. U.S. companies are increasingly rerouting cable projects to avoid the South China Sea, instead following waters that border Indonesia and the Philippines (Tan, 2024). Alongside this, the U.S. has been blocking cable projects that link to Hong Kong due to concerns around espionage and potential sabotage of communications (Tan, 2024). For example, parties manufacturing and laying the Bay-to-Bay Express Cable System withdrew their licensing application to the FCC after it was recommended by a U.S. agency to be denied due to the connection to Hong Kong (Noor, 2024b). Subsequently, Meta and Amazon filed a new application for the cable to be rerouted to the Philippines (Noor, 2024b). The rerouting and delays of the cables are expected to increase both the cost and complexity of the projects for secure communication channels. However, several other cable projects headed by Southeast Asian nations are still moving forward in the South China Sea (Noor, 2024b).

Taiwan has also pursued alternative options for internet connectivity. Taiwan's Ministry of Digital Affairs (MODA) has prioritized the establishment of low and medium earth orbit satellite networks as an alternative to subsea cables in the event of disaster or conflict (Hinrix, 2024). With the new implementation of satellite networks, Taiwan can rely on backup systems from non-Chinese private sector partners (Hinrix, 2024). The Taiwanese government has also taken steps to protect subsea cables. MODA has presented a report to the Executive Yuan, the main legislative body of Taiwan, designating Taiwan's subsea cables as essential infrastructure (Hiciano, 2025). MODA also announced plans to enhance Taiwan's resilience to such disruptions by expanding monitoring stations, providing subsidies to telecom operators for cable repairs, and investing in alternative communication infrastructure, such as microwave systems (Hiciano, 2025).

Responses from International Organizations

Increased threats to the security of subsea cables and the ability of cable companies to freely navigate the South China Sea have also prompted a response from a multilateral organization. The Quadrilateral Security Dialogue (the Quad)—an informal diplomatic partnership between the U.S., Australia, India, and Japan—announced in May of 2023 the Quad Partnership for Cable Connectivity and Resilience. Another partnership of interest in the region is the Association of Southeast Asian Nations (ASEAN). ASEAN benefits from being regionally

focused as it provides a platform for the Southeast Asian countries to exchange views and ideas on policy (Davenport, 2025). Such a platform allows for spreading awareness about subsea cable issues and then shaping ASEAN policy in the interest of the party members. In ASEAN's 2024 annual report, the group announced that they were planning to introduce subsea cable bilateral agreements between Singapore and Vietnam, Singapore and Cambodia, and Laos and Vietnam to promote trade (ASEAN, 2024).

Implications

While the tense geopolitical dynamics in the South China Sea have been an ongoing issue for many years, in recent years conflicts over subsea cables have begun to reflect these dynamics. Threats to subsea cables in the South China Sea have manifested most clearly around the island of Taiwan, where multiple incidents have been deemed suspicious of being intentional action from China. Heightened risks to this essential global infrastructure have prompted responses from both the U.S. and Taiwan exploring alternative options.

Red Sea

The Red Sea is a narrow extension of the Indian Ocean spanning 174,000 square miles and is located in the fault depression between Africa and the Arabian Peninsula (Schreiber and Ryan, 2025). As the shortest and most economical route from Asia to Europe, the Red Sea has been a major shipping route for over 150 years (Burgess, 2022). The advantageous location of the Red Sea also makes it an ideal place for subsea cables to connect Asia and Europe (Burgess, 2022). An estimated 90% of communications between Europe and Asia and 17% of global internet traffic traverse cables under the 14-mile-wide Bab el Mandeb Strait where the Red Sea meets the Gulf of Aden (Monaghan et al., 2024).

There have been three instances of subsea cable damage in the Red Sea that have either been suspected to be intentional sabotage and have been attributed to a state or non-state actor. In 2008, five cables in the Red Sea were damaged which led to suspicions that the damage was intentional (Borland, 2008). In 2013, there was suspected intentional damage to at least four cables when three unknown divers were caught attempting to cut a cable near Alexandria (Musil, 2013). In 2024, three cables were accidentally damaged by the anchor of a ship after the ship was attacked by Houthis in the Red Sea (Gambrell, 2024). These attacks have highlighted the vulnerabilities of subsea cables in the Red Sea, and the geopolitical consequences of subsea cable damage in this choke point.

Infrastructure

There are currently a total of fourteen operational subsea cables that pass through the Red Sea, eleven of which connect Asia and Europe (Gambrell, 2024; Burgess, 2022). ASN is the supplier of seven of the cables, SubCom is the supplier of four, and NEC is the supplier of three

(TeleGeography, n.d.). Telecom Egypt is a partial owner of seven cables and Saudi Telecom is a partial owner of five cables (Burgess, 2022).

Ownership of the critical subsea infrastructure in the Red Sea and involvement in the governance of telecommunications companies can be used as a tool by governments to gain influence in the Red Sea. Telecom Egypt is very involved in the cables in the area since many of the cables go above land in Egyptian territory in order to cross into the Mediterranean (Burgess, 2022). Telecom Egypt used to be fully owned by the Government of Egypt, but the Egyptian Ministry of Finance recently divested 10% of the company's total outstanding share (Economy Middle East, 2023). The Egyptian Ministry of Finance remains the main shareholder with a 70% ownership stake and the board of directors of the company remains the same (Economy Middle East, 2023). Telecom Egypt's partial ownership in many of the cables that pass through the Red Sea, along with the fee it charges for crossing Egyptian land, demonstrates Egypt's ability to leverage this geographical choke point for increased influence over subsea cables. Saudi Telecom is also majority owned by the government of Saudi Arabia, with the government having a 70% share in the company (stc Group, n.d.).

There are five cables that are either currently being laid in the Red Sea or will be laid in the future (TeleGeography, n.d.). In 2025, three out of five of these planned cables will become operational. Telecom Egypt is a partial owner of three of the planned cables (TeleGeography, n.d.). SubCom will be the supplier for two of these cables and ASN will be the supplier for two of these cables as well, indicating that SubCom and ASN are emerging as the top suppliers of subsea cables in the Red Sea, showing the influence of U.S. and European powers in the region (TeleGeography, n.d.).

One of the most significant cables that will be laid in this region in the near future is the SeaMeWe-6 cable (TeleGeography, n.d.). This cable is owned by a consortium of telecommunications companies and private businesses and will be ready for service by 2026 (TeleGeography, n.d.). The SeaMeWe-6 cable broadly starts in Tuas, Singapore and ends in Marseille, France and will connect Southeast Asia, South Asia, the Middle East, and Europe (TeleGeography, n.d.). There was an intense bidding war to determine whether SubCom or HMN Technologies would be the supplier for the SeaMeWe-6 cable. The U.S. intervened in the bidding process using diplomatic channels to ensure that SubCom would be the supplier instead of HMN Technologies (Brock, 2023). This intervention took place because of concerns over espionage, since HMN Technologies is a Chinese company (Brock, 2023). The U.S. government's involvement in the development of the SeaMeWe-6 cable demonstrated the strategic importance of the Red Sea as a channel for cables, as well as the impacts of U.S.-China competition on determining cable suppliers in the region.

Table 4 shows data on the cables in the Red Sea that have been suspected of being damaged intentionally including the cables' length in miles, owners, supplier, and when the

damage that was suspected to be intentional occurred. This data helps identify frequently attacked cables, as well as potential patterns with ownership and supplier contracts.

Table 4: Red Sea Cables Damaged in Suspected Attacks⁷

Date of Incident	Cable Name	Cable Length (Miles)	Cable Owners	Supplier
January - February 2008 ^d	FLAG Europe-Asia (FEA) ^e	17,399 ^a	Global Cloud Xchange ^e	SubCom ^e
January - February 2008 ^d	FALCON ^e	6,400 ^a	Global Cloud Xchange ^e	ASN ^e
January - February 2008 ^d , March 2013 ^c	SeaMeWe-4 ^e	12,428 ^a	Algerie Telecom, Bangladesh Submarine Cable Company Limited (BSCCL), Bharti Airtel, Etisalat UAE, National Telecom, Orange, Pakistan Telecommunications Company Ltd., Saudi Telecom, Singtel, Sparkle, Sri Lanka Telecom, Tata Communications, Telecom Egypt, Telekom Malaysia, Tunisie Telecom, Verizon ^e	ASN, Fujitsu ^e
March 2013 ^c	IMEWE ^e	7,513 ^a	Bharti Airtel, Etisalat UAE, Ogero, Orange, Pakistan Telecommunications Company Ltd., Saudi Telecom, Sparkle, Tata Communications, Telecom Egypt ^e	ASN, NEC ^e
March 2013 ^c	SeaMeWe-3 ^a	24,235 ^a	A1 Telekom Austria, AT&T, Altice Portugal, BICS, BT, CTM, China Telecom, Chunghwa Telecom, Cyta, Deutsche Telekom, Djibouti Telecom, Embratel, Etisalat UAE, Indosat Ooredoo, Jabatan Telekom Brunei, KDDI, KPN, KT, LG Uplus, Maroc Telecom, Myanmar Post and Telecommunication (MPT), National Telecom, OTEGLOBE, Omantel, Orange, Orange Polska, PCCW, PLDT, Pakistan Telecommunications Company Ltd., Rostelecom, Saudi Telecom, Singtel, Singtel Optus, Softbank Corp, Sri Lanka Telecom, Tata Communications, Telecom Argentina, Telecom Egypt, Telecom	ASN, Fujitsu, SubCom ^a

⁷ Table data from: ^aDufetre (2023), ^bGambrell (2024), ^cSaffo (2013), ^dSubmarine Cable Networks (2011), and ^eTeleGeography (n.d.).

			Italia Sparkle, Telekom Malaysia, Telkom South Africa, Telstra, Tunisie Telecom, Turk ASN, Fujitsu, SubCom Ostend, Belgium Geoje, South Korea 107 Telekom, Ukrtelecom, VNPT International, Verizon, Vocus Communications, Vodafone, eir ^a	
March 2013 ^c	TE North/TGN-Eurasia/SEACOM/Alexandros/Medex	2,258 ^a	Algerie Telecom, Cyta, PCCW, SEACOM, Tata Communications, Telecom Egypt ^e	ASN ^e
February 2024 ^b	Asia Africa Europe-1 (AAE-1) ^e	15,535 ^a	China Unicom, Djibouti Telecom, Etisalat UAE, Hyalroute, Metfone, Mobily, National Telecom, OTEGLOBE, Omantel, Ooredoo, PCCW, Pakistan Telecommunications Company Ltd., Reliance Jio Infocomm, Retelit, TIME dotCom, TeleYemen, Telecom Egypt, VNPT International, Viettel Corporation ^e	NEC, SubCom ^e
March 2013 ^c , February 2024 ^b	Europe India Gateway (EIG) ^e	9,321 ^a	AT&T, Altice Portugal, BT, Bayobab, Bharat Sanchar Nigam Ltd. (BSNL), Bharti Airtel, Djibouti Telecom, Gibtelecom, Libya International Telecommunications Company, Omantel, Saudi Telecom, Telecom Egypt, Telkom South Africa, Verizon, Vodafone, du ^e	ASN, SubCom ^e
February 2024 ^b	Tata TGN-Gulf (connects to SEACOM/Tata TGN-Eurasia in the Red Sea) ^e	2,505 ^a	Tata Communications ^e	SubCom ^e

Geopolitical Landscape

The Red Sea is one of the world’s most vulnerable choke points for subsea cables and shipping routes, while also being a geopolitically turbulent region. It is important to consider the role of the Red Sea as a major shipping hub since approximately 12% of all world shipping passes through the Red Sea and over 22,000 ships pass through the Bab el Mandeb Strait annually (Schreiber and Ryan, 2025). Most of the Red Sea, particularly the areas with the heaviest shipping traffic, such as the Gulf of Suez and the Bab el Mandeb Strait, are also quite shallow (Schreiber and Ryan, 2025). The scope of shipping traffic, combined with the shallow depth of the Red Sea, make the subsea cables in this area especially vulnerable to damage from anchor damage (Burgess, 2022). This vulnerability can be leveraged by threat actors to cause intentional damage to the cables—either using intentional anchor damage that is meant to look unintentional or by forcing innocent third party ships to drop their anchor in an unexpected

area. These factors create an environment with the potential to be disrupted by regional conflicts.

Until recently, the Red Sea was one of the safer areas to place subsea cables since it was relatively distant and protected from extremist groups in the region (Burgess, 2022). However, the increasing scope of conflict in the Middle East and North Africa region, as well as Houthi attacks on shipping since mid-November 2023, have made the Red Sea more vulnerable in recent years (Clapp, 2024). There also are several ongoing geopolitical issues in the region that have the potential to affect subsea cables running through the Red Sea. For instance, there are rising tensions between Somalia, Ethiopia, and Somaliland over naval ports and access to the Red Sea (Lawal, 2024). Somaliland recently agreed to lease a naval base with access to the port of Berbera, located in the Bab el Mandeb strait, to Ethiopia for 50 years (Lawal, 2024). These tensions could lead to prolonged diplomatic rifts, which could result in conflicts that may have the potential to damage subsea cables in the region.

There has also been a re-emergence of piracy around the Red Sea and the Horn of Africa, with nine incidents of piracy being recorded between 2023 and 2024 (Mitra et al., 2025). The first attack took place shortly after the Houthi attacks in the Red Sea began (Mitra et al., 2025). The risk of piracy has been classified as moderate by the EU Naval Force Maritime Security Centre (Mitra et al., 2025). If piracy becomes a greater issue, it could lead to accidental damage to the subsea cables in and around the Red Sea through ships dropping their anchors.

The conflict between Israel and Hamas is also a key issue in this region. As the Israel-Hamas conflict began to escalate, so did the tension between Iran and Israel (Froman, 2025). Iranian-backed groups such as Hezbollah, a political party and militant group in Lebanon, and the Houthis in Yemen, began to increase attacks in their respective regions as well (CFR.org Editors, 2024; Froman, 2025). It is unclear whether the recent ceasefire agreement between Israel and Hamas will also apply to Hezbollah and the Houthis as well (Froman, 2025).

While all of these conflicts have the potential to create disputes that can lead to damage to subsea cable infrastructure, the Houthis are the most visible current threat to subsea cable infrastructure in the Red Sea. The Houthis are an armed political and religious group from Yemen that emerged in the 1990s and have declared themselves to be a part of the Iranian 'Axis of Resistance' against Israel and the U.S. along with other groups such as Hamas and Hezbollah (BBC, 2024). The Houthis rose to prominence in 2014 following a civil war in Yemen and have gained control over key territories within the country (Clapp, 2024). Currently, the Houthis control the west side of the country, the Red Sea coast, and the capital (Clapp, 2024). Subsequently, the Houthis also have a significant ability to impact the security situation in the Bab el Mandeb strait (Clapp, 2024). In November 2023, the Houthis began to attack commercial shipping vessels in the critical Red Sea corridor, claiming these attacks were anti-Israel attacks (Clapp, 2024). Later that year, the group also posted material on the social networking platform Telegram that seemed to be threats against the subsea cables that pass through the Bab el Mandeb strait (Johnson, 2025). The Houthis continue to be a threat in the Red Sea and have continued their attacks in the area (Reuters, 2025).

Major Incidents

In January and February 2008, five cables were damaged in the Red Sea, including Flag Europe-Asia (FEA), FALCON, and SeaMeWe-4 (Submarine Cable Networks, 2011). At this time, only three cables connected Asia and Europe through the Red Sea. With two of the cables being damaged, there were widespread outages, with Egypt losing around 70% of its internet connectivity and India losing around 50-60% of internet connectivity (Borland, 2008). The damage to the cables and subsequent outages in the Middle East and Asia led to a series of conspiracy theories about intentional damage to the cable (Borland, 2008). The head of development of the International Telecommunications Union was quoted as saying that the damage may have been intentional (The Sydney Morning Herald, 2008). However, the disruption to the subsea cable infrastructure in 2008 was eventually attributed to anchor accidents and weather incidents (Musil, 2013).

In March 2013, three unknown divers in a fishing boat were arrested by the Egyptian Coast Guard after being caught cutting the SeaMeWe-4 subsea cable off the coast of Alexandria (Saffo, 2013). Around that time, there were multiple disruptions on cables in the Red Sea area including Europe India Gateway (EIG), IMEWE, SeaMeWe-3, and TE-North (Saffo, 2013). These disruptions were seen as routine, until the three divers were arrested, which prompted discussions about intentional damage to subsea cable infrastructure by nefarious actors (Saffo, 2013). There is no further information available about the three divers, including their potential motives or whether they were actually responsible for the damages to the other cables (Musil, 2013).

In March 2024, it was revealed that three subsea cables in the Red Sea had been cut, affecting 25% of all data flowing through the area (Gambrell, 2024). These cables were Asia-Africa-Europe 1, the Europe India Gateway, and Seacom and TGN-Gulf (Gambrell, 2024). The Presidential Leadership Council—which is the internationally recognized government of Yemen and does not contain any Houthi representatives—claimed in early February 2024 that the Houthis had been planning to attack subsea cables in the region (BBC, 2024; Gambrell, 2024; Salhani, 2024). The Houthis denied these allegations and claimed that the damage to the cables was caused by U.S. military and British military units that were operating in the area (Gambrell, 2024). A Houthi leader, Abdel Malek al-Houthi mentioned that the group had “no intention of targeting sea cables providing internet to countries in the region” (Ziady, 2024). The Israeli news outlet *Globes* also suggested that the cables may have been damaged by the Houthis (Ziady, 2024). It is unclear how the Houthis may have damaged the cables, since they are not known to have advanced diving capabilities and do not have allies that have the capability to cut the cables directly (Gardner, 2024). Subsea cable repairs in the area take time since vessels passing through the Red Sea are required to obtain a permit from Yemeni maritime authorities (Ziady, 2024). The Houthis also have threatened that cable-laying ships without the permit may not be allowed to pass (Gambrell, 2024).

Collectively, these incidents highlight the fragility of subsea cables in the region and have prompted discourse on the potential impact of intentional attacks to subsea cables in the Red Sea due to the concentration of cables in the area.

International Response

While there have not been specific responses to the cable damages, various actors in the international community have responded to the attacks on commercial shipping vehicles by the Houthis in the Red Sea. The responses to the threats from the Houthis include increased military presence from the United States as well as the European Union and the adoption of a resolution that condemned actions taken by the Houthis by the United Nations Security Council (Clapp, 2024).

Responses From States

When the Houthis started attacking shipping vessels in the Red Sea, the U.S. responded with Operation Prosperity Guardian and increased military presence in the Red Sea. Operation Prosperity Guardian (OPG) was launched in December 2023, and brought together countries such as Australia, Bahrain, Canada, Denmark, Greece, the Netherlands, Singapore, New Zealand, and the United Kingdom (Clapp, 2024). The U.S., through Operation Prosperity Guardian, recognized that the Red Sea is a critical waterway, and aimed to address attacks from the Houthis and other security challenges through increased patrols (Garamone, 2023; U.S. Department of Defense, 2023). However, many countries such as France, Spain, and Italy have chosen to distance themselves from Operation Prosperity Guardian because they believe it may escalate tensions in the region further (Jones, 2024). The U.S. also moved aircraft carrier *USS Dwight D. Eisenhower* to the Gulf of Aden and ship spotters claim to have seen guided-missile destroyer *USS Laboon* enter the Red Sea from the Suez Canal in late 2023 (Lagrone, 2023). In January 2024, the U.S. and the U.K. started direct strikes on Houthi targets in Yemen and the Houthis responded by firing a missile at the *USS Laboon* (Clapp, 2024).

Responses From International Organizations

In January 2024, the United Nations Security Council adopted a resolution that denounced the repeated assaults by the Houthi rebels 'in the strongest terms' and acknowledged the right to defend vessels in compliance with international law (Clapp, 2024). The European Union has also condemned the attacks on shipping and commercial vehicles by the Houthi rebels, and welcomed the UN Security Council resolution (Clapp, 2024). In February 2024, EU Naval Force (EUNAVFOR) operation ASPIDES was launched which seeks to ensure safe navigation for commercial vessels (Council of the European Union, 2024).

Implications

The Red Sea is a critical route and major choke point for international data traversing subsea cables. Simultaneously, geopolitical tensions in the Middle East and North Africa pose

threats to the security of existing cables in the Red Sea and new cable projects in the region. The sheer number of cables in the region makes it an incident hotspot, and since many of the U.S.'s major allies rely on these cables to support vital communications, the security of cables in the Red Sea is of vital interest to the U.S.

Key State Actors: U.S., China, and Russia

Although there are many important state actors that interact with the global subsea cable infrastructure, we identified three key states to examine for the purposes of this report: the United States of America, the People's Republic of China, and the Russian Federation. These three countries are actively engaging with subsea cables, each in their own unique way, and examining each one illuminates the central geopolitical tensions that underpin our understanding of subsea cable infrastructure. The U.S. and China are in a constant state of competition over contracts, cables, and influence, while Russia sees the infrastructure as an opportunity to gain an offensive edge over its enemies through sabotage and espionage.

