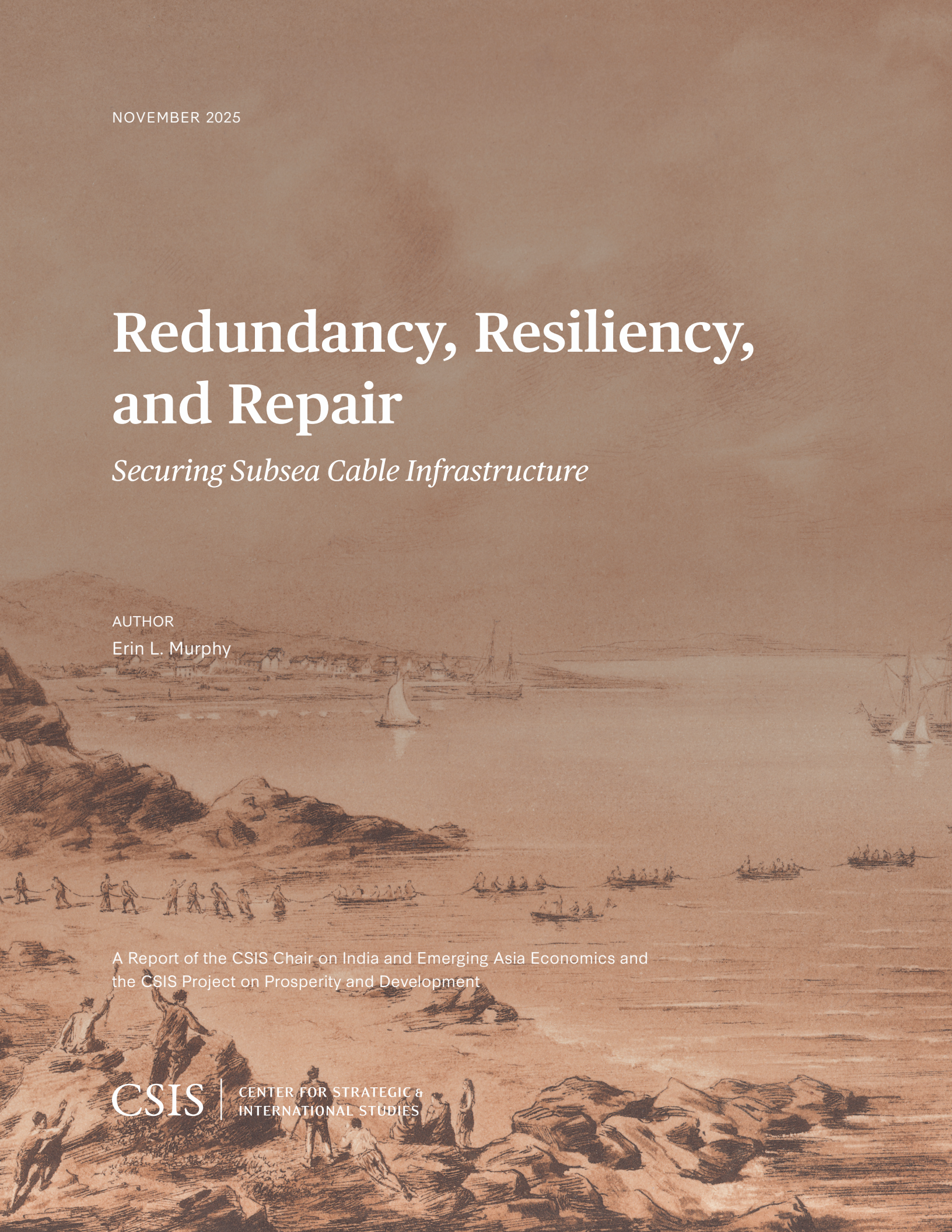
NOVEMBER 2025

# Redundancy, Resiliency, and Repair

## *Securing Subsea Cable Infrastructure*

AUTHOR
Erin L. Murphy



A Report of the CSIS Chair on India and Emerging Asia Economics and the CSIS Project on Prosperity and Development

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

NOVEMBER 2025

# Redundancy, Resiliency, and Repair

## *Securing Subsea Cable Infrastructure*

AUTHOR
Erin L. Murphy

A Report of the CSIS Chair on India and Emerging Asia Economics and the CSIS Project on Prosperity and Development

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

# About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values—nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).



Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

# Acknowledgments

The author would like to thank Thomas Bryja for his significant contributions to this report and the four country case studies covering Egypt, Ireland, Japan, and Singapore. His research helped inform key aspects of this report. The research team conducted interviews for each of the four case studies and would like to thank the following people for their insights, in addition to many more anonymous experts: Daniel Runde, Romina Bandura, Robert Beckman, Tara Davenport, Cian FitzGerald, Kristi Govella, Asha Hemrajani, Grace Koh, Tomohiro Nakamura, and Shinya Shimada. This report benefited immensely thanks to input from participants of four private roundtables hosted by CSIS from May 2024 through March 2025. The author also appreciates the feedback, insights, and information received from government officials, businesses, and academics during the country case study research.

This report was made possible by project support from the Smith Richardson Foundation.

# Contents

# Executive Summary

Subsea fiber-optic cables are the world's primary conduit for data, carrying 99 percent of data internationally, making them essential to the modern digital world and indispensable to both national and economic security.[1] Subsea cable infrastructure impacts nearly all aspects of daily life by providing access to the internet and delivering the data that underlies critical systems such as e-commerce and financial networks, communications, and telehealth and e-education. It is also a key part of the foundation for seismic, cutting-edge technologies such as AI, cloud computing, and quantum computing. Although the first subsea cable was laid between Dover and Calais nearly 175 years ago, this critical type of infrastructure shows no signs of ebbing in importance.

Today, more than 600 cables span 1.5 million kilometers globally and connect to more than 1,600 landing stations.[2] As a key component determining access to data and digital systems, this globe-spanning technology also carries significant strategic influence—access to data is a key currency of the modern era and is increasingly being counted among the critical components of geopolitical power, particularly as AI systems proliferate, including into military applications. As geopolitical tensions continue to rise and digital demands grow, the security, resiliency, and maintenance of cables have become urgent global priorities.

Against this backdrop, CSIS embarked on this study to examine current subsea cable infrastructure and highlight its importance to economic and national security. The study identifies the roles and responsibilities of key stakeholders in the industry in the public and private sectors, assesses the threats and challenges to maintaining a secure and resilient cable network, and provides a set of

recommendations for stakeholders to enhance the resiliency of subsea cable infrastructure based on in-depth research both in the United States and around the world. This report builds on the work of a 2021 CSIS study, *Securing the Subsea Network: A Primer for Policymakers*, as well as four new country case studies on Egypt, Ireland, Japan, and Singapore.[3]

## Repair, Redundancy, and Resiliency

The ecosystem to build, lay, and repair cables is small, consisting of four major manufacturers, and the market for cables today is dominated by a handful of hyperscalers—major tech companies that are driving the expansion of subsea fiber-optic cable networks. The four firms that dominate cable production include SubCom (United States), NEC (Japan), Alcatel Submarine Networks (France), and HMN Tech (China). Hyperscalers—including Google, Meta, Microsoft, and Amazon Web Services (AWS)—are the modern tech giants that provide cloud computing, digital infrastructure, and data processing and storage. These companies are increasingly investing, owning, and operating their own subsea fiber-optic cables or joining consortiums with global telecommunications companies or tech leaders. Collectively, manufacturers and hyperscalers are dependent on access to specialized ships, submersible vehicles that can lay and bury the cables, and the skilled crews and technicians necessary to manufacture, lay, repair, and test the cables. These stakeholders must navigate a complex planning, permitting, and financing environment to support new projects and keep existing cables operational.

Outside of new cable projects, the owners and operators of the cable must keep up with infrastructure maintenance and annual breakages. The majority of cable damage is caused by dropped anchors from commercial and fishing vessels that scrape across the ocean floor. Natural disasters, including earthquakes, undersea volcanoes, and storms, can also damage cables and cable landing stations onshore—threats that are likely to increase as climate change intensifies. Less likely, but of considerable concern to policymakers, is intentional sabotage or interference by state and non-state actors.

Repairs involve locating faults, raising damaged sections, splicing new cable, and reburying new cable. Depending on where the cable breaks, repair may require permits from a number of country, state, territory, or other government bodies. Many laws are informed by global frameworks, but each coastal country where a cable lands and its respective local jurisdictions may have their own legal hurdles and approval processes.

Governments and international organizations provide regulations and legal frameworks as well as protect and monitor cables using naval and other military resources. International frameworks like the UN Convention on the Law of the Sea (UNCLOS) and the 1884 Convention for the Protection of Submarine Telegraph Cables provide foundational governance for the sector. UNCLOS, for example, has been ratified by 171 parties and helps inform domestic laws and regulations.[4] However, both are outdated and inconsistently enforced. Other organizations promote cable protection best practices, coordinate security responses, and promote building a trusted cable network. This work includes providing an avenue for coastal states with subsea cable interests to fill in policy and regulatory gaps left by outdated or nonexistent frameworks.

As of July 2025, the United States has 90 cables registered, either in operation or planned.[5] Oversight for these systems is fragmented across federal, state, and tribal agencies, with no lead agency to streamline and facilitate policymaking, permitting, and regulatory processes. Key federal stakeholders include the Federal Communications Commission, which provides licenses and oversees rules and regulations; the Department of Homeland Security, which acts as the national coordinator for critical infrastructure, monitors cable-laying vessels, and develops interagency concepts for cable security and resilience in crises; the Department of State, which engages with global governments and institutions on subsea cable treaties and diplomacy and oversees digital policies and funding for digital infrastructure projects; Team Telecom, which reviews foreign investment in cable licenses; and U.S. federal financing and export credit agencies, which provide feasibility studies, project preparation financing, and project financing for global subsea cable projects.

While frameworks and regulations exist to guide installation of new cables as well as the repair of damaged cables, geopolitical tensions and active conflict are complicating efforts to build in redundancy and resiliency into the infrastructure. The South China Sea and the Red Sea, in particular, have become complicated and have delayed new projects and repairs. China has dragged out approvals or denied new projects for any cables that cross their territorial waters. Other cable projects have been rerouted to avoid China, adding more costs and time needed for construction.[6] Private sector companies, the United States, and like-minded partners and allies are increasingly concerned about China's role in the industry through HMN Tech and other state-directed investments in the infrastructure, as well as China's growing ability to deploy coercive methods such as denying permits.

At the same time, suspected Russian and Chinese activity has demonstrated the considerable risk posed to cable systems from deniable gray zone activities. Multiple incidents, including in the Baltic Sea and the Taiwan Strait, point to the potential weaponization of cable sabotage to disrupt adversaries at minimal cost and with few avenues for recourse. Given the strategic value of subsea cables, such activity, including the use of nominally civilian vessels to sabotage cables, highlights the fraught potential environment for cable security, particularly in the context of any potential NATO-Russia or Taiwan contingency.

Cable breakages in the Red Sea present a different security concern, particularly around the safety of the crew tasked with fixing the cable. Ships passing by the southern coast of Yemen are subject to attacks from Houthi terrorists as well as pirates. The Houthis have launched antiship missiles as part of an effort to air their anti-Israeli sentiments over the Gaza war. In early 2024, a UK-owned ship was hit by multiple missiles and forced to drop its anchor, subsequently damaging cables.[7] Though not a direct attack on cables themselves, this example illustrates the indirect threats to the infrastructure. These risks are likewise increasing the challenges of insuring cable repair ships, with insurance becoming highly challenging to obtain in the region.[8]

Taken together, the risks posed to subsea cables are proliferating in tandem with their critical role to the world's global digital systems and its ever-expanding need for data. Any broader effort to ensure the resiliency and redundancy of subsea cable systems will need to account for this array of challenges, ranging from environmental or incidental damage to malicious sabotage in peacetime or war.

## Recommendations

This study offers a set of strategic recommendations for the diverse set of stakeholders involved in subsea cable infrastructure—including cross-sectoral recommendations for the whole range of public and private sector actors involved in the sector, as well as more specific actions for the U.S. government, its allies and partners, financing institutions, and private sector companies. As emphasized throughout the report, strengthening coordination and clarifying roles across these groups is essential to enhancing the resilience of this critical global network.

### CROSS-SECTORAL

- Global governments must elevate subsea cables as a national security priority given their importance to connectivity, secure communications, and daily economic and other activity.
- Governments must streamline permitting and regulatory processes, identifying a single agency or point of contact to run the process.
- The international community must update global maritime treaties and frameworks to reflect modern threats and hold coastal countries accountable for enforcing laws.
- The public and private sectors must enhance information-sharing and collaborative efforts to better understand the threats and challenges facing each, as well as to develop best practices to address them.

### U.S. GOVERNMENT

- The U.S. government should designate a lead federal agency for cable coordination policy at both the federal and state levels.
- The United States should expand repair surge capacity via retrofitted naval ships or through funding construction of more cable repair ships for emergency purposes through the Trump administration's effort to rebuild America's shipbuilding capabilities.
- The government must reform protectionist maritime laws to reflect today's realities, establish protocols on anchorage incidents, and increase penalties for cable damage.
- The U.S. government must maintain diplomatic pressure to exclude high-risk vendors from subsea cable projects.

### U.S. ALLIES AND PARTNERS

- Like-minded countries can provide technical assistance and cybersecurity training to countries that lack the legislation and bureaucratic resources to protect subsea cable infrastructure.
- U.S. partners and allies should use naval assets to monitor high-risk areas and deploy assets as needed alongside repair vessels to repair cables during conflict or periods of high security risk.
- Like-minded countries can support strategic financing, particularly for cable projects in emerging markets or countries with geostrategic importance that may not reach the threshold for commercially viable cable projects.

### FINANCIAL INSTITUTIONS

- Financing agencies should offer debt and equity financing and technical assistance to support cable projects in emerging markets, especially where there is no clear business or profitability case.

### PRIVATE SECTOR

- Manufacturers and hyperscalers should engage more proactively with governments to align security and commercial priorities.

Subsea cables are vital to global connectivity, economic stability, and national security. As threats intensify and demand grows, the United States and its allies must act urgently to secure, modernize, and expand this infrastructure. Strategic investment, international cooperation, and public-private alignment are essential to safeguarding the world's digital arteries.

## Methodology

This report is informed by desktop research as well as dozens of interviews with government officials, hyperscalers, cable manufacturers, international organizations, academics, and scholars. CSIS researchers conducted four trips to locations that play an important role in the subsea cable sector—Egypt, Ireland, Japan, and Singapore—and insights drawn from these trips inform the four country case studies (published separately on the CSIS website) and this report. This report has also been peer reviewed by U.S. government officials, private sector players in the sector, and relevant scholars.

# Part I

## *Subsea Fiber-Optic Cables: The World's Communications Superhighway*

Nearly 175 years ago, the first international subsea communications cable network was laid on the ocean floor in Europe, marking the beginning of a new type of infrastructure that would become crucial to worldwide communication and commerce. The first transatlantic subsea telegraph cable was then laid in 1858, firmly ushering in this new era of global connectivity.[9] These early cables were made of telegraph wires and copper and insulated with hemp, India rubber, or gutta-percha, a substance used to create latex.[10] Devising methods to protect and armor the cable from undersea hazards was challenging and an ongoing experimental process, and today's cables use much of the same processes for protection that were used years ago.

Telegraph cables carrying simple messages soon transformed to telephone lines carrying conversations. Moving into the modern era, the cables now consist of fiber-optics carrying terabits of data per second. One of the world's oldest methods for carrying telecommunications is still one of its most vital and innovative technologies.

Since CSIS released a report in 2021, *Securing the Subsea Network: A Primer for Policymakers*, awareness of the impact of subsea cables on daily life and the importance of this critical infrastructure has continued to grow for a number of reasons.[11] First, the onset and persistence of the Covid-19 pandemic illustrated the ubiquity of the internet globally and its importance to nearly all aspects of everyday activities. Stable internet activity was essential to support work from home, telemedicine, e-learning and online schooling, and commerce. Second, the AI revolution is relentlessly driving the need for more data and increased connectivity, all of which fundamentally depends on subsea cables. Finally, and most ominously, rising geopolitical tensions have highlighted

concerns around competition and sabotage in the subsea cable sector. China has been increasing its foothold in the industry: China-based HMN Tech has established itself as one of the world's largest subsea cable manufacturers, albeit with a much smaller market share, and China likewise has a growing presence in cable repair. There are also concerns around intentional cuts and geopolitical tensions; Taiwan has suspected China of deliberately cutting cables, and Russia has been implicated on multiple occasions in intentionally cutting cables in the Baltic Sea.[12]

## The Importance of Subsea Cables

Subsea cables connect the world to the internet, carrying terabits of information over fiber-optics hardly bigger than the width of a hair. These fiber-optics pass through more than 600 current or planned cables spanning nearly than 1.5 million kilometers circumnavigating the globe (see Figure 1).[13] They provide the high-bandwidth connections necessary to support the rise of cloud computing, integrated 5G networks, and AI, transmitting messages and videos, financial transactions, diplomatic communications, essential intelligence, and a host of other digital information. Taken together, these demands will continue to increase the importance of and demand for subsea cables well into the future.

Demand for more ICT infrastructure is set to increase exponentially as more developing countries adopt digital resources and systems, including banking, education, health, and communications. This demand will also be reflected in the coming demographic changes taking place in different regions of the world and the digital needs that will empower their growth and development. According to UN projections, sub-Saharan Africa is expected to contribute over half of the world's population growth between 2022 and 2050. By 2050, one in every four people globally—and over a third of all young people aged 15 to 24—is likely to be African.[14] In the same vein, nine countries—the Democratic Republic of Congo, Egypt, Ethiopia, India, Indonesia, Nigeria, Pakistan, Tanzania, and the United States—will make up over half of estimated population growth between now and 2050.[15] These growing populations, mostly in developing states, will bring with them huge demand for digital resources, systems, data, and connectivity.

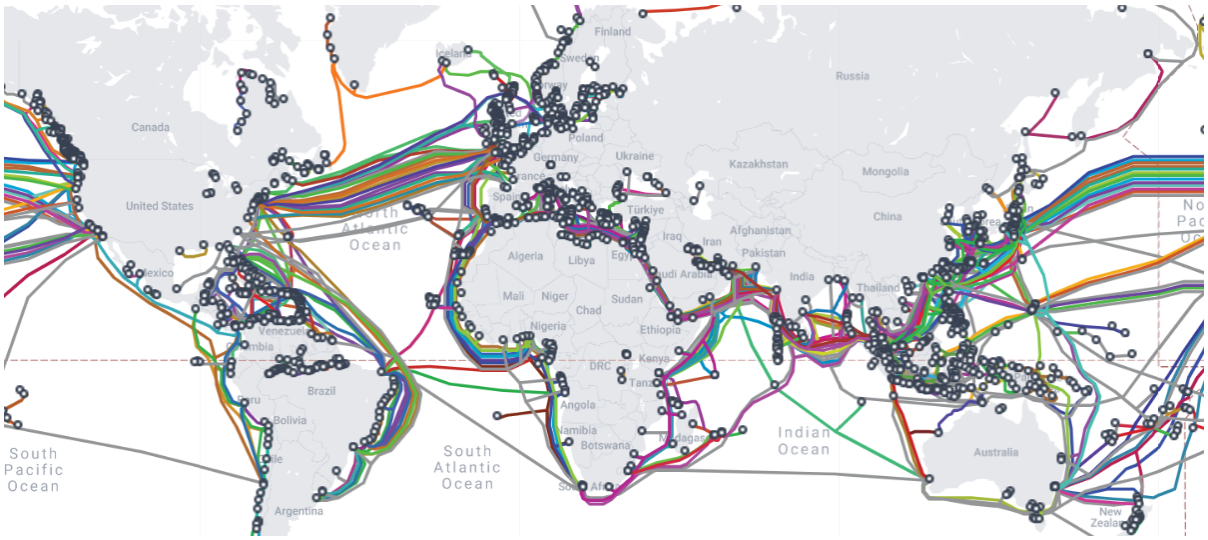
Likewise, as countries push ahead with adopting AI and venture into quantum computing, the need for additional subsea cable capacity will increase. The large language models, data centers, and storage systems necessary for this technology depend on consistent and reliable connectivity that can handle enormous amounts of data—and currently there is no substitute for the speed and dependability of wired connections. As these cutting-edge applications become more common and AI becomes further integrated into economies, the demand for connectivity will rise in parallel.

A final, very banal reason drives the demand for subsea cable infrastructure: Most cables are expected to have a 25-year lifespan, with underwater conditions, storms, and vessel traffic impacting the integrity of cables and their lifespan.[16] This necessitates constant maintenance to account for regularly occurring damage from accidents and environmental wear and tear.

Subsea cables are critical for nearly all aspects of commerce and business connectivity, and the connectivity they provide cannot be handled or replicated by satellites.[17] Compared to satellites,

subsea cables carry much more information per second and are vastly **more efficient and reliable**.[18] Satellites average an estimated 260 gigabits per second (Gbps) and are usually being used by thousands of customers, which can results in slow speeds during peak usage.[19] Subsea cables can process terabits of information per second (Tbps) more efficiently and at a lower cost.[20] Subsea cables form the backbone of data needs worldwide and are responsible for the vast majority of internet traffic. On the other hand, satellites provide wide-area coverage, making them ideal for connecting remote or rural locations where laying cables is impractical or cost-prohibitive.

Figure 1: Worldwide Subsea Fiber-Optic Cables, 2025




Source: "Submarine Cable Map," TeleGeography, https://www.submarinecablemap.com/.

