CENTER FOR
CYBERSECURITY
POLICY AND LAW

WHITEPAPER

SHORING UP SUBSEA SECURITY:

A Comprehensive Action Plan to Promote Submarine Cable Resiliency, Security & Governance

Alexander Botting

Alexis Steffaro
Luke O'Grady

SEPTEMBER, 2025

CENTER FOR CYBERSECURITY POLICY AND LAW

EXECUTIVE SUMMARY

Submarine cables are the essential infrastructure that enables the modern global economy, carrying over 95% of international data traffic and supporting everything from financial transactions to cloud services. As the world becomes more digitally interconnected and geopolitical tensions escalate, the resilience and security of these critical systems face increasing risks. In response, this paper

proposes a comprehensive action plan to drive the security and resilience of submarine cable infrastructure through stronger public-private collaboration and more effective policy frameworks.

The private sector has long prioritized resilience and risk mitigation. Companies invest heavily in redundancy, and route diversity, to ensure continuity of service, even in challenging environments. But sustained cooperation with governments is essential to ensure regulatory environments enable, rather than hinder, the deployment, maintenance, and protection of this foundational infrastructure.

Public and private stakeholders have recently demonstrated its shared commitment to protecting undersea cable infrastructure. The New York Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World ("New York Principles")[1] signed by 17 countries in September 2024, reflects growing international consensus around this issue. While high-level, the Principles identify important areas for cooperation, including the need to deepen public-private collaboration.

To be effective, these high-level commitments must be supported by tangible activities. Industry has long prioritized the resilience of submarine cable systems, applying best practices to mitigate relevant risks. Governments should view industry not only as a critical stakeholder, but as a proactive partner already working to secure this infrastructure. Moving forward, stronger collaboration is essential to ensure that regulatory environments support, rather than hinder, the deployment and maintenance of undersea cables.

This paper seeks to provide recommendations for action for the Principles, leveraging the resources and roles of the private and governmental sectors. Specifically, this paper offers concrete ideas for enhancing the resilience of the global submarine cable ecosystem primarily through greater route diversity and redundancy, rapid repair capacity, and secure supply chains.

This can be further enhanced by bolstering the security of individual cables against physical, technical, and supply chain threats; and establishing legal and institutional frameworks that improve risk awareness and deter disruptive activity, ultimately reducing disruptions of this critical infrastructure.

[1] The European Union, *The New York Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitized World* (2024) digital-strategy.ec.europa.eu/en/library/new-york-joint-statement-security-and-resilience-undersea-cables-globally-digitalized-world.

RECOMMENDATIONS

Ecosystem Resilience

1. **Governments** should ensure that permit requirements for the installation and repair of submarine cables are consistent with international treaty obligations and customary international law, be transparent, and establish clear timeframes that are as short as possible.
2. **Governments** should enhance clarity and predictability of rules, partners, and geographies that will factor into approvals decisions, including promoting transparency between national security agencies and submarine cable developers regarding national security risks. This includes assessments of national and economic security, trusted supply chains, and national competitiveness impacts.
3. **Governments** should establish clear security and resilience requirements which are aligned with international standards and harmonized with national security review processes.
4. **Governments and industry** should determine whether to pursue a strategy of diversification of pathways or concentration in Cable Protection Zones, with diversification the lower risk approach where feasible to implement.

   If diversification:

   4.1 **Governments** should foster commercial and regulatory conditions that support the development of diverse submarine cable landing sites and pathways, including streamlining permitting approvals processes.

   If concentration:

   4.2 **Governments** should ensure that CPZ are adopted with consultation and support of cable operators and are clearly defined on nautical charts.

   4.3 **Governments** should ensure that regulatory measures are in place to preclude fishing, non-essential marine transit, and other seabed activity within the CPZ in their territorial sea and ensure that oversight of CPZ protections is rigorously enforced and penalties are sufficient to deter non-compliance.

5. **Governments** should establish regulatory frameworks based on international best practices that embed submarine cable considerations into marine spatial planning processes, coordinated with adjacent states, ensuring early-stage coordination with submarine cable stakeholders during the planning and development of other marine activities.
6. **Governments** should share information with one another on the domestic approach they take and share lessons learned from implementation and adapt approaches as new

information is made available with the goal of harmonizing (to the extent possible) licensing and permitting requirements.

7. **Governments** should refrain from classifying submarine cable installation and repair activities as cabotage and from imposing cabotage or crewing restrictions on vessels performing repairs.
8. **Governments** should eliminate port entry requirements for cable ships engaged in installation or repair operations. For work within the territorial sea and archipelagic waters, establish annual pre-clearance procedures for cable ships and crews.
9. **Governments** should avoid imposing customs duties, taxes, and fees on submarine cable installation and repair activities, by enabling the establishment of Free Ports with bonded storage facilities at vessel base ports to facilitate deployment and expedite repairs.
10. **Governments** and industry should co-develop a strategy for emergency cable repair capacity, to enable additional government resources to be deployed in the event of a widespread disruption to cables.
11. **Governments** should streamline regulatory frameworks to ensure efficient cable repair and installation, while maintaining security and transparency. This includes improving permitting and liability regimes.
12. **Governments** and industry should conduct a comprehensive mapping of the submarine cable supply chain to identify potential choke points or areas of reliance on untrusted vendors and ensure that appropriate risk mitigations are in place.
13. **Governments** should maintain a published list of untrusted providers which will guide industry in the development of their supply chain partnerships.
14. **Governments** and industry should cooperate on sharing risk and incident data to identify protection gaps, enhance resilience, and detect and prevent malicious activities by state and non-state actors.

Infrastructure Security

15. **Industry** should continue to armor cables deployed at depths shallower than 2000 meters.
16. **Governments** should ensure the use of AIS tracking devices by vessels is mandatory in national law and enforce their use in accordance with IMO regulations.
17. **Governments** should explore making the use of VMS tracking mandatory within their EEZ to enhance visibility of activity near submarine cables, and enforcement of negligent activities.
18. **Governments and industry** should define clear security best practices for cable landing stations and work cooperatively to implement risk-based measures that enhance the overall resilience and security.
19. **Industry** owners of data should continue to implement comprehensive data risk mitigation frameworks including, where feasible, encrypting data in transit.