The U.S. and China both see subsea cables as an opportunity to project their power and maintain their status as great powers. The U.S. views China's market competition in subsea cable development as a threat to U.S. national security. The U.S. justifies itself by asserting that its actions are in pursuit of defending key national security interests. China, on the other hand, sees the U.S. as an obstacle to its growth. China perceives the U.S.'s actions as confrontational and unjustified, and as an attempt to cut China off from what it sees as reasonable and justified projections of influence and power in its sphere of influence. Each considers the other to be in violation of international norms and view their own actions as defensive necessities.

Russia interacts with global subsea internet infrastructure very differently. It is not competing with either the U.S. or China to lay subsea cables and project influence in that manner, and it does not equate market share of cable ownership with relative power in the same way as they do. Instead, Russia is concerned with offensive capabilities and opportunities to sabotage its enemies' critical subsea internet infrastructure. Specifically, Russia is uninterested in laying more cables and more concerned with developing highly advanced technologies that allow it to sabotage, spy on, and otherwise interfere with cables in regions it deems to be within its sphere of influence. Russian relations with the U.S. have been characterized by a high level of tension since the Obama administration, with Russia's 2014 and 2022 invasions of Ukraine acting as major points of contention between the two countries.

United States of America

The U.S. perspective of the global subsea cable infrastructure revolves around an assessment of threats to U.S. economic and national security. It is important to note that U.S. territory itself is not vulnerable to subsea cable attacks because of redundancy and overland networks. However, the U.S. perceives threats to subsea cables in China and Russia and subsequently has responded with robust measures to advance U.S. interests in alignment with national strategy.

Regulatory Landscape

In order to understand how the U.S. engages with subsea cables globally, it is first essential to understand how the U.S. interacts with cables domestically. The makeup of U.S. government agencies connected to subsea cables is extensive, but jurisdictional duties and authorities vary between each organization. Regulatory authority over the licensing and laying of submarine cables as well as the operation of communications cables in U.S. coastal waters is given to the Federal Communications Commission (FCC) (National Oceanic and Atmospheric Administration, 2024). The FCC is also responsible for authorizing transfers of existing cable licenses or any modifications to cables within U.S. waters (Federal Communications Commission [FCC], 2025). The Department of Homeland Security (DHS) also plays a role in cable resilience and security through the Cybersecurity and Infrastructure Security Agency (CISA), which falls under DHS' jurisdiction (DHS, 2024). In addition to CISA, the U.S. Coast Guard and U.S. Customs and Border Protection, both also under DHS, are responsible for detecting and responding to potential threats to subsea cables in the maritime environment (DHS, 2024).

The regulatory landscape of subsea cables in the U.S. is both complex and ambiguous. Subsea cables operate in a cross-jurisdictional manner involving multiple industries, which includes oftentimes contradictory compliance regulations (Department of Homeland Security [DHS], 2024). The current composition of oversight bodies on subsea cables described above is also complex, and as a result the need for cross-organizational cooperation to streamline industry projects is essential. Additionally, the infrastructure itself is expansive, including the cables themselves, landing stations, and software, and addressing each facet is key to cable resilience and security. The fragmented nature of subsea cable infrastructure highlights the need for cross-sector cooperation to build resilience in subsea cable infrastructure.

Geopolitical Tensions

The U.S. sees two main state actors as threats to the security of subsea cable infrastructure around the world: China and Russia. These two nations each occupy a different space in the U.S. perception, with Russia as a threat to subsea cables that are crucial pieces of internet infrastructure connecting U.S. allies in Europe, and China as the most dominant threat to U.S. national and economic security. Consequently, the U.S. response to each perceived threat also differs significantly.

U.S. Concerns about China

China's expansion in the subsea cable industry, particularly through the Belt and Road Initiative's Digital Silk Road, is perceived as a fundamental threat in the U.S. In 2015, China announced the Digital Silk Road and its goal of expanding digital technologies in developing countries as the digital connectivity subset of its Belt and Road Initiative (Williams, 2024). Digital Silk Road investments are in sectors such as telecommunication infrastructure (including subsea cables), artificial intelligence, ecommerce, mobile payment systems, surveillance technology,

and other technology systems in recipient countries (Gerwitz et al., 2025). In terms of subsea cables, the Digital Silk Road offers an attractive option to countries that want an alternative to U.S. providers after the 2013 Snowden disclosures revealed the U.S. and partnered allies used subsea cables for espionage (Burdette, 2023). A crucial part of the Digital Silk Road branding strategy is promoting Chinese technology companies. HMN Technologies, formerly Huawei Marine Networks, has been at the forefront of the Digital Silk Road in the subsea cable industry, and has subsequently expanded as a provider. According to data from TeleGeography, HMN Technologies has become the world's fastest-growing manufacturer and layer of subsea cables (Brock, 2023).

The primary concern for the U.S. regarding the expansion of Chinese companies in the subsea cable industry centers around espionage and surveillance. Digital Silk Road projects often grant Chinese multinational companies such as HMN Technologies access to data repositories. Although HMN Technologies asserts its independence, Chinese technology companies have a close relationship with the government, prompting concerns about the Chinese government having unrestricted access to data flows (Burdette, 2021). Additionally, under China's National Intelligence Law of 2017, Chinese citizens and organizations are required to comply with state intelligence services without the type of due process protections that would exist in a democracy (Burdette, 2021). Under this law, the Chinese government can access data transmitted via cables that do not connect to China—furthering China's reach into global subsea cable infrastructure, and posing significant threats to the security of sensitive U.S. communications (Burdette, 2021).

China's ability to lay cables is also a concern for the U.S. because of its rapid increase in market share and the potential technological independence that could follow. Despite the fact that in 2021 Chinese sponsored firms only held about 11% of the global market share, the speed with which China has increased global market share in subsea cables worries the U.S. (Runde et al., 2024). For example, China's HMN Technologies has installed 18% of the new subsea cables worldwide in the past four years, by length (Runde et al., 2024). Despite U.S. efforts to reduce dependency on Chinese cable systems in the Indo-Pacific region, there are 20 either live or almost operational cables sponsored by Chinese firms that have been established or are soon to be in 2021-2026 (Basu, 2024). More specifically, U.S. concerns stem from China's ability to develop its own subsea cable network independent from any other party. Since China has the fiber optic technology to lay and maintain its own cable infrastructure, the U.S. perceives the global network as more vulnerable to both sabotage and espionage (Billingsley, 2024). Additionally, Chinese dominance in the industry means Chinese companies are less vulnerable to U.S. export controls, in contrast to industries like semiconductors where Chinese innovation is restricted by export controls of U.S. technology (Basu, 2024).

In order to counter Chinese firms' ability to acquire contracts, and consequently access to sensitive U.S. data and communications, the U.S. established the Committee for the

Assessment of Foreign Participation in the U.S. Telecommunications Services Sector— colloquially known as Team Telecom. Team Telecom is an FCC oversight body that reviews applications and licenses for subsea cables that touch a U.S. territory to evaluate national security and law enforcement risks (Department of Justice, 2023). Chaired by the Attorney General and with participating committee members from the Department of Defense, Justice, and Homeland Security, Team Telecom undertakes comprehensive assessments on potential risks of projects meeting certain thresholds of foreign ownership or control and advises the FCC on whether to grant or deny the application (DOJ, 2023). Team Telecom has denied licenses for a number of subsea cable projects, such as the Pacific Light Cable Network meant to connect the U.S. with Hong Kong (Runde et al, 2024).

While Team Telecom mitigates risks to U.S. sensitive communications, the U.S. is simultaneously taking measures to prevent Chinese expansion in the subsea cable industry by hindering Chinese firms from gaining contracts in large cable projects. According to government documents, efforts to intervene in the process of Chinese firms securing contracts were pursued to secure these critical systems from 'malign foreign influences' in accordance with the national security strategy (DHS, 2024). This strategy involves offering financial incentives for projects that contract U.S. aligned companies as well as diplomatic pressures on consortium members to not partner with Chinese firms (Brock, 2023).

For example, Vietnam has been a key country where the U.S. and China have vied for influence, including over the manufacturing of new subsea cables. Aging cable infrastructure has led Vietnam to declare its intentions to lay ten new subsea cables by the year 2030 (Guarascio et al., 2024). According to an investigation by Reuters, the U.S. under the Biden administration lobbied against the use of Chinese contractors, specifically HMN Technologies, for the construction of these cables (Guarascio et al., 2024). The investigation revealed in meetings between Vietnamese officials and APTelecom, U.S. representatives argued that relative newcomer HMN Technologies would lead to less U.S. investment in the region and also suggested the possibility of cable sabotage. However, Beijing's offer for the cable project was cheaper, and so the U.S. campaign faced an uphill battle (Guarascio et al., 2024). Vietnam is still in talks to expand its cable infrastructure, and it is yet to be seen how this competition will resolve (Guarascio & Nguyen, 2024).

The competition over contracts creates an environment in which third party countries are forced to choose between two major powers vying for advantage. As a response to the meetings in Vietnam, China claimed that the U.S. is 'blatantly violating international rules and business operation models' (Guarascio et al., 2024). In response to the lost contract for the SeaMeWe-6 cable—another example of U.S. interference—the Chinese government increased delays in permit approvals of cables that route through Chinese controlled territories citing national security concerns (Basu, 2024). China's ability to stall cable projects aimed at improving efficiency for U.S. allies forces third parties to decide between U.S. providers and Chinese

providers, turning this infrastructure into a direct reflection of increasing U.S.-China competition (Kumar, 2023). Additionally, increased cost of projects for countries is becoming an inevitable reality for those who choose to partner with U.S. firms. Higher costs may provide an incentive to cooperate with a cheaper and less regulated China, and, therefore, poses a danger to the U.S. interest to maintain market dominance over subsea cable networks.

The Quadrilateral Security Dialogue (the Quad), a cooperative project between the United States, Australia, India, and Japan, is crucial to U.S. strategy undermining Chinese presence in the subsea cable industry (Cannon & Bhatt, 2024). Leveraging the Quad is a key aspect of countering China's expanding infrastructure projects in the Indo-Pacific and beyond (Smith, 2021). The nature of the Quad as an informal grouping has allowed the members to act cooperatively in areas of mutual interest and downplay potential disagreements (Cannon & Bhatt, 2024). This helps to portray a united front of U.S. partners against China, including efforts to develop cable infrastructure in the Indo-Pacific (Cannon & Bhatt, 2024).

At the 2023 Quad Leaders' Summit, the Quad announced the Quad Partnership for Cable Connectivity and Resilience, which aims to bring together the members of the Quad and the private sector to strengthen subsea cable security in the Indo-Pacific (Quad Joint Leaders' Statement, 2023). Australia also established the Indo-Pacific Cable Connectivity and Resilience Program in 2023, which involves the deployment of delegates to embassies in strategic locations to coordinate future investment opportunities in the Indo-Pacific (Cannon & Bhatt, 2024). On the U.S. side, the Department of State implemented the CABLES program, an initiative to inform potential customers in the East Asia Pacific region of the risks associated with partnering with China on subsea cable infrastructure (Department of State, 2024). In addition to this capacity building and information sharing, the Quad has engaged in trilateral investments amounting to \$95 million in subsea cable projects to obstruct various Chinese subsea cable projects (Cannon & Bhatt, 2024).

The U.S. is also attempting to increase options for Pacific Island countries to build subsea cables without Chinese involvement. Pacific island countries are increasingly a point of competition for influence between the U.S. and China. Due to a lack of existing infrastructure and abundant opportunity for investments, subsea cable development in the region is an opportunity for both the U.S. and China, and subsequently is a point of contention within the larger dynamic of U.S.-China competition (Sakai, 2024). As a component of the U.S. strategy to enhance the U.S.-Pacific Islands Partnership, the Biden administration announced in 2023 a U.S. Trade and Development Agency feasibility study for the proposed Central Pacific Cable. This cable would connect Guam to American Samoa and extend to up to 12 more Pacific Islands (The White House, 2023). Another example is the East Micronesia Cable, funded jointly between the U.S., Japan, and Australia, which will connect the Federated States of Micronesia, Kiribati, and Nauru (The White House, 2023). U.S. government financing of cables supports not only the

expansion of digital connectivity in remote regions but also aligns with the U.S. strategy to counter Chinese subsea cable financing and expand U.S. market presence.

U.S. Concerns about Russia

The U.S. views Russia as a significant threat in relation to subsea cable infrastructure. Russia's offensive capabilities and actions against subsea cables in key geopolitical hotspots, such as the Baltic Sea, have made it clear that cable sabotage is a part of the Kremlin's offensive arsenal (Boulègue, 2024). The Russian Navy operates a large fleet of military and intelligence vessels with espionage and sabotage capabilities (Boulègue, 2024). Russia's Main Directorate of Deep-Sea Research, (GUGI), is a part of Russia's Ministry of Defense, separate from the Navy, and hosts a variety of vessels with varying capabilities and purposes (Boulègue, 2024). With increasing incidents in the Baltic Sea, as well as Russia's invasion of Ukraine, Russia's ability to disrupt subsea cable infrastructure is a threat to the U.S. and its NATO allies. In response to Russia's current posture in the Baltic Sea, the U.S. is participating in NATO's Operation Baltic Sentry, as discussed in depth in the Baltic Sea regional case study.

Implications

The U.S., as a dominant actor in global subsea cable infrastructure, perceives threats from both China and Russia as subverting its international position, but for different reasons. Particularly in the case of China, U.S. measures to mitigate threats to secure communications involve private firms, leading national security concerns across the public and private spheres. Engaging in key strategic alliances and agreements, the U.S. projects influence globally, while stemming the expansion of Chinese dominance in crucial regions. Similarly, the U.S. and its NATO allies collaborate to mitigate the risks of Russian aggression in areas such as the Baltic Sea. The U.S. is balancing efforts to expand its own influence with efforts to stop China's expansion and Russia's aggression, making the topic of global subsea cables one of utmost importance to the U.S.'s greater geopolitical, economic, and security strategies.

People's Republic of China

Subsea cables are of great geopolitical and strategic value to China, especially in key areas such as information security, economic cooperation, military strategy and diplomatic influence. China is actively promoting the development of its subsea cable industry amid growing cybersecurity issues, domestic and international market competition, and geopolitical competition from the United States.

Regulatory Landscape

The State Oceanic Administration (SOA) is responsible for the examination and approval of internet subsea cable laying management (Davenport, 2012). The SOA, along with Chinese police, undertakes the examination and approval duties of cable routing review, survey, laying,

construction, maintenance and transformation, and specifies the responsibilities and obligations of enterprises and related personnel. The Law of the People's Republic of China on the Administration of the Use of Sea Areas and the Marine Environmental Protection Law of the People's Republic of China provides the legal basis for the protection of internet subsea cables (Zou, 2012). These laws also clarify the duties and powers of regulatory authorities and formulate penalties for acts that damage cables.

Growth in China's Subsea Cable Industry

China has worked for many years to develop its subsea cable technological capabilities and industry. As a result, Chinese firms have become some of the world's major subsea cable manufacturers with the market size expanding year by year (Zhou, 2021). In the past five years, the annual growth rate of China's subsea cable market has remained above 15% over previous years (Guiot, 2023). China's increased investment in the subsea cable industry furthers its intentions of becoming technologically independent and gaining a stronger position in global internet networks (China Academy of Information and Communications Technology [CAICT], 2023). Technological independence is an important factor for China as it can lessen reliance on foreign countries, particularly the United States. For example, China's semiconductor industry is currently under export controls by the U.S. to restrict growth (Friedman, et al, 2025). As U.S.-China competition grows more fierce, China faces the difficulty of access to advanced technologies to support growing industries.

China is promoting the development of the subsea cable industry by improving laws, regulations, and by implementing multi-dimensional policy to support industrial innovation and international cooperation (Central Government of the People's Republic of China, 2016). In terms of planning and construction, China regulates the setting of internet subsea cable landing pipeline corridors to create good conditions for cable laying. China also aims to advance the core technological aspects of subsea cables, such as high-speed data transmission technology cable material optimization (National Development and Reform Commission, 2020). The Chinese government has set up a number of scientific research projects and invested funds to support the research and development of these technologies.

China allows foreign companies to lay international internet subsea cables in waters under its jurisdiction, encouraging Chinese and foreign companies to cooperate. Additionally, China optimizes the approval process—such as setting up online application platforms—to improve efficiency (Xinhua Net, 2023). China's stance of permitting foreign companies to lay cables in Chinese waters promotes international cooperation and solidifies China's positioning as an enabler of global digital development. This policy also allows China to exert greater leverage in international digital standard and security framework negotiations.

China's International Strategy

On an international scale, China is focused on developing its subsea cable industry to gain influence in global infrastructure and technology. While China has been trying to promote global connectivity and build independent networks, the international competitive environment, geopolitical pressures, and regulatory challenges have limited China's global footprint (Burdette, 2021). In the future, whether China can successfully expand its influence in the global subsea cable market depends on whether it can cope with market access barriers, security issues and international governance rules.

The expansion of subsea cables is in line with China's broader geopolitical goals, such as the Belt and Road Initiative, which seeks to promote economic interconnectivity among the countries in the initiative (Wang et al., 2022). The initiative helps to further China's global influence by enabling it to open up greater digital connectivity in Asia, Europe, and Africa to contribute to the digital infrastructure needed for trade and communication and for technological exchanges.

The Belt and Road Initiative

The Belt and Road Initiative is a Chinese government foreign policy and development strategy covering nearly 70 countries and global regions and aims to expand trade, investment, and infrastructure links between countries with a focus on Africa, Asia, and Europe (Khatoon, 2022). The Belt and Road Initiative Action Plan states China should “jointly advance the construction of cross-border optical cables and other communications trunk line networks, improve international communications connectivity, and create an Information Silk Road” (Herlevi, 2024).

Subsea cables projects as part of the Belt and Road Initiative aim to improve development of cross-border trade, financial transactions, and the digital economy. China is also promoting the construction of telecommunications infrastructure in emerging markets and bringing the economies of countries along the route closer together (State Council of China, 2023). The Belt and Road Initiative has already found success in Southeast Asia with partnerships in countries like Pakistan and Cambodia. For example, the Pakistan and East Africa Connecting Europe (PEACE) cable, led by Hengtong Group and part of the Belt and Road Initiative's Digital Silk Road, has been a large commitment from China to expand its subsea cable presence. The PEACE cable assists the Middle East and North Africa and the China Pakistan Economic Corridor, a \$62 billion Belt and Road Initiative infrastructure project (Aluf, 2023).

Another cable project under the Belt and Road Initiative is the Cambodia-Hong Kong project, which has come to fruition after China and Cambodia reached a consensus to jointly promote trading and collaboration between the two countries (Liu, 2025). The project—which officially started on March 2, 2023—and is expected to be complete in July 2025, is the Cambodian government's first state-owned subsea cable, connecting Hong Kong, China, and

Sihanoukville, Cambodia, with a total length of nearly 3,000 km. The Cambodia-Hong Kong cable will be supplied by HMN Technologies (TeleGeography, n.d.).

Information Security

China has made the development of an autonomous and controllable subsea cable network a top priority in order to reduce its reliance on foreign-controlled infrastructure and reduce the risk of data leaks and surveillance (Rossiter, 2023). This follows Snowden's leaks of intelligence documents showing that the U.S. National Security Agency (NSA) conducts mass surveillance of subsea cables around the world (Burdette, 2021).

Subsea cables are also critical for military communications and national security. As a global data transmission infrastructure, its security directly affects the stability of the military command system, intelligence sharing, and strategic communications. As a result, China has made protecting its subsea cable network one of its national security priorities.

Geopolitical Tensions

As China's subsea cable industry grows, so do geopolitical tensions. In particular, China has faced challenges in expanding its influence in the subsea cable industry due to the U.S. viewing the increased competition as threatening. The U.S. Department of State has used its embassies to encourage countries to not sign with HMN Technologies for subsea cable projects (Brock, 2023a). An example of this is the SeaMeWe-6 cable project contract, which HMN Technologies failed to win because of U.S. lobbying (Brock, 2023a). This lobbying has continued in Vietnam and Singapore as the U.S. government has urged the two countries to not use HMN Technologies for any cable projects (Guarascio & Nguyen, 2024).