## The Subsea Cable Ecosystem

The subsea cable ecosystem has evolved since the first cables were laid in the 1850s, moving from the pioneering telegraph companies of the nineteenth century to the world's largest tech companies in the modern era. The current scope of the industry involves stakeholders from both the private and public sectors. In general, private sector actors—telecommunications companies, cable manufacturers, and tech titans—lead in financing, designing, manufacturing, laying, and repairing cables. The public sector likewise plays an expansive role in the sector, writing the rules that determine where cables can be positioned, reviewing ownership and access, and implementing laws that can mitigate accidents or other issues that could cause cable breaks or undermine national and economic security.

### CABLE MANUFACTURING AND INSTALLATION

This sector is highly concentrated among a few specialized companies which design, manufacture, and deploy physical cable systems: SubCom, based in the United States; the Nippon Electric Company (NEC), based in Japan; Alcatel Submarine Networks, based in France; and HMN Tech (formerly Huawei Marine Networks), based in China. These four companies control almost all of the global market. Due to the limited number of firms and their countries of origin, strategic vulnerabilities can arise through potential supply chain bottlenecks and geopolitical leverage. For

example, not all of these companies have their own ships; NEC must rely on contracting ships from other companies, potentially from China, which represents a geostrategic threat to Japan and the United States. In addition to building its presence in the industry through HMN Tech, China is the world's largest shipbuilder and could increase its share of cable installation and repair ships. As a result, companies that lack their own ships could find themselves with limited options for trusted suppliers, or China could deploy coercive measures by limiting or denying access to these ships to lay new cables or repair damaged cables. Other companies engaged in the manufacturing and installation of cables include NTT and KDDI from Japan and local telecom companies in countries where cables land or connect, such as Mobily, Vodafone, China Mobile, Embratel, and Liberty Latin America, among others.[21]

## CABLE OWNERS AND OPERATORS

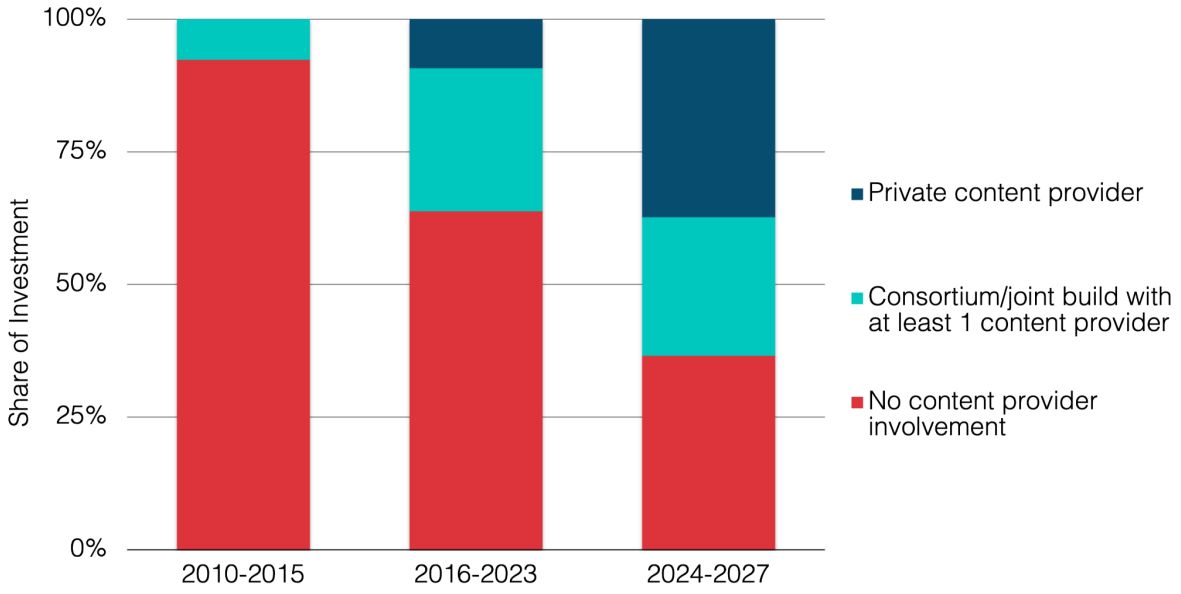
Prior to the twenty-first century, telecom companies were the primary financiers and operators of cables, but hyperscalers—today's large cloud service providers—have emerged recently as the dominant funders and owners of subsea cable capacity.

The dot-com bubble in the mid-1990s created "irrational exuberance" in subsea cable investment through 2001. At that time, cable startups flourished. According to a subsea cable manufacturer interviewed for this report, some startup cable manufacturers had their own ships to lay and repair the cables, providing more choice in the industry. Due to the dot-com bust and several technological advancements, many smaller companies in the sector folded, and telecommunications companies shifted their focus to different services and cable investment models that were more financially feasible. Maintaining ships loaded with cables became extremely expensive "floating storage warehouses," according to one cable manufacturer. Businesses could no longer afford to individually maintain ships dedicated to subsea cable installation and repair, contributing to the underinvestment in the cable laying and repair fleet that exists today.[22]

Investments in subsea cable infrastructure have since rebounded and are reaching significant new levels due to an increase in demand stemming from the proliferation of the internet, internet-based services, and big data.[23] Consumer demand around products related to cloud services, streaming services, social media, and general internet usage are driving this demand—hyperscalers, which dominate these services, account for 69 percent of all international bandwidth used today.[24]

The cable ownership landscape has been dramatically transformed by hyperscalers, companies that utilize significant amount of data and computing services, such as Amazon Web Services (AWS), Google, Microsoft, and Meta. Hyperscalers have mostly supplanted traditional telecom providers and common carriers as the primary drivers of global investment in subsea fiber-optic cables. Google is the world's largest owner and investor; between 2016 and 2018, the company invested billions in 14 global subsea cable projects and in the ensuing years announced plans for two transatlantic subsea cables, including the Grace Hopper, connecting the United States to the United Kingdom and Spain, and the Nuvem, connecting the United States and Bermuda to Portugal. In the Pacific, Google has announced Australia Connect, which will link to the existing Pacific Connect project.[25]

## Figure 2: Content Provider Share of Investment in New Submarine Cable Systems, 2010–2027




Source: Mike Constable, Lane Burdette, and Alan Mauldin, *The Future of Submarine Cable Maintenance: Trends, Challenges, and Strategies* (Washington, DC: Infra-Analytics and TeleGeography, June 2025), 88, https://www2.telegeography.com/hubfs/LP-Assets/Ebooks/The%20Future%20of%20Submarine%20Cable%20Maintenance_%20Trends%2C%20Challenges%2C%20and%20Strategies.pdf.

Likewise, Meta announced plans in early 2025 to build the longest subsea cable project in the world: a 50,000 km network connecting five continents and countries, including Brazil, India, South Africa, and the United States. Called Project Waterworth, this project is expected to significantly enhance data capacity and is projected to cost more than $10 billion.[26]

AWS has also joined consortiums or funded its own cable projects, including the 14,600 km JUPITER Cable System, which can push more than 60 Tbps through its cable. The JUPITER Cable System connects Japan to California and the Philippines. The JUPITER Cable Consortium includes Amazon, Meta, NTT, PCCW Global, PLDT, and SoftBank.[27]

Microsoft has been an active investor as well, supporting the MAREA cables linking Virginia to Spain, capable of carrying up to 160 Tbps, which Microsoft states is "more than 16 million times faster than the average home internet connection." Microsoft also owns parts of the New Cross Pacific cable system, which connects Northeast Asia to the United States, and Amitie, which connects the United States to Western Europe.[28]

In addition to HMN Tech, Chinese state-owned enterprises and telecom companies have been active investors as well, particularly in cable systems in the Indo-Pacific. China Telecom is the predominant player, as well as China Mobile, Huawei, and China Unicom, among others.[29] Many companies and governments complain that China gives its companies and state-owned enterprises an unfair advantage with heavy subsidies and suspected corrupt practices, such as through development incentives or coercive measures to compel support for projects. As noted

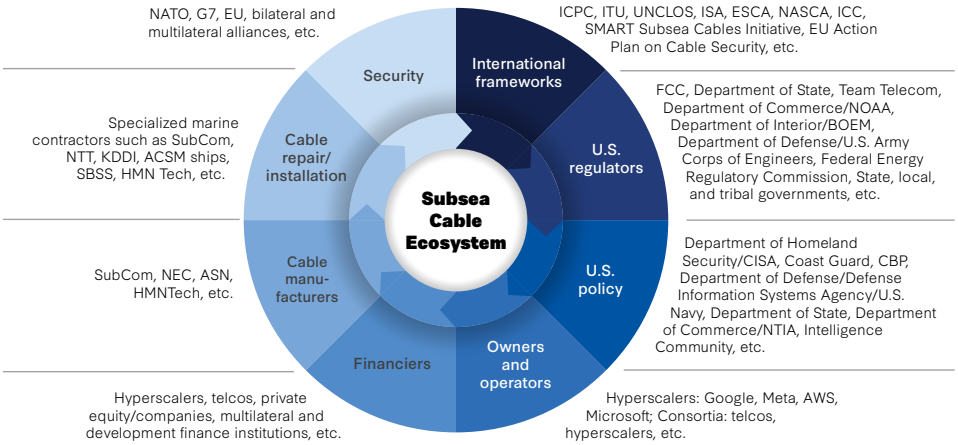
previously, Chinese telecoms and state-owned enterprises have been part of consortiums funding cable projects, but they can also band together to fund their own projects. China's ever-evolving Belt and Road Initiative (BRI) has moved from mostly mega-transportation infrastructure projects to information and communications technology (ICT) infrastructure through its Digital Silk Road. This effort has leveraged China's ability to use its own cable manufacturers, financiers, and telecom operators to provide a "one stop shop" for cable projects. One example of this is the Pakistan & East Africa Connecting Europe (PEACE) cable, a 15,000 km cable project linking Pakistan to France and Singapore, with landings in multiple countries across Europe, Africa, and Asia. A subsidiary of China's Hengtong Group, the country's largest cable manufacturer, owns the cable. HMN Tech provided the turn-key system, and China Mobile and China Telecom were involved in extension of the PEACE cable to Singapore.[30] As with the BRI, China subsidizes companies and state-owned enterprises like HMN Tech, China Telecom, China Telecom Global, China Unicom, and China Mobile, leading to market distortion and an uneven playing field for competitors.

## FINANCIERS

Financing submarine cables requires patience, given the high capital costs (potentially billions of dollars), specialized skill sets, unique resources (ships, engineers, and crew), and permitting and regulatory hurdles. Cables require significant sums of upfront capital. Given these costs, consortium structures became favored as a way of financing new cables in the 1990s and the first decades of the 2000s.[31] These consortia include hyperscalers as well as manufacturers and domestic telecommunications operators, though hyperscalers are the primary financiers of new projects today.

Multilateral development banks, such as the World Bank and Asian Development Bank, and U.S. financing and development agencies, including the U.S. International Development Finance Corporation (DFC), also provide financing to subsea cable projects. The DFC looks to use its diplomatic and financing heft primarily to finance projects in geostrategic locations. Development banks, which account for an estimated 5 percent of subsea cable financing, and financing and development agencies can offer concessional financing and longer tenors (repayment terms) to finance projects that are too risky for commercial banks.[32]

### Figure 3: Subsea Cable Ecosystem

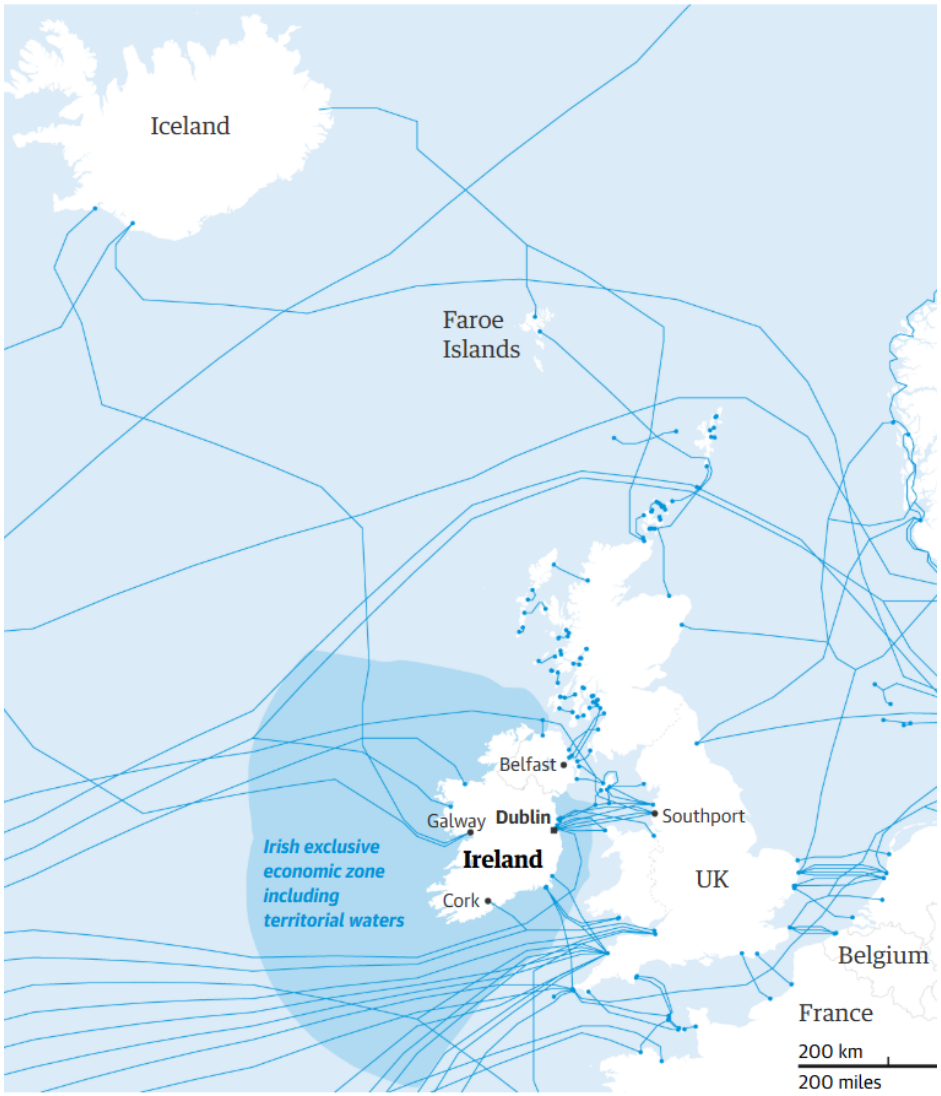



Source: CSIS.

## Ireland Country Case Study

Ireland occupies a storied place in subsea cable history and continues to remain an important point for connectivity. The first transatlantic cable connected County Kerry to Canada's Newfoundland in 1858.[33] Irish waters are now crossed by up to 75 percent of all cables in the Northern Hemisphere, as Ireland serves as a connection point between the United States, United Kingdom, and mainland Europe.[34] Fourteen cables land in the country directly, with more planned.[35] Ireland is also an important site for hyperscalers and the data centers that store, process, and connect information.[36]

Figure 4: Subsea Cable Network in and near Ireland




Source: "Calls for Ireland to boost defence of subsea internet cables," *The Guardian*, January 25, 2025, https://www.theguardian.com/world/jan/25/could-ireland-longheld-neutrality-make-it-vulnerable-to-infrastructure-attacks.

Ireland's most prevalent threats to its cables are accidents and aging infrastructure. But heightened geopolitical tensions in Europe coupled with cable breakages in the Baltic Sea, possibly the work of Russia's "shadow fleet" of oil tankers, may catalyze Ireland to undertake bureaucratic reforms and engage in greater engagement with the United Kingdom and European countries to protect this critical infrastructure.

Responsibility for monitoring and generating policy on subsea cables in Ireland is spread through various ministries, resulting in the lack of a single point of contact and less efficient or streamlined coordination on policy, protection, and resiliency.[37] Additionally, Ireland has not prioritized its maritime defenses, mostly due to a historical tendency to maintain neutrality by refraining from military alliances or partnerships.[38] As a result, the country is not prepared to handle threats coming from Russia or other hostile state actors, nor is it in a position to support regional monitoring and other cooperative efforts.[39]

To address these challenges and build redundancy and resiliency into the country's infrastructure, CSIS recommended the following actions in its Ireland country case study:

- **Ireland should establish a national security framework and build up its naval assets**, through personnel or ships, to address security threats in or near its waters. Domestic and government concerns suggest there will have to be a careful balance to strike in maintaining Ireland's neutral stance, but there should be a growing recognition that subsea cables are critical to the country's economic focus on hosting technology companies, data centers, and financial services.
- **Ireland should support efforts to build redundancy in the infrastructure**, primarily through streamlining bureaucratic processes and creating an inter-ministry process led by a single agency such as the Maritime Area Regulatory Authority (MARA).
- **Ireland should document incidents to better inform the nature of damage**, establish patterns, and provide remedies to prevent cable cuts. Ireland can also enhance its legal framework for holding ships accountable for damage by criminalizing such incidents.
- **Ireland should work with like-minded partners in the region and with the United States** to enhance information sharing, establish platforms for cooperative measures, and facilitate financing or capacity building to address threats in Ireland's territorial waters.
- **Ireland's government should work with the private sector** to better understand how to streamline its bureaucratic processes and procedures and to ensure its laws and frameworks better support the industry as well as network resiliency.[40]

For the full case study, see "The Strategic Future of Subsea Cables: Ireland Case Study," https://www.csis.org/analysis/strategic-future-subsea-cables-ireland-case-study.

## Redundancy: Laying the Groundwork

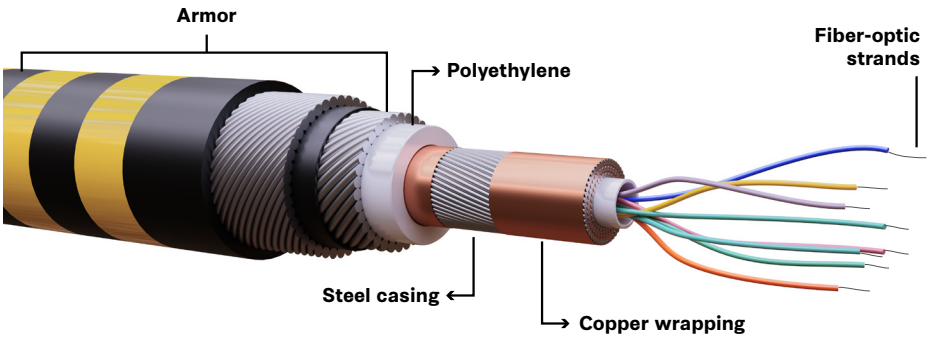
Subsea cable manufacturers and consortia must undertake extensive planning and surveying before laying any cables. The seabed floor must be checked for seismic activity, environmental concerns, and other potential bathymetric (seabed topography) issues. Permitting and regulatory issues are also taken into consideration to ensure the planned route will be accepted by any countries traversed by a cable. Another consideration is identifying alternative routes to ensure continuous connectivity and minimize disruptions in case of cable failure or outage. With the route of the cable determined, cable manufacturers will produce the cable, then load the finished product onto specialized vessels that can store and lay cables. The cables are spooled into large tubs and then unspooled to land on the ocean floor, typically by unmanned underwater vehicles or even divers.[41]

In shallow waters, submarine cables are buried under the seabed to prevent damage from passing ships, and at deeper depths, they lay right on the ocean floor. Cable-laying ships can use autonomous underwater plows and submersibles to dig trenches and then bury cables. Cables are typically not wider than a garden hose and are armored with a layer of galvanized steel and polyethylene to protect the optical fibers from water or other damage. Cables closer to shore or in rocky terrain or areas with high commercial traffic have additional layers of galvanized steel and special yarn to protect the fiber-optic threads. A copper sheet, or tape, is wrapped around the first layer of galvanized steel as a conductor. Repeaters are placed roughly every 60 to 70 km to boost and amplify the optical signal.[42]

To connect to other countries or islands, a branching unit, or spur, may be added to the main subsea cable to connect to other cables, permitting multiple landing points or other branching units. Branching units are larger than the cables they connect, as they need to accommodate the splicing and connection processes, maintain continued connectivity, and also withstand environmental threats.[43] Cables pass through cable landing stations, facilities located on coastlines where undersea fiber-optic cables connect data to terrestrial, or overland, networks.[44]

### Figure 5: Subsea Cable Structure

Each component has its own role in protecting cables from corrosion, electrical interference, ship anchors, rocky or challenging terrain, and rough seas, as well as sealing off water.




Note: Components differ depending on manufacturer and placement location. This artistic rendering is an approzimation of typical components.

Source: CSIS.

## Repairing Cut or Damaged Subsea Cables

Accidents from fishing or anchoring from commercial vessels are the primary driver of subsea cable damage. Methods for covering the costs of the repairs and holding responsible parties accountable vary by country but also by insurance company.

Should a cable within a consortium be damaged, the consortium typically files a joint claim to insurance companies. Almost all subsea cable operators have insurance to cover reapirs in the event of accidents or natural disasters.[45] If a specific vessel or company is determined to have been responsible for the damage, the company that owns the ship or the crew of the ship can be held accountable and may need to pay fines or serve jail time. This tends to be specific to the waters in which the cable breaks; countries like Singapore have anchorage laws and protection zones for subsea cables that hold companies liable.[46]

Repair permit requirements vary significantly from country to country; legal frameworks outline the scope of a country's territorial waters (0 to 12 nautical miles offshore) and exclusive economic zones (12 to 200 nautical miles offshore) which determine what permitting and regulatory rules apply.[47] While international frameworks provide general guidelines, national regulations play a crucial role in governing these activities. Entities involved in cable repair must engage with relevant authorities in each jurisdiction to ensure compliance with all applicable laws. Environmental and security concerns can further complicate the permitting process, as can visa requirements, which can take a long time to process or may require biometrics collection, further delaying maintenance and repair. Moreover, repairing submarine cables often requires coordination across multiple countries, especially when cables cross international boundaries.[48] This can involve complex negotiations to obtain the necessary permits and ensure compliance with each country's regulations.