20. **Governments and industry** owners of data should develop a process and timeline for transitioning to quantum-resistant algorithms when encrypting sensitive data, building upon previous work undertaken by the U.S., EU and the UK's NCSC.[2]
21. **Governments and industry** should map potential supply chain risks, to include those to the repair supply chain.
22. **Governments and industry** should continue to invest in research and development (R&D) to advance fiber sensing capabilities and establish clear guidance on the approvals process for, and use of, fiber sensing solutions.
23. **Governments and industry** should explore potential information sharing agreements to leverage real-time data regarding imminent natural disasters.

Legal and Institutional Frameworks

24. **Governments** should designate submarine cables, and associated infrastructure such as cable landing stations, as critical infrastructure.
25. **Governments** should ratify and implement national obligations under 1884 and UNCLOS, where applicable.
26. **Governments** should encourage IMO-required use of Automatic Identification System (AIS) tracking.
27. **Governments** should ensure that charting authorities update nautical charts regularly, showing all submarine cables, and all other human activities that could pose risks to them; ensure implementation of the amended IHO Resolution 4/1967; and mandate educational programs for employees of maritime vessels, to ensure they are aware of key cable pathways, and implement measures to avoid accidental disruption.
28. **Governments** should establish and rigorously enforce penalties for vessels and their employees that cause disruption to cables through negligence.
29. **Governments** should streamline federal permitting processes for submarine cable projects to reduce delays and improve clarity for infrastructure developers and harmonize sub-national laws and regulations governing submarine cable infrastructure.
30. **Governments** should leverage existing security cooperation agreements to conduct patrols in high-risk areas and share intelligence about potential threats.
31. **Governments and industry** should establish proactive two-way intelligence sharing mechanisms with trusted cable developers and vendors to pre-empt potential attacks, and support the evidentiary body needed to prosecute criminal activity.
32. **Governments** should establish a single point of contact to centralize information and serve as an initial liaison for government agencies, and private parties regarding existing and planned submarine cables.

[2] National Cyber Security Centre (NCSC), "Timelines for migration to post-quantum cryptography", (Apr. 19, 2025), https://www.ncsc.gov.uk/pdfs/guidance/pqc-migration-timelines.pdf.

33. **Governments** should publish clear guidance on high-risk equipment, entities and countries of concern, and trusted suppliers.
34. **Governments** should establish formal 1.5 track dialogues with trusted industry partners through existing regional and security groupings, such as the Quad and NATO, to support aligned approaches to submarine cable security and resilience.

INTRODUCTION

In 1969, the Advanced Research Projects Agency Network (ARPANET) was established by the U.S. Department of Defense, serving as the precursor to the modern internet, and consisted of 400 hosts[3] who retained access to all the internet's packet-switching capabilities. As of 2024, 5.5 billion people (68% of the global population) are online[4] and able to benefit from the abundant source of information that is the global internet.

The basis of this remarkable ascent is a network of more than 500 submarine fiber-optic cables, collectively spanning almost 1.5 million kilometers, largely laid by the private sector.[5] Today the most advanced cables can transmit 300-400 terabits per second or more along the ocean floor or "the entire digitized Library of Congress three times every second."[6] This technological achievement is driven by the global economy's demand for data, which has risen from roughly 100 GB of data per day in 1992 to an estimated 463 exabytes (463 billion GB) per day in 2025.

Subsea cables carry more than 95% of global data traffic. In addition to consumer usage, the connectivity provided by this global network of cables underpins the digital systems of critical sectors such as finance, energy, government services, and defense. A large share of the growing demand is for data centers equipped to host advanced-AI workloads across these sectors and others.[7] Submarine cables are now often strategically placed to directly service these data centers, helping power AI diffusion globally. Without rapid and reliable connectivity, the provision of these

---

[3] Vint Cerf, "Marking the birth of the modern-day Internet," *Google*, Jan. 1, 2013, blog.google/inside-google/googlers/marking-birth-of-modern-day-internet/.

[4] International Telecommunication Union (ITU), *Global Internet use continues to rise but disparities remain, especially in low-income regions*, (Geneva: 2024), www.itu.int/en/mediacentre/Pages/PR-2024-11-27-facts-and-figures.aspx.

[5] TeleGeography, "Submarine Cable Frequently Asked Questions," (last accessed Feb. 25, 2025). www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions.

[6] Chris Ciauri, "The Dunant subsea cable, connecting the US and mainland Europe, is ready for service," *Google*, Feb.3, 2021, cloud.google.com/blog/products/infrastructure/googles-dunant-subsea-cable-is-now-ready-for-service.

[7] Bhargs Srivathsan et al., "AI power: Expanding data center capacity to meet growing demand," *McKinsey & Company,* Oct. 29, 2024, https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/ai-power-expanding-data-center-capacity-to-meet-growing-demand

important sectors would be degraded. There are few alternatives to subsea cables, and none reach the capacity of which cables are capable.[8]

Given the critical role that they fill, submarine cables should be, and in many countries are categorized as critical infrastructure themselves, with additional attention afforded from industry and government stakeholders to ensure their security and resilience. It's essential that we have a clear understanding of potential risks to this infrastructure and how they are being mitigated by governments and industry today, and where additional activity is needed to ensure the security and resilience of this vital infrastructure. To do so, governments must also work closely with the private sector, the primary deployer and funder of this critical infrastructure, and consider how public policy initiatives could impact the drivers for continued or even increased deployment.