Other incidents related to subsea cable damage also have furthered geopolitical tensions. An incident exacerbating geopolitical tensions between China and Europe occurred regarding suspicions that the Chinese cargo ship *Yi Peng 3* was responsible for severing the BCS East-West Interlink cable connecting Sweden and Lithuania (Astier & Kirby, 2024). The Chinese foreign ministry denied having any responsibility despite a current investigation into the Chinese captain of the vessel (The Maritime Executive, 2024). Sweden also claimed that China denied their request for Swedish prosecutors to board the *Yi Peng 3*, but China had already allowed Swedish police to board as an observer (Bryant, 2024). However, from the perspective of the Chinese government, it was cooperating and communicating with the other parties involved while staying within its rights as the flag state of the ship, as granted in Article 113 in UNCLOS (UNCLOS, 1982).

Implications

China aims to expand its global network of subsea cables to increase its diplomatic and economic influence. At a national level, China has expanded legal protection surrounding information security. At the same time, China's diplomatic plans have been met with

competition and lobbying from the United States. China aims to continue using its initiatives to expand its global communications amidst international competition.

Russian Federation

Russia views subsea cable infrastructure differently than the U.S. and China do. It sees this infrastructure as an opportunity to engage in offensive action against its perceived enemies, which fits into Russia's broader geopolitical strategies. Instead of investing in cables themselves, Russia invests in developing offensive capabilities which allow it to engage in sabotage and espionage in key geopolitical regions.

Geopolitical Strategy

Russia's foreign policy and geopolitics are driven by many factors, but at the forefront is its persistent desire for status and recognition as a great state (Kotkin, 2016). Vladimir Putin's worldview revolves around the idea that the U.S. and its allies are trying to keep Russia down, that the U.S. and its allies act as a force counter to Russia's very existence, and that it will do everything in its power to establish itself as a global hegemon (Dickinson, 2022). Just hours before annexing Crimea in 2014, Putin gave a speech that elucidates this point perfectly saying: "[The West is] constantly trying to sweep us into a corner because we have an independent position, because we maintain it and because we call things like they are and do not engage in hypocrisy" (Putin, 2014). According to his speech, Putin sees the West (the U.S. and its allies) as the aggressor and Russia as the victim. Based on this worldview, all Russia wants to do is maintain its independence and sovereignty, to be free to exist without the fear of being put down and dominated by the West. In order to do this, Putin believes that Russia must project power throughout its sphere of influence and beyond, to show the West that Russia is in fact a great state, and that it will not allow itself to be relegated to the sidelines, as Putin claims has happened repeatedly in the past (Kotkin, 2016). This view justifies Russia's modern-day revisionist and hawkish foreign policy and influences how Russia interacts with internet infrastructure.

Since its invasion of Ukraine in 2022, Russia has made it clear that it has no issue disregarding international norms and regulations. However, even before Russia's invasion, the United States government and its NATO allies began to recognize the potentially disastrous effect that damage to the global internet cable infrastructure could have, along with Russia's ability to cause that damage (Wasiuta, 2023). As early as 2017, NATO military command warned the U.S. that Russia had developed the means to spy on, probe, and potentially damage subsea cables, leading to the approval in that same year of a plan to increase monitoring of Russian ships and submarines in the Atlantic Ocean (Wasiuta, 2023). In March of 2022, just a month after Russia invaded Ukraine, U.S. President Biden warned that Russia was considering attacks on critical infrastructure and said that there was intelligence that indicated those attacks would

include large-scale cyberattacks and attempts to sever the West's connection to the internet via sabotage of the global subsea cable infrastructure (Wasiuta, 2023).

Although there is a significant level of international concern surrounding Russia's offensive capabilities related to underwater internet infrastructure, there is also a growing consensus that Russia cannot unilaterally do enough to completely sever cables linking the U.S. to Europe (Scott, 2022). With more and more cables being laid every year, and alternative routes constantly being developed, the threat of Russia's offensive actions in the Atlantic does not need to be as large of a cause for concern as in the past. As U.S.-based companies like Meta and Google continue to lay more and more cables every year, the U.S. continues to diversify its options, leaving each cable less vulnerable to a devastating attack. Subsea cable infrastructure does not only make the internet run for one country, but for all of them. The internet is global, and, as such, the US's European and other allies abroad are just as incentivized to diversify, expand, and protect their infrastructure. Russia has the capability to cost companies millions of dollars in repairs, to sever important cables that would need to quickly be repaired, but not to unilaterally wipe out the internet. Therefore, although Russia's activity should be monitored and its aggression kept in check, Russia does not present the existential threat to the world's internet infrastructure that it desires to pose.

Russia's Offensive Capabilities

Russia has been developing and maintaining offensive capabilities in regard to global internet infrastructure for over a decade—through highly advanced clandestine and military technologies. In 2017, Russia's *Parliamentskaya Gazeta*, the official newspaper of Russia's Parliament, wrote about a specific vessel in Russia's fleet called the *Yantar*, which the article claims is equipped with technology designed for subsea tracking, and the ability to "connect" to deep sea cables (Andreev, 2017). The vessel raised concerns in the Pentagon when it spent a suspicious amount of time off the coast of Georgia's King's Bay, a key U.S. naval submarine base. Supposedly, the *Yantar* was collecting information on the US's submarine fleet located there, but it could also have been spying on subsea cables which make landfall in the area (Peter, 2018).

The U.S. is not the only country interested in the *Yantar*. In recent years, other governments have taken an interest in the vessel as well, as it has been spotted near Guantanamo Bay, close to subsea cables and other military targets near Greenland and Israel, around underwater infrastructure off the coast of Syria linking Turkey to Cyprus, and most recently, in late January 2025, was deployed to British waters (Bennetts, 2025). The Defense Secretary of the U.K., John Healy, in an address to the British Parliament, raised concerns about the *Yantar*, mentioning that it was also spotted in British waters in November 2024, loitering for a suspicious amount of time around underwater infrastructure (Bennetts, 2025). Additionally, Healy changed the rules of engagement for the British Navy, allowing its ships to get closer to

the *Yantar* in order to “monitor it every minute” while it is in British waters (Bennetts, 2025). Healy took the *Yantar*’s presence in British waters as a sign of “growing Russian aggression,” and the ship’s global presence can be interpreted as such, only on a much larger scale.

The *Yantar* is a part of Russia’s Main Directorate for Deep Sea Research (GUGI), an official organization within the Ministry of Defense (MoD). GUGI is responsible for maintaining much of Russia’s maritime espionage capabilities, hosting a wide range of ships ranging from surface vessels like the *Yantar*, to deep-sea submarines, and potentially possessing nuclear weapons in the form of Poseidon torpedoes (Kaushal, 2023). These primarily offensive capabilities housed in GUGI and openly displayed by Russia are, ironically, situated within the country’s defense apparatus, masking the true intention of Russia’s actions. Attribution challenges allow Russia to engage in more openly offensive behavior in the name of defense and national security, and to align its actions with its narrative that it is the victim of aggression from the U.S. and its allies, justifying them not only to its own citizens, but to the rest of the world.

Russia also acts aggressively through more covert means, such as the use of its shadow fleet. Russia’s shadow fleet is a fleet of ships estimated to be over 1,000 ships in size that was put together unofficially to circumvent the G7’s price cap on Russian oil exports (van Soest, 2025). These ships are operated under extremely convoluted ownership structures, fly different flags depending on the waters they are traversing, and often will shut off their GPS tracking to mask their locations (van Soest, 2025). Although the shadow fleet’s primary purpose is to avoid price caps on oil exports, the fleet is also widely believed to be engaging in other aggressive behaviors, in particular, sabotaging subsea cables. The complex ownership structures and flying of false flags allow Russia to maintain plausible deniability regarding the shadow fleet, making it a perfect tool to use for the second purpose of sabotage. It comes as no surprise that in the realm of subsea internet infrastructure, Russia distances itself just enough from the perpetrators of sabotage in areas such as the Baltic Sea to conveniently claim it has nothing to do with the attacks.

Russia and the Baltic Sea

At the tail end of 2024, three major internet cables were severed in the Baltic Sea, a region that has dealt with Russian aggression and influence since before the formation of the Soviet Union (Grylls, 2025). Although Russia denies any culpability in the three incidents, local governments in the region have concluded that Russia is responsible, and actions are being taken to prevent this type of activity moving forward. One such action is an operation called Baltic Sentry, a NATO mission aimed at protecting and patrolling Russian borders in the region, with the ultimate goal of protecting both the gas pipelines and the internet cables that are vital not just in the Baltics area, but for much of Europe as well (Grylls, 2025). The three cables cut in the Baltic Sea at the end of 2024 were all severed under suspicious circumstances, and at a

moment in time in which the countries around the Baltic Sea have been trying to distance themselves from reliance on Russia. The Estlink 2 cable, although not an internet cable but instead a large power cable, was cut by a ship called the *Eagle S*, which slowed down specifically as it crossed over the cable in the Baltic Sea (Grylls, 2025). Although the crew claims it was an accident, the Finnish government has pushed back on that narrative, illuminating the fact that the ship dragged its anchor along the seabed for 60 miles at the location of the cable (Grylls, 2025). The *Eagle S*, only a couple weeks prior to severing the Estlink 2 cable, was being monitored as it loitered around sensitive critical internet infrastructure off the Dutch coast, namely the Atlantic Crossing 1, a crucial subsea cable that connects the U.S. to Britain, the Netherlands, and Germany (Grylls, 2025). The vessel is believed to be a part of the Russian shadow fleet—but complex ownership makes it nearly impossible to tell who actually owns the boat and Russia maintains perfect plausible deniability when accused of being responsible for its actions (van Soest, 2025).

Russian Cables

Russia sees telecommunications infrastructure, including subsea cables, as a crucial aspect of national security, and as such, has incorporated almost all aspects of this infrastructure into the official national security and defense apparatus of the government. With very few cables connecting to the country, Russia's government has almost complete control over the laying and maintaining of this crucial internet infrastructure. Unlike China and the US, however, Russia does not see the laying of subsea cables as an opportunity to project influence, and as such, does not appear to have any aspirations to lay cables in other parts of the world and compete with the U.S. and China.

Russia does not have many subsea cables connecting it to the rest of the world, with a total of only 12 cables making landfall in the country (TeleGeography, n.d.). These cables are owned either by the Russian government, or the state-owned company Rostelecom (TeleGeography, n.d.). Rostelecom is a publicly traded telecommunications company in which the Russian government owns a majority of the shares (Sherman, 2022). In 2022, it was rumored that Rostec, Russia's national defense conglomerate, was going to incorporate Rostelecom into its own operations, formally absorbing the majority of Russia's telecommunication infrastructure into the military-industrial complex (Sherman, 2022). The CEO of Rostec, Sergei Chemezov, met Russian President Vladimir Putin in his days working for the KGB, and he reaps massive personal rewards for participating in various military exercises, research, and special operations (Sherman, 2022). This leaves the internet infrastructure under the umbrella of Russia's complex and long-standing systems of patronage, nepotism, and kleptocracy.

Implications

Russia owns the subsea cables that connect the Russian population to the worldwide internet, and by incorporating telecommunications infrastructure into preexisting national security structures, has insulated itself from the perceived threats of the West's encroachment and expansion. Conversely, by developing highly advanced technologies with inherently offensive capabilities and engaging in behavior well outside of its sphere of influence, Russia is attempting to project power and cement itself as a global player in the theater of war which the internet has become, while masking its aggressive activity behind the Ministry of Defense. By absorbing both its own infrastructure into existing defense structures and having its offensive capabilities run through GUGI, which also exists within the defense apparatus, Russia is signaling that all its actions are defensive and a reaction to the West's aggression rather than aggression of its own. This narrative and behavior in regard to subsea cables is in keeping with Russia's standard foreign policy practices, demonstrating that it sees this emerging landscape as another tool to push its global agenda onto the world and advance its foreign policy goals.

The Private Sector and Subsea Cable Infrastructure

Today, the majority of subsea cable infrastructure is owned and operated by private sector companies. Private ownership has been driven by the growing demand for reliable and high-capacity internet services, as well as the expansion of global trade and communication (Center for Strategic & International Studies [CSIS], 2022). Private sector companies have increasingly taken on the vast responsibility in building and maintaining these crucial networks to meet the demands of an ever-evolving digital economy (Gordon & Jones, 2022).

The “Big Four”

The construction and operation of subsea cables have become the domain of several major players in the private sector, often referred to as the "Big Four:" SubCom, Alcatel Submarine Networks (ASN), HMN Technologies, and Nippon Electric Company (NEC) (Runde et al., 2024). Collectively, these companies shape the global subsea cable landscape, contributing to technological advancements while operating within geopolitical constraints and responding to the demand for global data infrastructure.

SubCom, a U.S.-based firm with roots in Cold War-era intelligence projects, accounted for 22% of the subsea cable market by the number of cables delivered and 29% by cable length in 2023 (China Academy of Information and Communications Technology [CAICT], 2023). The company operates eight cable ships and plays a critical role in both military and commercial endeavors (Besch & Brown, 2024; Brock, 2023b). The company has been contracted to install secure communication infrastructure for the U.S. government and military, including subsea cables used for classified military communications (Satter, 2022). These communications can include encrypted command and control transmissions, secure data links between military bases, surveillance and reconnaissance data transfers, and communications supporting naval operations (Satter, 2022). In recent years, SubCom has also been integral to high-profile projects such as Google's Dunant transatlantic cable, which connects the U.S. to Europe, enhancing data capacity and redundancy for transatlantic communications (Brock, 2023b). The company's focus on Arctic routes and other resilient pathways has positioned it as a relevant player in the subsea cable landscape (Subcom, 2023).

ASN, based in France, accounted for 12% of the market by the number of cables delivered and 40% by cable length in 2023 (CAICT, 2023). The company has installed over 121 subsea cables worldwide, covering 850,000 kilometers of optical subsea systems (Alcatel Submarine Networks, 2025). Recently acquired by the French government in December of 2024, ASN is no longer a private company (Brock, 2023b). Despite this, its innovations in spatial-division multiplexing have significantly increased the efficiency and capacity of data transmission, enabling modern cables to handle exponentially higher volumes of data (Gross et al., 2023).

NEC, is a Japanese company with nearly a century of experience in the subsea cable sector, held both 7% of the market by the number of cables delivered and 7% by cable length in 2023 (CAICT, 2023). The company has developed several advancements in cable technology such as in spatial division multiplexing and molecular cable designs (NEC Corporation, 2023). NEC's work in these areas is aimed at improving bandwidth and flexibility to meet the increasing demand of data-driven economies (NEC Corporation, 2023).

HMN Technologies, a Chinese company, accounted for 23% of the market by the number of cables delivered and 18% by cable length in 2023 (CAICT, 2023). It develops route surveys, marine installations, and focuses on emerging markets. However, HMN Technologies has encountered challenges, particularly from the U.S. and its allies, who have raised concerns about the security risks associated with Chinese ownership of subsea cables. These concerns are focused on the possibility for cables to be exploited for espionage, risk of data interception, and the disruption of internet traffic (CSIS, 2022). Similar scrutiny applies to other Chinese companies in the industry, as governments evaluate potential vulnerabilities in critical infrastructure (CSIS, 2022).

New Ownership

Historically, most of the subsea cables were predominantly owned by a diverse range of actors, including telecommunication companies and international consortia (Gordon & Jones, 2022). Recently cable ownership has been shifting to major technology companies such as Google/Alphabet, Microsoft, Meta, and Amazon (Besch & Brown, 2024). Combined, these tech giants make up some of the world's largest providers of cloud technology and other online infrastructure (Law, 2023). As the demand for commercial internet services and cloud computing has grown, the private sector—particularly hyperscalers—have stepped in as a significant financier of subsea cables (Tréhu, 2024). These companies now own or lease around half of subsea cables now (Runde et al., 2024). These companies invest in subsea cables to support cloud computing operations and to maintain connections between global data centers (Dobberstein, 2024).

The financing of these subsea cables typically involves a mix of corporate capital, private equity, and sometimes loans from financial institutions, depending on the scale of the project (Tréhu, 2024). Tech companies often leverage their large financial resources to co-invest with cable construction firms, thereby sharing the high costs associated with these projects, which can range up to billions of dollars (Tréhu, 2024). By financing subsea cables, tech companies gain more control over the infrastructure supporting their operations, reducing dependence on external providers (Dobberstein, 2024). Direct ownership of this infrastructure helps reduce reliance on third-party providers and improves data security (Sherman, 2024). For instance,

Google solely financed 16 subsea cables, as well as has partly financed many more subsea cables (Mauldin, 2024).

The growing dominance of a few technology giants risks marginalizing smaller internet service providers (ISPs) and consolidating control over critical infrastructure (Dobberstein, 2024). This consolidation could stifle competition, reduce market diversity, and create barriers for smaller players seeking to compete in the global telecommunications industry (Dobberstein, 2024). The potential for monopolistic behavior raises concerns about fair access, fair competition, pricing power, and the ability of tech giants to dictate terms that could disadvantage smaller stakeholders (Insikt Group, 2023).

Maintenance and Repair

Ownership of subsea cables does not necessarily mean the owner has maintenance capabilities. There are many different actors who are in charge of maintaining and repairing subsea cables, including state-owned and private companies (Besch & Brown, 2024; International Cable Protection Committee [ICPC], 2024). According to the International Cable Protection Committee, there are roughly 60 major subsea cable ships operating today, which includes maintenance and repair ships as well as ships solely for laying cables (ICPC, 2024). Of the 60 cable ships worldwide, only a third of them can repair a cable (Swan, 2025). This is primarily because cable-laying is more profitable than maintenance (Tomaz & Voo, 2024).

A unique pressing challenge of cable maintenance is how the repair cable market works—specifically, who is repairing the subsea cables (Botting & Jordan-Zoob, 2024). There are several repair companies that the U.S. considers to be outside of “trusted” vendor sources. Theoretically, this introduces security concerns if the ship operators are influenced and controlled by a foreign adversary (Department of Homeland Security [DHS], 2024). For instance, there is a concentration of Chinese repair ships in strategic regions, including the Indo-Pacific, that has led to concerns in the U.S. about the reliance on Chinese companies for cable repairs (Runde et al., 2024). The U.S. has taken some measures to reduce the vulnerability of cable repair capabilities" (Runde et al., 2024).

Important players involved in both laying and repairing cables are Global Marine Systems Limited, Prysmian S.p.A, Orange Marine, Optic Marine (OMS) Group, and S.B. Submarine Systems Co., Ltd (SBSS) (ICPC, 2024; Blackridge Research and Consulting, 2024). A list of prominent actors includes:

- Global Marine Systems Limited is a United Kingdom based subsea cable installation, maintenance, and emergency repair company. With a fleet of three cable installation vessels, four maintenance and repair vessels, and one long-term charter vessel, the company operates worldwide (Besch & Brown, 2024).

- Prysmian Group is an Italian based company classifying as both an energy and telecommunications company. Operating a fleet of six vessels, Prysmian's *Leonardo da Vinci* ship is stated to be "the most capable cable layer in the market" as well as the largest on the market (Blackridge Research and Consulting, 2024).
- Orange Marine is a French based company that engages in funding, laying, maintaining, and repairing subsea cables. With a fleet of six cable ships and a survey vessel, Orange Marine represents 15% of the world's fleet of cable ships (Orange Marine, 2025).
- Optic Marine (OMS) Group is a global telecommunications infrastructure company, working primarily in Southeast Asia (OMS Group, 2025). With a fleet of five ships and one supply vessel, the company is working to expand its fleet with a new investment from several financial institutions (Kclark, 2024).
- S.B. Submarine Systems Co. Ltd (SBSS) is one of China's leading providers of subsea cable installation and a key installer in Asia. With a fleet of six ships, the company serves both fiber optic cables and power cable sectors (Besch & Brown, 2024; S.B. Submarine Systems, n.d.).

In 2023 KKR, a U.S. global investment firm signed an agreement with the OMS Group. KKR plans to commit \$400 million for solutions for OMS Group (OMS Group, 2025). KKR has avoided working with China, due to geopolitical concerns (Ruehl & Wiggins, 2024). This investment in the OMS Group to grow subsea infrastructure and maintenance capabilities in Southeast Asia, steers the company away from Chinese interests and investments.

Public-Private Partnerships

In the past decade, governments have shown increasing interests in subsea cables (Blue, 2024). Given that the private sector is heavily involved in subsea cable infrastructure, governments are finding it necessary to expand their involvement with companies (Kumar, 2023). The U.S. government claims that the subsea cable network's vital role in global communications is too critical to U.S. security to be left to markets (DHS, 2024). A new white paper by the U.S. Department of Homeland Security (DHS) highlights the importance of coordination between the government and the private sector while emphasizing subsea cable security and resilience. In the white paper, the DHS states that it also intends to enhance public-private partnerships, due to challenges associated with cross-sector collaboration (DHS, 2024).

For many decades, the U.S. company SubCom has laid cables for tech companies worldwide, including state-owned Chinese companies (Brock, 2023b). During the last five years, the company has worked almost exclusively as a subsea cable operator to the U.S. military, as well as working on sensitive U.S. projects (Brock, 2023b). The company is owned by Cerberus Capital Management, a New York-based private equity firm. The U.S. government assisted in

helping SubCom beat China's HMN Technologies for a contract to build the SeaMeWe-6 (Brock, 2023a; Dzieza, 2024).