Beyond differences in permitting and regulatory frameworks at the country, state, or territorial level, the process for repair is generally the same around the globe. Once the damage is located, cable operators either use their own repair ships or hire cable repair ships to fix the damage. Cable owners and operators enter into maintenance agreements for cable repairs either through private maintenance agreements, zone agreements, or individually negotiated contracts with cable repair companies. While the manufacturer may be the one laying the cable, it may not own the system. Therefore, if damage is detected, it might not be responsible for repairs unless under contract to do so. Instead, private agreements are often in place, and zones are contracted to one or two cable repair companies.[49]

Not every manufacturer or hyperscaler has its own cable repair ships; for example, SubCom and NTT have their own installation fleets (which are larger ships that carry more cable), but NEC, a major manufacturer, must hire contract repair ships (which are smaller and carry less cable) to address any damage to their cables.[50] Such ships raise damaged sections of cable with a grappling hook and specialized tools. The cable is then dragged to the ship, the damaged section is cut, and technicians splice in a new section of cable. The technicians test the repaired section to ensure its operating normally before lowering it back to the bottom of the ocean. The new section may be reburied using autonomous ploughs, depending on the original configuration of the cable and vessel traffic in the area. The crew then conducts final checks confirming the functionality of the repaired section.[51]

## Resiliency: Protecting Subsea Cables

The public sector plays a prominent role in the industry, either by implementing regulations to protect the infrastructure or providing monitoring, detection, and protection services. The primary way for governments to protect subsea cables is to devise a regulatory framework that deters accidents, including leveraging significant fines on companies whose ships cause damage and requiring cable operators to bury cables at certain depths in busy seaports. For example, Singapore enforces legal protections to deter accidental or intentional damage to its subsea cable infrastructure through its Telecommunications Act and penal code, which criminalizes damage to telecom cables or interference with public telecom systems or public services.[52] Additionally, UNCLOS and the New York Principles each provide guidance on damage repair and recommendations for laying cables. UNCLOS establishes that damage to subsea cables or other infrastructure within a state's maritime territory is subject to that state's criminal jurisdiction. The New York Principles—established during the 78th UN General Assembly in 2024 to bolster security and resilience for subsea cables, and endorsed with a joint statement by 30 member states—outline best practices for laying, repairing, and maintaining cables safely and securely.[53]

Naval and air assets can be deployed to monitor or deter risks to subsea cable infrastructure. This can be a particularly challenging task given the vastness of the distances covered, which requires governments to focus their security efforts on high-risk areas. For example, NATO has launched Operation Baltic Sentry, an effort to combine the use of frigates and maritime patrol aircraft, naval drones, and allied surveillance capabilities to protect subsea cables from intentional damage.[54] The United States has also instituted the Cable Security Fleet, a joint effort between the Departments of Transportation and Defense that allows the U.S. government to contract a fleet of privately-owned U.S.-flagged cable vessels to lay, maintain, and repair cables. These ships are to be made available to the government in times of emergency, such as an act of sabotage or a natural disaster that compromises multiple cables.[55]

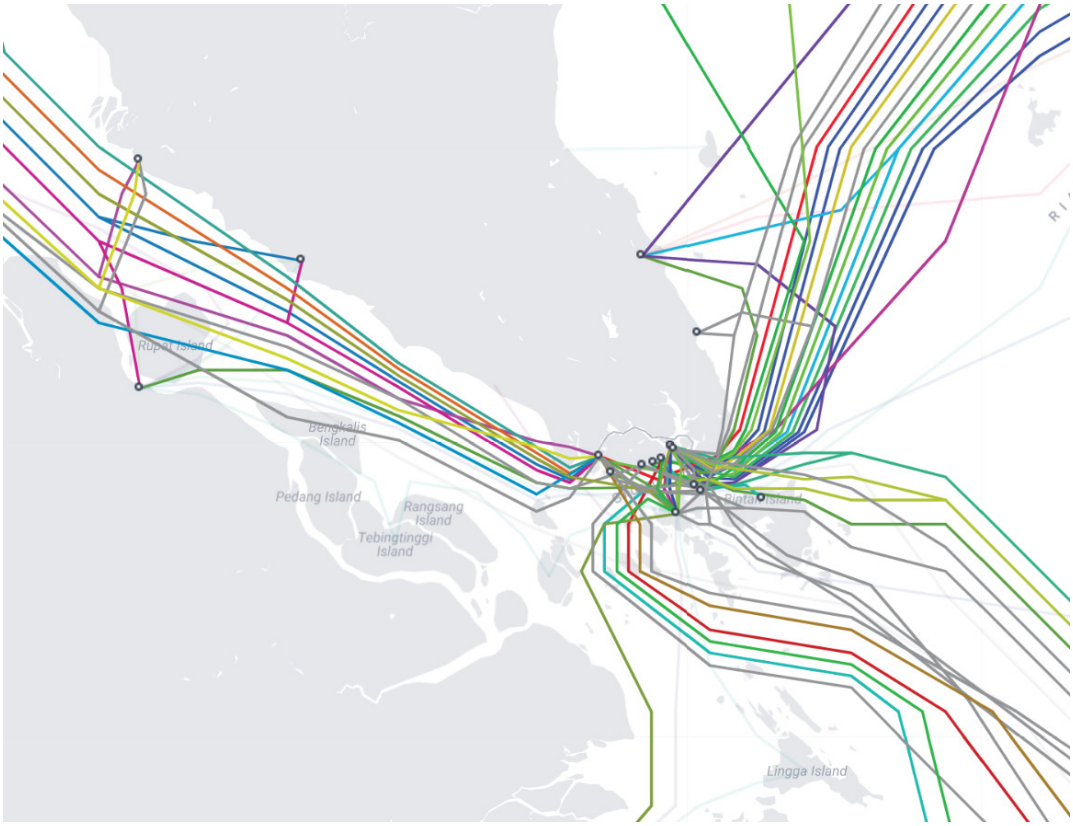
### Singapore Country Case Study

In 1871, Singapore was first linked to the world by a cable stretching from Madras, India, to Singaporean shores.[56] Today, the country is a global hub for subsea cables. Singapore is highly important in the subsea cable landscape due to its centrality in technological and financial industries and its policies that support a more resilient network. Singapore's government has been active in making the country attractive to tech industries and in enabling a secure environment to lay and protect the cables that power those industries. Thanks to its business-friendly legal and regulatory landscape, Singapore's digital economy accounted for 17.7 percent of its GDP as of 2024.[57]

The country also liberalized its telecommunications industry in 2000, paving the way for domestic and foreign companies to more easily get licenses to operate ICT-related businesses.[58] To further provide stable connectivity for these digital industries as well as account for the variety of commercial vessels that occupy its busy port, Singapore has

enacted laws that contribute to eliminating accidental cuts from anchoring or fishing vessels. Its Telecommunications Act and penal code impose steep fines or jail time if public telecom services are disrupted.[59] These laws have contributed to years without accidental cuts.[60]

Figure 6: Map of Subsea Cables Around Singapore




Source: "Submarine Cable Map," TeleGeography, https://www.submarinecablemap.com/country/singapore.

Challenges to Singapore's cable system extend beyond its maritime borders; cable manufacturers and owners must negotiate nearby Indonesia's protectionist cabotage laws. Cabotage laws govern a country's shipping routes in their territories and have been implemented by countries to protect local shipping industries and support the use of local labor. Indonesia's laws require Indonesian-flagged ships and crew for work in Indonesia waters, potentially delaying repairs or the laying of cables if such resources are in short supply.[61]

CSIS recommended the following actions in its Singapore country case study:

- **Singapore should lead on regional efforts to draft and implement best practices on protecting subsea cables.** Singapore has a strong track record in protecting cables from accidental cuts, not just through its laws but also via information and data collection. Sharing these best practices with its Southeast Asian

neighbors would enhance protection for cables that run through the region's waters. This also extends to broader cooperation in the international arena; Singapore can leverage its membership in the ICPC and in international institutions to share best practices, developments, and capabilities in monitoring the safety of cables and promoting and attracting new investments.

- **Singapore should engage with neighboring Indonesia and other countries with protectionist-leaning cabotage laws.** Singapore can illustrate the drawbacks of these cabotage laws, which can slow repairs and thus slow the connectivity needed for a strong economy. These choices have trade-offs: Indonesia would have to shift its support for ship-related labor toward supporting other industries that benefit from the use of cables, including finance, telecoms, e-commerce, and many others.[62]

For the full case study, see "The Strategic Future of Subsea Cables: Singapore Case Study," https://www.csis.org/analysis/strategic-future-subsea-cables-singapore-case-study.

# Part II

## *Global Oversight of the Subsea Cable Ecosystem*

The proliferation of subsea cables across international waters and coastal states and the importance of these cables to digital connectivity necessitate enhanced and proactive oversight, and a number of international organizations and global governments have taken up this important task. Without global frameworks and regulatory regimes, responses to the vulnerabilities of subsea cables, including addressing accidents or damage from natural disasters, would not be holistic or efficient. Some international organizations offer voluntary frameworks that countries can ratify, including UNCLOS and the 1884 Convention for the Protection of Submarine Telegraph Cables. These provide foundational regulations for countries to adopt, particularly in the case of oversight in territorial waters or in holding perpetrators of accidental or intentional damage accountable. However, not all countries have ratified these laws, particularly the 1884 Convention, nor have these frameworks kept up with advancements in digital infrastructure or the change in the type of stakeholders involved in manufacturing and financing the network.

Recent events indicate that policymakers are increasingly aware of the importance of subsea cables and the need to ensure their resiliency in the modern era. In 2024, the United States and like-minded countries from Asia, the Pacific Islands, and Europe issued a joint statement at the UN General Assembly. The "Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World" advocated for designing the network "with resilience, redundancy, and security in mind."[63] The statement also promoted greater public-private collaboration, greater cybersecurity and data risk mitigation efforts, and compliance with international law as reflected in UNCLOS.[64] The G7 also issued a leaders' communique at the 2023 Hiroshima summit, which

recognized the importance of protecting the infrastructure and building redundancy with trusted partners.[65] However, work remains to be done to carry these ambitions through to fruition.

Figure 7: Maritime Zoning Rules for Subsea Cables per UNCLOS


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

## International Organizations and Regulatory Bodies

There are several organizations and partnerships that provide frameworks, guidance, financing, and security measures for subsea cable infrastructure. Most of the recommendations and guidelines from these organizations lack enforceability if not ratified by a country. As a result, the implementation of recommendations and international frameworks is uneven across the globe.

## Table 1: International Policy and Frameworks

| Organization | Responsibilities |
|---|---|
| International Cable Protection Committee (ICPC) | The ICPC promotes the safeguarding of international cables against man-made and natural hazards. It has more than 160 members in more than 60 countries, representing 97 percent of the world's subsea telecom cables, including cable operators, owners, manufacturers, industry service providers, and governments. The ICPC provides recommendations on subsea cable laying and resiliency best practices.[66] |
| International Telecommunications Union (ITU) | The ITU is a specialized UN agency for digital technologies and is made up of 194 member states and more than 1,000 companies, universities, and international and regional organizations. It convenes multistakeholder dialogues on cable network resiliency, and the ITU, in partnership with the ICPC, has an International Advisory Board on Submarine Cable Resilience to promote dialogue and ways to collaborate to improve subsea cable resilience.[67] |
| United Nations Convention on the Law of the Sea (UNCLOS) | UNCLOS is an international treaty that governs the world's oceans and activities in and on the seas and defines territorial claims and other jurisdictions for states.[68] |
| International Seabed Authority (ISA) | The ISA is an autonomous international organization established under UNCLOS. It works with members to govern mineral resources activities, such as deep seabed mining, to protect the marine environment.[69] |

## Table 2: Regional, Government, Stakeholder-Led Initiatives

| Organization | Responsibilities |
|---|---|
| EU Action Plan on Cable Security | The EU Action Plan on Cable Security identifies steps to address each stage of the subsea communications and energy cable life cycle by preventing, detecting, responding, repairing, and deterring threats and damage to the infrastructure. It also outlines an action plan to address catastrophic cuts through prevention or recovery.[70] |
| European Subsea Cable Association (ESCA) | ESCA is a forum of European and international cable companies that promotes marine safety and the safeguarding of submarine cables from accidents and natural disasters.[71] |
| North American Submarine Cable Association (NASCA) | NASCA is a forum made up of companies that own, install, or maintain cables. It provides a platform to exchange information on policy issues related to technical and legal developments and standards as well as procedures for the industry.[72] |
| Science Monitoring and Reliable Telecommunications (SMART) Subsea Cables initiative | The SMART Subsea Cables initiative was established by the ITU, the Intergovernmental Oceanographic Commission (IOC) of the United Nations Educational, Scientific and Cultural Organization (UNESCO), and the World Meteorological Organization (WMO). It seeks to augment ocean monitoring and scientific research to provide a greater understanding of the state of the world's oceans by outfitting subsea cables with sensors.[73] |
| International Connectivity Coalition (ICC) | The ICC is a group that enables stakeholders to exchange information and conduct business transactions internationally. It supports transparent and streamlined regulations.[74] |

Table 3: Security

| Organization | Responsibilities |
|---|---|
| North Atlantic Treaty Organization (NATO) | NATO established the Maritime Centre for Security of Critical Underwater Infrastructure on protecting undersea cables, which provides a framework for coordinating multinational responses to threats against the infrastructure. NATO also created the Critical Undersea Infrastructure Coordination Cell and leads Operation Baltic Sentry. Depending on the nature of an international attack, NATO also could invoke Article IV, which calls for consultations among members and is invoked if there are security threats, or Article V, which calls for collective defense.[75] |
| Group of 7 (G7) | The 2023 G7 communique reflects the members' interest in collaborating more on subsea cable security. That communique also included language on national security and ensuring resiliency and trusted supply chains related to subsea cables that connect with allied and partner nations.[76] |
| European Union | In addition to the EU Action Plan on Cable Security, the European Union plans to enhance monitoring capabilities, establish a repair vessel reserve to repair damaged cables quickly, and use sanctions and other measures to deter Russia's "shadow fleet."[77] |

## FINANCING

Multilateral development banks (MDBs) and development finance institutions (DFIs) provide several types of financial support, such as debt and equity financing, grants, and technical assistance, to subsea cable projects in developing and middle-income countries to promote economic growth and development. Their engagement in this space has been limited and more often is directed toward the provision of digital services and terrestrial-based connectivity. MDBs and DFIs can similarly provide financing or personnel to undertake feasibility studies to explore whether a project is viable. These financing institutions can also provide technical assistance on a variety of levels, including to governments or project managers for developing contracts or designing projects. For subsea cable projects, financing is mostly targeted to supporting the build of the cable itself and improving a country's connectivity, not in financing the establishment of a cable manufacturing or shipbuilding plant. The table below provides examples of subsea cable projects in which such institutions have provided financing.

## Table 4: Examples Engagement by Global and Multilateral Financing Institutions

| | |
|---|---|
| World Bank | The World Bank provided financing in 2023 for preparatory activities for a Black Sea submarine cable project to improve digital connectivity and energy security for Georgia and the South Caucasus region.[78] |
| International Finance Corporation (IFC) | The IFC supported a branch of Google's Equiano cable to Nigeria and Togo, started in 2018, to connect Europe via Portugal to South Africa.[79] |
| Asian Development Bank (ADB) | The ADB provided a $25 million grant for a submarine cable connecting Samoa and Fiji in 2015. It also cofinanced the Avaroa cable project for the Cook Islands in 2020 and approved loans for a cable system connecting Palau to Guam in 2013.[80] |
| Inter-American Development Bank (IDB) | Through its private sector arm, IDB Invest, the IDB provided $6 million in 2015 in financing to a project in Ecuador that included supporting a new submarine cable through the Pacific Cable Communications Systems consortium and a fiber-optic cable production plant.[81] |
| Development Bank of Latin America (CAF) | In 2024, CAF provided a $140 million loan to provide the first subsea cable to El Salvador.[82] |
| European Bank for Reconstruction and Development (EBRD) | EBRD has been active in the subsea cable space, but more recently in subsea power cables. It also supports upgrading or building ICT infrastructure, including terrestrial fiber-optic networks, including a potential project in Nigeria expanding broadband infrastructure.[83] For subsea cables, in 2016, EBRD provided a $50 million loan to a Turkish telecom company to support a 20,000 km cable connecting Southeast Asia, India, the Middle East, and Europe.[84] |
| African Development Bank (AfDB) | The AfDB has injected nearly $3 billion in ICT infrastructure in Africa. This includes a cable connecting Seychelles to Tanzania that became operational in 2012 and its Central African Backbone project completed in March 2025 that connects several landlocked countries through terrestrial fiber-optic cable to subsea cables.[85] |

| | |
|---|---|
| Japan Bank for International Cooperation (JBIC) | In 2021, JBIC provided export finance to support Project Echo, which connects Singapore, Palau, and the United States; U.S. and Australian financing agencies also supported the cable system project.[86] |
| Australian Infrastructure Financing Facility for the Pacific (AIFFP) | The AIFFP provided financial support to several subsea cable projects across the Pacific Islands and Timor-Leste.[87] |

# Part III

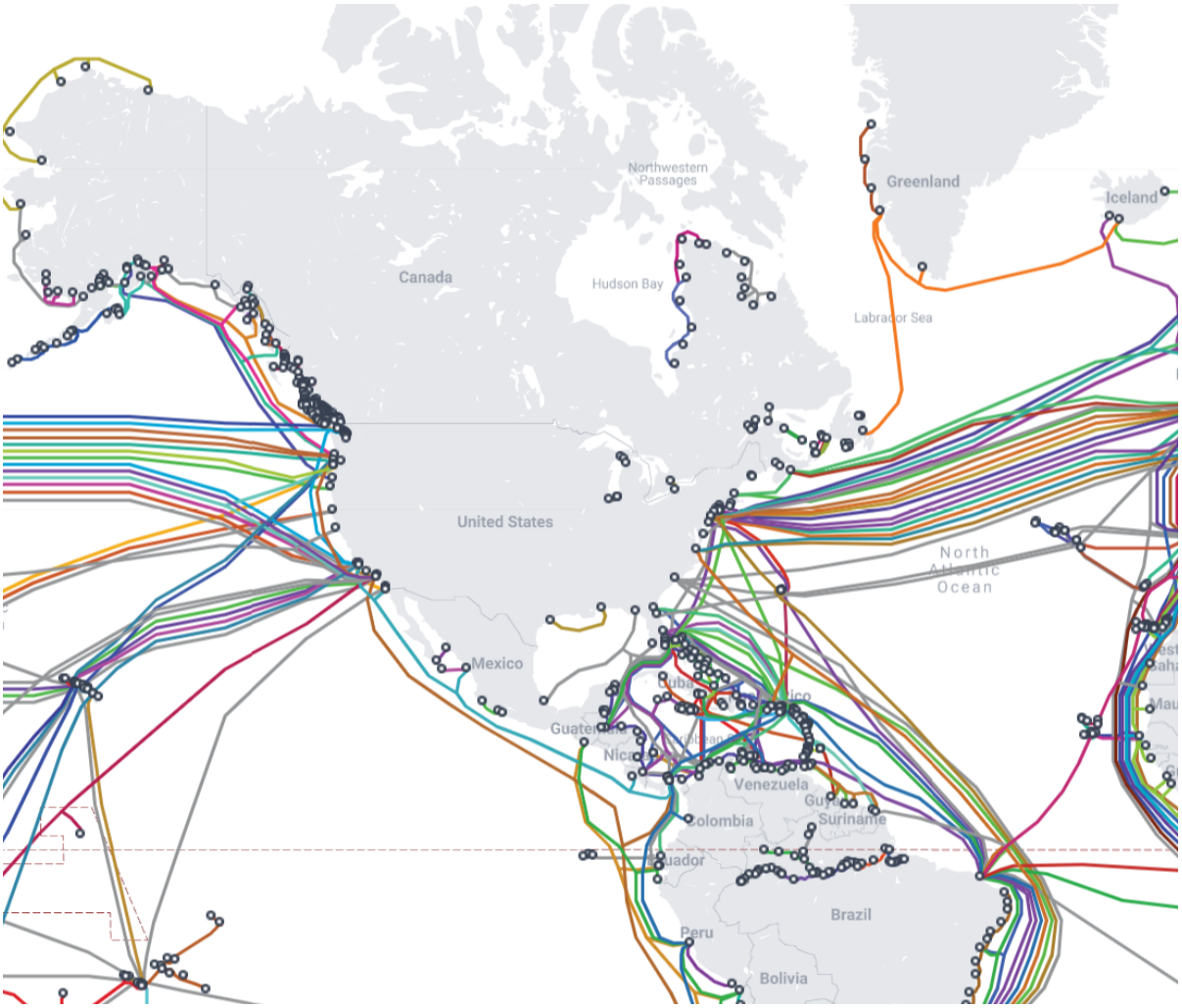
## *The Subsea Cable Landscape in the United States*

### U.S. Connectivity: Oversight and Roles

The United States currently has dozens of cable landing stations and 90 registered current or planned cables connecting to nearly all continents, making it the most connected country in the world.[88] It serves as a major connecting point across the Pacific and Atlantic Oceans and has considerable data needs, particularly given the heavy presence of hyperscalers, an ever-expanding digital economy, and the advent of AI and other cutting-edge technologies. This complex and growing ecosystem involves a web of public and private stakeholders who will help determine the future role of subsea cable infrastructure.