The Risk Profile for Submarine Cables

The International Cable Protection Committee (ICPC) estimates that between 150 and 200 submarine cable faults occur each year, affecting the availability of these critical systems to transmit data.[9] The vast majority, approximately 70%, are caused by accidental physical damage from fishing activity or anchoring. The remainder result from natural events (such as storms or earthquakes), abrasion, or internal system failures. These risks are longstanding and for the most part well-managed though at significant cost to industry.[10]

Recent disruptions to submarine cable communications and rising geopolitical tensions, however, have spurred governments to intensify scrutiny of submarine cable accidents. The growth in global conflicts and rising geopolitical tensions have given rise to concerns of nation state sabotage - in particular by China and Russia. These concerns have been amplified by recent high-profile instances

---

[8] Compare Eutelsat's OneWeb constellation of 648 satellites that claimed a total usable capacity of 1.1 Tbps. *See* Ben Griffin, "Six myths and the reality behind OneWeb's low earth orbit revolution." *Eutelsat*, Mar. 24, 2022, https://oneweb.net/resources/six-myths-and-reality-behind-onewebs-low-earth-orbit-revolution.; Starlink's December 2023 metrics anticipate 230,000 Gbps by the end of 2024. *See* Brian Wang, "SpaceX Starlink Orbital Capacity and Usable Capacity," *NextBigFuture*, Dec. 22, 2023, https://www.nextbigfuture.com/2023/12/spacex-starlink-orbital-capacity-and-usable-capacity.html

[9] Manny Pham, "UN, ITU Launch Advisory Body to Strengthen Submarine Cable Resilience," *Submarine Telecoms Forum*, Dec.13, 2024, subtelforum.com/un-itu-launch-body-to-boost-submarine-cable-resilience/?utm_source=chatgpt.com.

[10] Public estimates vary from hundreds of thousands to millions of dollars. In 2011, ICPC estimated that a cable break can average $1-3 million to repair. *See* Dean Veverka, "Under the Sea," *Shipping and Marine Magazine*, Sept. 15, 2011, https://www.iscpc.org/documents/?id=201; Today, repairs of the March 2024 cable breaks on the west coast of Africa were estimated to cost $2 million each. *See* Emma Okonji, "Subsea Cable Cut: 35 Networks Restored, Full Restoration of Cables to Gulp $8m," *Submarine Telecoms Forum*, Mar. 26, 2024, https://subtelforum.com/8m-to-restore-subsea-cable-services/#:~:text=By%20Emma%20Okonji%2C%20Arise%20News&text=According%20to%20him%2C%20it%20will,were%20affected%20by%20the%20cut.; Moreover, repairs to subsea cables are typically not recouped through insurance or through litigation. Rather, the cable owner bears the full brunt of the cost.

of cable disruptions in the Baltic Sea and the Taiwan Strait, the latter of which saw more cable disruptions in January 2025 than in either 2023 or 2024.[11]

Concerns of reported investments by each country in developing new capabilities that could be used for sabotage operations have further exacerbated these concerns.[12][13] It is worth noting, however, that accidental incidents remain by far the largest cause of physical disruption, and the subsea cable industry has long established mechanisms for managing these. The rise in perceived threat from sabotage is challenging given the difficulty of distinguishing between accidental and deliberate damage.[14] So called gray zone tactics increase the concerns of governments, risking (though perhaps requiring) hasty responses and increased pressure on the commercial sector. Both government and industry may need additional tools and frameworks to better differentiate true accidents from purposeful damage.

Additionally, over the past decade, many governments in Europe, North America, and Asia have sought to enhance the trustworthiness of telecommunications infrastructure, including subsea cables, by reducing dependence on 'untrusted' or 'high risk' vendors. Initial efforts focused heavily on addressing reliance on Chinese vendors like Huawei and ZTE for 4G and 5G Radio Access Networks (RAN). Increasingly, this scrutiny has extended to cloud infrastructure, data centers, and submarine cable networks and to their owners and business partners. Government concern, in this instance, focuses on the potential for data exfiltration or malicious cybersecurity operations through remote control or access through untrusted equipment. These efforts should continue, and this paper offers supporting recommendations.

That said, physical damage – whether gray or black and white – remains the largest source of disruption to the operation of subsea cable infrastructure today, and for the foreseeable future. As such, public policy should seek to improve protection from physical damage, which will promote both resilience of the subsea cable infrastructure as well as deterrence of malicious action. Resilience reduces the impact of physical disruptions, which proportionately decreases the incentives for malicious action and safeguards the foundation on which many other critical services operate. The most effective means to ensure uninterrupted data flows globally, is by ensuring services can mitigate disruption through redundant infrastructure and rapid repair. Put simply,

---

[11] Keoni Everington, "2 Taiwan-Matsu Undersea Cables Disconnected," *Taiwan News,* Jan. 22, 2025, https://www.taiwannews.com.tw/news/6021043

[12] Jim Sciutto, "US sees increasing risk of Russian 'sabotage' of key undersea cables by secretive military unit," *CNN*, Sept. 6, 2024, https://www.cnn.com/2024/09/06/politics/us-sees-increasing-risk-of-russian-sabotage-undersea-cables

[13] Erin Murphy and Matt Pearl, "China's Underwater Power Play: The PRC's New Subsea Cable-Cutting Ship Spooks International Security Experts," *Center for Strategic & International Studies (CSIS)*, Apr. 4, 2025, https://www.csis.org/analysis/chinas-underwater-power-play-prcs-new-subsea-cable-cutting-ship-spooks-international

[14] Shane Croucher, "Sweden Issues Update in China Cable Cutting Probe," *Newsweek*, Apr. 15, 2025, https://www.newsweek.com/sweden-issues-update-china-cable-cutting-probe-2059874#:~:text=Swedish%20investigators%20have%20said%20they,to%20their%20newly%20released%20report; Dodge Billingsley, "Taiwan Suspects Chinese Ship of Cutting Undersea Data Cables," *Tradoc G2*, Apr. 17, 2025, https://oe.tradoc.army.mil/product/taiwan-suspects-chinese-ship-of-cutting-undersea-data-cables; Andrea Palasciano and Oliver Crook, "Baltic Sea Cable Cuts Can't Be Accident, EU Tech Chief Says," *Bloomberg*, Jan. 14, 2025, https://www. bloomberg.com/news/articles/2025-01-14/baltic-sea-cables-damage-can-t-be-accident- eu-tech-chief-says.