China also has been making investments in both private and state-owned firms in the subsea cable sector (Kumar, 2023). There are three Chinese companies with investments in subsea cables that are entirely state owned: China Mobile, China Telecom, and China Unicom. Specifically, China Telecom has investments in subsea cables going back decades, investing in a cable in 1999 and another in 2016 (Sherman, 2021). All three of the companies have raised U.S. government security concerns. The U.S. Federal Communications Commission (FCC) labeled the companies as "subject to influence and control of the Chinese government" (Sherman, 2021). With increased political tensions, both U.S. and Chinese cable companies are now shifting and choosing sides in great-power politics when working with governments.

Advancements in Cable Technology

Despite U.S. pushback on China's HMN Technologies, Chinese enterprises have continued to gradually expand their share in the global subsea cable market. China has made major breakthroughs in research and innovation of subsea cable-related technologies (Kumar, 2023). In 2024, China's Southern Power Grid—a state-owned company—successfully developed the country's first subsea cable-laying robot. This robot can complete the comprehensive operation of "search, dig, and bury" at the cable laying speed of 1 KM/H (Liu, 2024). This greatly improves the construction efficiency. The robot has subsea cable detection availability and positioning methods that integrate an "acoustic-optical-magnetic-electric" multi-mode information which can assist in navigation near the seafloor and positioning in low-visibility environments. (Liu, 2024). The robot also offers two travel modes, crawler and sled, which were designed to effectively solve the problem of traveling on the soft soil seabed (Liu, 2024).

China has also achieved advancements in subsea cable transmission technology. For instance, China Unicom achieved a groundbreaking single-wave rate of 1.2 Tbit/s in the Hong Kong backhaul section of the ADC subsea cable, enabling a per-fiber-pair transmission capacity in the C-band of over 33 Tbit/s. With the system utilizing 8 pairs of optical fibers, the total design capacity exceeds 160 Tbit/s. The technological breakthrough represents a 71.8% improvement in spectral efficiency compared to conventional 200 Gbit/s transmission technology (Zeng, 2024). This marks a new world record for the real-time transmission rate of standard single-mode fiber, equivalent to supporting the streaming of hundreds of 4K HD movies, or several AI model training datasets per second (Yangtze Optical Fiber and Cable, 2024). The technological breakthrough not only drives the upgrading of global communication networks but also provides stronger support for future data-intensive applications such as AI computing, cloud computing, and ultra-high-definition streaming.

U.S and European companies also are innovating. For instance, U.S. and European companies developed the multi-core fiber (MCF) technology. This new technology can enable manufacturing, testing, and maintenance operations at faster speeds. MCF is capable of carrying more light and information at a lower cost (Quigley & Cantono, 2023). MCF technology dramatically increases data transmission capacity and efficiency by integrating multiple cores in a single fiber. In 2024, Google, in collaboration with the NEC, started planning to build a subsea fiber optic cable system connecting the Philippines and the U.S. It will be the world's first commercial project using MCF technology in subsea fiber optic cables, and it is expected to be completed by the end of 2025 (Google and NEC, 2024). With the expansion of online services, internet connectivity, cloud services, and AI, the use of MCF has the potential to become a part of the global telecommunications industry.

Implications

The private sector is deeply intertwined with the health of global subsea cable networks, with private companies financing, owning, laying, and repairing the cables. This sector has grown extensively as the demand for internet connectivity continues to grow globally. At the same time, these private actors have become wrapped up in the geopolitical contests between major global actors.

References

Executive Summary

- KV Cable. (2023). A comprehensive summary of submarine fiber optic cable types and distribution around the world in one article. <https://kvcable.com/a-comprehensive-summary-of-submarine-fiber-optic-cable-types-and-distribution-around-the-world-in-one-article-favorites/>
- Mauldin, A. (2023, May 4). *Do Submarine Cables Account For Over 99% of Intercontinental Data Traffic?* <https://blog.telegeography.com/2023-mythbusting-part-3>

Policy Recommendations

- A resolution calling upon the United States Senate to give its advice and consent to ratification of the United Nations Convention on the Law of the Sea. S. Res. 466. 118th Congress. (2023). <https://www.congress.gov/bill/118th-congress/senate-resolution/466/text>
- Ahlander, J., Rasmussen, L., & Solsvik, T. (2024, December 21). *Chinese Ship Linked To Baltic Sea Cable Breach Resumes Voyage*. gCaptain. <https://gcaptain.com/chinese-ship-linked-to-baltic-sea-cable-breach-resumes-voyage/>
- Andreev, A. (2017). *Корабль спецназначения “Янтарь” вошёл в Средиземное море*. [The Special Purpose Ship *Yantar* entered the Mediterranean Sea] <https://www.pnp.ru/politics/korabl-specnaznacheniya-yantar-voshyol-v-sredizemnoe-more.html>
- Brock, J. (2023, March 24). U.S. and China wage war beneath the waves – Over internet cables. *Reuters*. <https://www.reuters.com/investigates/special-report/us-china-tech-cables/>
- Channer, H. (2024, January 17). Improving Public-Private Partnerships on Undersea Cables: Lessons from Australia and Its Partners in the Indo-Pacific. *Indo-Pacific Outlook*. 1(2). <https://manoa.hawaii.edu/indopacificaffairs/article/improving-public-private-partnerships-on-undersea-cables-lessons-from-australia-and-its-partners-in-the-indo-pacific/>
- Convention for the Protection of Submarine Telegraph Cables, March 14, 1884, <https://nsarchive.gwu.edu/sites/default/files/documents/5975790/National-Security-Archive-Convention-for-the.pdf>
- Critical Infrastructure Security and Resilience. (n.d.). CISA. Retrieved March 4, 2025, from <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience>
- Department of Homeland Security [DHS]. (2015). 2015 Communications Sector-Specific Plan. <https://www.cisa.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf>
- European Commission. (2024, December 5). Additional €142 million to support submarine networks and connectivity infrastructure under Connecting Europe Facility (CEF) Digital. <https://digital-strategy.ec.europa.eu/en/news/additional-eu142-million-support-submarine-networks-and-connectivity-infrastructure-under>
- Gallagher, J. C., Carter, N. T., Comay, L. B., Figliola, P. M., Gatz, L., Keating-Bitonti, C., Lipiec, E., Marshak, A. R., Sheikh, P. A., & Ward, E. H. (n.d.). *Protection of Undersea Telecommunication Cables: Issues for Congress* (R47648; p. 53). Library of Congress.
- Goodman, M. P., Runde, D. F., & Hillman, J. E. (2020, February 26). Connecting the Blue Dots. Center for Strategic & International Studies. <https://www.csis.org/analysis/connecting-blue-dots>
- Grylls, G. (2025, January 22). *Nato’s underwater war against Russian and Chinese cable-cutters*. <https://www.thetimes.com/world/europe/article/natos-underwater-war-against-russian-and-chinese-cable-cutters-trc90sjn6>
- Guilfoyle, D., Paige, T. P., & McLaughlin, R. (2022). *The final frontier of cyberspace: The seabed beyond national jurisdiction and the Protection of Submarine Cables: International & Comparative Law Quarterly*. Cambridge Core. <https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/final-frontier-of-cyberspace-the-seabed-beyond-national-jurisdiction-and-the-protection-of-submarine-cables/4A40325D1A18927145A36B70ADCD35AD>
- Humphreys, B. E. (2024). *The 2024 National Security Memorandum on Critical Infrastructure Security and Resilience* (IF12716). Library of Congress.

International Cable Protection Committee. (2025, February 10). *About the ICPC*. <https://www.iscpc.org/about-the-icpc/>

International Cable Protection Committee, *Best Practices*, 2020, <https://www.iscpc.org/documents/?id=3733>

International Maritime Organization. (n.d.). *Registration of ships and fraudulent registration matters*. International Maritime Organization. <https://www.imo.org/en/OurWork/Legal/Pages/Registration-of-ships-and-fraudulent-registration-matters.aspx>

International Telecommunication Union. (n.d.) *International Advisory Body for Submarine Cable Resilience*. <https://www.itu.int/digital-resilience/submarine-cables/advisory-body/>

Kirby, P. (2024, December 27). *Estonia navy to protect undersea power link after main cable damaged*. BBC. <https://www.bbc.com/news/articles/c1elq7lx9qdo>

Kuznietsov, Serhii. (2021). The “Genuine link” Concept: Is It Possible to Enhance the Strength? *Lex Portus*, 7(6), 65 - 89. https://lexportus.net.ua/vipusk-6-2021/kuznietsov_2021_763.pdf

Office of the Staff Judge Advocate. (2021). Military Activities in the Exclusive Economic Zone. *International Law Studies*, 97(45), 45-52. <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2944&context=ils>

Office of the Staff Judge Advocate. (2021). U.S. Position on the U.N. Convention on the Law of Sea. *International Law Studies*, 97(81), 81 - 88. [https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2949&context=ils#:~:text=Some%20of%20the%20benefits%20of,going%20cargoes%3B%20\(2\)%20UNCLOS](https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2949&context=ils#:~:text=Some%20of%20the%20benefits%20of,going%20cargoes%3B%20(2)%20UNCLOS)

Peter, L. (2018, January 3). What makes Russia’s new spy ship Yantar special? <https://www.bbc.com/news/world-europe-42543712>

Quad Leaders’ Summit Fact Sheet. (2023, May 20). The American Presidency Project. <https://www.presidency.ucsb.edu/documents/quad-leaders-summit-fact-sheet>

SHAPE Public Affairs Office. (2025, January 14). *Baltic Sentry To Enhance NATO’s Presence In The Baltic Sea*. Shape NATO. <https://shape.nato.int/news-releases/baltic-sentry-to-enhance-natos-presence-in-the-baltic-sea>

Staff Writer with AFP. (2025, January 28). *Taiwan Identifies 52 ‘Suspicious’ Chinese Ships for Close Monitoring*. The Defense Post. <https://thedefensepost.com/2025/01/28/taiwan-chinese-ships-monitoring/>

Tagliapietra, S. (2024, January 11). The European Union’s Global Gateway: An institutional and economic overview. *The World Economy*. 47(4), 1326-1335. <https://doi-org.offcampus.lib.washington.edu/10.1111/twec.13551>

The White House. (2023, September 25). FACT SHEET: *Enhancing the U.S.-Pacific Islands Partnership*. <https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/09/25/fact-sheet-enhancing-the-u-s-pacific-islands-partnership/>

United Nations Convention on the Law of the Sea, December 10, 1982, https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

United Nations Convention on Conditions for Registration of Ships, February 7, 1986. https://unctad.org/system/files/official-document/tdrsconf23_en.pdf

U.S. Department of Defense. (2023, November 13). *New Uncrewed Undersea Capabilities Strengthen AUKUS Partnership*. <https://www.defense.gov/News/Releases/Release/Article/3586592/new-uncrewed-undersea-capabilities-strengthen-aukus-partnership/>

U.S. Department of Justice. (2023, September 20). *Team telecom*. National Security Division. <https://www.justice.gov/nsd/team-telecom>

van Soest, H. (2025). *Countering Russia’s “Shadow Fleet.”* <https://www.rand.org/pubs/commentary/2025/01/countering-russias-shadow-fleet.html>

Wahden, B., Lukas. (2024). *Will Russia denounce the United Nations Convention on the Law of the Sea (UNCLOS)?* Institut de Recherche Stratégique De L’École Militaire. <https://www.irsem.fr/strategic-brief-no-68-2024.html>

Watterson, J., Christopher, Osborn, Stephen., Grant, Samuel. (2020) Open registries as an enabler of maritime sanctions evasion. *Marine Policy*, 119, 1 - 6. <https://www.sciencedirect.com/science/article/pii/S0308597X20300385?via%3Dihub>

Windward. (n.d.). *UPDATED: Illuminating Russia’s Shadow Fleet*. Windward.ai. <https://windward.ai/knowledge-base/illuminating-russias-shadow-fleet/>

Technical Analysis of Subsea Cable Infrastructure

- Gallagher, J. C. (2022, September 13). Undersea telecommunication cables: Technology overview and issues for Congress (CRS Report No. R47237). Congressional Research Service.
- Gervasi, P. (2023, March 28). Diving deep into submarine cables: The undersea lifelines of internet connectivity. Kentik. <https://www.kentik.com/blog/diving-deep-into-submarine-cables-undersea-lifelines-of-internet-connectivity/>
- IBM. (2024, March 21). Hyperscale data center. <https://www.ibm.com/think/topics/hyperscale-data-center>
- Inven AI. (2024). Top 22 hyperscale data center companies. <https://www.inven.ai/company-lists/top-22-hyperscale-data-center-companies>
- Linden Photonics. (2023, February 6). What is underwater cable and how does underwater cable work? <https://www.lindenphotonics.com/what-is-underwater-cable-and-how-does-underwater-cable-work>
- Network Encyclopedia. (2024, January). Submarine communication cables: Secrets of the ocean depths. <https://networkencyclopedia.com/submarine-communication-cables-secrets-of-the-ocean-depths/>
- Ruffino, J. (2024, January 22). Baltic subsea cables: A story of resilience, not fear. Internet Society Pulse Blog. <https://pulse.internetsociety.org/blog/baltic-subsea-cables-resilience-not-fear>
- Swinhoe, D. (2021, August 26). What is a submarine cable? Subsea fiber explained. Data Center Dynamics. <https://www.datacenterdynamics.com/en/analysis/what-is-a-submarine-cable-subsea-fiber-explained/>
- Orange Matter. (2023, January 24). Hyperscalers: The complete guide. <https://orangematter.solarwinds.com/2023/01/24/hyperscalers-the-complete-guide>
- Red Hat. (2022, December 20). What is a hyperscaler? <https://www.redhat.com/en/topics/cloud-computing/what-is-a-hyperscaler>

Major Attacks

- Addis, B. (2025, February 26). *Now it's a Taiwan cable cut and the ship is a mystery*. Daily Kos. <https://www.dailykos.com/stories/2025/2/26/2306289/-Now-it-s-a-Taiwan-cable-cut-and-the-ship-is-a-mystery>
- Agence France Presse. (2024, December 3). *Finnish Authorities Say New Internet Cable Cuts Accidental*. Barron's. <https://www.barrons.com/news/sweden-suspects-sabotage-as-internet-cable-with-finland-damaged-d744b3dd>
- Agence France Presse. (2025, February 21). *Swedish Police Investigate New Baltic Sea Cable Damage*. The Moscow Times. <https://www.themoscowtimes.com/2025/02/21/swedish-police-investigate-new-baltic-sea-cable-damage-a88112>
- Aggarwal, M. (2025, January 14). *When American allies' undersea cables are severed, suspicion falls on Russia and China*. NBC News. <https://www.nbcnews.com/news/world/undersea-cables-are-cut-suspicion-falls-russian-chinese-vessels-rcna187105>
- Ahlander, J., & Jacobsen, S. (2025, February 3). *Sweden says ship broke Baltic Sea cable by accident*. Reuters. <https://www.reuters.com/world/europe/sweden-rules-out-sabotage-baltic-sea-cable-damage-case-2025-02-03/>
- Aikman, I. (2025, January 27). *Sweden seizes ship after suspected Baltic Sea cable sabotage*. BBC. <https://www.bbc.com/news/articles/cqx9g5wwp89o>
- Al Jazeera. (2024, November 19). *Germany says 'sabotage' presumed in damaged Baltic Sea telecom cables*. Al Jazeera. <https://www.aljazeera.com/news/2024/11/19/germany-says-sabotage-presumed-in-damaged-baltic-sea-telecom-cables>
- Al Jazeera. (2025, February 21). *Finland, Sweden probe suspected sabotage of undersea telecoms cable*. Al Jazeera. <https://www.aljazeera.com/news/2025/2/21/finland-sweden-probe-suspected-sabotage-of-undersea-telecoms-cable>
- AP News. (2025, January 26). *Sweden seizes vessel suspected of 'sabotage' after undersea data cable rupture in Baltic Sea*. AP News. <https://apnews.com/article/latvia-denmark-underwater-cable-damage-investigation-63da5ef0d577bca12bbe118d527d3a14>

- Arthur, C. (2013, March 28). *Undersea internet cables off Egypt disrupted as navy arrests three*. The Guardian. <https://www.theguardian.com/technology/2013/mar/28/egypt-undersea-cable-arrest>
- Astier, H., & Kirby, P. (2024, November 19). *Germany suspects sabotage behind severed undersea cables*. BBC. <https://www.bbc.com/news/articles/c9dl4vxw501o>
- Bir, Burak. (2024, January 27). *Undersea data cable between Sweden, Latvia damaged: Reports*. Anadolu Agency. <https://www.aa.com.tr/en/europe/undersea-data-cable-between-sweden-latvia-damaged-reports/3463230>
- BBC. (2022, October 20). *Damaged cable leaves Shetland cut off from mainland*. BBC. <https://www.bbc.com/news/uk-scotland-north-east-orkney-shetland-63326102>
- Braw, E. (2023, February 21). *China Is Practicing How to Sever Taiwan's Internet*. Foreign Policy. <https://foreignpolicy.com/2023/02/21/matsu-islands-internet-cables-china-taiwan/>
- Braw, E. (2024, November 21). *Suspected sabotage by a Chinese vessel in the Baltic Sea speaks to a wider threat*. Atlantic Council. <https://www.atlanticcouncil.org/blogs/new-atlanticist/suspected-sabotage-by-a-chinese-vessel-in-the-baltic-sea-speaks-to-a-wider-threat/>
- Brennan, D. (2025, January 13). *Baltic Sea undersea 'sabotage' sets stage for escalating NATO-Russia contest*. ABC News. <https://abcnews.go.com/International/baltic-sea-undersea-sabotage-sets-stage-escalating-nato/story?id=117594533>
- Brovko, L. (2024, December 26). *A Russian shadow fleet vessel that could have damaged an underwater cable was detained in Finland*. Bable.ua. <https://babel.ua/en/news/113986-a-russian-shadow-fleet-vessel-that-could-have-damaged-an-underwater-cable-was-detained-in-finland>
- Burdette, L. (2024, November 21). *What To Know About Submarine Cable Breaks*. TeleGeography. <https://blog.telegeography.com/what-to-know-about-submarine-cable-breaks>
- Burgess, M. (2022, July 22). *The Unsolved Mystery Attack on Internet Cables in Paris*. Wired. <https://www.wired.com/story/france-paris-internet-cable-cuts-attack/>
- Burgess, M. (2024a, April 1). *A Ghost Ship's Doomed Journey Through the Gate of Tears*. Wired. <https://www.wired.com/story/houthi-internet-cables-ship-anchor-path/>
- Burgess, M. (2024b, July 29). *Saboteurs Cut Internet Cables in Latest Disruption During Paris Olympics*. Wired. <https://www.wired.com/story/saboteurs-cut-internet-cables-in-latest-disruption-during-paris-olympics/>
- Cable Theft Costs Vietnam \$6M*. (2007, June). Photonics. https://www.photonics.com/Articles/Cable_Theft_Costs_Vietnam_6M/a29904
- Cahyafitri, F., & Cahyafitri, R. (2013, June 29). *Indosat spends Rp 10 billion replacing stolen underwater cable*. The Jakarta Post. <https://www.thejakartapost.com/news/2013/06/29/indosat-spends-rp-10-billion-replacing-stolen-underwater-cable.html>
- Chang, W. (2025, February 26). *Taiwan detains Chinese-crewed ship suspected of cutting undersea cable*. CNN. <https://amp.cnn.com/cnn/2025/02/25/asia/taiwan-detains-ship-undersea-cable-intl-hnk>
- Cinia. (2025, February 24). *Damage has been detected in Cinia's C-Lion1 submarine cable*. Cinia. <https://www.cinia.fi/uutiset/cinian-c-lion1-merikaapelissa-on-havaittu-vaurio>
- Clark, R. (2024, March 7). *Red Sea cable breaks highlight global vulnerabilities*. Light Reading. <https://www.lightreading.com/cable-technology/red-sea-cable-breaks-highlight-global-vulnerabilities>
- Davenport, T. (2015, December). *Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis*. *Catholic University Journal of Law and Technology*, 24(1), 57-109. https://scholarship.law.edu/jlt/vol24/iss1/4?utm_source=scholarship.law.edu%2Fjlt%2Fvol24%2Fiss1%2F4&utm_medium=PDF&utm_campaign=PDFCoverPages
- Department of Homeland Security. (2024, December 18). *Priorities for DHS engagement on subsea cable security & resilience (White Paper)*. Cybersecurity and Infrastructure Security Agency. https://www.dhs.gov/sites/default/files/2024-12/24_1218_srcr_Priorities-for-DHS-Engagement-on-Subsea-Cable-Security-Resilience_18-Dec-24.pdf
- Desmarais, A. (2024a, September 21). *Officials are worried about Internet blackouts. How vulnerable are underwater cables to attack?*. Euronews. <https://www.euronews.com/next/2024/09/21/officials-are-warning-about-the-vulnerability-of-underwater-cables-how-protected-are-they>
- Desmarais, A. (2024b, October 15). *Europe's Achilles Heel? Why the Baltic region is the most vulnerable to subsea sabotage*. Euronews. <https://www.euronews.com/next/2024/10/15/europes-achilles-heel-why-the-baltic-region-is-the-most-vulnerable-to-subsea-sabotage>