In the United States, there are more than a dozen federal agencies that oversee various aspects of laying, repairing, and protecting subsea commercial cables. State, local, tribal, and territorial (SLTT) governments also play a role in regulatory oversight and permitting. U.S. states have specific legislation that governs their role in regulation and oversight when cables enter their jurisdictions. The Submerged Lands Act of 1953 allows coastal states to lay territorial claims three geographical miles from their baseline, meaning they can administer permits, issue development rights, or institute marine protections.[89] No single lead agency is currently responsible for coordinating the redundancy, repair, and resilience of subsea cables. Therefore, the private sector—including cable manufacturers, hyperscalers, and owners and consortia of investors—must navigate numerous regulatory processes to obtain the necessary approvals and permits to lay, repair, or replace cables.

Figure 8: The U.S. Subsea Cable Network




Source: "Submarine Cable Map," TeleGeography, https://www.submarinecablemap.com/.

## U.S. GOVERNMENT AGENCIES INVOLVED IN SUBSEA CABLE INFRASTRUCTURE

The tables below lay out the role each government agency plays in the regulatory ecosystem for subsea cables.

### Table 5: Primary Regulators of Subsea Cables in the United States

| Agency | Responsibilities |
|---|---|
| Federal Communications Commission (FCC) | The FCC issues licenses for cables that land or originate in the United States. It oversees rules and regulations around subsea cable licenses and coordinates with key agencies and departments to ensure the security of the infrastructure (see Team Telecom reference for further information).[92] |
| Department of State (DOS) | The DOS preapproves all FCC cable license grants and revocations. |
| Department of Commerce (DOC) - National Oceanic and Atmospheric Administration (NOAA) | NOAA regulates the impact of cables on marine life and ecosystems. It also issues permits related to marine sanctuaries and endangered species, conducting consultations for cables that could have such impact.[93] |
| Department of Interior (DOI) - National Parks Service (NPS), Fish and Wildlife Service (FWS), Bureau of Ocean Energy Management (BOEM) | The NPS and FWS grant rights-of-way on public lands and refuges. The FWS enforces Endangered Species Act, if applicable. The BOEM regulates undersea energy and cable activities in the outer continental shelf (OCS) and coordinates with federal, state, and local agencies.[94] |
| Department of Defense (DOD) - U.S. Army Corps of Engineers (USACE) | USACE issues permits for cable projects affecting waterways.[95] |
| Environmental Protection Agency (EPA) | The EPA ensures environmental compliance under the National Environmental Policy Act for cable projects affecting public lands and resources. |
| State and local governments | State and local governments issue coastal zone permits, enforce state law, and approve land use and zoning for cable landing stations. |

## Table 6: Government Entities Involved in Subsea Cable Policy in the United States

| Agencies | Responsibilities |
|---|---|
| National Security Council (NSC) | The NSC coordinates interagency national security policy. |
| Department of State (DOS) | The DOS drafts or contributes to international treaties and cable diplomacy and leads the CABLES program, a U.S. government initiative to enhance subsea cable infrastructure and improve digital connectivity, particularly in the Pacific Islands. The DOS also houses the Bureau of Cyberspace and Digital Policy (CDP), which oversees digital policies and funding for digital infrastructure projects. |
| Department of Homeland Security (DHS) | The DHS serves as the United States' critical infrastructure protection agency and works closely with private sector builders, owners, and operators of critical infrastructure, to include subsea cables. It regularly coordinates with the cable industry on security and resilience policy issues. |
| DOC - National Telecommunications and Information Administration (NTIA) | The NTIA advises the president on telecommunications and information policy issues. It focuses on connectivity, spectrum, safety, and innovation. |

## Table 7: Government Entities Responsible for Subsea Cable Security and Monitoring in the United States

| Agency | Responsibilities |
|---|---|
| Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (Team Telecom) | Team Telecom reviews foreign participation in the telecommunications sector for national security and law enforcement concerns and offers recommendations to the FCC for approving, denying, or imposing conditions on cable licenses. Its core members include the U.S. attorney general (who also serves as chairperson) and the secretaries of defense and homeland security, with advisory roles for the heads of several other departments and agencies. Team Telecom agencies also conduct routine compliance monitoring with licensed entities based on the conditions imposed.[96] |
| DHS - Cybersecurity and Infrastructure Security Agency (CISA) | CISA is the national coordinator for critical infrastructure protection. CISA's Sector Risk Management Agency (SRMA) supports the ICT sector. CISA also monitors cable-laying vessels, supports Team Telecom risk analysis and regional coordination with SLTT authorities, and develops interagency concepts for cable security and resilience in crises.[97] |
| DHS - U.S. Coast Guard and Customs and Border Protection (CBP) | The Coast Guard and CBP provide maritime security and law enforcement around critical cable infrastructure. |
| Office of the Director of National Intelligence (ODNI) and intelligence agencies | The ODNI and U.S. intelligence agencies assess threats through all-source information and inform the executive and legislative branches of threats and challenges. |
| DOD - U.S. Navy | The Navy owns more than 40,000 nautical miles of cables and maintains and lays cables on its sole cable ship, the USNS *Zeus.* It operates the Naval Sea Floor Cable Protection Office.[98] |

## Table 8: U.S. Bilateral Development Agencies Involved in Subsea Cables

| Agency | Responsibilities |
|---|---|
| U.S. International Development Finance Corporation (DFC) | The DFC provides debt or equity financing to support subsea cable projects in developing economies overseas. For example, the DFC provided a $190 million loan to support a 15,200 km subsea cable connecting Singapore to the United States, with branches in Guam and Indonesia.[99] |
| U.S. Trade Development Authority (USTDA) | The USTDA provides feasibility study and pilot project financing for subsea cable projects overseas. For example, the USTDA gave a grant for a feasibility study to Indonesian company PT Super Sistem Data for a domestic subsea cable system in 2023.[100] |
| Export-Import Bank of the U.S. (EXIM) | EXIM facilitates the financing of subsea cable projects by supporting U.S. companies involved in exporting equipment and services for these projects. For example, EXIM provided a $28 million long-term guarantee to Tyco Submarine Systems Ltd. in Morristown, NJ, to sell equipment and services to Mauritius Telecom Ltd. for the construction of a cable connecting southern Africa and Southeast Asia.[101] |

## Why Has the United States Neglected to Ratify UNCLOS?

UNCLOS is an international regime for governing how nations interact with each other with respect to the world's oceans and seas, including who can lay claims and who has a legal basis to lay claims. It acts as a body through which countries can dispute boundaries or harmful actions undertaken by other countries. It is one of the most comprehensive frameworks from an international organization to address the world's vast waterways and myriad of resources, and since its inception, it has adopted additional agreements and protections on fishing and marine life. The International Tribunal for the Law of the Sea (ITLOS), along with other international courts and tribunals, interprets and applies UNCLOS provisions to specific disputes and evolving situations. UNCLOS has been the primary mechanism countries in Southeast Asia—especially the Philippines, a U.S. ally—have used in disputes over claims in the South China Sea.[90]

The United States, despite adhering to most UNCLOS standards through a presidential proclamation during the Reagan administration, refuses to ratify the treaty due to its provisions on deep seabed mining. UNCLOS—often referred to as the "constitution for the oceans," has been signed onto by 171 parties since its inception in 1982. The United States joins Eritrea, South Sudan, Turkey, Venezuela, and others in not ratifying the agreement. Despite revisions to the treaty in 1994, the U.S. Senate did not hold hearings at the time due to continued objection to the deep seabed mining provision governed by the International Seabed Authority (ISA) and its royalty schemes on mining resources. Hearings were eventually held in 2004, at which point the Senate Foreign Relations Committee unanimously recommended adopting the treaty, but no further action was taken.

Arguments for and against joining UNCLOS now essentially center around whether it would give the United States leverage to support its own objectives and push back on hostile countries that are undermining the framework, particularly China and Russia. Opponents to joining UNCLOS argue that the United States would gain no further benefit. In other words, it would create more bureaucratic red tape and costs both financially and diplomatically—especially on deep seabed mining—and impede U.S. sovereignty. Opponents also note the weakness of the regime in enforcement: UNCLOS's rulings in favor of the Philippines and the country's claims in the South China Sea have not been recognized by China.

Advocates believe the United States would have more leverage over China by ratifying UNCLOS, giving the framework both credibility and heft. Those in favor also argue that U.S. companies are disadvantaged in terms of deep-sea exploration; China and Russia have received nine exploration permits, giving them an edge in deep-sea mining. Russia and China have also used the United States' non-role in UNCLOS against it: The U.S. State Department in 2023 initiated an extended continental shelf claim in the Arctic and Pacific Oceans, an area within UNCLOS's jurisdiction for seabed mining. China and Russia

pushed back, citing that there was no basis for the claim because the United States has not signed UNCLOS.

States that have not ratified UNCLOS typically cannot enforce its provisions against other states as a matter of treaty law. Despite this, there are aspects of UNCLOS that fall under customary international law (CIL), which has binding authority on all states regardless of treaty ratification. The aspects of UNCLOS that trigger CIL include the traditional uses of the ocean (ships passing through international waters, sea navigation), meaning that international ships, whether commercial, cruise, or fishing, can pass through waters to get from one destination to another. States that are not party to UNCLOS are generally expected to adhere to these provisions because they are considered part of the broader framework of international law. Non-signatories may face challenges in asserting rights or resolving disputes through UNCLOS's formal mechanisms, such as ITLOS. The United States still conducts freedom of navigation operations on the basis of CIL to challenge maritime claimant issues, including regarding China's territorial claims in the South China Sea or as it relates to protecting freedom of navigation in the Indian Ocean.[91]

# Part IV

## *Challenges and Threats to Subsea Cable Redundancy, Resiliency, and Repair*

Global subsea cable networks are subject to cross-cutting threats and obstacles, including accidental cuts by fishing and other commercial vessels and natural disasters, as well as permitting and regulatory issues that slow or halt the laying of new cable or repair of damaged cable. Likewise, the threat of sabotage and espionage by state and non-state actors make subsea cables subject to wider strategic and geopolitical competition. This combination of challenges and threats makes cable redundancy, resiliency, and repair critical policy priorities.

These challenges and threats are not new, but their economic and security implications are more severe today due to growing global interconnectedness, a rising number of consumers, accelerating technological competition, and escalating geopolitical tensions. Studies show that internet shutdowns have increased effects for larger and more interconnected economies. Deloitte estimates that

> . . . for a highly Internet connected country, the per day impact of a temporary shutdown of the Internet and all of its services would be on average $23.6 million per 10 million population. With lower levels of Internet access, the average estimated GDP impacts amount to $6.6 million and to $0.6 million per 10 million population for medium and low Internet connectivity economies, respectively.[102]

This section outlines the key threats and challenges to laying, maintaining, and safeguarding subsea cable infrastructure, categorizing them into physical and non-physical risks. It also sets the stage for a roadmap of recommendations to strengthen subsea cable security and ensure it meets future demographic, technological, and national security demands.

## Physical Threats

TeleGeography estimates there is an average of 200 cable breaks annually around the world, mainly due to accidents, natural disasters, and aging equipment.[103] The exact number of intentional cuts is unknown, as they can be hard to prove.[104] An accidental cut, earthquake damage, or sabotage can disrupt acces to the internet not just for one country, but for many.

### ACCIDENTAL CUTS AND HUMAN ACTIVITY

Regions with heavy maritime traffic, including nearby ports, shipping lanes, and fishing activity, leave subsea cables highly vulnerable to damage. Vessels—including fishing boats, container ships, and naval ships—frequently pass over or drop anchors in areas where cables are buried. Some cables, especially those laid in the early 2000s, are often buried at shallow depths, making them more susceptible to damage from anchor drags. Even cables buried at a depth of more than one meter are threatened by deeper excavation and more sophisticated equipment, particularly from larger or newer vessels such as those involved in deepwater fishing. Accidents can result in ships dropping anchor during stormy weather and being dragged, unintentionally dropping an anchor due to mechanical failure or human error, or simply not knowing (or considering) that subsea cables lay beneath the ship. The locations of commercial subsea cables are open-source and publicly available, with the hope that the information provided can assist vessels in avoiding accidental cuts.

There are growing concerns that the potential mass advent of deep-sea mining for critical minerals such as cobalt, copper, manganese, and nickel could raise the risk of damage to cables. Given the importance of these minerals to critical and emerging technology, including semiconductors, missiles, fighter jets, and medical devices, deep sea mining will likely become another area of geopolitical competition, kicking off mining activity that could disturb or damage cables. The International Seabed Authority (ISA) is still working to finalize the rules governing mining in the sea and is facing pressure from the United States to do so. However, it will also need input from countries whose territorial waters are impacted as well as the private sector entities responsible for seabed mining activity that might impact subsea cables.[105]

### NATURAL DISASTERS

Earthquakes, volcanic eruptions, underwater landslides, and storms can all damage or break cables. The United Kingdom's National Oceanography Centre estimates that natural disasters accounted for 25 percent of cable cuts between 1965 and 2019.[106] This phenomenon was well illustrated by the March 2011 Tohoku earthquake, which reached a magnitude of 9.0 and spurred a devastating tsunami as well as nuclear fallout from the Fukushima nuclear power plant. At least seven trans-Pacific and intra-Asia cables were cut, impacting communications and internet access, including internet traffic to the United States. Asian telecom operators were able to partially restore service by rerouting optical communications traffic over undamaged cables and via satellites. Japan also benefited from having most of its cable landing stations some distance south of the earthquake, meaning most of the country's cables remained out of harm's way.[107] Radioactivity released from the earthquake's nuclear fallout, however, did prevent quick repair of some cables, as radiation levels were too high for ships and workers to safely enter areas near the damaged nuclear power plant in Fukushima.[108]

Similarly, in December 2006, the magnitude 7.1 Hengchun earthquake broke nine subsea cables in the Strait of Luzon between Taiwan and the Philippines and knocked out internet in the region. The damage impacted connectivity in China, Hong Kong, Japan, the Philippines, Singapore, and Taiwan, disrupting banking, airline bookings, e-commerce, and email. Despite internet traffic being rerouted through undamaged cables, connectivity lagged for weeks. Eleven ships were dispatched and spent the next 49 days repairing more than 20 breaks in the nine cables to restore connectivity back to pre-earthquake levels. According to a press release issued by the ICPC, the lengthy repairs were due to several reasons, including extensive damage to multiple cables across a wide area, the severity of the damage, the difficulty in reaching cables that had been buried in underwater landslides, the availability of cable repair vessels, and, to top it off, adverse sea conditions.[109]

Another example of the potential impact of natural disasters comes from the 2022 Tonga volcano. The eruption triggered tsunamis and underwater avalanches that inflicted multiple points of damage on two cables: the international cable connecting Tonga to the world via Fiji and a domestic cable. The volcanic plume also prohibited satellite communications. Tonga was completely cut off from the internet and global communications, complicating aid and rescue missions until satellite activity was restored when the skies cleared. It took a month to repair the Fiji cable and would take 18 months for both cables to be fully repaired and for connectivity to be completely restored. The delay in domestic cable repairs was driven by an absence of the quantity and type of cable needed; because proper cables were not available locally, it took five months to confirm the correct order from Alcatel Submarine Networks (ASN). After the order was placed, it took ASN a further seven months to manufacture the cable and another four months for the order to be shipped from ASN in France to Tonga. The actual repair of the cable only took eight days.[110]

### CLIMATE CHANGE

There have been few studies on the impacts of climate change on subsea cables and landing stations, but the studies and analyses so far suggest climate change will have wide-ranging impacts on the integrity of cables and threaten cable landing stations onshore. A February 2023 paper in *Earth-Science Reviews* assesses the widespread impacts of climate change, including sea level rise and storm flooding that could impact landing stations, rising ocean temperatures that could shift fishing areas and therefore force vessels to relocate to areas where they are unfamiliar with the presence of cables, or more intense storms that could cause underwater landslides or rough seas that could damage cables.[111]

The ICPC also released an issue paper on the impacts of climate change on subsea cables and noted a few examples that caused damage. The floods caused by Hurricane Maria in 2017 forced officials to cut power to a landing station in Puerto Rico to prevent damage to the telecommunications equipment at the site. Intense storms in the Caribbean in 2015 damaged several cables and landing stations. In 2020, river flooding caused cable faults in systems connecting western and southern Africa, negatively impacting connectivity.[112]

### INTENTIONAL CUTS OR DAMAGE TO LANDING STATIONS

Though relatively rare, intentional damage to undersea cable systems may include physical damage to cables, such as cutting cables at sea or on land, or attacking cable landing stations. Recent suspected attacks on undersea communications and power cable infrastructure, including in

the Taiwan Strait and Baltic Sea, have raised concerns among governments as to how to protect the infrastructure amid the perceived increased usage of gray zone tactics, which involve acts of sabotage or subversion that fall below the threshold of war.

European authorities, particularly in Finland and Estonia, have raised concerns about Russia sabotaging critical cable infrastructure in Europe.[113] In 2024 and early 2025, there were at least three incidents in the Baltic Sea that damaged seven different telecommunications links that connect Baltic states like Estonia, Finland, Germany, Latvia, and Sweden.[114] In November 2024, authorities suspected a Chinese-flagged ship carrying fertilizer from Russia of accidentally or intentionally cutting two cables connecting Lithuania to Sweden and Finland to Germany. In December 2024, Finland detained a Russian tanker flagged in the Cook Islands on suspicion of cutting a power cable between Finland and Estonia. Finnish authorities believe these ships to be part of Russia's "shadow fleet" of vessels used to avoid sanctions on its oil exports. In late January, Norway briefly detained a Norwegian-owned, Russian-crewed cargo ship on route to Russia on suspicion of severing a cable between Sweden and Latvia.[115] Impacted countries and the European Union believe these incidents were intentional, with the latter calling them "a series of suspected attacks on critical infrastructure."[116] In January 2025, NATO deployed a coordinated group of warships in an operation named Baltic Sentry to specifically deter such attacks. NATO also conducts an annual multinational maritime exercise, Freezing Winds.[117]

Taiwan reportedly has also been the victim of intentional cable cuts by China. In 2023, Taiwan officials accused China of cutting cables connecting Taiwan's main island to its outlying islands of Matsu; the damage caused an internet blackout. Beijing denied any intentional cuts and said they were accidental.[118] In February 2025, Taiwan's coast guard detained a cargo ship and its Chinese crew to investigate if the ship deliberately cut an undersea internet cable. The Togo-flagged ship, called the *Hong Tai*, had been spotted near the cable for several days and did not respond to hails from Taiwan's coast guard. Shortly after the ship dropped anchor, Taiwan's telecom company Chunghwa Telecom was alerted of damage to the cable.[119] In April 2025, Taiwanese prosecutors formally charged the *Hong Tai's* captain with deliberately cutting the cable, marking the first time Taiwan has taken such action.[120] Given tensions between Taiwan and China and the ambiguity of gray zone tactics, it still remains unclear if China deliberately cut the cables.

### TAPPING OR ESPIONAGE

In CSIS's research and interviews with experts in both the public and private sectors, the general consensus was that espionage and tapping are extremely unlikely for several reasons. Cable locations at the bottom of the sea are difficult to tamper with, particularly if there is no reason to repair a cable. Some noted that one day it may become more technically feasible to tap cables and decrypt the enormous amounts of information, but this is currently considered technologically infeasible or highly difficult. These experts conceded, and studies support, that landing stations may be a bigger and easier target. Operators are likely to receive immediate notification of any damage to a cable, but the landing stations themselves are more accessible and would be a higher-value target given the number of cables that end at these stations and connect to terrestrial infrastructure.[121]

The United States has urged cable and telecommunications companies to avoid using Chinese companies to repair or lay new cables due to the possibility of Chinese entities intercepting and

monitoring sensitive communications. In September 2024, the United States, Australia, France, Japan, Singapore, South Korea, and the United Kingdom issued a joint statement during the UN General Assembly calling for undersea cables to be kept secure from risks such as surveillance, sabotage, and data theft.[122]

Though technology to capture, decrypt, and analyze the terabits of data that shoot through cables is not widespread, technology does exist that could be used to tackle this data collection: submarine line terminal equipment (SLTE). SLTEs connect the data from subsea cables to terrestrial, or land-based, networks, helping to translate the data into readable information.[123] Like cable manufacturers, there are few SLTE producers, including ASN, Ciena (United States), HMN Tech, NEC, and Finland's Nokia.[124] Experts interviewed for this project highlighted the vulnerabilities of SLTEs, particularly where HMN Tech or high-risk vendors could be involved. They posited a scenario in which data traversing the ocean that reaches an SLTE in the landing station could be optically split, with one set of data going to the intended customer or target and the other to a malicious actor. The interviewees noted that this is technologically possible, saying that a country like China could use their devices, whether in a data center or subsea cable buildout, and be able to clandestinely siphon off information. However, private sector actors have pushed back on this idea, noting the amount of encrypted data and the computationally infeasibility of grabbing the data, decrypting it, and using for any sort of useful espionage purposes.