creating redundancy means laying more cables across differing routes to serve the increasing global demand and help address these risks. This paper therefore recommends:

- **Enhancing the resilience of the global submarine cable ecosystem:** developing policies that allow the private sector to build global submarine networks with sufficient redundancy and diversity of routes; ensure availability of repair capacity; and bolster supply chain resilience to withstand the impact of threats to the ecosystem.
- **Ensuring the security of individual submarine cables:** making it more difficult and costly for those causing disruption of submarine cable infrastructure, whether by physical, technical, or supply chain tactics, while enabling industry to be cost effective with their decision making.
- **Implementing appropriate legal and institutional frameworks:** reinforcing security and resilience measures with legal and governance frameworks that promote awareness of risks, facilitate multi-stakeholder coordination, reduce instances of unintentional disruption, and adequately deter acts of aggression.

ENHANCING THE RESILIENCE OF THE CABLE ECOSYSTEM

Efforts to enhance resilience can be divided into two components: reducing the impact of individual incidents and enhancing our ability to recover from incidents. Governments and industry must continue to drive redundancy and diversity in submarine cable infrastructure to enable traffic rerouting and minimize the impact of incidents. At the same time, robust repair and maintenance capabilities are critical for restoring the functionality after cable cuts occur.

I. Cable Redundancy

Building redundancy into submarine cable routes is essential to ensuring the resilience and reliability of global communications networks. To bolster resilience, companies can design cable networks with redundancy in mind by ensuring each network node connects to at least two others, ensuring opportunities to reroute traffic when necessary.

OTHER TECHNOLOGIES

Low Earth Orbit (LEO) satellites can provide limited support during crises, but they cannot replace fiber networks, given their vastly smaller capacity than subsea cables, submarine cables can handle data rates measured in terabits per second, far outpacing the gigabits per second capability of LEO satellites and those in geostationary orbit (GEO). Moreover, LEO satellites still rely on terrestrial and subsea infrastructure for backhaul.

Submarine cables also offer much lower latency. Data in fiber-optic cables travels at two-thirds the speed of light, with transoceanic cables typically experiencing latency under 100 milliseconds. In contrast, GEO satellites, at 36,000 km above Earth, have a latency of 600-800 milliseconds. While LEO satellites positioned at 1,200 km reduce latency, they still experience higher delays than fiber connections, which are critical for real-time applications like video calls and virtual financial transactions.

In certain circumstances, satellites, microwave, or other technologies can, however, serve as valuable backup systems that allow traffic to be rerouted when primary cables sustain damage.

Additionally, agreements with other cable owners allow for traffic transfer between networks during outages.[15]

Typically, the private sector embarks on a submarine cable project when projected demand indicates that additional capacity and redundancy are necessary, as the cost of a single project can run into the hundreds of millions of U.S. dollars.[16] The cost of permitting and licensing is a non-trivial portion of this budget, requiring the retention of experts in a variety of fields to meet requirements, and inevitable delays create significant overages. The uncertainty disincentivizes investment and ultimately undermines resilience. While expanding the global network of cables is critical for meeting future demand and improving resilience, the high costs and slow permitting and licensing timelines often deter potential investors.[17] Streamlining permitting and licensing processes and regulatory oversight, while maintaining security standards, is necessary to address these challenges.[18]

In addition to the cost of permitting and licensing application, administrative hurdles for undersea cable projects have become increasingly intricate, with multiple layers of oversight across international, national, regional, and local jurisdictions. This level of complexity is unsustainable and must be streamlined to support future connectivity needs. Over the past few years, average permitting and licensing timelines in the United States have increased from under 12 months to more than three years.[19] The national security regime can result in a denial of a landing license after years of investment, although earlier guidance could redirect the cable operators to more palatable

---

[15] Congressional Research Service (CRS), *Protection of Undersea Telecommunication Cables: Issues for Congress*, Aug. 7, 2023, p. 3. https://crsreports.congress.gov/product/pdf/R/R47648.

[16] For example, the trans-Pacific Bifrost Cable System spans over 20,000 kilometers and is estimated to cost approximately $760 million. *See* Submarine Cable Networks, "Bifrost," (last accessed May. 22, 2025), www.submarinenetworks.com/en/systems/trans-pacific/bifrost.; The Southeast Asia-Middle East-Western Europe 6 (SEA-ME-WE 6) will span 19,000 kilometers and will cost an estimated $500 million. *See* Telecom Review, "The Vast Network Below: A Closer Look at Submarine Cable System Projects in Asia," Sept. 8, 2023, www.telecomreviewasia.com/news/featured-articles/3597-the-vast-network-below-a-closer-look-at-submarine-cable-system-projects-in-asia/.

[17] This paper treats permitting and licensing processes as a single administrative hurdle. Permitting processes typically address environmental or historical impacts on the physical environment by submarine cables, while licensing processes typically address security concerns regarding the submarine cable operator's activities. Governments can choose to treat these two regimes separately, depending on sovereign priorities.

[18] European Commission, *Recommendation on Secure and Resilient Submarine Cable Infrastructure*, (Brussels, 2024), pg. 5, https://ec.europa.eu/newsroom/cipr/items/822835/.

[19] Department of Homeland Security (DHS), Priorities for DHS Engagement on Subsea Cable Security & Resilience, Dec. 18, 2024, www.dhs.gov/publication/priorities-dhs-engagement-subsea-cable-security-resilience.

routes or partners.[20] This lack of transparency and predictability in the approval process further discourages investment, reducing opportunities for redundancy.