- Forum Staff. (2025, January 28). *Undersea cable cutting attacks appear linked to the PRC*. Indo-Pacific Defense Forum. <https://ipdefenseforum.com/2025/01/undersea-cable-cutting-attacks-appear-linked-to-the-prc/>
- France24. (2008, January 30). *Cable havoc leaves Egypt and India off the Web*. France24. <https://www.france24.com/en/20080130-cable-havoc-leaves-egypt-india-off-web-egypt-india-telecom>
- Fredriksen, B., Pettersen, B. M., Hesla, G. K., Eriksen, I., & Guldahl, H. (2022, June 26). *The Cable Mysteries*. NRK. <https://www.nrk.no/nordland/xl/russiske-tralere-krysset-kabler-i-vesteralen-og-svalbard-for-brudd-1.16007084#intro-authors--expand>
- Gambrell, J. (2024, March 4). *Houthi rebels deny severing three Red Sea underwater cables*. PBS. <https://www.pbs.org/newshour/world/houthi-rebels-deny-severing-three-red-sea-underwater-cables>
- Guldahl, H., & Eriksen, I. (2024, May 26). *This is what the damaged Svalbard cable looked like when it came up from the depths*. NRK. <https://www.nrk.no/tromsogfinnmark/this-is-what-the-damaged-svalbard-cable-looked-like-when-it-came-up-from-the-depths-1.16895904>
- Hantover, L. L., (2014). *The Cloud And The Deep Sea: How Cloud Storage Raises The Stakes For Undersea Cable Security And Liability*. *Ocean and Coastal Journal*, 19(1), 1-28. <https://digitalcommons.maine.law.maine.edu/oclj/vol19/iss1/2/>
- Hendriks, M. S., & Halem, H. (2024, February 19). *From space to seabed: Protecting the UK's undersea cables from hostile actors*. Policy Exchange. https://policyexchange.org.uk/publication/from-space-to-seabed/#contents_accordion
- HGC Global Communications. (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. <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-telecommunication-hub>
- Hinck, G. (2017, November 21). *Cutting the Cord: The Legal Regime Protecting Undersea Cables*. Lawfare. <https://www.lawfaremedia.org/article/cutting-cord-legal-regime-protecting-undersea-cables>
- Humbert, M. (2022, October 24). *Fiber-optic Submarine Cable near Faroe and Shetland Islands Damaged; Mediterranean Cables also Cut*. High North News. <https://www.highnorthnews.com/en/fiber-optic-submarine-cable-near-faroe-and-shetland-islands-damaged-mediterranean-cables-also-cut>
- Hunter, G. S. (2023, June 11). *Cable Cutters*. The Wire China. <https://www.thewirechina.com/2023/06/11/cable-cutters-matsu-taiwan-china-undersea-internet-cables/>
- International Cable Protection Committee. (n.d.). *Critical infrastructure submarine telecommunications cables*. International Cable Protection Committee. <https://www.iscpc.org/documents/?id=141>
- International Maritime Organization. (n.d.). *Registration of ships and fraudulent registration matters*. International Maritime Organization. <https://www.imo.org/en/OurWork/Legal/Pages/Registration-of-ships-and-fraudulent-registration-matters.aspx>
- Kauranen, A., Lehto, E., Adomaitis, N., Ahlander, J., Jacobsen, S., Sytas, A., Ringstrom, A., Johnson, S., Olenska, A., & Luoma, E. (2025, February 23). *Underwater Sabotage: A Baltic Sea Timeline*. MarineLink. <https://www.marinelink.com/news/underwater-sabotage-a-baltic-sea-timeline-522672#:~:text=OCTOBER%202023:%20BALTICCONNECTOR%20GAS%20PIPE%20AND%20CABLES,a%20port%20near%20St%20Petersburg%20in%20Russia.>
- King, C. (2022, October 23). *Serious incident involving CUT underwater cables in South of France affects internet worldwide*. Euro Weekly News. <https://euroweeklynews.com/2022/10/23/serious-incident-involving-cut-underwater-cables-in-south-of-france-affects-internet-worldwide/>
- Kirby, P. (2024, December 27). *Estonia navy to protect undersea power link after main cable damaged*. BBC. <https://www.bbc.com/news/articles/c1elq7lx9qdo>
- Kottasová, I. (2024, November 21). *European officials cry sabotage after two internet cables are cut in the Baltic Sea*. CNN. <https://www.cnn.com/2024/11/19/europe/sabotage-undersea-cables-cut-baltic-sea-intl/index.html>
- Kulha, S. (2021, November 11). *Norway's strategic underwater research observatory has cables cut, removed in suspicious act*. National Post. <https://nationalpost.com/news/world/norways-strategic-underwater-research-observatory-has-cables-cut-removed-in-suspicious-act>

- Kwai, I., Anderson, C., & Lemola, J. (2025, February 21). *Europe vows to step up Baltic Sea security after a new cable break*. The New York Times. <https://www.nytimes.com/2025/02/21/world/europe/baltic-sea-cable-sweden>
- Lee, Y. (2021, February 5). *China's latest weapon against Taiwan: the sand dredger*. Reuters. <https://www.reuters.com/graphics/TAIWAN-CHINA/SECURITY/jbyvrnzerve/>
- Leicester, J. (2022, October 21). *French police probe multiple cuts of major internet cables*. AP News. <https://apnews.com/article/technology-europe-france-marseille-business-49d27ccc0195f1c48b33a5634232031f>
- Lemola, J., & Chutel, L. (2024, December 26). *Finland Says Vessel Suspected of Cutting Cable May Be Part of Russia's 'Shadow Fleet'*. The New York Times. <https://www.nytimes.com/2024/12/26/world/europe/finland-estonia-cables-russia.html>
- Le Monde, AP News, & Agence France Presse [AFP]. (2024, July 29). *Fiber optic networks 'sabotaged' in parts of France*. Le Monde. https://www.lemonde.fr/en/france/article/2024/07/29/fiber-optic-networks-sabotaged-in-parts-of-france_6703674_7.html
- Libell, H. P., & Chutel, L. (2025, January 31). *Norway Seizes Russian-Crewed Ship Suspected of Cutting an Undersea Cable*. The New York Times. <https://www.nytimes.com/2025/01/31/world/europe/norway-russia-ship-baltic-undersea-cable.html>
- Lii, W. (2023, April 15). *After Chinese Vessels Cut Matsu Internet Cables, Taiwan Seeks to Improve Its Communications Resilience*. The Diplomat. <https://thediplomat.com/2023/04/after-chinese-vessels-cut-matsu-internet-cables-taiwan-shows-its-communications-resilience/>
- LIRNEasia. (2007, June 2). *Vietnam's submarine cable 'lost' and 'found'*. LIRNEasia. <https://lirneasia.net/2007/06/vietnams-submarine-cable-lost-and-found/>
- Lott, A. (2024, December 31). *Christmas Day Cable Cuts in the Baltic Sea*. EJIL:Talk. <https://www.ejiltalk.org/christmas-day-cable-cuts-in-the-baltic-sea/#:~:text=In%20December%202024%2C%20the%20submarine,is%20described%20here%20and%20here.>
- Martin, A. (2022, October 19). *Fishing vessel, not sabotage, to blame for Shetland Island submarine cable cut*. The Record. <https://therecord.media/fishing-vessel-not-sabotage-to-blame-for-shetland-island-submarine-cable-cut>
- McCartney, M. (2025, February 26). *Coast Guard Boards China-Owned Ship Over Undersea Cable Sabotage*. Newsweek. <https://www.newsweek.com/taiwan-seizes-china-owned-ship-undersea-cable-sabotage-2036517>
- Miller, G., Dixon, R., & Stanley-Becker, I. (2025, January 19). *Accidents, not Russian sabotage, behind undersea cable damage, officials say*. The Washington Post. <https://www.washingtonpost.com/world/2025/01/19/russia-baltic-undersea-cables-accidents-sabotage/>
- Ministry of Defence. (2023, October 19). *Damaged telecommunications cable between Sweden and Estonia*. Government Offices of Sweden. <https://government.se/articles/2023/10/damaged-telecommunications-cable-between-sweden-and-estonia/>
- Moss, S. (2024, December 3). *Sweden-Finland terrestrial Internet cable cut, sabotage suspected*. Data Center Dynamics. <https://www.datacenterdynamics.com/en/news/sweden-finland-terrestrial-internet-cable-cut-sabotage-suspected/>
- Moss, S. (2022, October 24). *Saboteurs cut fiber cables in France, in second incident this year*. Data Center Dynamics. <https://www.datacenterdynamics.com/en/news/saboteurs-cut-fiber-cables-in-france-in-second-incident-this-year/>
- Newdick, T. (2021, November 11). *Norwegian Undersea Surveillance Network Had Its Cables Mysteriously Cut*. The Warzone. <https://www.twz.com/43094/norwegian-undersea-surveillance-network-had-its-cables-mysteriously-cut>
- Newdick, T. (2022, January 11). *Undersea Cable Connecting Norway With Arctic Satellite Station Has Been Mysteriously Severed*. The Warzone. <https://www.twz.com/43828/undersea-cable-connecting-norway-with-arctic-satellite-station-has-been-mysteriously-severed#:~:text=The%20latest%20disruption%20involves%20one,was%20first%20widely%20reported%20yesterday.>

- News Wires. (2025, January 26). *Sweden launches sabotage probe after another data cable damaged in Baltic Sea*. France24. <https://www.france24.com/en/europe/20250126-another-undersea-cable-damaged-in-baltic-sea-latvia-dispatches-warship>
- Nilsen, T. (2022, January 9). *Disruption at one of two undersea cables to Svalbard*. The Barents Observer. <https://www.thebarentsobserver.com/arctic/disruption-at-one-of-two-undersea-cables-to-svalbard/119477>
- O'Sullivan, D. (2025, January 27). *Sweden seizes and boards ship suspected of cable damage in Baltic Sea*. Euronews. <https://www.euronews.com/2025/01/27/sweden-seizes-ship-suspected-of-cable-damage-in-baltic-sea>
- Pollard, N., & Kauranen, A. (2023, October 17). *Sweden says telecom cable with Estonia damaged but operating*. Reuters. <https://www.reuters.com/world/europe/sweden-says-telecom-cable-with-estonia-damaged-2023-10-17/>
- Porter, T. (2024, December 3). *A cut internet cable on Russia's doorstep raises the prospect of more sabotage*. Business Insider. <https://www.businessinsider.com/cut-internet-cable-in-finland-causes-outage-possible-sabotage-2024-12#:~:text=The%20severance%20of%20two%20overland,Finland%2C%20affecting%20thousands%20of%20households>
- Preuitt, L. (2009, April 9). *\$250K Reward Out for Vandals Who Cut AT&T Lines*. NBC Bay Area. <https://www.nbcbayarea.com/news/local/south-bay-dead-zone/1871913/>
- Radio Jamaica News. (2008, March 4). *Cable theft leaves St. Catherine communities without phone service*. Radio Jamaica News. <https://radiojamaicanewsonline.com/local/cable-theft-leaves-st-catherine-communities-without-phone-service>
- Reed, S. (2024, March 5). *Damage to Cables Under Red Sea Highlights Mideast Conflict's Broader Threats*. The New York Times. <https://www.nytimes.com/2024/03/05/business/red-sea-middle-east-conflict.html>
- Reuters. (2013, March 27). *Egypt catches divers cutting Internet cable amid disruptions*. Reuters. <https://www.reuters.com/article/technology/egypt-catches-divers-cutting-internet-cable-amid-disruptions-idUSBRE92Q1AQ/>
- Reuters. (2025a, February 21). *Finland, Sweden investigate suspected sabotage of Baltic Sea telecoms cable*. Reuters. <https://www.reuters.com/world/europe/sweden-investigates-possible-breach-undersea-cable-baltic-sea-prime-minister-2025-02-21/>
- Reuters. (2025b, February 25). *China says Taiwan 'manipulating' undersea cable cutting incident before facts clear*. Reuters. <https://www.reuters.com/world/asia-pacific/china-says-taiwan-manipulating-undersea-cable-cutting-before-facts-clear-2025-02-26/>
- Rintakumpu, F., Arts, S., & Ondraskova, J. (2025, January 10). *Tensions Under the Baltic Sea*. The German Marshall Fund of the United States. <https://www.gmfus.org/news/tensions-under-baltic-sea>
- Rosman, R. (2024, December 31). *What to know about Finland, Russia's 'shadow fleet' and a severed cable*. NPR. <https://www.npr.org/2024/12/31/nx-s1-5243302/finland-russia-severed-undersea-cable-shadow-fleet>
- Runde, D. F., Murphy, E. L., & Bryja, T. (2024, August 16). *Safeguarding subsea cables: Protecting cyber infrastructure amid great power competition*. Center for Strategic and International Studies. <https://www.csis.org/analysis/safeguarding-subsea-cables>
- Saffo, P. (2013, April 4). *Disrupting Undersea Cables: Cyberspace's Hidden Vulnerability*. Atlantic Council. <https://www.atlanticcouncil.org/blogs/new-atlanticist/disrupting-undersea-cables-cyberspaces-hidden-vulnerability/>
- Schwartz, M., Xiao, M., & Mellen, R. (2024, December 11). *E.U. Vessels Surround Anchored Chinese Ship After Baltic Sea Cables Are Severed*. The New York Times. <https://www.nytimes.com/2024/11/27/world/europe/baltic-sea-cables-chinese-ship.html>
- Sharwood, S. (2025, January 6). *Taiwan reportedly claims China-linked ship damaged one of its submarine cables*. The Register. https://www.theregister.com/2025/01/06/taiwan_china_submarine_cable_claim/
- Shephard News Team. (2025, January 9). *Joint Expeditionary Force launches AI protection net for undersea cables*. Shephard Media. <https://www.shephardmedia.com/news/naval-warfare/joint-expeditionary-force-launches-ai-protection-net-for-undersea-cables/>
- Singel, R. (2007, June 27). *Vietnamese Fisherman Charged With Harvesting Fiber Optic Cable*. WIRED. <https://www.wired.com/2007/06/vietnamese-fi-1/>

- Smith, P. (2008, February 12). *New focus on undersea Internet cable security after cuts*. The Christian Science Monitor. <https://www.csmonitor.com/World/terrorism-security/2008/0212/p99s01-duts.html>
- Staff Writer with AFP. (2025, January 28). *Taiwan Identifies 52 'Suspicious' Chinese Ships for Close Monitoring*. The Defense Post. <https://thedefensepost.com/2025/01/28/taiwan-chinese-ships-monitoring/>
- Staalesen, A. (2022, February 11). *'Human activity' behind Svalbard cable disruption*. The Barents Observer. <https://www.thebarentsobserver.com/security/human-activity-behind-svalbard-cable-disruption/160886>
- Starosielski, N. (2015, November 4). *How can we protect the internet's undersea cables?*. World Economic Forum. <https://www.weforum.org/stories/2015/11/how-can-we-protect-the-internets-undersea-cables/#:~:text=And%20there%20was%20speculation%20about,about%20200%20times%20each%20year.&text=The%20fact%20is%20it's%20incredibly%20difficult%20to%20monitor%20these%20lines.>
- Tatlow, D. K. (2025, January 10). *Exclusive—Chinese Patents Reveal Aim to Cut Undersea Cables*. Newsweek. <https://www.newsweek.com/china-conflict-undersea-cables-cutting-internet-data-subsea-marine-baltic-taiwan-2012396>
- The Daily Star. (2007, November 14). *Submarine cable link 'sabotaged' again*. The Daily Star. <https://www.thedailystar.net/news-detail-11573>
- The Financial Express. (2007, November 20). *Submarine link restored after 2nd 'cut' in 6 days*. The Financial Express. <https://today.thefinancialexpress.com.bd/last-page/submarine-link-restored-after-2nd-cut-in-6-days>
- The Maritime Executive. (2024, December 18). *Bulker Accused of Cutting Baltic Cables May Have Tried Once Before*. The Maritime Executive. <https://maritime-executive.com/article/chinese-bulker-accused-of-cutting-baltic-cables-may-have-tried-once-before>
- Thompson, P. (2024, July 29). *French infrastructure was targeted for a 2nd time during the Olympics, with internet and phone cables cut across the country*. Business Insider. <https://www.businessinsider.com/french-fiber-optic-cables-cut-phone-internet-services-infrastructure-attack-2024-7>
- Tobin, M., & Chiang, V. (2023, March 9). *Internet outage has Taiwan worried about threat from Chinese sabotage*. The Washington Post. <https://www.washingtonpost.com/world/2023/03/09/taiwan-matsu-internet-access-china-fishing/>
- Tobin, M., Xiao, M., & Chang Chien, A. (2025, January 5). *Taiwan Says It Suspects a Chinese-Linked Ship Damaged an Undersea Internet Cable*. The New York Times. <https://www.nytimes.com/2025/01/07/world/asia/taiwan-internet-cable-china.html>
- Traficom. (2024, December 26). *Traficom participates in investigating cable damage in the Gulf of Finland*. Traficom. <https://traficom.fi/fi/ajankohtaista/traficom-mukana-selvittamassa-suomenlahden-kaapelivaurioita>
- United Nations Convention on the Law of the Sea. December 10, 1982, https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf
- Webmaster. (2011a, March 18). *Submarine Cable Cuts in Jan-Feb, 2008 in the Persian Gulf and the Mediterranean*. Submarine Cable Networks. <https://www.submarinenetworks.com/en/nv/news/cable-cuts-in-jan-feb-2008>
- Webmaster. (2011b, March 18). *Undersea Cable Cuts in the Mediterranean Affected 14 Countries*. Submarine Cable Networks. <https://www.submarinenetworks.com/en/nv/news/cable-cuts-affected-14-countries>
- Weissberger, A. (2022, November 5). *Sabotage or Accident: Was Russia or a fishing trawler responsible for Shetland Island cable cut?*. IEEE ComSoc Technology Blog. <https://techblog.comsoc.org/2022/11/05/was-russia-or-a-fishing-trawler-responsible-for-shetland-island-cable-cut/>
- Windward. (n.d.). *UPDATED: Illuminating Russia's Shadow Fleet*. Windward.ai. <https://windward.ai/knowledge-base/illuminating-russias-shadow-fleet/>
- Wollan, M. (2009, April 10). *California: Vandals Cut Phone Cables, Police Say*. The New York Times. https://www.nytimes.com/2009/04/10/us/10brfs-VANDALSCUTPH_BRF.html
- Young, I. (2024, February). *Submarine Cable Damage around the Red Sea*. gCaptain. <https://forum.gcaptain.com/t/submarine-cable-damage-around-the-red-sea/68625>