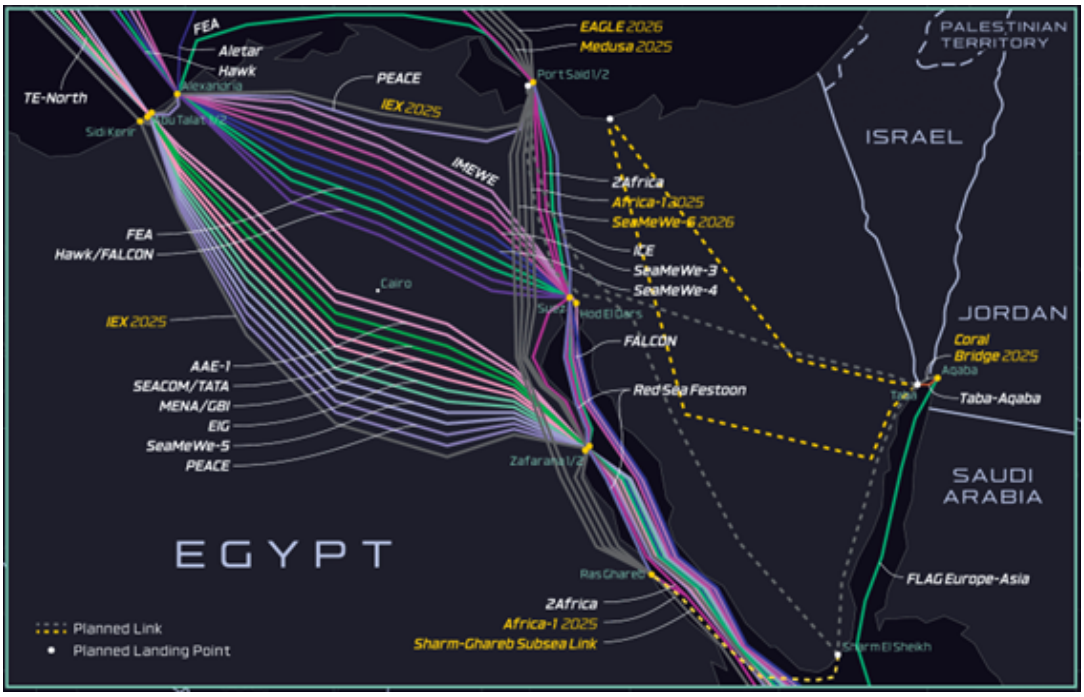
## Egypt Country Case Study

Egypt occupies a crucial role in subsea cable infrastructure as a key connection point between continents. Seventeen percent of the world's internet activity pass through cables in its territorial waters.[125] A British telegraph company laid the first cables that connected the United Kingdom to Egypt and to India in 1870.[126] Today, 90 percent of communications traffic for Europe to Asia passes through Egypt and its cables in the Red Sea.[127] The country is also home to data centers and major ICT players. These factors underly the government's Digital Egypt Strategy, which promotes digital infrastructure, labor upskilling, and investment incentives to attract companies and new projects.[128]

The majority of Egyptian cables pass through the Suez Canel or the Bab al Mandab Strait off the coast of Yemen. This concentration of cables creates chokepoints where accidents could sever multiple cables at once. Additionally, the cables near Yemen and Djibouti are in close proximity to terrorist and piracy activities, leading to inadvertent damage and making it difficult for ships to safely repair cut cables.[129] For example, in February 2024, a U.K.-owned and Belize-flagged ship, *Rubymar*, was struck by Houthi antiship missiles. The ship dropped its anchor but drifted for several days, ultimately sinking weeks after the attack.[130] The anchor dragged along the sea floor, damaging communications cables in its path and disrupting internet communications for millions in the region and beyond.[131] Though the Houthis did not directly target subsea cables, these types of attacks could inadvertently cause damage to cables should ships drop anchor or sink.

These threats, as well as Egypt's key location for cable connectivity, have raised the specter of regional competition from countries such as Israel, Morocco, Oman, and Saudi Arabia.[132] This could have negative economic impacts for Egypt if hyperscalers and other cable operators choose a competing market.

Figure 9: Subsea Cable Network in Egypt




Source: "Submarine Cable Map 2025," TeleGeography, https://submarine-cable-map-2025.telegeography.com/.

CSIS proposed the following recommendations in its Egypt country case study:

- **Egypt should streamline its regulatory system** to provide more transparency and ease of doing business. Like other countries featured in the case studies, Egypt's permitting and regulatory process is fragmented and touches several different agencies and ministries. Selecting a key agency, such as the National Telecommunications Regulatory Authority, could provide greater clarity and speed in approvals.
- **Egypt will also have to consider greater security measures** to build confidence in its ability to provide for the safety of cables and mitigate potential damage. The country can consider boosting its naval capabilities to patrol the Red Sea and Bab al Mandab Strait and enhance its monitoring efforts through technologies such as acoustic monitoring networks or underwater unmanned submersibles to enhance detection capabilities. Additionally, Egypt could enhance real-time monitoring of cable infrastructure to help track and even prevent unintentional or intentional damage.

- **Egypt can engage with multilateral financing institutions**, such as the African Development Bank or World Bank, to finance new routes and attract new partners to support future projects. Given Egypt's role as a regional hub, bringing in development finance institutions could help lower costs, connect to other locations that typically would not be as commercially attractive for corporate players but would benefit from greater connectivity, and support broader efforts to bring more redundancy to the infrastructure to support resiliency against accidental damage. Having more cables benefits Egypt as well, particularly as it looks to institute its Digital Egypt Strategy. Greater use of AI both in Egypt and countries that connect to its cables will require more bandwidth and stable connectivity. New financing can help meet these growing demands.

For the full Egypt country case study, see "The Strategic Future of Cables: Egypt Case Study," https://www.csis.org/analysis/strategic-future-subsea-cables-egypt-case-study.

## Non-Physical Threats and Challenges

Subsea cable repair, resiliency, and redundancy are also at risk from a number of non-physical threats, including geopolitics, market concentration, cabotage laws, lack of government coordination, and complex permitting processes.

### BUREAUCRATIC OVERLOAD

In interviews with private sector stakeholders, the number one concern was permitting procedures, which added months if not years to project timelines and increased costs for project implementation.

For the United States, cables cut across environmental stewardship, foreign affairs, homeland security, commerce, military, and other issues, and may fall within the responsibilities and interests of multiple federal agencies which are in turn authorized, appropriated, and overseen by various congressional committees. There are also state and local laws that govern cable landing sites and territorial waters. Government authorities typically rely on the private sector to sort out the requirements and necessary engagements within jurisdictions, meaning that adhering to proper permitting and regulatory requirements, including maritime sanctuary and environmental issues, can result in lengthy and complex processes.

In a report by the Congressional Research Service, researchers assessed that this fragmented regulatory system posed risks to cable infrastructure, including exacerbating gaps in actual or perceived legal authorities and gaps in how existing legal authority is exercised. The laws and regulations also reflect a lack of familiarity with subsea cable technologies and installation and repair operations, suggesting that laws often do not take into account what is needed by the private sector to lay, maintain, and repair cables, nor do they show recognition that a lack of streamlined systems prevents quick repairs and better resiliency in the network.[133]

## GEOPOLITICS

Geopolitical tensions add another layer of complexity to the security, repair, and laying of subsea cables, particularly in regions such as the South China Sea and Taiwan Strait. The competition for control over maritime territories and underwater resources raises concerns that cables could become collateral damage in larger geopolitical conflicts, especially with plans to exploit the seabed for critical minerals. For example, a cable under construction called the Southeast Asia-Japan Cable 2 (SJC2), connecting 11 cable landing stations in Cambodia, mainland China, Hong Kong, Japan, Singapore, South Korea, Taiwan, Thailand, and Vietnam, was reportedly delayed because of China and concerns related to waters around Hong Kong. Geopolitical tensions have resulted in the rerouting of new subsea cables, including Apricot, a 12,000 km subsea cable connecting Guam, Indonesia, Japan, the Philippines, Singapore, and Taiwan, which originally was set to pass through the South China Sea.[134] These cables were rerouted to avoid Chinese waters.[135]

For private sector actors, the main obstacles related to cables located in the South China Sea are permitting and regulatory issues, as China is imposing stricter requirements and taking longer to approve or deny permits for work located in what it sees as Chinese territorial waters. China has also requested permits for cable laying in claimed territorial waters beyond 12 miles, in apparent contravention of international maritime law.[136] In CSIS's interviews with stakeholders and government officials, interviewees noted that China has not issued any permits for laying or repairing cables for non-Chinese-owned cables for at least two years.

There are also growing concerns around cooperation between Russia and China and their efforts to potentially sabotage subsea cables. For example, the Chinese vessel *Yipeng-3* transited from a port call in Russia through waters where the BCS East-West Interlink cable connecting Lithuania and Sweden was cut by the ship's anchor. The dropped anchor continued to drag a further 178 kilometers (110 miles) across the ocean floor and cut the C-Lion 1 cable connecting Finland and Germany. Authorities from Finland and Germany were convinced these actions were deliberate. Given these types of incidents, Chinese and Russian ships are often viewed with suspicion, as they were when China's *Shunxing-39* and Russia's *Vasili Shukshin* were spotted near Taiwan in January 2025. Taiwan authorities were concerned of potential damage but also of potential collusion between the two countries to conduct such activities.[137]

## POTENTIAL COMPETITION IN SUBSEA CABLE DEPLOYMENT

China's HMN Tech is one of the four major cable manufacturers, and China has significant strength in shipbuilding, which gives the country a potential edge in cable laying and repair.[138] HMN Tech makes up a small percentage of cable manufacturing, only joining the industry in 2008, and the United States has undertaken efforts to ensure it remains small, including through sanctioning the company and pressuring companies and countries to exclude China from digital infrastructure projects. HMN Tech also faces an uphill battle in competing with U.S. hyperscalers' overwhelming presence and ability to scale rapidly.[139]

Countries like the United States, Japan, and other U.S. regional allies recognize the issue around the prevalence of Chinese hardware in critical infrastructure and have sought to block Chinese companies from subsea cable projects, including involving U.S. investment and firms.[140] China's HMN Tech has rapidly expanded its share of the cable manufacturing market and has provided an

estimated 18 percent of the subsea cables (in terms of the total length of cable) laid worldwide since 2019, though the real number may be higher. The company website states that it is involved in 100 submarine cable projects in 78 countries and regions, including for cable repair.[141] As with other digital and transportation infrastructure China has offered, it typically undercuts competitive bids with the help of Chinese government subsidies or assistance.

During the 2020–21 cable tender process for SeaMeWe-6, a cable project linking Singapore to France, the U.S. government coordinated pressure and incentives to block a winning bid from China's HMN Tech in favor of U.S.-based SubCom. The interagency review committee Team Telecom warned investors that HMN Tech was likely to be placed on the Commerce Department's Entity List, and the Commerce Department reportedly pushed for SubCom to be the selected vendor. As a carrot, the U.S. Trade and Development Agency offered $3.8 million in training grants to five telecommunications companies along the cable route.[142] The development consortium eventually flipped to SubCom, despite HMN Tech's bid being approximately one-third cheaper.[143] Additionally, China Mobile and China Telecom, two Chinese state-owned enterprises who represented 20 percent of invested capital, withdrew from the consortium. HMN Tech and three other Chinese submarine cable companies were formally added to the Entity List in December 2021.[144]

Additionally, in June 2020, Team Telecom recommended the FCC partially block the Pacific Light Cable Network project that would have connected Los Angeles to Hong Kong over national security concerns. The U.S. government's direct intervention to keep HMN Tech from winning business or to prohibit cables that would directly link U.S. and Chinese territories has proven effective in curbing China's market position.

### CABOTAGE LAWS

Private sector stakeholders point to cabotage laws, many from more than a century ago, in lengthening the timeline of laying cables and preventing greater redundancy in the network. For the United States, the Merchant Marine Act of 1920, also known as the Jones Act, restricts domestic shipping services to vessels that are U.S.-built, U.S.-owned, U.S.-flagged, and U.S.-staffed. All ships must also be at least 75 percent U.S.-owned, at least 75 percent U.S.-crewed, and assembled entirely in the United States, with all "major components of the hull and superstructure" fabricated domestically.[145] Unfortunately for the United States, most ships do not meet those requirements, and most of the appropriately trained crew are international. This delays or prevents laying or repairing cables that are in U.S. waters. There may be a workaround based on a December 2024 compliance update from U.S. Customs and Border Patrol if the ship is providing a service, but repair vessels still must determine whether they fall within the Jones Act exception.[146]

Similarly, for Southeast Asia, Indonesia's cabotage laws are a major challenge. Law No. 17/2008 ("Cabotage Laws") came into force in May 2011 and generally limits domestic sea transportation to Indonesian-flagged vessels. These vessels can be owned by an Indonesian individual, a wholly Indonesian-owned company, or an Indonesian joint venture foreign investment company where the Indonesian partner must hold at least 51 percent of the company.[147] These rules were marginally relaxed in 2024, allowing some types of vessels to be allowed in Indonesian waters if there were no Indonesian options. Howevere, the law may still require cable repair operations to find an

Indonesian-flagged ship or eventually flag their ship under the Indonesian banner. This becomes problematic for cables coming out of or landing in Singapore, as it has limited territorial waters and many of those cables traverse Indonesian water. Singapore is a regional hub, and hyperscalers and cable companies often cite cabotage as a significant challenge for laying and repairing cables.

### NON-BINDING LEGAL FRAMEWORKS

As discussed in earlier sections, the legal basis for submarine cable regulation stems from international law and conventions dating back to 1884, and the law has not evolved with the times. The two main international laws that govern subsea cables are the 1884 Convention for the Protection of Submarine Telegraph Cables and UNCLOS. International organizations, like the ICPC, offer frameworks and guidelines, but these are recommendations only.

Three dozen countries signed the 1884 Convention for the Protection of Submarine Telegraph Cables, including the United States and Russia, but not China. The treaty makes it illegal to damage a submarine cable in peacetime. It also dictates that the flag state or nationality of the ship that caused the damage has jurisdiction to investigate and prosecute cable incidents. There are few rules regarding who can board vessels or investigate incidents outside of this provision, demonstrating that the internationalization of the infrastructure and overlapping territorial waters do now require updated provisions to resolve cable cutting incidents.[148] These rules should be updated, and as with other frameworks, they need to be enforced.

How and to what extent one holds the actors responsible for cable damage depends on where the cable lies. If a cable is damaged in territorial waters, countries can exercise Article 21 of UNCLOS. Countries can also exercise rights to repair and maintain cables under Article 58 of the same framework, as well as within each country's own laws.[149] Some countries have their own laws related to responsibility and accountability for damaged cables, such as Singapore and Australia, including levying fines and prison sentences for those responsible for damaging cables.[150] There are also avenues to target the country under which a ship is flagged; countries such as the Bahamas, the Cook Islands, Liberia, Malta, the Marshall Islands, and Panama allow ships to use their flags to sail in international waters. Shipowners often fly flags from another country to take advantage of favorable laws—or to camouflage their identities. These countries are unlikely to have the capacity to conduct investigations should ships with their flags cause damage, which should put more pressure on these governments to either conduct enhanced due diligence of parties using their flag or to better track or deny flags to suspicious ships.[151]

The ICPC assesses only some countries enforce their existing obligations under UNCLOS. The implementation of the frameworks and regulations is not consistent across the globe, though several countries do enforce its provisions. UNCLOS says that every state "should" adopt laws and regulations to make cable cutting a punishable offense for any of its nationals or flagged ships, but many states do not have such laws. Most Southeast Asian countries, excluding Singapore, Thailand, and Vietnam, have not passed or enacted national legislation criminalizing damage to subsea cables in their territorial waters.[152] This could be due to lack of capacity, lack of interest, or both.

Under UNCLOS, states have jurisdiction over cable incidents occurring in their territorial waters (within 12 nautical miles of their coasts). Beyond that, law enforcement jurisdiction is unclear. States

have exclusive rights to natural resources in their EEZs (within 200 nautical miles of their coasts) and may take measures to protect those rights—but it is unclear how this applies to submarine cables. It is legally unclear whether coastal states or the private firms who own the cables have control over cables in an EEZ—something insurance companies may need to clarify. Beyond 200 nautical miles, only flag states and states of the nationality of a perpetrator have clear jurisdiction over cable cutting. Any jurisdiction by victim states is unclear.

### LACK OF REPAIR CAPACITY

There is a significant shortfall in the number of purpose-built vessels worldwide for laying and repairing subsea cables. Just 22 of the 77 cable ships worldwide are designed to attend to damage in the estimated 750,000–900,000 miles of subsea cables.[153] As the length of total subsea cables in service is anticipated to increase by a projected 48 percent by 2040, there will likely be a proportional increase in cable faults due to the threats listed above, raising concerns about the global ability to keep up with cable repair.[154] Concurrent with these net increases in cables, two-thirds of cable repair ships will reach the end of their service life by 2040.[155]

Several subsea cable manufacturers have their own repair vessels, but these small fleets could be quickly overrun by multiple cuts in the event of a natural disaster or conflict, delaying timely repair. This has become a critical concern for Japan. For example, the Japanese company NEC does not own cable vessels and has relied on ships from other companies in Japan as well as from China, South Korea, and other countries to lay and repair cables. Because NEC must contract with companies in and outside of Japan, they do not necessarily have priority in the queue.[156] This can result in repair delays and add to the length of time needed to lay new cables. As a result, Japan may experience heightened pressure to rely on a high-risk vendor for repairs, such as China's HMN Tech.

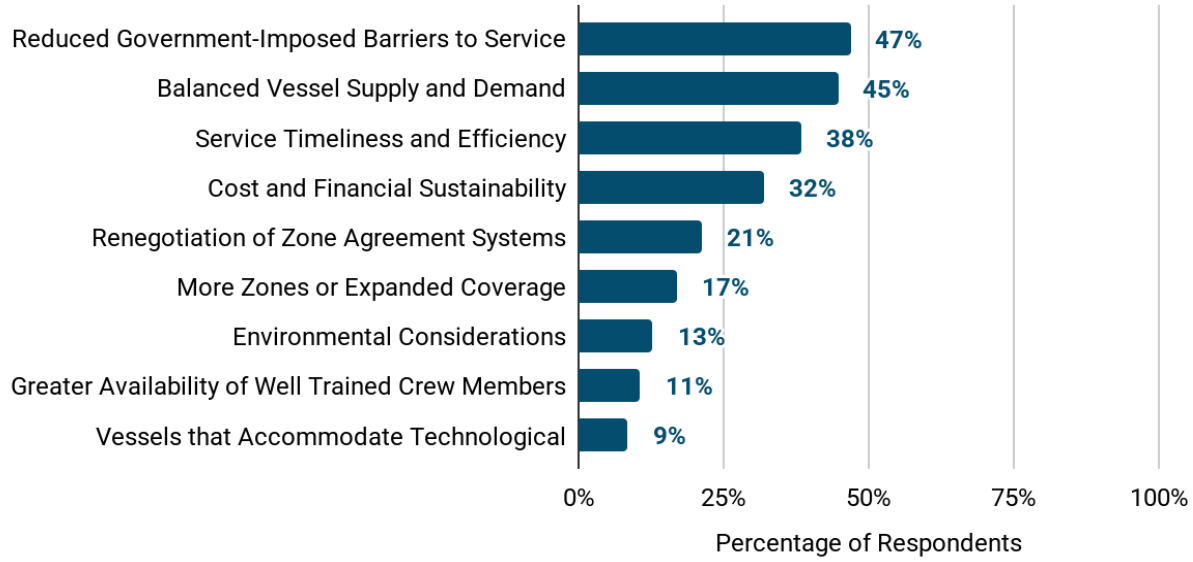
It is unclear how many cable ships China has, but HMN Tech offers end-to-end services to its customers and investors in the subsea cable project life cycle.[157] China is the world's largest shipbuilder and is likely expanding its capacity in the sector, meaning that companies involved in subsea cable projects around the world may come to purchase or rely on Chinese ships.[158] For example, in late March 2025, reports emerged that the China Ship Scientific Research Centre (CSSRC) and its affiliated State Key Laboratory of Deep-sea Manned Vehicles was developing a ship with cable-cutting equipment that can operate at depths of up to 4,000 meters.[159] Subsea cable ships are typically outfitted with equipment to repair damaged or cut cables, but Chinese scientists alleged this was for "marine resource development." It is unclear how cable cutters promote marine resource development, but this also suggests that research ships could be used for the dual purposes of cutting and possibly repairing.

U.S.-owned SubCom has cable repair ships, but the U.S. government lacks surge capacity if several cables are cut in a coordinated manner, which could happen during a contingency in the South China Sea, Baltic Sea, or another chokepoint. The U.S. government has one dedicated vessel, the 40-year-old USNS *Zeus*, and through the newly implemented Cable Security Fleet has chartered two U.S.-flagged commercial ships, the *CS Dependable and CS Decisive*.[160]

Repairs can happen relatively quickly, but only if the proper ships and crew are available nearby. Once the damage to a cable has been located, repairs can take about two to three weeks on average.

However, that can extend to months depending on the extent of the damage, the availability of cable repair ships, the ability to get permits (for cables territorial waters of a country or other jurisdiction), weather, and safety. For example, repairs can be significantly delayed if there is an active conflict or if there are radiation concerns from a compromised nuclear plant, as was the case in the aftermath of the Japanese Tohoku earthquake.

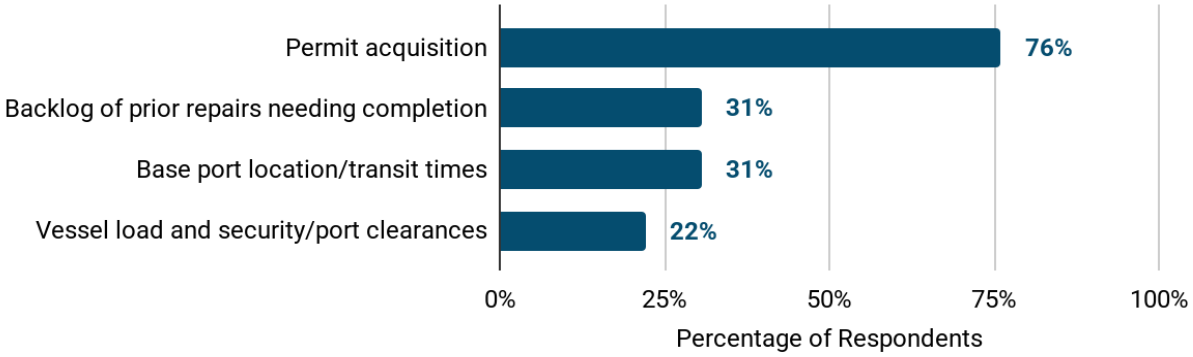
### Figure 10: What Are Your Top Three Wishes for the Future of Marine Maintenance by 2030?