Some of the complexity stems from the multitude of agencies involved, with organizations operating under specific statutorily mandated priorities, such as historical or environmental preservation, national security, or other standards. They often impose conditions or modifications to address concerns such as landing site locations, cable protection, national security, and environmental preservation. They often operate without coordination, layering unnecessary redundancies into the licensing and permitting processes. In the US alone, it is estimated that no less than eleven agencies participate in the approval process for connecting a new cable, including federal entities with permitting and review responsibilities that apply to commercial undersea cables, agencies that may be engaged depending on specific impacts or locations of the cable project, and other technical expertise and protection roles related to subsea cables.[21] For the private sector, this creates a complex web of intersecting governmental interests, which is challenging to navigate for even the most experienced companies. Moreover, the opacity with which some agencies operate - some through necessity, some through choice - casts more uncertainty over the outcome than necessary.

Moreover, these agencies frequently lack sufficient understanding of existing cables and their repair and protection requirements, which ultimately can expose cables to greater risks. In some cases, challenges with permitting in specific areas have led to more geographic clustering that increases vulnerability to single points of failure. Lengthy and inefficient processes also can discourage trusted vendors from competing, creating space for untrusted providers offering significantly lower bids due to state-backed financial assistance.[22]

The permitting actions of one country can have implications for the connectivity of others. To maintain efficient connectivity and ensure seamless installation and repair of submarine cables, countries should align their permitting requirements with the United Nations Convention on the Law of the Sea (UNCLOS) principles, as recommended by the International Committee for the Protection of Cables.[23] Excessive jurisdictional assertions by neighboring countries risk impeding the

---

[20] The disposition of the landing license for the Pacific Light Cable Network (PLCN), after nearly 13,000 miles of cable had already been laid, is often cited as an example of stranded investment. *See* Peter Judge, "Google and Facebook Abandon US-China Cable Plan Over Security Fears," *Data Center Dynamics*, Feb. 7, 2020, www.datacenterdynamics.com/en/news/report-google-and-facebook-abandon-us-china-cable-plan-over-security-fears/; "*US-China Row Moves Underwater in Cable Tangle*," BBC, Jun. 18, 2020, www.bbc.com/news/world-asia-53088302.; Daphne Leprince-Ringuet, "Facebook and Google Drop Plans for Underwater Cable to Hong Kong after Security Warnings," *Zdnet*, Sept. 1, 2020, www.zdnet.com/home-and-office/networking/facebook-and-google-drop-plans-for-underwater-cable-to-hong-kong-after-security-warnings/.

[21] CRS, *Protection of Undersea Telecommunication Cables*, pg. 17.

[22] Matthew Goodman and Matthew Wayland, "Securing Asia's Subsea Network: US Interests and Strategic Options," *CSIS*, Apr. 5, 2022, www.csis.org/analysis/securing-asias-subsea-network-us-interests-and-strategic-options.

[23] United Nations (UN), *Convention on the Law of the Sea*, Dec. 10, 1982, https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf.; *See also* ICPC, *Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables Version 1.2*, (last accessed May 22, 2025), pg. 5, https://www.iscpc.org/documents/?id=3733.

development of new cables and the maintenance of existing ones, thereby undermining regional and global connectivity.[24] Coordination of international permitting and licensing regulations are also discussed below in the section on Legal Frameworks.

Easing permitting timelines and simplifying processes would accelerate development, deployments, and maintenance. By reducing these barriers, trusted vendors would face fewer delays, making it easier for them to deploy and maintain cables in a timely manner. Coordination of agencies would also cut down the complexity of these processes.[25] These improvements would not only encourage investment in submarine cables but also strengthen the resilience and security of global communications infrastructure by ensuring that reliable and secure providers can compete effectively on a global scale.

While streamlining permitting processes and adhering to international treaties can bolster the global supply of submarine cables, there are scenarios where laying multiple new cables is not commercially viable. For example, in remote islands, limited consumer demand and geographic isolation may make it financially impractical for private investors to finance additional cables. In such cases, local governments, partner nations, or development finance organizations should explore funding options for satellite-based solutions to strengthen local resiliency. These efforts can mitigate the risks of single points of failure and ensure reliable connectivity for isolated regions.

Recommendations: 1-3

II. Strategy for Cable Routes and Landing Stations

At a national level, development of an overarching strategy for multiple cable routes and landing points is critical to enhancing the resilience of submarine cable networks by ensuring that the impact of any incident is minimized. Redundancy enables the rerouting of data traffic if one segment has failed, enhancing network resilience, and reducing the incentive for malicious actors to disrupt networks, as the financial and operational impact is reduced.

At a global level, route diversity - the routing between two points over more than one geographic or physical path with no common points - is a common best practice.[26] At a national level, however, government and industry stakeholders must determine whether to pursue:

a) Diversification of cable pathways and landing stations
b) Concentration of cable pathways and landing stations with rigorously enforced government protections

---

[24] ICPC, *Government Best Practices*, pg. 8.

[25] As recommended by the EU. "Member States should be made aware of the usefulness to appoint an authority to facilitate and coordinate the permit-granting processes." *See* European Commission, *Recommendation on Secure and Resilient Submarine Cable Infrastructure*, pg. 5.

[26] CSRIC, *Clustering of Cables and Cable Landings*, Aug. 2016, pg. 4, https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG4A_Final_091416.pdf.

The clustering of cables and landing stations can heighten the risk posed by a single attack or accidental incident in the absence of rigorously enforced protections against fishing and anchoring. Thus, governments and industry stakeholders may choose to diversify routes and landings, which minimizes the impact of a single catastrophic incident. This is the case in the U.S. where pathways and landing points on the East Coast are increasingly diversified.

Yet diversification is not always possible. While cable routes and landings are carefully planned by cable owners and operators to reduce the impact of a single incident, areas such as the South China Sea, Taiwan Strait, and Baltic Sea face growing challenges from maritime disputes and increasing hostility from certain countries.[27] Coastal and marine environments are increasingly crowded, making it challenging to provide multiple pathways that won't intersect with fishing or anchoring. Many countries lack either sufficient coastline to support redundant cable routes or a centralized authority to effectively manage competing commercial and strategic interests. Companies may not want to land cables in areas without adequate connectivity or proximity to population centers.