Risks and Threats

- AP News. (2025, February 25). Taiwan is investigating a Chinese-crewed ship believed to have severed an undersea cable. *AP News*. <https://apnews.com/article/taiwan-undersea-cable-penqhu-islands-china-14bfd6ddad184d77ae45068fee9b37d2>
- Cwalina, A. (2022). Concerns grow over possible Russian sabotage of undersea cables. *Atlantic Council*. <https://www.atlanticcouncil.org/blogs/ukrainealert/concerns-grow-over-possible-russian-sabotage-of-undersea-cables/>
- Bafoutsou, G., Papaphilippou, M., & Dekker, M. (2023, July). *Subsea cables - what is at stake?* The European Union Agency for Cybersecurity [ENISA]. <https://www.enisa.europa.eu/sites/default/files/publications/Undersea%20cables%20-%20What%20is%20a%20stake%20report.pdf>
- Bell, B. (2025, February 24). Russia's escalating hybrid war: The "Shadow Fleet" and undersea internet cable sabotage. *The Generation*. <https://the-generation.net/russias-escalating-hybrid-war-the-shadow-fleet-and-undersea-internet-cable-sabotage/>
- Burgess, M. (2022, November 2). The most vulnerable place on the internet. *WIRED*. <https://www.wired.com/story/submarine-internet-cables-egypt>
- Cable Laying/Repair Ship -T-ARC. (2021). America's Navy. <https://www.navy.mil/Resources/Fact-Files/Display-FactFiles/Article/2232652/cable-layingrepair-ship-t-arc/>
- Caro, C. J. V. (2024, November 26). Underwater geopolitics. *RealClearDefense*. https://www.realcleardefense.com/articles/2024/11/26/underwater_geopolitics_1074698.html
- Coker, J. (2024). Submarine cables at risk of cyber attacks. *Infosecurity Magazine*. <https://www.infosecurity-magazine.com/news/submarine-cables-risk-cyber-attacks/>
- Congressional Research Service. (2023). *Protection of undersea telecommunication cables*. <https://crsreports.congress.gov/product/pdf/R/R47648>
- Crisis24. (2024, December 20). Rising geopolitical tensions highlight vulnerabilities in global undersea cable networks. *Crisis24*. <https://crisis24.garda.com/articles/rising-geopolitical-tensions-highlight-vulnerabilities-in-global-underseas-cable-networks>
- Eleftherakis, D., & Vicen-Bueno, R. (2020). Sensors to increase the security of underwater communication cables: A review of underwater monitoring sensors. *Sensors*, 20(3), 737. <https://doi.org/10.3390/s20030737>
- European Commission. (2024, February 26). *Commission Recommendation (EU) 2024/779 of 26 February 2024 on Secure and Resilient Submarine Cable Infrastructures*. Official Journal of the European Union. <https://eur-lex.europa.eu/eli/reco/2024/779/oj>
- European Parliament. (2022). Submarine cables: Critical infrastructure for global communications and the economy. Policy Department for External Relations, Directorate General for External Policies of the Union. https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA%282022%29702557_EN.pdf
- European Union Institute for Security Studies. (2024). Submarine cables: Strategic vulnerabilities in a digital world. *ISS Europa*. https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_2024-19_Submarine%20cables.pdf
- Farge, E. (2024, December 12). UN body to protect vulnerable submarine cables after ruptures. *Reuters*. <https://www.reuters.com/technology/un-body-protect-vulnerable-submarine-cables-after-ruptures-2024-12-12/>
- Financial Times. (2024). China's growing grip on the world's undersea cable network. <https://ig.ft.com/subsea-cables/>
- Guarascio, F., Nguyen, P., & Brock, J. (2024, September 17). Inside the US push to steer Vietnam's subsea cable plans away from China. *Reuters*. <https://www.reuters.com/business/media-telecom/inside-us-push-steer-vietnams-subsea-cable-plans-away-china-2024-09-17/>
- Hellenic Shipping News. (2024). Malacca Strait: How one volcano could trigger world chaos. <https://www.hellenicshippingnews.com/malacca-strait-how-one-volcano-could-trigger-world-chaos/>

- Indo-Pacific Affairs. (2024). Entangled: Southeast Asia and the geopolitics of undersea cables. <https://manoa.hawaii.edu/indopacificaffairs/article/entangled-southeast-asia-and-the-geopolitics-of-undersea-cables/>
- Integral Consulting. (2024, April 10). Submarine cables face geohazard risks with significant societal impacts. JD Supra. <https://www.jdsupra.com/legalnews/submarine-cables-face-geohazard-risks-2821485/>
- International Cable Protection Committee. (2021, March). Submarine cable protection and the environment (Issue 2). https://www.iscpc.org/publications/submarine-cable-protection-and-the-environment/ICPC_Public_EU_March%202021.pdf
- International Cable Protection Committee. (2022). Government best practices for protecting and promoting resilience of submarine telecommunications cables. <https://www.iscpc.org/publications/icpc-best-practices/>
- Internet Society. (2023). Are subsea cables feeling the heat from climate change? <https://pulse.internetsociety.org/blog/are-subsea-cables-feeling-the-heat-from-climate-change>
- Jackson, A. (2024, November 25). The consequences of severed subsea communications cables. Data Centre Magazine. <https://datacentremagazine.com/networking/the-consequences-of-severed-subsea-communications-cables>
- Khazan, O. (2013, July 16). The creepy, long-standing practice of undersea cable tapping. *The Atlantic*. <https://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/>
- Leicester, J., & Burrows, E. (2025, January). NATO launches Operation Baltic Sentry to protect undersea infrastructure. *AP News*. <https://apnews.com/article/764964a275530915c2cc5af1125ec125>
- McNamara, E. (2024, August 28). Reinforcing resilience: NATO's role in enhanced security for critical undersea infrastructure. *NATO Review*. <https://www.nato.int/docu/review/articles/2024/08/28/reinforcing-resilience-natos-role-in-enhanced-security-for-critical-undersea-infrastructure/index.html>
- Monaghan, S., & Darrah, M. (2024, March 7). Red Sea cable damage reveals soft underbelly of global economy. Center for Strategic and International Studies. <https://www.csis.org/analysis/red-sea-cable-damage-reveals-soft-underbelly-global-economy>
- Nakamura, H. (2023, June 29). The enemy below: Fighting against Russia's hybrid underwater warfare. Center for Maritime Strategy. <https://centerformaritimestrategy.org/publications/the-enemy-below-fighting-against-russias-hybrid-underwater-warfare/>
- Network Computing. (2023). Geopolitics and climate change heighten undersea cable concerns. <https://www.networkcomputing.com/network-cabling/geopolitics-and-climate-change-heighten-undersea-cable-concerns>
- Norwegian Institute of International Affairs. (2022). The subsea cable cut at Svalbard January 2022: What happened, what were the consequences, and how were they managed? <https://www.nupi.no/en/publications/cristin-pub/the-subsea-cable-cut-at-svalbard-january-2022-what-happened-what-were-the-consequences-and-how-were-they-managed>
- Patel, N. (2025). How fiber optic cables power the internet and the future of AI. *The Verge*. <https://www.theverge.com/24351247/ciena-fiber-optic-internet-subsea-cables-wdm-ai-hyperscale-data-decoder-podcast-interview>
- Qiu, W. (2011, March 19). Submarine cables cut after Taiwan earthquake in Dec 2006. *Submarine Networks*. <https://www.submarinenetworks.com/en/nv/news/cables-cut-after-taiwan-earthquake-2006>
- Runde, D. F., Murphy, E. L., & Bryja, T. (2024, August 16). *Safeguarding subsea cables: Protecting cyber infrastructure amid great power competition*. Center for Strategic and International Studies. <https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition>
- Sherman, J. (2021, September 13). Cyber defense across the ocean floor: The geopolitics of submarine cable security. Atlantic Council. <https://www.atlanticcouncil.org/in-depth-research-reports/report/cyber-defense-across-the-ocean-floor-the-geopolitics-of-submarine-cable-security/>
- Sontag, S., Drew, C., & Drew, C. (1998). *Blind man's bluff: The untold story of American submarine espionage*. HarperCollins.
- Submarine Networks. (2011, June 20). AAG (Asia-America Gateway) Submarine Cable System. <https://www.submarinenetworks.com/en/systems/trans-pacific/aag>

- Sze, S. (2023). Enhancing the resilience of undersea cables in the Indo-Pacific. S. Rajaratnam School of International Studies. <https://rsis.edu.sg/rsis-publication/rsis/enhancing-the-resilience-of-undersea-cables-in-the-indo-pacific/>
- Thompson, N. (2025, January 8). The undersea cable war hits Taiwan. The Cipher Brief. https://www.thecipherbrief.com/column_article/the-undersea-cable-war-hits-taiwan
- United Nations Office for Disaster Risk Reduction. (2022). *Climate change and infrastructure resilience: the impact of extreme weather events on undersea cables*. <https://www.undrr.org/explainer/the-invisible-toll-of-disasters-2022#:~:text=In%20January%2C%20when%20Tonga%20was,and%20to%20provide%20human%20contact>
- Veverka, D. (2011, September). Under the sea. *Shipping and Marine*, 14-15. <https://www.iscpc.org/documents/?id=201>
- Wall, C., & Morcos, P. (2021, June 11). Invisible and vital: Undersea cables and transatlantic security. Center for Strategic and International Studies. <https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security>

International Agreements and Forums

- Convention for the Protection of Submarine Telegraph Cables, March 14, 1884, <https://nsarchive.gwu.edu/sites/default/files/documents/5975790/National-Security-Archive-Convention-for-the.pdf>
- Geneva Conventions of the Continental Shelf and High Seas, November 7, 1958, https://treaties.un.org/doc/Treaties/1964/11/19641122%2002-14%20AM/Ch_XXI_01_2_3_4_5p.pdf
- Guilfoyle, D., Paige, T. P., & McLaughlin, R. (2022, July 25). The final frontier of cyberspace: The seabed beyond national jurisdiction and the Protection of Submarine Cables: International & Comparative Law Quarterly. Cambridge Core. <https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/final-frontier-of-cyberspace-the-seabed-beyond-national-jurisdiction-and-the-protection-of-submarine-cables/4A40325D1A18927145A36B70ADCD35AD>
- Hayes, J. F., & Schwartz, M. (2008). A history of transatlantic cables. <https://ieeexplore.ieee.org/document/4623705/>
- International Cable Protection Committee. (n.d.). *Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables*. <https://www.iscpc.org/documents/?id=3733>
- International Cable Protection Committee. (2023). *Join the ICPC*. <https://iscpc.org/join-the-icpc/>
- International Cable Protection Committee. (2025a). *About the ICPC*. <https://www.iscpc.org/about-the-icpc/>
- International Cable Protection Committee. (2025b). *Member List*. <https://www.iscpc.org/about-the-icpc/member-list/>
- International Telecommunication Union. (n.d.a). *About International Telecommunication Union (ITU)*. <https://www.itu.int/en/about/Pages/default.aspx>
- International Telecommunication Union. (n.d.b). *Member States*. <https://www.itu.int/hub/membership/our-members/directory/?myitu-members-states=true&request=countries>
- International Telecommunication Union. (n.d.c). *International advisory body for submarine cable resilience*. <https://www.itu.int/digital-resilience/submarine-cables/advisory-body/>
- International Telecommunication Union. (1992, December 22). *Constitution of the International Telecommunication Union*. <https://www.itu.int/en/council/Documents/basic-texts/Constitution-E.pdf>
- International Telecommunication Union. (2012a). *United States of America Proposals for the Work of the Conference*. World Conference on International Telecommunications. <https://2009-2017.state.gov/documents/organization/196244.pdf>
- International Telecommunication Union. (2012b). *Final Acts—World Conference on International Telecommunications*. <https://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf>
- International Telecommunication Union. (2025a). *Panel 4 – Legal and Regulatory Frameworks for Cable Protection* [Video], YouTube. <https://www.youtube.com/watch?v=NrbFjtcQAMM&list=TLPQMjgwMjIwMjI4-V5u57LYw&index=11>

- International Telecommunication Union (2025b). *Press briefing on International Advisory Body for Submarine Cable Resilience* [Video]. YouTube. <https://www.youtube.com/watch?v=b03h3I6VQKM&list=TLPQMDYwMjIwMjFxpjDE4NqA&index=37>
- Institute of International Law. (1913). *Manual of the Laws of Naval War*. August 9, 1913. <https://ihl-databases.icrc.org/en/ihl-treaties/oxford-manual-1913>
- Oxford, Manual of the Laws of Naval War, August 9, 1913. <http://hrlibrary.umn.edu/instreet/1913a.htm>
- Statement of Roger Rufe President, The Ocean Conservancy {PRIVATE} Before the Senate Committee on Foreign Relations. (2003). (testimony of Roger Rufe). <https://www.foreign.senate.gov/imo/media/doc/RufeTestimony031021.pdf>
- United Nations Convention on the Law of the Sea, December 10, 1982, https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf
- United Nations Convention on the Territorial Sea and the Contiguous Zone, November 26, 1964, https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XXI-1&chapter=21
- U.S. Department of Defense. (2015). Department of defense law of war manual. <https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf>

Case Study: Baltic Sea

- Agence France-Presse (2025). *Sweden to send three ships, aircraft to NATO's Baltic patrol mission: PM*. NewsBank. https://infoweb-newsbank-com.offcampus.lib.washington.edu/apps/news/document-view?p=WORLDNEWS&t=&sort=YMD_date%3AD&hide_duplicates=2&fld-base-0=alltext&maxresults=60&val-base-0=%28Sweden%20to%20send%20three%20ships%2C%20aircraft%20to%20NATO%27s%20Baltic%20patrol%20mission&docref=news/19E0FD4854EBA2F8
- Alcatel Submarine Networks. (n.d.). *About us*. Alcatel Submarine Networks. <https://www.asn.com/about-us/>
- Altman, H. (2025). *Drone Boats Being Rushed To Help Prevent Baltic Seafloor Cable Sabotage*. The Warzone. <https://www.twz.com/news-features/drone-boats-being-rushed-to-help-prevent-baltic-seafloor-cable-sabotage>
- Astier, H., & Kirby, P. (2024). *Germany suspects sabotage behind severed undersea cables in the Baltic*. BBC News. <https://www.bbc.com/news/articles/c9d14vxw501o>
- BBC. (2025). *Lithuanian army, power grid operator to boost security of subsea infrastructure*. NewsBank. https://infoweb-newsbank-com.offcampus.lib.washington.edu/apps/news/document-view?p=WORLDNEWS&t=&sort=YMD_date%3AD&hide_duplicates=2&fld-base-0=alltext&maxresults=60&val-base-0=Lithuanian%20army%2C%20power%20grid%20operator%20to%20boost%20security%20of%20subsea%20infrastructure&docref=news/19E189E950BA41D0
- Benner, T. (2025). *The Underwater Battlefield: Protecting Submarine Critical Infrastructure*. Internationale Politik Quarterly. <https://ip-quarterly.com/en/underwater-battlefield-protecting-submarine-critical-infrastructure>
- Bockmann, M. (2024). *Russia-linked cable-cutting tanker seized by Finland 'was loaded with spying equipment'*. Lloyds List. <https://www.lloydslist.com/LL1151955/Russia-linked-cable-cutting-tanker-seized-by-Finland-was-loaded-with-spying-equipment>
- Braw, E. (2024). *The Baltic Sea's Bad Actors*. Foreign Policy. https://foreignpolicy.com/2024/12/04/russia-china-baltic-sea-nato-subsea-cables-ais-spoofing/?utm_content=gifting&tpcc=gifting_article&gifting_article=cnVzc2lhLWNoaW5hLWJhbHRpYy1zZWEtbmF0by1zdWJzZWVtY2FibGVzLWVpcy1zcG9vZmluZw==&pid=CW941515
- Brennan, D. (2025). *Baltic Sea undersea 'sabotage' sets stage for escalating NATO-Russia contest*. ABC News. <https://abcnews.go.com/International/baltic-sea-undersea-sabotage-sets-stage-escalating-nato/story?id=117594533>
- Brovko, L. (2024). *A Russian shadow fleet vessel that could have damaged an underwater cable was detained in Finland*. Babel. <https://babel.ua/en/news/113986-a-russian-shadow-fleet-vessel-that-could-have-damaged-an-underwater-cable-was-detained-in-finland>

- Browne, R. (2024). *Undersea cable cuts in the Baltic Sea are stoking geopolitical tensions — here's what's going on*. CNBC. <https://www.cnbc.com/2024/11/28/explainer-baltic-sea-undersea-cable-cuts-stoke-geopolitical-tensions.html>
- Bryant, M., & Sauer, P. (2024). *Swedish police focus on Chinese ship after suspected undersea cable sabotage*. The Guardian. <https://www.theguardian.com/world/2024/nov/20/sweden-denmark-undersea-cable-sabotage-navy-investigation>
- Buchholz, K. (2025). *Baltic Sea Cable Incidents Pile Up – Who Is To Blame*. Forbes. <https://www.forbes.com/sites/katharinabuchholz/2025/01/31/baltic-sea-cable-incidents-pile-up-who-is-to-blame/>
- CE Noticias Financieras: English (2025). *Brussels targets China and Russia over Baltic incidents and calls for Eu-wide reaction*. NewsBank. https://infoweb-newsbank-com.offcampus.lib.washington.edu/apps/news/document-view?p=WORLDNEWS&t=&sort=YMD_date%3AD&hide_duplicates=2&fld-base-0=alltext&maxresults=60&val-base-0=%28Brussels%20targets%20China%20and%20Russia%20over%20Baltic%20incidents%20and%20calls%20for%20EU-wide%20reaction&docref=news/19E7E4DE6BAA67E0
- Chiappa, C., & Ngendakumana, P. (2023). *'Everything indicates' Chinese ship damaged Baltic pipeline on purpose, Finland says*. Politico. <https://www.politico.eu/article/balticconnector-damage-likely-to-be-intentional-finnish-minister-says-china-estonia/#:~:text=Finland%20and%20Estonia%20have%20been%20investigating%20the,cables%20connecting%20Estonia%20to%20Finland%20and%20Sweden.>
- Desmarais, A. (2024). *Europe's Achilles Heel? Why the Baltic region is the most vulnerable to subsea sabotage*. Euronews. <https://www.euronews.com/next/2024/10/15/europes-achilles-heel-why-the-baltic-region-is-the-most-vulnerable-to-subsea-sabotage>
- Dufetre, R. (2023). *The data roads under the seas. American hegemony over the global undersea cable network and its potential challengers*. University of Chicago. <https://doi.org/10.6082/UCHICAGO.7155>
- Eastern Light. (n.d.). *Eastern Light dark fiber build-out*. Eastern Light. <https://easternlight.se/build-out/>
- European Union External Action Service. (2024). *Joint Statement by the European Commission and the High Representative on the Investigation into Damaged Electricity and Data Cables in the Baltic Sea*. European Union. https://www.eeas.europa.eu/eeas/joint-statement-european-commission-and-high-representative-investigation-damaged-electricity-and_en#:~:text=We%20will%20propose%20further%20measures,repair%20capabilities%2C%20and%20in%20international%20cooperation.
- Elisa. (n.d.). *About Us*. Elisa. <https://elisa.com/corporate/>
- Encyclopædia Britannica, inc. (2025). *Baltic Sea*. Encyclopædia Britannica. <https://www.britannica.com/place/Baltic-Sea>
- Ericsson (n.d.). *About us*. Ericsson. <https://www.ericsson.com/en/about-us/company-facts/our-purpose>
- European Commission. (2025). *Visit of Henna Virkkunen, Executive Vice-President of the European Commission, Andrius Kubilius and Magnus Brunner, European Commissioners, to Finland: joint press statement* [Video]. Audiovisual Service of the European Commission. <https://audiovisual.ec.europa.eu/en/video/I-267460>
- European Parliament. (2024). *Security and defense implications of China's influence on critical infrastructure in the European Union*. Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202405719
- Fingrid. (2017). *EstLink 2 – second high-voltage direct current link between Finland and Estonia*. Fingrid. <https://www.fingrid.fi/en/grid/construction/arkisto/estlink-2/>
- Government Communication Unit. (2024). *12 European Countries Crack Down on Russia's 'Shadow Fleet'*. Embassy of Estonia Helsinki. <https://helsinki.mfa.ee/en/12-european-countries-crack-down-on-russias-shadow-fleet/>
- Kayali, L. (2023). *Sorry Russia, the Baltic Sea is NATO's lake now*. POLITICO. <https://www.politico.eu/article/nato-lake-what-sweden-and-finland-will-change-in-the-baltics-russia-ukraine-war/>
- Lott, A. (2024). *Christmas Day Cable Cuts in the Baltic Sea*. Blog of the European Journal of International Law. <https://www.ejiltalk.org/christmas-day-cable-cuts-in-the-baltic-sea/>