Note: Data from survey of industry by TeleGeography.

Source: Constable, Burdette, and Mauldin, *The Future of Submarine Cable Maintenance*, 87.

### Figure 11: What Are the Primary Challenges to Optimize Repair Timeframes in the Regions Where You Operate?



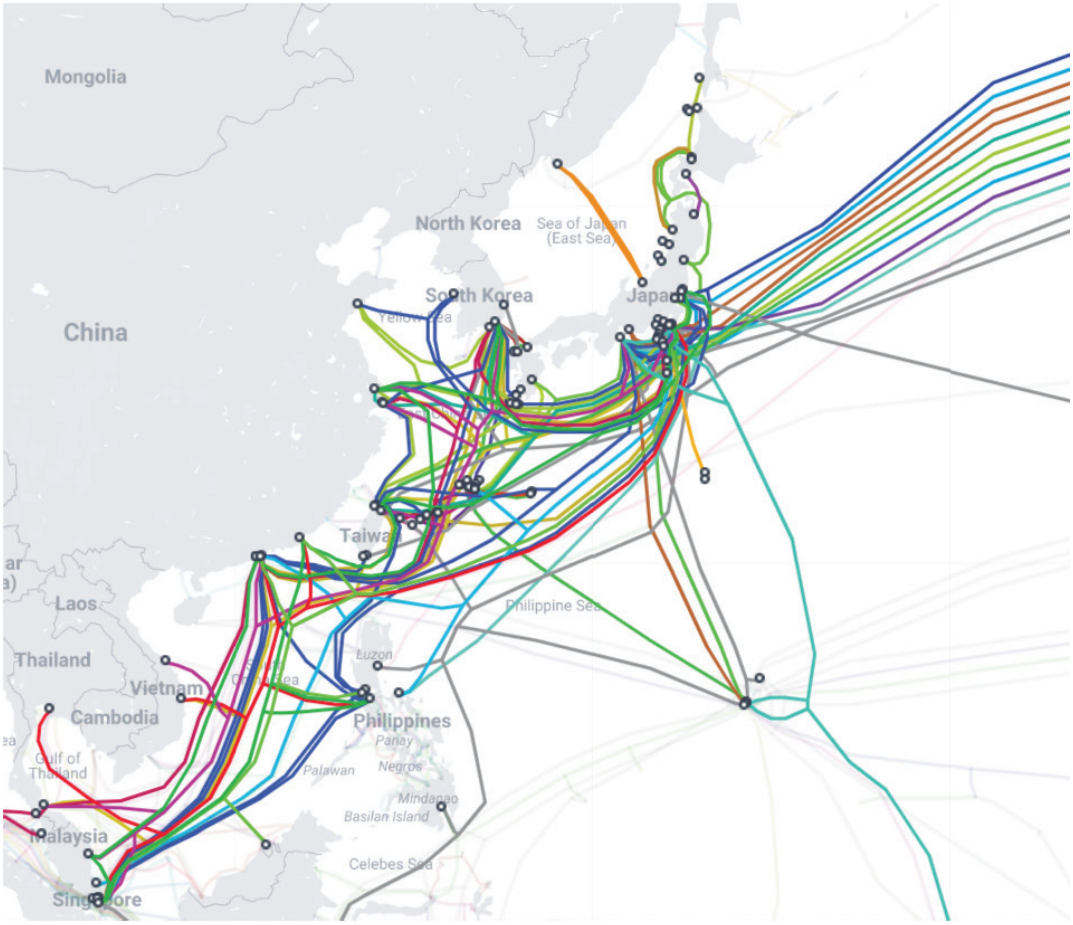

Note: Data from survey of industry by TeleGeography.

Source: Constable, Burdette, and Mauldin, *The Future of Submarine Cable Maintenance*, 24.

## Japan Country Case Study

As seen in the other three case studies covering Ireland, Singapore, and Egypt, Japan plays an important part in the subsea cable industry and global connectivity. The country is typically the first landing point for trans-Pacific cables coming from the United States, helping to connect the United States with the rest of Asia. Japan's NEC is also one of the top cable manufacturing companies, and the country is home to Japanese companies with cable laying and repair capabilities, Nippon Telegraph and Telephone (NTT) and the KDDI Corporation.

Figure 12: Map of Subsea Cables Connecting to Japan




Souce: "Submarine Cable Map," TeleGeography, https://www.submarinecablemap.com/country/japan.

Japan's primary concerns regarding the integrity of its cables relate to natural disasters, accidents, and, increasingly, geopolitical tensions. Japan is on the so-called "Ring of Fire," a geologically active part of the world located around the Pacific Ocean, known for earthquakes, volcanos, and seismic-related disasters. Japan must also be mindful of its fishing industry, which is dependent on seasonal changes that drive schools of fish into

commercial fishing areas at certain times. Cable laying or repair ships could disrupt this fishing, so cable companies must negotiate to find the right time to lay any new cables.

Japan is also situated near China and Russia, each of whom have been suspected in deliberate cable cuts. Though there is no evidence of cuts or interference happening in Japanese waters, the Japanese government remains concerned that significant increases in geopolitical tensions between the United States and China and Russia leave the country vulnerable. China is also a competitor, both in manufacturing cables and in providing the ships that can lay and repair them.

The Japanese government recognizes the criticality of cables and has designated subsea cables as critical to its national security. The Ministry of Economy, Trade, and Industry is set to expand its cable laying capabilities through the country's Economic Security and Protection Act.[161] Its Ministry of Internal Affairs and Communications, the primary ministry for subsea cable policy, is also officially working with the European Union on the security and resiliency of subsea cables.[162]

CSIS provided the following recommendations as part of the Japan case study:

- **Japan should leverage its shipbuilding capabilities and work with partners and allies to increase the number of laying and repair ships.** Japan is the third-largest shipbuilder in the world, with 7 percent of the market, and its neighbor South Korea has 17 percent. China, by contrast, holds nearly three-fourths of the market.[163] Japan should work with South Korea and the United States, which is actively pursuing rebuilding its own shipbuilding industry, to soften China's lead in dominating the industry.
- **Japan should identify new routes for cables and landing stations.** There are two schools of thought around identifying new routes for cables: (1) creating a designated cable corridor where multiple cables would be situated, lessening the impact on critical fishing areas and commercial lanes, or (2) selecting multiple new geographic routes to add more cables. The first option would likely allow for faster deployment of cables but does leave those cables at risk for being cut all at once. The second option requires the same bureaucratic and fishing union negotiations, but the variety in locations protects against multiple cable cuts and easier rerouting of traffic should a cut occur.
- **Japan should leverage its partnerships and alliances to increase the number of cables built**, cooperate on security measures, and ensure greater resiliency in the network. Washington and Tokyo have a long-standing relationship and generally see eye-to-eye on the importance of having a digital network that is safe, secure, and built and operated by trusted partners. Neighboring South Korea, with which Japan often has a strained relationship, would also be a good partner given its role in the shipbuilding industry and it alertness to threats from China.

To read the full Japan country case study, see "The Strategic Future of Subsea Cables: Japan Case Study," https://www.csis.org/analysis/strategic-future-subsea-cables-japan-case-study.

# Part V

## *Recommendations for Enhancing Redundancy, Resiliency, and Repair of Subsea Cables*

This section provides recommendations for stakeholders in the subsea cable space, including for all stakeholders in the sector, the U.S. government and its partners and allies, country governments around the world, multilateral and development financing agencies, and the private sector. Subsea cable infrastructure affects nearly all aspects of society, including communications, economic transactions, and national security. More coordination among stakeholders and enhanced understanding of the sector as a whole will help enhance the overall resiliency of the network.

## Crosscutting Recommendations for Public and Private Sector Stakeholders

### REDUNDANCY

1. **Make subsea cable infrastructure a national security priority**. Disruptions to subsea cables have great potential to yield detrimental effects on the global economy by disrupting access to the internet, e-commerce, financial transactions, communications, and other activity. The interconnectedness of subsea systems also means that disruptions in one region can quickly affect others, as demonstrated by incidents in Egypt in early 2024 and as recently as September 2025 as well as in the aftermath of the 2011 earthquake in Japan. A natural disaster akin to the 2011 Tohoku earthquake or a coordinated attack on multiple subsea cables could have significant consequences, requiring international cooperation to ensure the security and resilience of subsea cable systems and enable a quick rebuild. As a worst case, intentional damage to subsea cables, perceived or real, could be seen as an act of

aggression and escalate tensions between nations. Countries need to be prepared to respond to such attacks and deter potential aggressors that see subsea cables as a legitimate target during a conflict or as part of gray zone activity, particularly since such action could sever vital financial, military, and communications links.

Given the strategic importance of subsea cables to so many critical areas, this infrastructure and its resiliency should be elevated to a national security priority. Policy action can take many shapes, whether subsea cables are highlighted in national security strategies, included in major summits such as NATO's annual summits or ASEAN's East Asia Summit, reflected in language in joint statements among global leaders or in legislative priorities, and allocated budget and bureaucratic resources to support their repair, resiliency, and redundancy.

2. **Pursue permitting reform.** Countries should streamline subsea cable permitting processes, including elevating a main point of contact within government agencies when there are overlapping jurisdictions, to ensure a timely process to lay or repair cables. The process should include flexibility, particularly where strict cabotage laws are present, in the case of emergencies where multiple cables are damaged or fail.

### REPAIR

1. **Update global maritime laws or reform domestic laws.** The United Nations should update relevant laws and frameworks that govern subsea cables. Equally important is the implementation and enforcement of these laws in national jurisdictions. The laws in place today are outdated and unevenly enforced.

   Such a move starts with formal recognition that subsea cables are critical infrastructure and are a national security priority. Updates to UNCLOS, the 1884 Convention for the Protection of Submarine Telegraph Cables, or other frameworks should put the onus of damage to subsea cables on perpetrators. Additionally, more signatories should be sought for the 1884 convention to reflect the increase in the number of global stakeholders and coastal territories involved in subsea infrastructure. UNCLOS does not hold nonstate actors responsible for damage, even in the case of an act of terror. Non-signatories to UNCLOS are also not bound by it, but instead by customary law. Because it is unlikely that UNCLOS can be formally amended today given bureaucratic processes and geopolitics, it behooves countries to adopt UNCLOS into domestic law. These updates can reflect best practices and build on the success of countries such as Singapore, which has seen a dramatic reduction in accidental cable cuts.[164] Australia demonstrates another option through its use of Schedule 3A of the Telecommunications Act 1997 to provide protection zones for cables of national significance, Sydney and Perth being two specific locations. This includes criminal penalties of up to a decade in jail for damaging a cable in one of these zones.[165] High fines could deter cable cuts, accidental or otherwise.

   Frameworks and international laws should reflect the importance of subsea cables to economic and national security, provide better guidelines for investigating damage to cables in international waters, and include the imposition of fines and prison time on the actor responsible for the damage and the country under which the perpetrating ship is flagged.

## RESILIENCY

1. **Provide capacity building on legal frameworks and enforcement.** The ITU, ICPC, and governments with known best practices should work with relevant government ministries, telecommunications operators, and other private sector stakeholders in coastal states where cables land or cross territorial waters. They should help these states update domestic law and enforcement to mitigate and prevent accidental or intentional damage. The ITU's International Advisory Body for Submarine Cable Resilience could be the main arbiter on organizing dialogues among stakeholders and providing resources for capacity building. This effort should include providing technical assistance and resources to identify gaps in laws and regulations, update legal frameworks, and streamline permitting.
2. **Plan ahead for the impacts of climate change on cables and landing stations.** Cable owners and manufacturers should use climate modeling, storm data, and geographical information system (GIS) analysis to identify the best locations to lay and land cables amid shifting climatological risks and patterns. This will have to be done in coordination with permitting governments to coordinate new locations to accommodate the realities of climate change, rising sea levels, stronger storms, and more dangerous storm surges. Manufacturers should also consider increasing the armoring of at-risk portions of cables in shallow water or in areas where storm activity and sediment shifts are more likely to occur.
3. **Enhance public-private sector partnership and communication.** The public and private sector have different concerns related to subsea cables, and only through consistent engagement can they bridge these differences. Governments tend to focus on threats, no matter how improbable, to the cable network, while the private sector focuses on the challenges of permitting, regulation, and profitability. Each side must engage with one another to enhance mutual understanding and improve communication, which will lead to a resilient infrastructure and one that makes more commercial sense for companies. This cooperation can occur on a number of issues, including financing, cybersecurity, intelligence sharing on threats, assistance with repair or patrols, permitting, the use of diplomatic pressure where needed, and support for international laws and regulations that help mitigate risks of accidental or intentional damage.

   The U.S. government and like-minded countries should also work with the private sector on financing cables to small islands, including for the Pacific Islands, and developing states to support cable connectivity more broadly. These areas often lack immediate commercial viability for investors and consortia, creating a deep digital divide and potential strategic and national security risks if high-risk vendors step in the fill the vacuum.

4. **Establish a fund for cable laying and repair in emerging economies.** Related to the prior recommendation, global governments, multilateral financing agencies, and international organizations should establish a joint fund or blended finance facility to support new cable projects in emerging economies or to repair catastrophic damage, such as was seen in the aftermath of the Tohoku earthquake and Tonga volcanic eruption or as might occur in areas of active conflict. A joint fund could help ease commercial viability issues and

encourage private sector manufacturers and hyperscalers to connect emerging economies that may not be able to finance such projects. In instances of catastrophic damage to subsea cable system, such funding could help speed repairs or offset the potential lack of insurance when deploying cable repair ships to conflict zones or areas with significant security issues, such as in parts of the Red Sea, where Houthi rebels operate, or in the Gulf of Aden, where piracy has been reported.

5. **Increase security around landing sites.** In CSIS's discussions with academics, government officials, and cable owners and operators, there were shared concerns around the consistency of global security measures around cable landing sites. Cable landing sites are at risk for physical attacks and storm surges or damage. Global standards should be put in place that govern all cable landing sites, including steps to increase the physical security of sites, such as perimeter fencing, access control systems, and security cameras to monitor the area. For locations at risk from natural disasters, cable landing site buildings should be reinforced, have backup power systems, and have measures in place to prevent or mitigate flooding.

## Recommendations for the U.S. Government

### REDUNDANCY

1. **Establish a single federal point of contact.** The United States should designate a lead agency to coordinate among federal, state, and local agencies to ease the process of permitting for cables laying and repair as well as to facilitate manufacturers and hyperscalers contributions to national security measures to protect cables. The legal and regulatory hurdles facing the sector have consistently proven problematic for undertaking timely and efficient cable laying and repair projects. A lead agency can coordinate policy and national security concerns, support the private sector, and undertake efforts to streamline the permitting and regulatory process. This could be done by appointing the lead for Team Telecom to one or two agencies: one to focus on national security and foreign policy concerns, led by DHS' CISA, and the other on permitting and regulatory issues, led by the FCC. CISA should coordinate with the Departments of State, Commerce, and Defense as well as intelligence and financing agencies to monitor threats and identify opportunities for strategic work in the industry. The FCC should take the lead on coordinating with federal, state, local, and tribal authorities that engage on the permitting process to ensure it is streamlined, efficient, and cost-effective.

### REPAIR

1. **Upgrade surge capacity for cable repair.** When multiple cables are damaged, the speed at which cables can be repaired is critical. The U.S. government should find ways to support the cable repair industry, either by retrofitting Navy ships with cable repair equipment or working with allies and partners to support the building of a trusted fleet of ships to help with the repair and laying of cables. However, such vessels also require skilled technicians and crew to operate. Skills and vocational training will need to be provided to ensure

readiness, and it may make sense to allow for U.S. naval officers with cable laying and repair experience to participate in surge activities when needed.

2. **Update laws against breakages.** In CSIS's interviews, interlocutors expressed that the fines for breaking U.S. laws around anchorage and accidental damage to cables were minimal and provided no deterrent effect. Singapore and Australia offer examples of using significant fines or jail time to the offending ship and country under which the ship is flagged to mitigate accidental cuts and damage from commercial and fishing vessels. The United States should consider updating its law to enforce stricter penalties against the ship's crew, the cable company, and the country under which the ship is flagged to ensure accountability and prevention of accidents.
3. **Update maritime laws.** The Jones Act must be revised to reflect the reality of U.S. shipping resources and related manpower. Though the Trump administration has prioritized shipbuilding, this will not automatically translate to a new fleet of cable laying and repair ships, especially in the short-to-medium term. Crews are also made up of an array of nationalities, and the ability to crew such ships with only Americans is not realistic in the short-to-medium term. The Jones Act should allow, at the very least, ships built from partner and trusted countries, and visas should be issued for crew performing repairs or laying cables in U.S. territorial waters.

## RESILIENCY

1. **Partner with allies to monitor areas at risk for sabotage.** The United States and its partners and allies, including NATO and its Indo-Pacific allies, should work together to provide air and naval assets to patrol or act as deterrence in areas where cables could be intentionally cut. The ocean is vast, however, and monitoring the whole network is not plausible. Having a capacity to specifically monitor suspicious vessels, including Russian shadow fleets or Chinese fishing vessels, would likely enhance the United States' ability to deter potential sabotage or other nefarious activity.

   International cooperation among like-minded defense forces is also necessary to respond to shadow fleet activity in international waters suspected of monitoring undersea cables. Enhancing and replicating efforts like NATO's Operation Baltic Sentry is important to demonstrate a physical presence to deter malicious activities. In the absence of an international response, actors like China and Russia are emboldened to pursue such gray zone activities with impunity.

   Partners and allies should also find ways to collaborate, such as through joint statements, international fora, or other opportunities to call out irresponsible behavior from countries or ships.

2. **Mobilize financing agencies to support cable projects in developing countries.** As previously highlighted in the recommendations, the commercial case for subsea cable projects in developing and island countries is not always apparent, though there may be a strong strategic and development case. Development financing agencies like the DFC

and USTDA, in partnership with like-minded allies and partners, should finance projects to enhance these countries' connectivity. Greater connectivity can help deliver follow-on development impacts, allowing greater public access to medical, educational, commercial, and financial services. This would also allow the United States and like-minded countries to be more competitive in geostrategic areas, including the Pacific Islands and South and Southeast Asia, where digital and ICT projects have been limited to date.

3. **Maintain diplomatic pressure while strengthening partnerships.** The United States has utilized a full suite of diplomatic and economic tools to ensure high-risk vendors are excluded from major new subsea cable projects. The United States has already deployed diplomatic pressure and encouraged co-financing with allies for subsea cable projects in the Pacific to ensure high-risk vendors do not join critical infrastructure projects. These efforts can be expanded to other regions as well, including the Middle East and Latin America. The United States should also look to allies and partners, including bilateral treaty allies, NATO, and partnerships like the Quad (a strategic partnership among Australia, India, Japan, and the United States), to ensure trusted vendors work on this critical infrastructure and pool resources to support repair and monitoring.
4. **Enhance information sharing and communication between the U.S. government and the private sector.** The United States should find ways to share intelligence with the private sector on emerging risks and ongoing threats. Information sharing from the private sector with the intelligence community and policymakers is also vital to getting a better understanding of what the manufacturers and hyperscalers are seeing as they are laying, repairing, and monitoring networks, putting the environment into context and adding real-world and real-time information to assessments. To do this, the U.S. government must provide clearances to trusted providers in the subsea cable industry to classified information as the basis for shared and confidential discussions regarding threats and opportunities.

   In working with the private sector, the United States must ensure it protects the industry's trade secrets. The landscape is competitive, and sharing threats or information that may reveal proprietary technology would likely result in companies unlikely to want to engage with the United States. As with government intelligence sources, confidential business information and intellectual property must be protected as well.

## Recommendations for Allies and Partners

### REDUNDANCY

1. **Support projects in strategic and developing countries.** Partner and allied governments should use available financing tools, including debt finance, export credit authority, and grants, to fund or de-risk subsea cable projects to strategic countries or those at risk of incorporating high-risk vendor technology into their systems. This will not only support greater redundancy within networks but also ensure that friendly-country technology is utilized, bringing about a more secure network.

## REPAIR

1. **Utilize naval capacity to support cable networks.** Allies and partners, particularly within NATO and the Quad, should consider how to use their respective naval capacities to support repairs in conflict or insecure areas and monitor high-risk areas for suspicious vessels. This may also involve retrofitting or using naval cable ships to aid in repairs.

   For example, cable manufacturers in CSIS's interviews expressed concern with the difficulties of obtaining insurance for repair ships operating in the Red Sea. Given the activities of the Houthi rebels as well as pirates from Yemen and Djibouti, insurance companies felt the areas were too dangerous and too risky to support cable repair ships. Given these security threats, navies from nearby countries should coordinate to protect ships repairing or laying cables, using assistance from allied or partner countries from Europe, North America, or Asia. This type of coordination can also be deployed in areas where suspicious incidents have occurred, including in the Baltic or South China Seas. Some of this work has been initiated and should be replicated elsewhere. NATO announced its Operation Baltic Sentry, which involves using frigates and maritime patrol aircraft to surveille and protect critical assets, to include subsea cables. NATO Secretary General Mark Rutte, in launching Baltic Sentry, noted the law supports the alliance's efforts to counter threats, "including possible boarding, impounding, and arrest."[166]

   Some naval ships, whether old ships in line to be decommissioned or those with capacity to be retrofitted to repair cables, should be part of an emergency cable repair fleet stationed in high-risk regions to aid in quick repairs. Such locations can include areas with elevated geological activity, a significant number of fishing vessels, or suspicious activity by geostrategic competitors.[167]

   Finally, as referenced earlier in the recommendations, international cooperation to patrol with naval and air assets and a roadmap for responding to shadow fleet activities in and around undersea cables can demonstrate consequences against such gray zone activities, providing additional deterrence and defense capabilities.