Where route diversification is not feasible or practical, industry and government stakeholders have sometimes turned to concentrate pathways in Cable Protection Zones (CPZs) to reduce the risk of damage from other maritime activities. CPZs can restrict potentially harmful conflicts with other maritime activities like anchoring and fishing and should streamline permitting for new cables. Australia has implemented CPZs near Sydney and Perth, for instance, and New Zealand has identified ten CPZs, where anchoring and fishing are banned.[28]

There are valid concerns about the unintended risks of clustering cable infrastructure in narrow corridors. Mandatory CPZs and cable corridors may undermine resilience by limiting spatial separation between cables, for instance, making installations and maintenance more difficult, and increasing the chances that a single natural or man-made event could damage multiple cables.[29] Without a comprehensive and coordinated approach to marine spatial planning, it will become increasingly difficult to build and maintain the subsea cable network amid growing competition for limited seabed space. Integrating cable infrastructure planning into broader ocean governance frameworks is essential to balance commercial, environmental, and strategic priorities.

To mitigate these risks, ICPC recommends specific best practices for maintaining spatial separation during the installation and maintenance of cables, which are widely utilized by industry. These include adopting and enforcing minimum separation distances between cable ships and other

---

[27] CSIS, "Securing Asia's Subsea Network."

[28] Australian Communications and Media Authority (ACMA), "Rules for operating around submarine cables," (last accessed May 22, 2025), https://www.acma.gov.au/rules-operating-around-submarine-cables; Ministry of Transport, "Protecting New Zealand's Undersea Cables," (last accessed May 22, 2025), https://www.transport.govt.nz/about-us/what-we-do/queries/protecting-new-zealands-undersea-cables.

[29] "The Australian Maritime Safety Authority and the Fisheries Management Authority perform some surveillance of cable protection zones. But the cable owners and operators who responded to the same ACMA report unanimously indicated that current protection zone monitoring arrangements were unsatisfactory." *See* Jessica Woodall, "Australia's Vulnerable Submarine Cables," *Australian Strategic Policy Institute,* May 31, 2013, https://www.aspistrategist.org.au/australias-vulnerable-submarine-cables/.

vessels. A concentration approach also requires coordination across government agencies, to ensure that agencies approving fishing and shipping activities are familiar with submarine cables: their exact location, operational requirements, vulnerabilities, status as critical infrastructure, and the statutory and treaty protections that apply to them.[30]

Governments must also commit resources to enforcing protection measures and penalize non-compliance, which they've historically been reluctant to do. In 2021, for instance, the captain of the Maersk Surabaya was initially arrested on charges of negligent conduct for causing $1 million in damages to the Australia Singapore Cable.[31] Despite causing damage in the CPZ, the case was eventually dropped by the Australian Commonwealth Director of Public Prosecutions.

Thus, even with protections against accidental disruption, most governments will consider the concentration of risk too great, particularly if there are natural hazard risks to key pathways or they consider sabotage to be a realistic prospect.

Recommendations: 4-6

[30] ICPC, *Government Best Practices*, pg. 6.

[31] Paul Lipscombe, "Court Drops Case Against Ship Captain Blamed for Vocus Cable Cut," *Data Center Dynamics,* May 17, 2023, www.datacenterdynamics.com/en/news/court-drops-case-against-ship-captain-blamed-for-vocus-cable-cut/.; Jessie Jacob, "Let's take a close look at how we protect our undersea cables," *Australian Strategic Policy Institute*, Aug. 30, 2024, www.aspistrategist.org.au/lets-take-a-close-look-at-how-we-protect-our-undersea-cables/.

III. Repair Capacity

Ensuring continued robust repair capacity for submarine cables is critical to maintaining the resilience of global communications infrastructure. Prompt and efficient repairs minimize the duration and impact of disruptions, but several factors complicate the process, including cabotage restrictions, permitting requirements, port entry requirements, customs duties and fees, high costs, and limited repair capacity. Repairing damaged cables is a costly, complex, and time-consuming process, though most systems have well-stocked strategic repair supplies that enable repairs within two weeks, barring complicating factors such as weather, geopolitical tensions, remoteness of location, or other factors detailed below.

In 2023, there were 206 submarine cable repairs globally, with an average time of 21 days from the time a repair ship was notified to its deployment, and an average transit time of 7.5 days for the repair ship to reach its destination.[32] In the United States, an average of 3.3 repairs occurred annually. The primary causes of repair delays included multiple event delays (53%), prior repair backlogs (24.2%), operational delays (7.6%), permitting delays (6%), and unspecified delays (4.6%), while 4.6% of repairs faced no delays.[33] While the total number of repairs and repair vessels has remained relatively stable, the overall repair response time has nearly doubled, exacerbating the risks of prolonged disruptions. Addressing these challenges is essential to safeguard connectivity and ensure resilience of the broader submarine cable ecosystem.

Cabotage Restrictions: Many countries apply cabotage regulations, which typically govern the transport of goods and passengers between domestic ports, to submarine cable installation and repair. These requirements often mandate the use of domestically built, flagged, and crewed vessels, driving up costs, delaying urgent repairs, and at times compromising safety and efficiency.[34] Cable installation and repair do not involve transport between ports and therefore fall outside the traditional scope of cabotage.[35] These rules can undermine maintenance, delay critical repairs due to burdensome waiver processes, and even harm the connectivity of neighboring countries.