- Martin, A. (2025). *Finnish investigators suspect Baltic Sea cable damage was intentional*. The Record. <https://therecord.media/finland-investigators-undersea-cable-damage-appears-intentional#>
- Ministry of Defence (2023). *Damaged telecommunications cable between Sweden and Estonia*. Government Offices of Sweden. <https://government.se/articles/2023/10/damaged-telecommunications-cable-between-sweden-and-estonia/>
- Ministry of Defence, Foreign, Commonwealth & Development Office, The Rt Hon Sir Keir Starmer KCB KC MP, & The Rt Hon John Healey MP. (2025). *Joint Expeditionary Force activates UK-led reaction system to track threats to undersea infrastructure and monitor Russian shadow fleet*. GOV.UK. <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>
- Motrunch, M. (2023). *Collaborating to Uncover 'Putin's Shadow War' in Scandinavia*. Global Investigative Journalism Network. [https://gijn.org/stories/uncovering-putins-shadow-war-scandinavia/#:~:text=\(AIS%20is%20a%20marine%20tracking,an%20agent%20of%20the%20Kremlin](https://gijn.org/stories/uncovering-putins-shadow-war-scandinavia/#:~:text=(AIS%20is%20a%20marine%20tracking,an%20agent%20of%20the%20Kremlin)
- Moyer, J. (2024). *The UK-led Joint Expeditionary Force's Impact on Northern European Security*. The Wilson Center. <https://www.wilsoncenter.org/article/uk-led-joint-expeditionary-forces-impact-northern-european-security>
- North Atlantic Treaty Organization. (2025). *NATO launches 'Baltic Sentry' to increase critical infrastructure security*. NATO. https://www.nato.int/cps/en/natohq/news_232122.htm
- Pancevski, B. (2024). *China Lets European Investigators Board Ship Suspected of Sabotage After Weeks of Secret Talks*. The Wall Street Journal. <https://www.wsj.com/world/china-lets-european-investigators-board-ship-suspected-of-sabotage-after-weeks-of-secret-talks-e68a2b75>
- Pawlak, J. (2024). *Charting the challenges in the Baltic Sea*. War on the Rocks. <https://warontherocks.com/2024/05/charting-the-challenges-in-the-baltic-sea/#:~:text=Crucially%2C%20the%20Baltic%20Sea%20is,Russia's%20White%20Sea%2DBaltic%20Canal>
- Rahr, A. (2025). *Baltic Sea: Europe's brewing security crisis*. News.Az. <https://news.az/news/-baltic-sea-europes-brewing-security-crisis>
- Reuters. (2024). *Chinese ship linked to Baltic Sea cable breach resumes voyage*. Reuters. <https://www.reuters.com/world/chinese-ship-linked-baltic-sea-cable-breach-resumes-voyage-2024-12-21/>
- Rintakumpu, F., & Arts, S., & Ondraskova, J. (2025) *Tensions Under the Baltic Sea*. The German Marshall Fund of the United States. <https://www.gmfus.org/news/tensions-under-baltic-sea>
- Schreiber, B.C., Ryan, W.B. (2025). *Red Sea*. Encyclopedia Britannica. <https://www.britannica.com/place/Red-Sea>
- SHAPE Public Affairs Office. (2025). *Baltic Sentry To Enhance NATO's Presence In The Baltic Sea*. Shape NATO. <https://shape.nato.int/news-releases/baltic-sentry-to-enhance-natos-presence-in-the-baltic-sea>
- Souisa, H. (2024). *Finland Estonia Connection (FEC) Submarine Cable System Map*. Fiber Atlantic. <https://www.fiberatlantic.com/cable/51a687JhtU3qKJPU5bt>
- Swedish Coast Guard. (2024). *Yi Peng 3 has left Scandinavia*. kustbevakningen. <https://www.kustbevakningen.se/en/more-news/yi-peng-3-has-left-scandinavia/>
- Tegler, E. (2023). *Investigating the Chinese Ship That 'Accidentally' Hit Undersea Lines*. Forbes. <https://www.forbes.com/sites/erictegler/2023/11/28/investigating-the-chinese-ship-that-accidentally-hit-undersea-lines/>
- TeleGeography. (n.d.). *Submarine Cable Map*. <https://www.submarinecablemap.com/>
- The Maritime Executive. (2024). *Chinese bulker accused of cutting Baltic cables may have tried once before*. The Maritime Executive. <https://maritime-executive.com/article/chinese-bulker-accused-of-cutting-baltic-cables-may-have-tried-once-before>
- Trakimavičius, L. (2021). *The Hidden Threat to Baltic Undersea Cables*. NATO Energy Security Centre of Excellence. <https://www.enseccoe.org/publications/the-hidden-threat-to-baltic-undersea-power-cables/>
- Voltri, J., & ERR News. (2023). *Estonia releases first photo of damaged communications cable*. ERR. <https://news.err.ee/1609147393/estonia-releases-first-photo-of-damaged-communications-cable>
- Yadav, N. (2025). *Baltic subsea cable damage was accidental, not sabotage - US and European officials*. Data Center Dynamics. <https://www.datacenterdynamics.com/en/news/baltic-subsea-cable-damage-was-accidental-not-sabotage-us-and-european-officials/>

Wallace, B. (2024). *Tensions Rise with Suspicious European Subsea Cable Cuts*. Network Computing. <https://www.networkcomputing.com/network-management/tensions-rise-with-suspicious-european-subsea-cable-cuts>

Case Study: South China Sea

- Association of Southeast Asian Nations (ASEAN). (2024). *ASEAN: Enhancing connectivity and resilience*. https://asean.org/wp-content/uploads/2024/12/ASEAN-AR-2024_e-pub_web.pdf
- Baum, A., Nikhita Salgame, & Ania Zolyniak. (2025). *Water Wars: Trump, Taiwan, and the Philippines*. Lawfare. <https://www.lawfaremedia.org/article/water-wars--trump--taiwan--and-the-philippines>
- BBC. (2023). What is the south china sea dispute?. BBC News. <https://www.bbc.com/news/world-asia-pacific-13748349>
- Braw, E. (2023, February 21). *China Is Practicing How to Sever Taiwan's Internet*. Foreign Policy. <https://foreignpolicy.com/2023/02/21/matsu-islands-internet-cables-china-taiwan/>
- Chang, W. (2025, February 26). *Taiwan detains Chinese-crewed ship suspected of cutting undersea cable*. CNN. <https://amp.cnn.com/cnn/2025/02/25/asia/taiwan-detains-ship-undersea-cable-intl-hnk>
- Cheung, E., Ripley, W., & Tsai, G. (2021, July 23). *How Taiwan is trying to defend against a cyber 'World War III'*. CNN Business. <https://www.cnn.com/2021/07/23/tech/taiwan-china-cybersecurity-intl-hnk/index.html>
- Chiang, V. and Tobin, M. (2023, March 9). *Internet outage has Taiwan worried about threat from Chinese sabotage*. The Washington Post. <https://www.washingtonpost.com/world/2023/03/09/taiwan-matsu-internet-access-china-fishing/>
- Congressional Research Service. (2023, August 21). *China Primer: South China Sea Disputes*. <https://crsreports.congress.gov/product/pdf/IF/IF10607>
- Davenport, Tara Maria. (2025). *The protection of submarine cables in Southeast Asia: The security gap and challenges and opportunities for regional cooperation*. <https://www.sciencedirect.com/science/article/pii/S0308597X24004354>
- Desurmont, J.M. (2024, May 21). *Territorial Claims and Subsea Cables: The Geopolitics of Invisible Lines in the South China Sea*. Bloomsbury Intelligence & Security Institute. <https://bisi.org.uk/reports/territorial-claims-and-subsea-cables-the-geopolitics-of-invisible-lines-in-the-south-china-sea>
- Guo, R. (2018). *South China Sea - an Overview | ScienceDirect Topics*. [www.sciencedirect.com](https://www.sciencedirect.com/topics/engineering/south-china-sea). <https://www.sciencedirect.com/topics/engineering/south-china-sea>
- Hiciano, L. (2025). *Undersea cable to Penghu severed, Chinese-funded ship suspected*. Taipei Times. <https://www.taipeitimes.com/News/taiwan/archives/2025/02/25/2003832488>
- Hinrix, F. (2024). *Building Resilience in Taiwan's Internet Infrastructure from Geopolitical Threats - The Henry M. Jackson School of International Studies*. The Henry M. Jackson School of International Studies. <https://jsis.washington.edu/news/building-resilience-in-taiwans-internet-infrastructure-from-geopolitical-threats/>
- Lee, C. (2024). *Undersea cables emerge as source of friction in South China Sea*. Voice of America; Voice of America (VOA News). <https://www.voanews.com/a/undersea-cables-emerge-as-source-of-friction-in-south-china-sea/7819426.html>
- Maizland, L., & Fong, C. (2025). *Why China-Taiwan relations are so tense*. Council on Foreign Relations. <https://www.cfr.org/background/asia-taiwan-relations-tension-us-policy-trump>
- Noor, E. (2024a). *Entangled: Southeast Asia and the Geopolitics of Undersea Cables | Center for Indo-Pacific Affairs*. Center for Indo-Pacific Affairs. <https://manoa.hawaii.edu/indopacificaffairs/article/entangled-southeast-asia-and-the-geopolitics-of-undersea-cables/>
- Noor, E. (2024b). *Subsea Communication Cables in Southeast Asia: A Comprehensive Approach is Needed*. Carnegie Endowment for International Peace. <https://carnegieendowment.org/research/2024/12/southeast-asia-undersea-subsea-cables?lang=en>
- PR Release. (2024). *NEC Completes Asia Direct Cable (ADC) Submarine Cable - Submarine Networks*. Submarinenetworks.com. <https://www.submarinenetworks.com/en/systems/intra-asia/adc/nec-completes-adc-cable>

- Runde, D. F., Murphy, E. L., & Bryja, T. (2024). *Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition*. Csis.org. <https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition>
- Schrag, J. (2021). How much trade transits the South China Sea?. ChinaPower Project. <https://chinapower.csis.org/much-trade-transits-south-china-sea/#:~:text=The%20United%20Nations%20Conference%20on,one%2Dthird%20of%20global%20shipping.>
- Shan, S. (2023, February 17). *Lienchiang Internet to be restored by end of April*. Taipei Times. <https://www.taipetimes.com/News/taiwan/archives/2023/02/17/2003794526>
- Tan, R. (2024). Escalating contest over South China Sea disrupts international cable system. *ProQuest*. <https://www.proquest.com/globalnews/blogs-podcasts-websites/escalating-contest-over-south-china-sea-disrupts/docview/3112647657/sem-2?accountid=14784>
- TeleGeography. (n.d.). <https://www.submarinemap.com/>
- Tobin, M., Xiao, M., & Chien, A. C. (2025, January 7). *Taiwan says it suspects a Chinese-linked ship damaged an undersea internet cable*. The New York Times. <https://www.nytimes.com/2025/01/07/world/asia/taiwan-internet-cable-china.html?auth=login-google1tap&login=google1tap>
- TPE. Submarine Cable Networks. (n.d.). <https://www.submarinenetworks.com/en/systems/trans-pacific/tpe>
- Wang, J. (2025). *Chinese Vessel Cuts Taiwan Internet Cable in Apparent Sabotage; Service largely unaffected in episode highlighting vulnerability of vital global infrastructure following Baltic Sea incidents*. Proquest.com. <https://www.proquest.com/globalnews/docview/3151848634/5F327BBAE01247A3PQ/2?accountid=14784&sourcetype=Blogs>
- Wang, L. (2025). CHT to lay new undersea cables. Taipei Times. <https://www.taipetimes.com/News/front/archives/2025/02/12/2003831730>
- Yun-yao, S., Chin, J. (2023, August 4). *War games show Taiwan's key role in the region*. Taipei Times. <https://www.taipetimes.com/News/taiwan/archives/2023/08/04/2003804227>

Case Study: Red Sea

- BBC. (2024). *Who are the Houthis and why are they attacking Red Sea ships?* BBC. <https://www.bbc.com/news/world-middle-east-67614911>
- Borland, J. (2008). *Analyzing the internet collapse*. MIT Technology Review. <https://www.technologyreview.com/2008/02/05/222155/analyzing-the-internet-collapse>
- Brock, J. (2023). U.S. and China wage war beneath the waves—Over internet cables. *Reuters*. <https://www.reuters.com/investigates/special-report/us-china-tech-cables/>
- Burgess, M. (n.d.). The most vulnerable place on the internet. *Wired*. <https://www.wired.com/story/submarine-internet-cables-egypt/>
- CFR.org Editors. (2024). *What is hezbollah?* Council on Foreign Relations. <https://www.cfr.org/backgrounder/what-hezbollah>
- Clapp, S. (2024). *Maritime security: Situation in the red sea and eu response*. European Parliamentary Research Service.
- Council of the European Union. (2024). *Security and freedom of navigation in the Red Sea: Council launches EUNAVFOR ASPIDES*. <https://www.consilium.europa.eu/en/press/press-releases/2024/02/19/security-and-freedom-of-navigation-in-the-red-sea-council-launches-new-eu-defensive-operation/>
- Dufetre, R. (2023). *The data roads under the seas. American hegemony over the global undersea cable network and its potential challengers*. University of Chicago. <https://doi.org/10.6082/UCHICAGO.7155>
- Economy Middle East. (2023). *An inside look into Telecom Egypt's operations and future plans*. Economy Middle East. <https://economymiddleeast.com/news/an-inside-look-into-telecom-egypts-operations-and-future-plans/>
- Fargher, J. (2024). *The Red Sea: Britain's uncertain link*. Council on Geostrategy.
- Froman, M. (2025). *The Israel-Hamas cease-fire and its implications*. Council on Foreign Relations. <https://www.cfr.org/article/israel-hamas-cess-fire-and-its-implications>

- Gambrell, J. (2024). *3 Red Sea data cables cut as Houthis launch more attacks in the vital waterway*. AP News. <https://apnews.com/article/red-sea-undersea-cables-yemen-houthi-rebels-attacks-b53051f61a41bd6b357860bbf0b0860a>
- Garamone, J. (2023). *Ryder gives more detail on how operation prosperity guardian will work*. U.S. Department of Defense. <https://www.defense.gov/News/News-Stories/Article/Article/3624836/ryder-gives-more-detail-on-how-operation-prosperity-guardian-will-work/>
- Gardner, F. (2024). *Could the Houthis sabotage undersea cables?* <https://www.bbc.com/news/world-middle-east-68231945>
- Jones, M. G. (2024). *EU states try to “strike the right balance” on US operation in Red Sea*. Euronews. <https://www.euronews.com/my-europe/2024/01/02/red-sea-why-have-some-eu-nations-distanced-themselves-from-the-us-operation-against-the-ho>
- Johnson, K. (2025). *The houthis’ next target may be underwater*. *Foreign Policy*. <https://foreignpolicy.com/2024/02/07/houthi-red-sea-attacks-submarine-cables/>
- Lagrone, S. (2023). *‘Operation Prosperity Guardian’ Set to Protect Ships in the Red Sea, Carrier IKE in Gulf of Aden*. USNI News. <https://news.usni.org/2023/12/18/operation-prosperity-guardian-set-to-protect-ships-in-the-red-sea-carrier-ike-in-gulf-of-aden>
- Mitra, S., Robinson, L., & Gallagher, P. (2025). *Somali pirates use the Red Sea Crisis and war in Gaza to stage their return*. CNN. <https://www.cnn.com/2025/02/22/world/somali-pirates-red-sea-gaza-dg/index.html>
- Musil, S. (2013). *Egypt’s military arrests divers cutting undersea Internet cables*. CNET. <https://www.cnet.com/tech/services-and-software/egypts-military-arrests-divers-cutting-undersea-internet-cables/>
- Monaghan, S., Darrach, M., Jakobsen, E., & Svendsen, O. (2024). *Red sea cable damage reveals soft underbelly of global economy*. <https://www.csis.org/analysis/red-sea-cable-damage-reveals-soft-underbelly-global-economy>
- Reuters. (2025). *Yemen’s Houthis launched missile at US fighter jet, missed*. *Reuters*. <https://www.reuters.com/world/middle-east/yemens-houthis-launched-missile-us-fighter-jet-missed-2025-02-22/>
- Saffo, P. (2013). *Disrupting undersea cables: Cyberspace’s hidden vulnerability*. *Atlantic Council*. <https://www.atlanticcouncil.org/blogs/new-atlanticist/disrupting-undersea-cables-cyberspaces-hidden-vulnerability/>
- Salhani, J. (2024). *Beyond the red sea: Who are the houthis up against inside yemen?* Al Jazeera. <https://www.aljazeera.com/features/2024/1/18/beyond-the-red-sea-who-are-the-houthis-up-against-inside-yemen>
- Schreiber, B.C., Ryan, W.B. (2025). *Red Sea*. Encyclopedia Britannica. <https://www.britannica.com/place/Red-Sea>
- Sherman, J. (2021). *Cyber defense across the ocean floor: The geopolitics of submarine cable security*. *Atlantic Council*. <https://www.atlanticcouncil.org/in-depth-research-reports/report/cyber-defense-across-the-ocean-floor-the-geopolitics-of-submarine-cable-security/>
- Smith, P. (2008). *New focus on undersea Internet cable security after cuts*. *Christian Science Monitor*. <https://www.csmonitor.com/World/terrorism-security/2008/0212/p99s01-duts.html>
- Submarine Cable Networks. (2011). *Submarine cable cuts in jan-feb, 2008 in the persian gulf and the mediterranean*. Submarine Cable Networks. <https://www.submarinenetworks.com/en/nv/news/cable-cuts-in-jan-feb-2008>
- stc Group. (n.d.). *Stc group | our history*. <https://www.stc.com/content/stcgroupwebsite/sa/en/who-we-are/our-history.html>
- TeleGeography. (n.d.). *Submarine cable map*. <https://www.submarinemap.com/>
- The Sydney Morning Herald. (2008). *Saboteurs may have cut Mideast telecom cables: UN agency*. The Sydney Morning Herald. <https://www.smh.com.au/technology/saboteurs-may-have-cut-mideast-telecom-cables-un-agency-20080219-1sv3.html>
- U.S. Department of Defense. (2023). *Statement from secretary of defense lloyd j. Austin iii on ensuring freedom of navigation*. U.S. Department of Defense. <https://www.defense.gov/News/Releases/Release/Article/3621110/statement-from-secretary-of-defense-lloyd-j-austin-iii-on-ensuring-freedom-of->

[n/https%3A%2F%2Fwww.defense.gov%2FNews%2FReleases%2FRelease%2FArticle%2F3621110%2Fstate-ment-from-secretary-of-defense-loyd-j-austin-iii-on-ensuring-freedom-of-n%2F](https://www.defense.gov/News/Releases/Release/Article/23621110/Statement-from-secretary-of-defense-loyd-j-austin-iii-on-ensuring-freedom-of-n/)

Van Dalen, D., Ndhlovu, M., & Gopaldas, R. (2024). *Impact of Red Sea crisis on Africa – red flag or red herring?* ISS Africa. <https://issafrica.org/iss-today/impact-of-red-sea-crisis-on-africa-red-flag-or-red-herring>

Ziady, H. (2024). *Red Sea cables have been damaged, disrupting internet traffic* | CNN Business. CNN. <https://www.cnn.com/2024/03/04/business/red-sea-cables-cut-internet/index.html>

Key Actors: United States of America

Basu, P. (2024, July 19). *Explore Pacific Forum's insightful Indo-Pacific analysis*. Pacific Forum.

<https://pacforum.org/publications/pacnet-50-multilateralism-key-for-de-risking-indo-pacific-subsea-cables/>

Billingsley, D., & Billingsley, D. (2024, October 17). *China creating undersea cable network in response to United States isolation efforts*. Foreign Military Studies Office. <https://fmso.tradoc.army.mil/2024/china-creating-undersea-cable-network-in-response-to-united-states-isolation-efforts/>

Boulègue, M. (2024). *Arctic seabed warfare against data cables: Risks and impact for US critical undersea infrastructure*. Wilson Center Polar Institute.

<https://www.wilsoncenter.org/sites/default/files/media/uploads/documents/Seabed-Warfare-Cables%20%281%29.pdf>

Cannon, B. J., & Bhatt, P. (2024, January 25). *The Quad and Submarine Cable Protection in the Indo-Pacific: Policy Recommendations*. Institute for Security & Development Policy. <https://isdpc.eu/wp-content/uploads/2024/01/Brief-Cannon-Jan-25-2023-final3-updated.pdf>

Department of Homeland Security. (2024, December 18). *Priorities for DHS engagement on subsea cable security & resilience*. U.S. Department of Homeland Security. https://www.dhs.gov/sites/default/files/2024-12/24_1218_srcr_Priorities-for-DHS-Engagement-on-Subsea-Cable-Security-Resilience_18-Dec-24.pdf

Federal Communications Commission (n.d.). *Submarine Cables*. Federal Communications Commission.

<https://www.fcc.gov/submarine-cables#:~:text=The%20FCC%27s%20International%20Bureau%2C%20Telecommunications,10530.>

Gerwitz, J., O'Neil, S., Rockefeller, N., Rockefeller, D., Segal, A., Smith, S., Best, L., & Collins, M. (2025). *Assessing China's Digital Silk Road Initiative*. Council on Foreign Relations. <https://www.cfr.org/china-digital-silk-road/>

Guarascio, F., Phuong, P., & Brock, J. (2024, September 14). *Exclusive: Inside the US push to steer Vietnam's subsea cable plans away from China* | reuters. Reuters. <https://www.reuters.com/business/media-telecom/inside-us-push-steer-vietnams-subsea-cable-plans-away-china-2024-09-17/>

Kumar, R. (2023, November 15). *Securing the digital seabed: Countering China's underwater ambitions*. Air University (AU). https://www.airuniversity.af.edu/JIPA/Display/Article/3588497/securing-the-digital-seabed-countering-chinas-underwater-ambitions/#_ftn8

National Oceanic and Atmospheric Administration. (2024, October 16). *Submarine cables - domestic regulation* | National Oceanic and Atmospheric Administration. <https://www.noaa.gov/general-counsel/gc-international-section/submarine-cables-domestic-regulation>

North Atlantic Treaty Organization. (2025, January 14). *NATO launches "Baltic Sentry" to increase critical infrastructure security*. North Atlantic Treaty Organization.

https://www.nato.int/cps/en/natohq/news_232122.htm

Runde, D. F., Murphy, E. L., & Bryja, T. (2024, August 16). *Safeguarding subsea cables: Protecting cyber infrastructure amid great power competition*. Center for Strategic and International Studies.