## RESILIENCY

1. **Support technical assistance and capacity building around cybersecurity.** Allies and partners should provide training and assistance for heightened cybersecurity and protective measures to governments and relevant private sector actors in countries through which cables traverse territorial waters or come ashore. This can be based on laws similar to those in Singapore and Australia and follow best practices on how to protect landing stations and related equipment from environmental hazards or physical attacks. Importantly, training and technical assistance on cybersecurity best practices will contribute to secure and high-integrity digital communications, ensuring that information passing through fiber-optics is uncompromised and secure.

## Recommendations for Financial Institutions

### REPAIR

1. **Provide political risk products and insurance for repair ships operating in conflict or high-risk zones.** The DFC and MDBs should explore the use of financial products to support companies contracted to repair cables in regions like the Red Sea or where conflict could erupt. The DFC offers political risk insurance, which covers up to $1 billion of an investment when losses are incurred for crises such as political violence and terrorism.[168] While the product is focused on losses incurred, financing agencies can consider guarantees or other types of insurance for these subsea cable projects, as they contribute to development and improved livelihoods.

### RESILIENCY

1. **Provide financing tools to support new cable projects.** Building redundancy is not just important to ensuring that communications and business continue unabated when damage occurs; it is also critical to extending connectivity to emerging and island economies. Subsea cable projects are expensive, with costs varying from $30,000 to $50,000 per kilometer of cable.[169] MDBs and DFIs can provide an array of financing options and de-risking tools to provide secure connectivity through subsea cable projects. Debt financing, technical assistance, feasibility studies, and blended finance can be used by these agencies to build redundancy and greater connectivity for emerging markets.

# Conclusion

Subsea cable infrastructure is critical to global communications, economic transactions, and national security. As demand for this infrastructure continues to rise, driven by demographic growth, the AI revolution, and the need to replace aging cables, its strategic importance will only intensify. At the same time, disruptions to these networks, coupled with high regulatory barriers, carry far greater economic and security consequences than ever before. Since an earlier subsea cable report published by CSIS in 2021, the threats posed by adversarial actors such as Russia and China have grown more acute, underscoring the urgency for action.

The United States must prioritize the security, resilience, and modernization of subsea cables. But it cannot meet this challenge alone. Close cooperation with allies and partners will be essential to securing this vital infrastructure for the future.

The rising geopolitical tensions and need for stable, secure, and reliable digital connectivity should catalyze the United States and its partners and allies to undertake a full assessment of the vulnerabilities in this critical infrastructure and implement a plan of action to build resiliency and security. If the United States intends to preserve its leadership in the global economy and stay at the forefront of technological innovation, it must focus robust investment and other resources in the redundancy, resiliency, and rapid repair of subsea cable infrastructure—the critical arteries of the digital age.

# About the Author

**Erin L. Murphy** is the deputy director for the Chair on India and Emerging Asia Economics and senior fellow of Emerging Asia Economics at the Center for Strategic and International Studies. In this role, she focuses her research on bridging private capital and public initiatives to power strategic infrastructure investments in the Indo-Pacific. She has spent her career in several public and private sector roles and more than two decades working in the Indo-Pacific. From 2007 to 2012, Murphy served as an analyst on Asian political and foreign policy issues at the Central Intelligence Agency. She returned to government from 2020 to 2022 as director for the Indo-Pacific at the U.S. International Development Finance Corporation (DFC), overseeing a multibillion-dollar pipeline focused on infrastructure, energy, digital, and healthcare investments and supported DFC engagement in initiatives such as the Trilateral Infrastructure Partnership, the Quad, the G7 Partnership for Global Infrastructure and Investment, and the Indo-Pacific Economic Framework. From 2013 to 2020, she founded and led a boutique advisory firm focused on Myanmar and emerging economies in Southeast Asia. Murphy received her master's degree in Japan studies and international economics from the Johns Hopkins School of Advanced International Studies and her bachelor's degree in international relations and Spanish from Tufts University. She was also a 2017–2018 Hitachi international affairs fellow in Japan with the Council on Foreign Relations and a Japan Exchange and Teaching (JET) Program assistant language teacher from 2001 to 2003 in Saga, Japan. Murphy is also the author of *Burmese Haze: US Policy and Myanmar's Opening—and Closing* (Association for Asian Studies, 2022).

# Endnotes


1 Alan Mauldin, "Do Submarine Cables Account for 99% of Intercontinental Data Traffic?," TeleGeography, May 4, 2023, https:// blog.telegeography.com/2023-mythbusting-part-3.

2 "Submarine Cable Frequently Asked Questions," TeleGeography, https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions.

3 Jonathan E. Hillman, *Securing the Subsea Cable Network: A Primer for Policymakers* (Washington, DC, CSIS, March 2021), https://www.csis.org/analysis/securing-subsea-network-primer-policymakers.

4 "Chronological lists of ratifications of, accessions and successions to the Convention and the related Agreements," United Nations, September 22, 2025 (last updated), https://www.un.org/depts/los/reference_files/chronological_lists_of_ratifications.htm.

5 Melissa A. Mahle, "Subsea Cables and US National Security," Steptoe, July 20, 2025, https://www.steptoe.com/en/news-publications/stepwise-risk-outlook/subsea-cables-and-us-national-security.html.

6 Alan Weissberger, "China seeks to control Asian subsea cable systems; SJC2 delayed, Apricot and Echo avoid South China Sea," IEEE ComSoc Technology Blog, March 14, 2023, https://techblog.comsoc.org/2023/03/14/china-seeks-to-control-asian-subsea-cable-systems-apricot-and-echo-avoid-south-china-sea/.

7 Zachary Folk, "Four Fiber Optic Cables Damaged In Red Sea: Here's What We Know," Forbes, March 4, 2024, https://www.forbes.com/sites/zacharyfolk/2024/03/04/four-fiber-optic-cables-damaged-in-red-sea-heres-what-we-know/.

8 Interview with a subsea cable manufacturer, December 30, 2024

9 "The Evolution and Engineering of Subsea Cables," Cable World News, February 12, 2025, https://www.cableworldnews.com/news/the-evolution-and-engineering-of-submarine-cables/.

10 Samuel Morse, "Chapter III: Heroes of the Telegraph," *ww*, https://web.archive.org/web/20081201131615/http://www.globusz.com/ebooks/Telegraph/00000013.htm.

11 Hillman, *Securing the Subsea Network*.

12 Koh Ewe and I-ting Chiang, "Taiwan jails China captain for undersea cable sabotage in landmark case," BBC, June 12, 2025, https://www.bbc.com/news/articles/cwy3zy9jvd4o; and Bill Whitaker, "Concerns about possible Russian sabotage persist amid rash of cable cuts in the Baltic Sea," CBS News, September 28, 2025, https://www.cbsnews.com/news/concerns-about-possible-russian-sabotage-baltic-sea-cable-cuts-60-minutes-transcript/.

13 "Submarine Cable Frequently Asked Questions," TeleGeography, https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions; Madison L. Long, "Information Warfare in the Depths: An Analysis of Global Undersea Cable Networks," U.S. Naval Institute, *Proceedings*, vol. 149/5/1, no. 443, May 2023, https://www.usni.org/magazines/proceedings/2023/may/information-warfare-depths-analysis-global-undersea-cable-networks; and Roland Nuijits, "Submarine Cable Industry Trends: Challenges and Opportunities," Ciena, October 13, 2023 https://courses.sidnlabs.nl/anet-2023/slides/Submarine_Cable_Industry_Trends_2023-ext.pdf.

14 Chido Munyati, "Empower Africa's youth to create jobs, growth and peace," World Economic Forum, January 9, 2024, https://www.weforum.org/stories/2024/01/empower-africa-s-youth-to-create-jobs-growth-and-peace.

15 United Nations, "9.7 Billion on Earth, but growth rate slowing, says new UN population report," United Nations, 2019, https://www.un.org/en/academic-impact/97-billion-earth-2050-growth-rate-slowing-says-new-un-population-report.

16 Phil Gervasi, "Diving Deep into Submarine Cables: The Undersea Lifelines of Internet Connectivity," Kentik, March 28, 2023, https:// www.kentik.com/blog/diving-deep-into-submarine-cables-undersea-lifelines-of-internet-connectivity.

17 "Submarine Cable Frequently Asked Questions," TeleGeography.

18 Hillman, *Securing the Subsea Network*.

19 "Satellite Internet- A Quick Primer and Survey of Solutions to Improve Performance," Mushroom Networks, n.d., https://www.mushroomnetworks.com/blog/satellite-internet-a-quick-primer-and-survey-of-solutions-to-improve-performance.

20 Rob Verger, "A 10-million-pound undersea cable just set an internet speed record," *Popular Science*, March 5, 2019, https://www.popsci.com/submarine-cable-data-transfer-record/.

21 "Submarine Cable Map," TeleGeography, https://submarinecablemap.com.

22 Interview with subsea cable manufacturer; Tim Stronge, "Submarine Cables: Are We in a New Bubble?," TeleGeography, 2017, https://www2.telegeography.com/hubfs/2017/presentations/telegeography-ptc17-submarine.pdf; and Chris van Zinnicq Bergmann, "Perspectives on the Financing of Submarine Cable Projects," Submarine Telecoms Forum, March 29, 2022, https://subtelforum.com/perspectives-on-the-financing-of-submarine-cable-projects/.

23 Paul Brodksy, "Building Tomorrow's Internet: A 2025 Update on Cable Investment," TeleGeography, May 15, 2025, https://blog.telegeography.com/building-tomorrows-internet-an-update-on-new-cable-investment.

24 "Priorities for DHS Engagement on Subsea Security & Resilience," Department of Homeland Security, December 18, 2025, https://www.dhs.gov/sites/default/files/2024-12/24_1218_scrc_Priorities-for-DHS-Engagement-on-Subsea-Cable-Security-Resilience_18-Dec-24.pdf.

25 Bob Wallace, "Amazon, Meta and Google Plan Subsea Cable Expansion," Network Computing, February 7, 2025, https:// www.networkcomputing.com/enterprise-connectivity/amazon-meta-google-plan-subsea-cable-expansion.

26 Kitty Wheeler, "How Meta's Investing in the Longest Sea Cable in the World," Technology Magazine, February 27, 2025, https:// technologymagazine.com/articles/metas-investment-plans-in-the-worlds-longest-sea-cable; Gaya Nagarajan and Alex-Handrah Aime, "Unlocking global AI potential with next-generation subsea infrastructure," Engineering at Meta, February 14, 2025, https:// engineering.fb.com/2025/02/14/connectivity/project-waterworth-ai-subsea-infrastructure/; and Ingred Lunden, "Meta confirms 'Project Waterworth,' a global subsea cable project spanning 50,000 kilometers," TechCrunch, February 14, 2025, https:// techcrunch.com/2025/02/14/meta-confirms-project-waterworth-a-global-subsea-cable-project-spanning-50000km/.

27 "JUPITER," Submarine Cable Networks, n.d., https://www.submarinenetworks.com/en/systems/trans-pacific/jupiter.

28 "Cross-Atlantic Cable deployed," Microsoft, n.d., https://news.microsoft.com/announcement/cross-atlantic-cable-deployed/; "Amitie/AEC-3," Submarine Cable Networks, https:// www.submarinenetworks.com/en/systems/trans-atlantic/amitie; and "NCP," Submarine Networks, https:// www.submarinenetworks.com/en/systems/trans-pacific/ncp.

29 Anna Gross et al., "How the US is pushing China out of the internet's plumbing," *Financial Times*, June 13, 2023, https://ig.ft.com/subsea-cables/.

30 "Peace," Submarine Cable Networks, https:// www.submarinenetworks.com/en/systems/asia-europe-africa/peace.

31 Bergmann, "Perspectives on the Financing of Submarine Cable Projects."

32 Stronge, "Submarine Cables: Are We in a New Bubble?"; and Doug Brake, "Submarine Cables: Critical Infrastructure for Global Communications," Information Technology & Innovation Foundation, April 2019, https://www2.itif.org/2019-submarine-cables.pdf.

33 Robert McCabe and Brendan Flynn, "Under the radar: Ireland, maritime security capacity, and the governance of subsea infrastructure," *European Security* 33, no. 2 (2023): 324–344, https://doi.org/10.1080/09662839.2023.2248001.

34 CTPSR Maritime Security Programme, *Rethinking Sovereignty and Security at the Maritime Frontier: Pirates, Proxies, Passwords and Pipelines* (Coventry, UK: Coventry University, January 2024), 23, https://pure.coventry.ac.uk/ws/portalfiles/portal/94160200/Rethinking_Maritime_Sovereignty_and_Security_CTPSR_MSP_Special_Report_Jan_2024_FINAL.

35 "International Connectivity for Communications Consultation," Government of Ireland, May 2024, 2, https://assets.gov.ie/static/documents/international-connectivity-for-telecommunications-consultation.pdf.

36 "Data Centres: A Cornerstone of Ireland's Foreign Direct Investment and Economic Growth – A view from Jason O'Conaill, Industry Expert," Data Centres Ireland, n.d., https://www.datacentres-ireland.com/data-centres-a-cornerstone-of-irelands-foreign-direct-investment-and-economic-growth-a-view-from-jason-oconaill-industry-expert/.

37 McCabe and Flynn, "Under the radar."

38 "Neutrality: Ireland's policy of military neutrality," Government of Ireland, n.d., https://www.ireland.ie/en/dfa/role-policies/international-priorities/peace-and-security/neutrality/.

39 Romina Bandura and Thomas Bryja, "The Strategic Future of Subsea Cables: Ireland Case Study," CSIS, July 23, 2025, https://www.csis.org/analysis/strategic-future-subsea-cables-ireland-case-study.

40 Ibid.

41 "How Submarine Cables Are Laid and Repaired," Amissiontech, August 23, 2024, https:// www.amissiontech.com/news/how-submarine-cables-are-laid-and-repaired.html.

42 Winston Qiu, "Next Generation Submarine Network – Innovative Repeater Technology," Submarine Cable Networks, September 18, 2020, https://www.submarinenetworks.com/en/nv/insights/next-generation-submarine-network-innovative-repeater-technology.

43 Neal S. Bergano and Bruce Nyman "Submerged plant equipment," in *Undersea Fiberoptic Communication Systems*, ed. José Chesnoy (London, Academic Press, 2016), 651–669, https://www.sciencedirect.com/topics/engineering/branching-node; and "Subsea Cable System 101," OpticalCloudInfra, August 24, 2017, https://opticalcloudinfra.com/wp-content/uploads/2017/08/2017_08_24-Subsea-Cable-System-Tutorial.pdf.

44 "EXA knowledge center|Cable Landing Station (CLS)," EXA Infrastructure, https://exainfra.net/exa-infrastructure-knowledge-centre/cable-landing-station/; and Phil Gervasi, "Diving Deep into Submarine Cables: The Undersea Lifelines of Internet Connectivity," Kentik, March 28, 2023, https://www.kentik.com/blog/diving-deep-into-submarine-cables-undersea-lifelines-of-internet-connectivity/.

45 "Submarine cable damage and repair: claims and remedial issues," Leadvent Group, June 2, 2025, https://www.leadventgrp.com/blog/submarine-cable-damage-and-repair-claims-and-remedial-measures.

46 "Portmarine Circular No. 03 of 2017 Prohibiting of Anchoring in the Straits of Malacca and Singapore," Maritime and Port Authority of Singapore, January 19, 2017, https://www.mpa.gov.sg/media-centre/details/prohibition-of-anchoring-in-the-straits-of-malacca-and-singapore.

47 Andy Palmer-Felgate et al., "Marine Maintenance in the Zone – A Global Comparison of Repair Commencement Times," Suboptic, 2013, https://minz.org.nz/i/2018-challenges/Marine-maintenance-in-the-zones.pdf.

48 Jeslyn Tan, "Securing the backbone: Security challenges to and governance of submarine cables in the Indo-Pacific," Melbourne Asia Review, June 3, 2024, https://www.melbourneasiareview.edu.au/securing-the-backbone-security-challenges-to-and-governance-of-submarine-cables-in-the-indo-pacific/.

49 Interview with U.S. government officials, May 15, 2025

50 Sarah Whiteford, "How is subsea cable repaired?," One Step Power, April 26, 2021, https://www.onesteppower.com/post/subsea-cable-repair; and "Cable ships of the world," International Cable Protection Committee, updated May 29, 2025, https://www.iscpc.org/information/cableships-of-the-world/.

51 "How Submarine Cables Are Laid and Repaired," Amissiontech, August 23, 2024, https:// www.amissiontech.com/news/how-submarine-cables-are-laid-and-repaired.html.

52 "Telecommunications Act 1999," Government of Singapore, December 1, 1999, https://www.unclos.org sso.agc.gov.sg/Act/TA1999; and "Penal Code 1871," Government of Singapore, December 31, 2021, https://sso.agc.gov.sg/act/pc1871.

53 U.S. Department of State, "Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World," press release, September 26, 2024, https://2021-2025.state.gov/joint-statement-on-the-security-and-resilience-of-undersea-cables-in-a-globally-digitalized-world/; "United Nations Convention on the Law of the Sea," United Nations, November 16, 1994, https://unclos.org; and "New York joint statement on the security and resilience of undersea cables in a globally digitalize world," Government of the United Kingdom, November 29, 2024, https:// www.gov.uk/government/publications/

new-york-joint-statement-on-the-security-and-resilience-of-undersea-cables/new-york-joint-statement-on-the-security-and-resilience-of-undersea-cables-in-a-globally-digitalized-world.

54 "NATO launches 'Baltic Sentry' to increase critical infrastructure security," NATO, January 14, 2025, https:// www.nato.int/cps/en/natohq/news_232122.htm.

55 "Chapter 532-Cable Security Fleet," U.S. House of Representatives, 46 USC Ch. 532, December 20, 2019, https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title46-chapter532&edition=prelim.

56 Ulrich Speidel, "A short history of Singapore's role in the cable world," APNIC, September 12, 2022, https://blog.apnic.net/2022/09/12/a-short-history-of-singapores-role-in-the-cable-world/.

57 "Singapore Country Commercial Guide: Digital Economy," U.S. International Trade Adminitration, updated August 22, 2025, https://www.trade.gov/country-commercial-guides/singapore-digital-economy.

58 "2023 Investment Climate Statements: Singapore," U.S. Department of State, 2023, https://www.state.gov/reports/2023-investment-climate-statements/singapore/.

59 "Telecommunications Act 1999," December 1, 1999, Government of Singapore, https://sso.agc.gov.sg/Act/TA1999; and "Penal Code 1871," Government of Singapore," September 16, 1872, https://sso.agc.gov.sg/act/pc1871.

60 Erin Murphy and Thomas Bryja, "The Strategic Future of Subsea Cables: Singapore Case Study," CSIS, September 24, 2025, https://www.csis.org/analysis/strategic-future-subsea-cables-singapore-case-study.

61 "Ownership, Cabotage and flag issues relating to Indonesian Maritime Assets (Part 1)," Watson Farley & Williams, September 2016, https://www.wfw.com/wp-content/uploads/2019/07/WFW-Indonesia-1.pdf.

62 Murphy and Bryja, "The Strategic Future of Subsea Cables: Singapore Case Study."

63 U.S. Department of State, "Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World," press release, September 16, 2024, https://2021-2025.state.gov/joint-statement-on-the-security-and-resilience-of-undersea-cables-in-a-globally-digitalized-world/.

64 Winston Qiu, "US and its Allies Issue Joint Statement on the Security and Resilience of Undersea Cables," Submarine Cable Networks, October 7, 2024, https:// www.submarinenetworks.com/en/nv/insights/us-and-its-allies-issue-joint-statement-on-the-security-and-resilience-of-undersea-cables.

65 "G7 Hiroshima Leaders' Communique," G7, May 20, 2023, https://www.mofa.go.jp/policy/economy/summit/hiroshima23/documents/pdf/Leaders_Communique_01_en.pdf?v20231006

66 "About the ICPC," International Cable Protection Committee, May 29, 2025, https:// www.iscpc.org/about-the-icpc/.

67 "Submarine Cable Resilience," International Telecommunications Union, n.d., https://www.itu.int/digital-resilience/submarine-cables/.

68 "United Nations Convention on the Law of the Sea," United Nations, November 16, 1994, https://unclos.org.

69 "About ISA," International Seabed Authority, https://www.isa.org.jm/about-isa/.

70 Joint Communication to the European Parliament and Council, "EU Action Plan on Cable Security," European Commission, February 21, 2025, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025JC0009.

71 "About Us," European Subsea Cables Association, https://www.escaeu.org/about-us/.

72 "North American Submarine Cable Association," North American Submarine Cable Association, n.d., https://www.n-a-s-c-a.org.

73 "SMART Cables," SMART Cables, https://www.smartcables.org/.

74 "International Connectivity Coalition," International Connectivity Coalition, n.d., https:// www.internationalconnectivitycoalition.com.

75 Zelie Petit, "Beneath NATO's Radars: Unaddressed Threats to Subsea Cables," CSIS, *Strategic Technologies* (blog), December 2, 2024, https:// www.csis.org/blogs/strategic-technologies-blog/beneath-natos-radars-unaddressed-threats-subsea-cables.

76 "G7 Hiroshima Leaders' Communique," G7, May 20, 2023, https://www.mofa.go.jp/policy/economy/summit/hiroshima23/documents/pdf/Leaders_Communique_01_en.pdf?v20231006.