Countries should further refrain from classifying cable work as cabotage and avoid imposing vessel or crewing restrictions in territorial seas, archipelagic waters, and Exclusive Economic Zones. These restrictions are also inconsistent with international law, particularly UNCLOS Articles 79, 87, and 51, which affirm the freedom to install and maintain cables in these zones.[36]

Port Entry Requirements: In some jurisdictions, repair vessels are required to dock at domestic ports for regulatory clearance, even when no crew members embark or disembark. This requirement disrupts repair timelines, forcing delays in addressing critical damage. Eliminating

---

[32] ICPC, "Global Cable Repair Data Analysis," 2024, www.iscpc.org/events/2024-plenary-meeting/.
[33] *Ibid.*
[34] ICPC, *Government Best Practices*, pg. 8.
[35] ICPC, *Government Best Practices*, pg. 8.
[36] UN, *Convention on the Law of the Sea*, pg. 55.

unnecessary port entry requirements would reduce downtime for repairs and streamline operations, ensuring faster restoration of services in emergencies or other disruptions.[37]

Customs Duties and Fees: Customs duties, taxes, and fees imposed by certain states on submarine cable repair operations often treat these projects as revenue-generating opportunities. These charges not only increase the cost of capacity for users but can also discourage new cable landings, directly undermining government policies aimed at encouraging the development of cable infrastructure. Additionally, disputes over these financial obligations can lead to significant delays in both installation and repair processes. Governments should avoid levying customs duties, taxes, and fees on submarine cable installation and repair activities and remove tariffs on imported submarine equipment.[38] The most effective way to do so is through the establishment of free ports and bonded storage facilities.

Free ports[39] are designated areas where goods can be imported, stored, handled, or re-exported without being subject to standard customs duties, taxes, and certain regulations. Typically located near major transport hubs like seaports, airports, or national borders, free ports are designed to reduce customs barriers. When used in tandem with bonded storage facilities[40] – specialized warehouses that allow companies to store imported submarine cables under customs bond without immediate payment of duties – these zones can significantly improve the logistics of cable installation and repair. Given that submarine cables are often manufactured abroad, such facilities offer secure and cost-effective storage until materials are needed. Together, free ports and bonded storage provide an attractive framework for reducing costs, minimizing delays, and strengthening the resilience of undersea cable infrastructure.

In cases when the cable repair ship and associated spare plant are arriving from a foreign port, the process of clearing in and out should also be streamlined to avoid delays, ideally without the requirement of a port call. A small number of coastal states require an importation bond for the vessel to be issued by the ship operator or cable owner, which is the cause of significant delays.

Repair Capacity Constraints: While historically the number of specialized repair vessels has generally been sufficient to meet global demand, maintaining timely repair capabilities remains essential for submarine cable resilience. The fleet of dedicated repair ships is limited in size and geographically dispersed, which can lead to delays—particularly in remote or high-traffic areas. Although most repair operations are handled by trusted entities, a small number of providers with limited transparency have contributed to concerns about overreliance on a narrow vendor base. For

---

[37] ICPC, *Government Best Practices*, pg. 9.

[38] *Ibid.*, pg. 10.

[39] The Guardian, "What is a free port? All you need to know about the free-trade zones." Jul. 6, 2019, www.theguardian.com/politics/2019/jul/06/what-is-a-free-port-all-you-need-to-know-about-free-trade-zones-brexit.

[40] Maersk, "What is a bonded warehouse? Definition and benefits for your business." Sept. 6, 2024, www.maersk.com/logistics-explained/storage-and-warehousing/2024/09/06/bonded-warehouses-explained.

example, foreign-controlled firms like China's S.B. Submarine Systems (SBSS) participate in repair efforts in the North Pacific region. In a geopolitical crisis, uncertainty around the availability or willingness of certain providers to act swiftly could hinder timely restoration of damaged cables and impact regional connectivity.

The high cost and complexity of repair operations, coupled with the limited repair capacity, may necessitate government support in some instances. The U.S. established the Cable Security Fleet (CSF) in 2021, to ensure rapid response and repair capacity during emergencies. While this program strengthens U.S. capabilities, each new repair ship costs over $100 million, requiring a long-term commitment. Governments should ensure private sector involvement in developing public policy initiatives to boost repair, to understand the impact on current commercial arrangements as it may inadvertently reduce incentives for private industry to invest in and maintain commercial repair capacity.

A more balanced approach would be for governments and industry to collaboratively develop an emergency response capability, designed for targeted interventions in exceptional circumstances, such as major natural disasters or acts of sabotage. For instance, a government's military assets could be deployed in a limited and clearly defined capacity, depending on the nature of the threat or disruption. Together, governments and industry should establish a framework that defines potential triggers for emergency deployment and outlines the roles, responsibilities, and resources needed to respond effectively.

Supply Chain Constraints: The process can be further delayed if suitable replacement cable or other equipment is unavailable for the specific ocean floor topography. For example, repairing the 2022 break to the Tonga Domestic Cable Extension (TDCE) represented an extreme edge case, where supply chain and logistical challenges significantly led to a repair time of seven months.[41] While such cases are rare, they highlight the importance of maintaining sufficient repair stock and minimizing external delays to ensure rapid restoration.

Permitting Complexity: Countries should also streamline regulatory frameworks to enable efficient cable repair and installation without compromising security. This includes addressing permitting and liability regimes while avoiding reliance on untrusted vendors. While total repair numbers have risen slightly over the past decade, the repair rate per kilometer has declined. At the same time, the delay between fault notification and the start of repairs has doubled, primarily due to prolonged permit approvals from coastal state authorities—a challenge that has worsened over time.[42]

Addressing these regulatory and logistical barriers is essential to improving response times and strengthening the resilience of global communications infrastructure. Streamlined cabotage rules,

---

[41] Paul Lipscombe, "Tonga's Domestic submarine cable fixed 18 months after volcanic eruption," *Data Center Dynamics*, Jul. 14, 2023, www.datacenterdynamics.com/en/news/tongas-domestic-submarine-cable-fixed-18-months-on-from-volcanic-eruption/.

[42] ICPC, *A Global Comparison of Repair Commencement Times: Update on the Analysis of Cable Repair Data*, May 14, 2021.

simplified port entry requirements, and the elimination of excessive customs duties and fees are also critical steps towards fleet optimization thus strengthening the global submarine cable system's resilience.

Recommendations: 7-11

IV. Secure Supply Chains

Resilience is also reliant upon access to uninterrupted provision of the trusted components necessary for laying, repairing, and maintaining submarine cables. Without this, the redundancy and resilience of these networks will deteriorate, and chokepoints may emerge. Currently, most of the world's cable installation and repair services are concentrated among a few global and regional providers. The market is simply unable to support additional resources. Submarine cable operators often mitigate cable fault risks through regional or zonal cable maintenance agreements, pooling resources to secure cable ships that service vast multi-geographic areas, as there are no distinct national maintenance markets.[43] Further, no individual nation has sufficient cable repair demand to make a national solution commercially viable.