<https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition>

Sakai, M. (2024, January 1). *Does Pacific Islands Remain: U.S.-China Competition*. Pacific Forum.

<https://pacforum.org/publications/pacnet-2-can-the-pacific-islands-remain-friends-to-all-amid-us-china-competition/>

Smith, S. (2021, May 27). *The quad in the indo-pacific: What to know*. Council on Foreign Relations.

<https://www.cfr.org/in-brief/quad-indo-pacific-what-know>

- U.S. Department of Justice. (2023, September 20). *Team telecom*. National Security Division. <https://www.justice.gov/nsd/team-telecom>
- U.S. Department of State. (2024, May). *United States International Cyberspace & Digital Policy Strategy*. <https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/>
- The White House. (2023, September 25). FACT SHEET: *Enhancing the U.S.-Pacific Islands Partnership*. <https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/09/25/fact-sheet-enhancing-the-u-s-pacific-islands-partnership/>
- Wall, C., & Morcos, P. (2021, June 11). *Invisible and vital: Undersea cables and transatlantic security*. Center for Strategic and International Studies. <https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security>
- Williams, E. (2024, May 9). *China's Digital Silk Road taking its shot at the Global Stage*. East Asia Forum. <https://eastasiaforum.org/2024/05/09/chinas-digital-silk-road-taking-its-shot-at-the-global-stage/>

Key Actors: People's Republic of China

- Aluf, Dale. (2023). *China's subsea Cable power play in the Middle East and North Africa*. Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2023/05/ChinasGrowingInfluence_052423-1.pdf
- Astier, H., & Kirby, P. (2024). Germany suspects sabotage behind severed undersea cables in the Baltic. BBC News. <https://www.bbc.com/news/articles/c9d14xw501o>
- Brock, J. (2023a, March). U.S. and China wage war beneath the waves - over internet cables. *Reuters*. <https://www.reuters.com/investigates/special-report/us-china-tech-cables/>
- Brock, J. (2023b). US backs Pacific undersea internet cable amid China competition. *Reuters*. <https://www.reuters.com/world/us-backs-pacific-undersea-internet-cable-amid-china-competition-2023-09-28/>
- Bryant, Miranda. (2024). *Sweden says China denied request for prosecutors to board ship linked to severed cables*. <https://www.theguardian.com/world/2024/dec/23/china-refused-investigation-into-ship-linked-to-severed-baltic-cables-says-sweden>
- Burdette, L. (2021). Leveraging Subsea cables for Political Gain: US Responses to Chinese Strategy. *Journal of Public & International Affairs*. <https://jpia.princeton.edu/news/leveraging-submarine-cables-political-gain-us-responses-chinese-strategy>
- Central Government of the People's Republic of China (2016). *国务院关于印发“十三五”国家战略性新兴产业发展规划的通知*. [Notice of The State Council on Issuing the 13th Five-Year Plan for the Development of National Strategic Emerging Industries. Documents of The State Council]. https://www.gov.cn/zhengce/content/2016-12/19/content_5150090.htm
- China Academy of Information and Communications Technology (2023). *全球海底光缆产业发展研究报告*。中国信息通信研究院产业与规划研究所. [Global subsea cable industry Development Research Report. Institute of Industry and Planning, China Academy of Information and Communications Technology]. <http://www.caict.ac.cn/kxyj/qwfb/ztbg/202307/P020230718390842938808.pdf>
- Davenport, T. (2012). Submarine Communications Cable and Law of the Sea: Problems in Law and Practice. *Ocean Development & International Law*. 43 (3), 201-242. <https://doi.org/10.1080/00908320.2012.698922>
- Financial Times. (2023). *US-backed telecoms firms block China's role in subsea cable projects*. <https://ig.ft.com/subsea-cables/>
- Friedman, R., O'Casey, M., Xing, J. (2025). U.S. Strengthens Export Controls on Advanced Computing Items, Semiconductor Manufacturing Items. *The Global Trade Law Journal*. 3(2). 179-199. <https://www.hklaw.com/en/insights/publications/2025/05/us-strengthens-export-controls-on-advanced-computing>
- Guarascio, F., & Nguyen, P. (2024, December 12). Exclusive: Singapore, Vietnam firms in talks for new undersea cables, sources say. *Reuters*. <https://www.reuters.com/technology/singapore-vietnam-firms-talks-new-undersea-cables-sources-say-2024-12-13/>
- Guiot, B. (October 10, 2023). Subsea Cables---The Underwater Backbone of the Digital Age. *Natixis*. <https://home.cib.natixis.com/articles/subsea-cables-the-underwater-backbone-of-the-digital-age>

- He, H., Sun, F., Wang, Z., Lin, C., Zhang, C., Xiong, R., Deng, J., Zhu, X., Xie, P., & Zhang, S. (2022). China's battery electric vehicles lead the world: Achievements in technology system architecture and technological breakthroughs. *Green Energy and Intelligent Transportation*, 1(1), 100020. <https://www.sciencedirect.com/science/article/pii/S2773153722000202>
- Hengtong Group. (2023). PEACE Cable Project Overview. <http://www.peacecable.net/news/0/3>
- Herlevi, A. (2024, March 14). *China's Strategic Space in the Digital Undersea*. Mapping China's Strategic Space. <https://strategicspace.nbr.org/chinas-strategic-space-in-the-digital-undersea/>
- Khatoon, A. (2022). China's Belt and Road Initiative: An analysis of its role in global peace, development, and implications. *Journal of Humanities, Social and Management Sciences (JHSMS)*, 3(2), 40–61. https://www.researchgate.net/publication/367528000_China's_Belt_and_Road_Initiative_an_analysis_of_its_role_in_global_peace_development_and_implications
- Koshino, Y. (2024). The Changing Subsea cables Landscape. *EUSS*. <https://www.iss.europa.eu/publications/briefs/changing-submarine-cables-landscape>
- Liu S. (2025). “一带一路”新算力基建需求爆发,在沪央企启动跨洋海缆项目. [“The Belt and Road” new computing power infrastructure demand broke out, and the central enterprises in Shanghai launched the trans-oceanic subsea cable project | Shanghai Accelerated Run. *Interface news*. https://www.toutiao.com/article/7463086010340262441/?upstream_biz=doubao&use_xbridge3=true&loader_name=forest&need_sec_link=1&sec_link_scene=im&source=m_redirect&wid=1738930103269
- National Development and Reform Commission, PRC (2020). *关于扩大战略性新兴产业投资培育壮大新增长点增长极的指导意见*. [Guiding Opinions on Expanding Investment in Strategic Emerging Industries, Cultivating and Expanding New Growth Points and Growth Poles. Open government information.] <https://zfxxgk.ndrc.gov.cn/web/iteminfo.jsp?id=17239>
- Ridgewell, H. (2024, November 23). *Chinese vessel suspected of severing submarine cables still anchored in Baltic Sea*. <https://www.voanews.com/a/chinese-vessel-suspected-of-severing-submarine-cables-still-anchored-in-baltic-sea-/7873826.html>
- Rossiter, A. (2023). Subsea cables in an age of geopolitical competition. *Trends Research*, February, 19. https://trendsresearch.org/insight/undersea-cables-in-an-age-of-geopolitical-competition/?srsltid=AfmBOoqE8Z2Zw_qayMAK1lqH9sD2hrgZCRPZDEp2LWslqax6s-S6z8P
- Sherman, J. (2021, September 13). *Cyber defense across the ocean floor: The geopolitics of submarine cable security*. Atlantic Council. <https://www.atlanticcouncil.org/in-depth-research-reports/report/cyber-defense-across-the-ocean-floor-the-geopolitics-of-submarine-cable-security/>
- State Council of China. (2023). A Key Pillar of the Global Community of Shared Future http://www.scio.gov.cn/zfbps/zfbps_2279/202310/t20231010_773734.html
- TeleGeography. (n.d.) *Submarine cable map*. <https://www.submarinemap.com/>
- The Maritime Executive. (2024, December 18). Bulker Accused of Cutting Baltic Cables May Have Tried Once Before. The Maritime Executive. <https://maritime-executive.com/article/chinese-bulker-accused-of-cutting-baltic-cables-may-have-tried-once-before>
- Wang, C. N. (2022). *China Belt and Road Initiative (BRI) Investment Report 2021*. Green BRI Center, International Institute of Green Finance (IIGF), 9(5). https://www.bhrrc.org/documents/37186/Nedopil-2022_BRI-Investment-Report-2021.pdf
- Xinhua Net. (2023). *China Welcomes, Supports Laying of International Subsea cables in Waters Under its Jurisdiction*. Xinhua Net. <https://english.news.cn/20231229/d1c0846ab5ce40bda46cd5256cff434b/c.html>
- Zhou, L. (2021). *China Builds Subsea cable Bases Amid Digital Infrastructure Rivalry*. South China Morning Post. <https://www.scmp.com/news/china/diplomacy/article/3159328/china-builds-undersea-cable-bases-amid-digital-infrastructure>
- Zou, K. (2012). China's Ocean Policymaking: Practice and Lessons. *Coastal Management*, 40 (2), <http://dx.doi.org/10.1080/08920753.2012.652514>

Key Actors: Russian Federation

- Andreev, A. (2017, August 10). *Корабль спецназначения “Янтарь” вошёл в Средиземное море*. [The Special Purpose Ship *Yantar* entered the Mediterranean Sea] <https://www.pnp.ru/politics/korabl-specnaznacheniya-yantar-voshyol-v-sredizemnoe-more.html>
- Bennetts, M. (2025, January 24). *Russian spy ship Yantar has been snooping on the seas for ten years*. <https://www.thetimes.com/world/europe/article/russian-spy-ship-yantar-snooping-seas-ten-years-tst07tbrn>
- Dickinson, P. (2022, July 3). Putin’s poisonous anti-Western ideology relies heavily on projection. *Atlantic Council*. <https://www.atlanticcouncil.org/blogs/ukrainealert/putins-poisonous-anti-western-ideology-relies-heavily-on-projection/>
- Grylls, G. (2025, January 22). *Nato’s underwater war against Russian and Chinese cable-cutters*. <https://www.thetimes.com/world/europe/article/natos-underwater-war-against-russian-and-chinese-cable-cutters-trc90sjn6>
- Kaushal, S. (2023, May 25). *Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure*. <https://rusi.org/>
- Kotkin, S. (2016, May-June). Russia’s Perpetual Geopolitics: Putin Returns to the Historical Pattern. In *Foreign affairs* (New York, N.Y.) (Vol. 95, Issue 3, pp. 2–9). Council on Foreign Relations. https://link.gale.com/apps/doc/A451952536/BIC1?sid=summon&u=wash_main
- Peter, L. (2018, January 3). *What makes Russia’s new spy ship Yantar special?* <https://www.bbc.com/news/world-europe-42543712>
- Putin, V. (2014, March 18). Transcript: Putin says Russia will protect the rights of Russians abroad. *Washington Post*. https://www.washingtonpost.com/world/transcript-putin-says-russia-will-protect-the-rights-of-russians-abroad/2014/03/18/432a1e60-ae99-11e3-a49e-76adc9210f19_story.html
- Scott, M. (2022, September 29). *Will Russia attack undersea internet cables next?* POLITICO. <https://www.politico.eu/article/everything-you-need-to-know-about-the-threat-to-undersea-internet-cables/>
- Sherman, J. (2022, April 22). It Looks Like Russia Is Bringing Its State-Owned Telecom Provider Into Its National Security Apparatus. *Slate*. <https://slate.com/technology/2022/04/russia-rostec-rostelecom-internet-national-security.html>
- TeleGeography. (n.d.). *Submarine Cable Map*. <https://www.submarinecablemap.com/submarine-cable/far-east-submarine-cable-system>
- van Soest, H. (2025, January 16). *Countering Russia’s “Shadow Fleet.”* <https://www.rand.org/pubs/commentary/2025/01/countering-russias-shadow-fleet.html>
- Wasiuta, O. (2023, September 28). RUSSIAN THREATS TO THE SUBMARINE INTERNET CABLE INFRASTRUCTURE. *Zeszyty Naukowe SGSP*, 87, 357–378. <https://doi.org/10.5604/01.3001.0053.9127>

The Private Sector Subsea Cable Infrastructure

- Alcatel Submarine Networks. (n.d.). *About Us*. Alcatel Submarine Networks. <https://www.asn.com/about-us/>
- Besch, S., & Brown, E. (2024, December 16). *Securing Europe’s Subsea Data Cables | Carnegie Endowment for International Peace*. Carnegie Russia Eurasia Center. <https://carnegieendowment.org/research/2024/12/securing-europes-subsea-data-cables?lang=en¢er=russia-eurasia>
- Blackridge Research and Consulting. (2024, December 27). *Global top 8 cable laying vessel (CLV) companies [2025]*. <https://www.blackridgeresearch.com/blog/list-of-global-top-cable-laying-layer-vessel-clv-ship-companies-operators-owners-suppliers-in-the-world>
- Blue, A. (2024, September 24). *Submarine Data Cables: Latest target of the u.s.-china rivalry | Journal of Public and International Affairs*. Princeton University. <https://jpia.princeton.edu/news/submarine-data-cables-latest-target-us-china-rivalry>

- Botting, A., & Jordan-Zoob, I. (2024, February 28). *Optical Core Infrastructure: The hidden highway of connectivity*. Wilson Center. <https://www.wilsoncenter.org/article/optical-core-infrastructure-hidden-highway-connectivity>
- Brock, J. (2023a, March). U.S. and China wage war beneath the waves - over internet cables. *Reuters*. <https://www.reuters.com/investigates/special-report/us-china-tech-cables/>
- Brock, J. (2023b). *SubCom's role in subsea cables for U.S. and beyond*. *Reuters*. Retrieved from <https://www.reuters.com/investigates/special-report/us-china-tech-subcom/>
- China Academy of Information and Communications Technology. (2023). *Global submarine cable industry development research report* [Review of Global submarine cable industry development research report]. In China Academy of Information and Communications Technology. China Academy of Information and Communications Technology. https://www.caict.ac.cn/kxyj/qwfb/ztbg/202307/t20230707_440299.htm
- Center for Strategic & International Studies. (2022). *Securing Asia's Subsea Network: U.S. Interests and Strategic Options*. Retrieved from <https://www.csis.org/analysis/securing-asias-subsea-network-us-interests-and-strategic-options>
- Department of Homeland Security. (2024, December 18). Priorities for DHS engagement on subsea cable security & resilience. https://www.dhs.gov/sites/default/files/2024-12/24_1218_scrp_Priorities-for-DHS-Engagement-on-Subsea-Cable-Security-Resilience_18-Dec-24.pdf
- Dobberstein, L. (2024, September 25). *Hyperscalers tying up the world in Submarine Cables*. The Register® - Biting the hand that feeds IT. https://www.theregister.com/2024/09/25/aspi_hyperscaler_cables/
- Dzieza, J. (2024, April 16). *The invisible seafaring industry that keeps the internet afloat*. The Verge. <https://www.theverge.com/c/24070570/internet-cables-undersea-deep-repair-ships>
- Gordon, L. W., & Jones, K. L. (2022, February). *Global Communications Infrastructure: Undersea and beyond*. https://csps.aerospace.org/sites/default/files/2022-02/Gordon-Jones_UnderseaCables_20220201.pdf
- Gross, A., Heal, A., Campbell, C., Clark, D., & Bott, I. (2023, June 12). *Subsea cables: How the US is pushing China out of the internet's plumbing*. <https://ig.ft.com/subsea-cables/>
- Insikt Group. (2023, June 27). *The escalating global risk environment for submarine cables*. Recorded Future. <https://www.recordedfuture.com/research/escalating-global-risk-environment-submarine-cables>
- International Cable Protection Committee (2024, November 25). *Cables of the World*. <https://www.iscpc.org/information/cables-of-the-world/>
- Kclark. (2024, June 24). *OMS group signs \$292.5M agreement for global expansion*. SubTel Forum. <https://subtelforum.com/oms-group-signs-292-5m-agreement-for-global-expansion/>
- Kumar, R. (2023, November 15). *Securing the digital seabed: Countering China's underwater ambitions*. Air University (AU). <https://www.airuniversity.af.edu/JIPA/Display/Article/3588497/securing-the-digital-seabed-countering-chinas-underwater-ambitions/>
- Law, M. (2023, February 15). *Top 10 biggest cloud providers in the world in 2023*. Technology Magazine. <https://technologymagazine.com/top10/top-10-biggest-cloud-providers-in-the-world-in-2023>
- Liu, HL [刘海林]. (2024). *我国首台作业时速公里级水下敷缆机器人完成下水测试*. [China's first underwater cable-laying robot with an operating speed of km/h has completed the launching test]. CCTV.com. <https://local.cctv.com/2024/12/12/ARTIiIQJXdv3kr4vS5UeMsYM241212.shtml>
- Mauldin, A. (2024, December 18). *A (refreshed) list of content providers' Submarine Cable Holdings*. TeleGeography's Official Blog. <https://blog.telegeography.com/telegeography-content-providers-submarine-cable-holdings-list-new>
- NEC Corporation. (2023, February 10). *Beyond the seas: NEC's submarine cable system*. https://www.nec.com/en/global/onlinetv/en/discovernec_submarinecable.html
- OMS Group. (2025). <https://opticmarine.com/>
- Orange Marine. (2025). <https://marine.orange.com/en/>
- Quigley, B., & Cantono, M. (2023, September 12). *Delivering multi-core fiber technology in Subsea Cables* | Google Cloud Blog. Google. <https://cloud.google.com/blog/products/infrastructure/delivering-multi-core-fiber-technology-in-subsea-cables>
- Ruehl, M., & Wiggins, K. (2024, February 1). *KKR raises record \$6.4BN for Asia Fund in infrastructure rush*. <https://www.ft.com/content/c25c33c7-f24c-4a1e-bce0-fa7dd8fc49fb>

- Runde, D. F., Murphy, E. L., & Bryja, T. (2024, August 16). *Safeguarding subsea cables: Protecting cyber infrastructure amid great power competition*. CSIS. <https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition>
- S.B. Submarine Systems. (2021). <https://www.sbss.com/en/site/about>
- Sherman, J. (2021). *Beijing's growing influence on the Global Undersea Cable Network*. Jamestown. <https://jamestown.org/program/beijings-growing-influence-on-the-global-undersea-cable-network/>
- Sherman, J. (2024, December 11). *The Global Submarine Cable Network, Cybersecurity and ...* The Global Submarine Cable Network, Cybersecurity and Resilience, and Risks to U.S. National Security . <https://www.commerce.senate.gov/services/files/9D566360-52C7-4FB9-B30B-1A5A86B9A69E>
- Satter, R. (2022, November 23). *Exclusive: How a small U.S. firm set out to unwind China's influence over the world's internet cables*. Reuters. <https://www.reuters.com/investigates/special-report/us-china-tech-subcom>
- Submarine Cable Networks. (n.d.). TPU. Submarine Cable Networks. <https://www.submarinenetworks.com/en/systems/trans-pacific/tpu>
- Swan, D. (2025, January 6). Highly vulnerable mesh holds the globe together - Communications. *The Age*. Available from NewsBank: Access World News – Historical and Current: <https://infoweb-newsbank-com.offcampus.lib.washington.edu/apps/news/document-view?p=WORLDNEWS&docref=news/19DEAB8B08294B60>.
- Tomaz, P., & Voo, J. (2024, October 10). *Submarine cables: The achilles' heel of cyberspace in the Asia-Pacific*. IISS Cyber Power Matrix. <https://www.iiss.org/cyber-power-matrix/submarine-cables-the-achilles-heel-of-cyberspace-in-the-asia-pacific/>
- Tréhu, C. (2024, March). *The rise of hyperscalers and their role in subsea cable infrastructure*. German Marshall Fund of the United States. <https://www.gmfus.org/sites/default/files/2024-03/iaip2404.pdf>
- Yangtze Optical Fiber and Cable. (2024, April 11). *China Telecom, ZTE and YOFC jointly set world record for real-time transmission of over 120Tbit/s on a single fibre in S+C+L band*. Prnewswire.com; Cision PR Newswire. <https://www.prnewswire.com/news-releases/china-telecom-zte-and-yofc-jointly-set-world-record-for-real-time-transmission-of-over-120tbits-on-a-single-fibre-in-scl-band-302114161.html>
- Zeng, ZY. [曾震宇]. (2024). *中国联通ADC海缆投产*. [China Unicom ADC submarine cable launched] Guangming. *Digital.gmw.cn*. https://digital.gmw.cn/2024-12/26/content_37763063.htm