77 "Joint Communication to strengthen the security and resilience of submarine cables," European Commission, February 21, 2025, https://digital-strategy.ec.europa.eu/en/factpages/joint-communication-strengthen-security-and-resilience-submarine-cables.

78 World Bank, "World Bank Approves $35 Million Investment for Black Sea Submarine Cable Project Preparatory Activities," press release, May 21, 2024, https://www.worldbank.org/en/news/press-release/2024/05/21/world-bank-approves-35-million-investment-for-black-sea-submarine-cable-project-preparatory-activities.

79 "Connecting Africa to the World," International Finance Corporation, 2023, www.ifc.org/content/dam/ifc/doc/2023-delta/infra-factsheet-submarine-cables-2023.pdf.

80 "ADB Grants USD 25 Million for Samoa-Fiji Submarine Cable," Submarine Telecoms Forum, November 30, 2015, https://subtelforum.com/11adb-grants-usd-25-million-for-samoa-fiji-submarine-cable/; "Crossing the Expanse: A Connected Cook Islands," Asian Development Bank, February 17, 2023, https://www.adb.org/news/videos/crossing-expanse-connected-cook-islands; and "Palau: North Pacific Regional Connectivity Investment Project," Asian Development Bank, last updated June 2025, https://www.adb.org/projects/46382-001/main.

81 "Telconet S.A.," IDB Invest, https://idbinvest.org/en/projects/telconet-sa.

82 "CAF supports the leap in air and digital connectivity in El Salvador with USD 465 million in loans," Development Bank of Latin America and the Caribbean, July 18, 2024, https:// www.caf.com/en/currently/news/caf-supports-the-leap-in-air-and-digital-connectivity-in-el-salvador-with-usd-465-million-in-loans/.

83 "Nigeria Sovereign Fibre Project," EBRD, October 2025, https:// www.ebrd.com/home/work-with-us/projects/psd/56618.html#customtab-2dd5cc6e57-item-9d579bd048-tab.

84 "EBRD Funds Turkey's Investment in High-Tech Undersea Cable System," Submarine Telecoms Forum, September 21, 2016, https://subtelforum.com/22ebrd-funds-turkey-s-investment-in-high-tech-undersea-cable-system/.

85 "Seychelles- Submarine Cable Project- Results Brief 2022," African Development Bank Group, March 22, 2024, https://www.afdb.org/en/documents/seychelles-submarine-cable-project-results-brief-2022; "Congo - Central Africa Backbone (CAB) Project - Congo Component," World Bank Group, March 2025, https:// mapafrica.afdb.org/en/projects/46002-P-CG-GB0-002; and "Over 66 million Africans Gain Digital Access Owing to African Development Bank Infrastructure Push," African Development Bank Group, May 16, 2025, https:// www.afdb.org/en/success-stories/over-66-million-africans-gain-digital-access-owing-african-development-bank-infrastructure-push-83705.

86 Winston Qiu, "US-Japan-Australia Trilateral Partnership for Indo-Pacific Infrastructure Investment," Submarine Cable Networks, March 29, 2021, https://www.submarinenetworks.com/en/nv/insights/us-japan-australia-trilateral-partnership-for-indo-pacific-infrastructure-investment.

87 "AIFFP advances $2B infrastructure investments in the Pacific," Australia-Pacific Business Connections, February 4, 2025, https://apibc.org.au/2025/aiffp-advances-2b-infrastructure-investment-in-the-pacific/.

88 "Submarine Cable Landing Licenses," Federal Communications Commission, n.d., https://www.fcc.gov/research-reports/guides/submarine-cable-landing-licenses.

89 "Submerged Lands Act (SLA) of 1953," Bureau of Ocean Energy Management, 1953, https:// www.boem.gov/sites/default/files/documents/The%20Submerged%20Lands%20Act%20of%201953.pdf.

90 Guy Standing, "Here's why the UN's law of the sea needs and overhaul," World Economic Forum, December 12, 2022, https://www.weforum.org/stories/2022/12/here-s-why-un-law-sea-overhaul; and Caitlin Keating-Bitonti, *United Nations Convention on the Law of the Sea (UNCLOS): Living Resources Provisions*, CRS Report No. R47744 (Washington, DC: Congressional Research Service, December 2024), https://www.congress.gov/crs-product/R47744.

91 Saarang Ramabhadran, "Navigating Coastlines: The United States & UNCLOS," TULJ, March 5, 2025, https://www.texasulj.org/post/navigating-coastlines-the-united-states-unclos; and Anthony Wells, "The United Nations Convention on the Law of the Sea and the U.S. Navy," U.S. Naval Institute, June 1, 2021, https://blog.usni.org/posts/2021/06/01/the-united-nations-convention-on-the-law-of-the-sea-and-the-u-s-navy.

92 "Submarine Cables," Federal Communications Commission, n.d., https://www.fcc.gov/submarine-cables.

93 "Submarine Cables-Domestic Regulation," National Oceanic and Atmospheric Administration, https://www.noaa.gov/general-counsel/gc-international-section/submarine-cables-domestic-regulation.

94 Nicole T. Carter et al., *Protection of Undersea Telecommunication Cables: Issues for Congress*, CRS Report No. R47648 (Washington, DC: Congressional Research Service, August 2023), https://www.congress.gov/crs-product/R47648.

95 "33 CFR 322 - Permits for Structure or Work in or Affecting Navigable Waters of the United States," U.S. Army Corps of Engineers, n.d., https://www.nap.usace.army.mil/portals/39/docs/regulatory/regs/33cfr322.pdf.

96 "Priorities for DHS Engagement on Subsea Cable Security & Resilience," Department of Homeland Security, December 18, 2024, https://www.dhs.gov/sites/default/files/2024-12/24_1218_scrc_Priorities-for-DHS-Engagement-on-Subsea-Cable-Security-Resilience_18-Dec-24.pdf.

97 Ibid.; and "Sector Risk Management Agencies," Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, n.d., https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/sector-risk-management-agencies.

98 "NSCPO Background," Naval Facilities Engineering Systems Campaign, n.d., https://www.navfac.navy.mil/Directorates/Planning-Design-and-Construction/Products-and-Services/NAVFAC-Ocean-Facilities-Office/Naval-Sea-Floor-Cable-Protection-Office/NSCPO-Background/.

99 "Public Information Summary: Trans Pacific Networks Cayman Co.," U.S. International Development Finance Corporation, n.d., https://www.dfc.gov/sites/default/files/media/documents/9000093543.pdf.

100 U.S. Embassy Jakarta, "Press Release: USTDA, Super Sistem Partner on Subsea Cable for Indonesia," press release, July 12, 2023, https://id.usembassy.gov/ustda-super-sistem-partner-on-subsea-cable-for-indonesia.

101 "EX-IM Bank Finances Mauritius Portion of Africa-Asia Undersea Cable Transaction Agreements Signed at Ex-Im Bank Headquarters," EXIM, May 9, 2000, https://www.exim.gov/news/ex-im-bank-finances-mauritius-portion-africa-asia-undersea-cable-transaction-agreements-signed.

102 Cary Stier, "The economic impact of disruptions to Internet connectivity: A Report for Facebook," Deloitte, October 2016, https://www.deloitte.com/ug/en/Industries/tmt/perspectives/the-economic-impact-of-disruptions-to-internet-connectivity-report-for-facebook.html.

103 "Submarine Cable Frequently Asked Questions," TeleGeography, n.d., https:// www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions.

104 Carter, *Protection of Undersea Telecommunication Cables*.

105 Bob Wallace, "Deep Seabed Mining a Threat to Global Subsea Cable Network Safety, Environment," Network Computing, July 8, 2024, https://www.networkcomputing.com/enterprise-connectivity/deep-seabed-mining-a-threat-to-global-subsea-cable-network-safety-environment; and Amelie Bottollier-Depois, "New deep sea mining rules lack consensus despite US pressure," Phys.org, July 18, 2025, https:// phys.org/news/2025-07-deep-sea-lack-consensus-pressure.html.

106 Priya Anika Rajan, "NOC: Natural Disasters Responsible for 25% of Subsea Cable Damage," World Ports Org., May 9, 2025, https:// www.worldports.org/noc-natural-disasters-responsible-for-25-of-subsea-cable-damage.

107 Eliza Strickland, "Why the Japan Earthquake Didn't take Down the Country's Internet," IEEE Spectrum, March 14, 2011, https:// spectrum.ieee.org/why-the-japan-earthquake-didnt-cripple-the-countrys-internet.

108 Interview with hyperscaler. June 23, 2025

109 International Cable Protection Committee, "Subsea Landslide is Likely Cause of SE Asian Communications Failure," press release, March 21, 2007, https://www.iscpc.org/documents/?id=9.

110 Paul Lipscombe, "Tonga's Domestic submarine cable fixed 18 months after volcanic eruption," Data Center Dynamics, July 14, 2023, https://www.datacenterdynamics.com/en/news/tongas-domestic-submarine-cable-fixed-18-months-on-from-volcanic-eruption/; and Anne Brice, "A volcanic eruption severed communications in Tonga. The reason lay deep under the sea," UC Berkeley News, May 9, 2024, https://news.berkeley.edu/2024/05/09/submarine-communications-cables.

111 M.A. Clare et al., "Climate change hotspots and implications for the global subsea telecommunications network," *Earth Science Reviews* 237 (February 2023), https://doi.org/10.1016/j.earscirev.2022.104296.

112 Mike Clare, "Submarine Cable Protection and the Environment," International Cable Protection Committee, May 20, 2023, https:// iscpc.org/publications/submarine-cable-protection-and-the-environment/ICPC_Public_EU_May%202023.pdf.

113 Seth Jones, "Russia's Shadow War Against the West," CSIS, *CSIS Briefs*, March 18, 2025, https://www.csis.org/analysis/russias-shadow-war-against-west.

114 Katharina Buchholz, "Baltic Sea Cable Incidents Pile Up- Who Is To Blame?," Forbes, January 31, 2025, https://www.forbes.com/sites/katharinabuchholz/2025/01/31/baltic-sea-cable-incidents-pile-upwho-is-to-blame/.

115 Jill Goldenziel, "Law Can't Stop Undersea Cable Cuts," *Forbes*, February 13, 2025, https://www.forbes.com/sites/jillgoldenziel/2025/02/13/law-doesnt-protect-undersea-cables-russia-and-china-know-it/.

116 "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 External Action, December 26, 2024, https://www.eeas.europa.eu/eeas/joint-statement-european-commission-and-high-representative-investigation-damaged-electricity-and_en.

117 "NATO Naval Forces Conclude Multinational Exercise Freezing Winds Off the Coast of Finland," NATO, November 29, 2024, https://shape.nato.int/news-archive/2024/nato-naval-forces-conclude-multinational-exercise-freezing-winds-off-the-coast-of-finland.

118 Wayne Chang, "Taiwan detains Chinese-crewed ship suspected of cutting undersea cable," CNN, February 26, 2025, https://www.cnn.com/2025/02/25/asia/taiwan-detains-ship-undersea-cable-intl-hnk/index.html.

119 Ibid.

120 "Taiwan charges captain of China-linked ship with damaging subsea cable," Al-Jazeera, April 11, 2025, https://www.aljazeera.com/news/2025/4/11/taiwan-charges-captain-of-china-linked-ship-with-damaging-subsea-cable.

121 Carter, *Protection of Undersea Telecommunication Cables*.

122 Christy Lee, "Undersea cables emerge as source of friction in South China Sea," VOA, October 11, 2024, https://www.voanews.com/a/undersea-cables-emerge-as-source-of-friction-in-south-china-sea/7819426.html.

123 "Submarine Cable Networks," Submarine Cable Networks, https:// www.submarinenetworks.com/en/stations.

124 "Submarine Cable Systems Companies- Alcatel Submarine Networks (France) and Prysmian S.p.A (Italy) are the Key Players," Markets and Markets, n.d., https://www.marketsandmarkets.com/ResearchInsight/submarine-cable-system-market.asp; and "Submaine Line Terminal Equipment - SLTE," HMNTech, n.d., https://www.hmntech.com/enDryPlants/37412.jhtml.

125 Matt Burgess, "The Most Vulnerable Place on the Internet," *Wired*, November 2, 2022, https://www.wired.com/story/submarine-internet-cables-egypt/.

126 Sebastian Moss, "The colonial roots of Egypt's submarine cable routes," Data Center Dynamics, September 19, 2022, https://www.datacenterdynamics.com/en/analysis/the-colonial-roots-of-egypts-submarine-cable-routes/.

127 Alan Mauldin, "The Red Sea: A Key Subsea Cable Crossroads Under Siege," TeleGeography, January 17, 2024, https://blog.telegeography.com/the-red-sea-a-key-subsea-cable-crossroads-under-siege.

128 "Cabinet highlights Egypt's foreign direct investment success in FY2023/2024," Business Today Egypt, December 31, 2024, https://www.businesstodayegypt.com/Article/1/5829/Cabinet-highlights-Egypt%E2%80%99s-foreign-direct-investment-success-in-FY2023-2024.

129 Jun Qiao et al., "The Geopolitical Importance of Bab el-Mandeb Strait: A Strategic Gateway to Global Trade," Middle East Political and Economic Institute, February 28, 2024, https://mepei.com/the-geopolitical-importance-of-bab-el-mandeb-strait-a-strategic-gateway-to-global-trade/.

130 "Rubymar, a UK-owned cargo ship hit by Yemen's Houthis, sinks in the Red Sea," Al-Jazeera, March 2, 2024, https://www.aljazeera.com/news/2024/3/2/rubymar-cargo-ship-earlier-hit-by-houthis-has-sunk-yemeni-government-says.

131 Matt Burgess "The Most Vulnerable Place on the Internet," *Wired*, November 2, 2022, https://www.wired.com/story/submarine-internet-cables-egypt/.

132 Paul Cochrane, "How Saudi Arabia is redrawing the map of the future with fibre-optic cables," Middle East Eye, April 5, 2023, https://www.middleeasteye.net/news/saudi-arabia-fibre-optic-cables-internet-future-map-redrawing.

133 Carter, *Protection of Undersea Telecommunication Cables*.

134 "Apricot," Submarine Cable Networks, n.d., https://www.submarinenetworks.com/en/systems/intra-asia/apricot; and Winston Qiu, "Echo Cable System Overview," Submarine Cable Networks, April 15, 2021, https://www.submarinenetworks.com/en/systems/trans-pacific/echo/echo-cable-system-overview.

135 Joe Brock, "U.S. and China wage war beneath the waves- over internet cables," Reuters, March 24, 2023, https://www.reuters.com/investigates/special-report/us-china-tech-cables/.

136 Demetri Sevastopulo, "China exerts control over internet cable projects in South China Sea," *Financial Times*, March 13, 2023, https://www.ft.com/content/89bc954d-64ed-4d80-bb8f-9f1852ec4eb1.

137 John Dotson, "Strangers of a Seabed: Sino-Russian Collaboration on Undersea Cable Sabotage Operations," Jamestown Foundation, *China Brief*, vol. 25, no. 3, February 14, 2025, https://jamestown.org/program/strangers-on-a-seabed-sino-russian-collaboration-on-undersea-cable-sabotage-operations/.

138 Raghvendra Kumar, "Securing the Digital Seabed: Countering China's Underwater Ambitions," *Journal of Indo-Pacific Affairs*, November 15, 2023, https://www.airuniversity.af.edu/JIPA/Display/Article/3588497/securing-the-digital-seabed-countering-chinas-underwater-ambitions/.

139 Joe Brock, "U.S. and China wage war beneath the waves- over internet cables," Reuters, March 24, 2023, https://www.reuters.com/investigates/special-report/us-china-tech-cables/.

140 Samuel Bashfield, "Defending seabed lines of communication," Australian Journal of Maritime & Ocean Affairs, July 5, 2024, https://www.tandfonline.com/doi/full/10.1080/18366503.2024.2363607?cookieSet=1#d1e111.

141 Ibid.; and "New-build Submarine Cable System Solution," HMNTech, n.d., https://www.hmntech.com/enNewBuild.jhtml.

142 Jeff Pao, "Internet cables the next front in US-China tech war," *Asia Time*s, March 28, 2023, https://asiatimes.com/2023/03/internet-cables-the-next-front-in-us-china-tech-war/.

143 Ibid.

144 "U.S. adds Huawei Marine Networks to Entity List," Converge! Network Digest, December 16, 2021, https://convergedigest.com/us-adds-huawei-marine-networks-to/.

145 Colin Grabow, Inu Manak, and Daniel J. Ikenson, "The Jones Act: A Burden America Can No Longer Bear," CATO Institute, June 28, 2018, https://www.cato.org/publications/policy-analysis/jones-act-burden-america-can-no-longer-bear#endnotes.

146 "What Every Member of the Trade Community Should Know About: The Jones Act," U.S. Customs and Border Protection, December 2024, https://www.cbp.gov/sites/default/files/2024-12/Jones%20Act%20ICP_Complete_04DEC24.pdf.

147 Marinza Savanthy, "Indonesia's Cabotage Rule Reaffirmed: Legal Certainty for Foreign Vessel Use in Offshore Petroleum and Energy Operations," ADCO Law, September 23, 2025, https:// adcolaw.com/blog/indonesias-cabotage-rule-reaffirmed-legal-certainty-for-foreign-vessel-use-in-offshore-petroleum-and-energy-operations/.

148 "1884 Convention for the Protection of Submarine Telegraph Cables," Centre for International Law, March 14, 1884, https:// cil.nus.edu.sg/wp-content/uploads/2019/02/1884-Convention-for-the-Protection-of-Submarine-Telegraph-Cables-1.pdf.

149 "United Nations Convention on the Law of the Sea," United Nations, December 10, 1982, https://www.un.org/depts/los/convention_agreements/texts/unclos/UNCLOS-TOC.htm.

150 "Rules for operating around submarine cables," Australian Communications and Media Authority, Australian Government, n.d., https://www.acma.gov.au/rules-operating-around-submarine-cables.

151 Jill Goldenziel, "Law Can't Stop Submarine Cable Sabotage. Russia And China Know It.," *Forbes*, February 13, 2025, https:// www.forbes.com/sites/jillgoldenziel/2025/02/13/law-doesnt-protect-undersea-cables-russia-and-china-know-it/.

152 Amy Paik and Jennifer Counter, "International law doesn't adequately protect undersea cables. That must change.," Atlantic Council, January 25, 2024, https:// www.atlanticcouncil.org/content-series/hybrid-warfare-project/international-law-doesnt-adequately-protect-undersea-cables-that-must-change/.

153 Long, "Information Warfare in the Depths"; and Anna Blue, "Submarine Data Cables: Latest Target of the U.S.-China Rivalry," Princeton University, *Journal of Public and International Affairs*, September 24,2024, https://jpia.princeton.edu/news/submarine-data-cables-latest-target-us-china-rivalry.

154 "It's Going to Take $3 Billion to Ensure Submarine Cable Repair Ships Can Keep the World Connected," TeleGeography, June 30, 2025, https://blog.telegeography.com/submarine-cable-maintenance-data.

155 Ibid.

156 Interview with subsea cable manufacturer, March 4, 2025

157 "Marine Engineering," HMN Tech, n.d., https://www.hmntech.com/enProjectImplementation.jhtml.

158 Matthew P. Funaiole, Brian Hart, and Aidan Powers-Riggs, "Ship Wars: Confronting China's Dual-Use Shipbuilding Empire," CSIS, March 2025, https://www.csis.org/analysis/ship-wars-confronting-china s-dual-use-shipbuilding-empire.

159 Stephen Chen, "China unveils a powerful deep-sea cable cutter that could reset the world order," *SCMP*, March 22, 2025, https://www.scmp.com/news/china/science/article/3303246/china-unveils-powerful-deep-sea-cable-cutter-could-reset-world-order.

160 Douglas R. Burnett,, "Repairing Submarine Cables Is a Wartime Necessity," U.S. Naval Institute, *Proceedings*, vol. 148/10/1, no. 436, October 2022, https://www.usni.org/magazines/proceedings/2022/october/repairing-submarine-cables-wartime-necessity.

161 Karin Kaneko, "METI may list undersea cables and satellites as critical for economic security," *Japan Times*, April 16, 2025, https://www.japantimes.co.jp/business/2025/04/16/economy/economic-security-plan/.

162 "Memorandum of Cooperation on submarine cables for secure, resilient and sustainable global connectivity," Ministry of Internal Affairs and Communications, Government of Japan, May 2022, https://www.soumu.go.jp/main_content/000890460.pdf.

163 Kim Nam-hee and Park Su-hyeon, "Japan ramps up shipbuilding with national yard, industry merger," *Chosun Daily*, July 4, 2025, https://www.chosun.com/english/industry-en/2025/07/04/OVR7ZM6UJRGBZLAN5FV5HPGNIQ/.

164 "Telecommunications Act 1999," Government of Singapore, 2020 Revised edition, https://sso.agc.gov.sg/Act/TA1999; and "Penal Code 1871," Government of Singapore, 2020 Revised edition, https://sso.agc.gov.sg/act/pc1871.

165 Karl Hoerr, "What lies beneath: Undersea cables and the laws protecting them," LSJ Online, December 16, 2024, https://lsj.com.au/articles/what-lies-beneath-undersea-cables-and-the-laws-protecting-them/.

166 "NATO launches 'Baltic Sentry' to increase critical infrastructure security," NATO, January 14, 2025, https://www.nato.int/cps/en/natohq/news_232122.htm.

167 Ibid.

168 "Political Risk Insurance," U.S. International Development Finance Corporation, https:// www.dfc.gov/what-we-offer/our-products/political-risk-insurance.

169 Daniel F. Runde et al., *Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition* (Washington, DC: CSIS, August 2024), https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition.

**COVER PHOTO** ZU_09/GETTY IMAGES

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | **www.csis.org**