Beyond repair and operational risks, market dominance by untrusted vendors has even further implications. Authoritarian regimes, particularly China, can exploit this dominance to impose their vision of internet governance on global communications infrastructure. This issue parallels the challenges faced during the rollout of 5G communications when Chinese companies like Huawei and ZTE leveraged government subsidies to dominate the telecommunications market, especially in emerging economies. These risks prompted democratic nations to ban equipment from untrusted vendors, culminating in expanded commitments to secure telecommunications and subsea cables by the G7 in 2024 and the Quad partnership in 2023.[44]

China continues to lead in advanced optical communications research, producing 37.7% of the field's research compared to just 12.8% from the U.S., underscoring the urgency for democratic nations to restrict high-risk vendors from developing and controlling optical core network infrastructure.[45] Governments must prioritize mapping risks within submarine cable supply chains, ensuring redundancy, and reorienting these supply chains to mitigate vulnerabilities. There is a critical need for increased research and development outside of China to diversify technological innovation and reduce dependency on a single country.

Collaboration between cable operators and governments to mitigate these risks is equally critical. Governments should work with industry to map the supply chain for submarine cable installation

---

[43] ICPC, *Government Best Practices*, pg. 9.

[44] Alex Botting and Ines Jordan-Zoob, "Competing Visions for the Future of the Internet: China's Strategy to Control the Highways of Connectivity," *Wilson Center*, May 9, 2024, www.wilsoncenter.org/article/competing-visions-future-internet-chinas-strategy-control-highways-connectivity.

[45] Dr. Jennifer Wong Leung et al., "ASPI's Critical Technology Tracker," *Australian Strategic Policy Institute,* Mar. 1, 2023, www.aspi.org.au/report/critical-technology-tracker.

and repairs to identify potential choke points or areas of reliance on untrusted vendors. Sharing risk and incident data fosters the identification of patterns, gaps in existing protection measures, and areas where resilience can be enhanced. It also aids in the detection and prevention of malicious activities by state and non-state actors. By integrating risk assessments, advanced security technologies, and collaborative data-sharing efforts, governments and operators can significantly bolster the resilience of undersea telecommunications networks.

Recommendations: 12-14

SECURING SUBMARINE CABLES

Since the construction of the first submarine cable between England and France in 1850, physical damage to cables has been a common issue. While the number of cables deployed has increased significantly, the number of cable cuts has grown at a much slower rate, due to public-private efforts to reduce cable breaks. Today, as discussed earlier, there are 150 to 200 cable cuts reported globally each year, with the primary causes being accidental human activities such as fishing and anchoring, alongside natural hazards like volcanic eruptions, earthquakes, and tsunamis.[46] These persistent risks highlight the ongoing need for public-private efforts, such as cable awareness programs, ensuring that key maritime stakeholders, such as fishers and vessel operators, are aware of cable locations to prevent accidental damage.

Additionally, there has been growing attention on the security of submarine cables due to their critical role in economic, military, and public security, particularly in light of heightened geopolitical tensions. While these concerns are valid, they are not unique to submarine cables but apply broadly to all communication networks. Overall, the primary risks to submarine cables remain accidental and natural disruptions, rather than direct threats to data confidentiality and availability. Reducing these incidents is critical to identifying truly malicious actions.

Governments and industry are already addressing security risks in multiple workstreams. Recognizing ongoing efforts is necessary to deconflict and coordinate public policy initiatives that will yield actual benefits.

I. Physical Security of Cables

Submarine cables are designed to endure extreme pressure, stress, and various known threats. A typical cable measures approximately 20 millimeters in diameter, with more heavily protected

---

[46] United Nations, “International panel set up to help protect undersea cables,” Nov. 29, 2024, www.unognewsroom.org/story/en/2441/submarine-cable-resilience-itu-29-november-2024.

versions reaching 50 millimeters.[47] Several layers of insulation and protection cover the fibre optic strands that form the transmission medium at the core of the cable to protect them from the harsh marine environment.[48]

While most submarine cables rest directly on the seafloor for the majority of their deployment, they are often buried as they get closer to shore. According to the United States' National Oceanic and Atmospheric Administration (NOAA), cables are usually buried between 0.6 and 1.5 meters beneath the seabed in water shallower than 2,000 meters[49]. Despite these precautions, submarine cables are not impervious to damage. Physical damage from external events remains a significant risk. These incidents have various causes, including damage caused by natural hazards, accidental human activity, and intentional human activity.

Natural Hazards: Just as wildfires, storms, landslides, and earthquakes cause damage to terrestrial fiber-optic cables, natural hazards in the marine environment can pose similar risks to submarine fiber-optic cables. While more infrequent than accidental damage, submarine cables have been disrupted by volcanic eruptions, earthquakes, tsunamis and strong waves, ocean currents, and underwater landslides.[50]

Accidental Human Disruption: Since submarine cables are not visible from the water's surface and can be mischarted, their presence is not always apparent to vessels. Combined with error or carelessness from some maritime operators, accidental submarine cable cuts occur routinely. Today, 70 percent of global damage to submarine cables is caused by fishing and anchoring.[51] Ships can damage a submarine cable during anchoring, either by deploying the anchor directly onto it, dragging the anchor across it as it tries to secure itself,[52] or accidental anchor deployment while underway.[53] Similarly, fishing vessels can damage submarine cables when using specialized equipment such as trawl otter-boards, beam trawls, scallop dredges, clam dredges, and net anchors.

---

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

[48] *Ibid.*

[49] National Oceanic and Atmospheric Administration, "Submarine Cables - Domestic Regulation," (last accessed Feb. 25, 2025). www.noaa.gov/general-counsel/gc-international-section/submarine-cables-domestic-regulation.

[50] For instance, on March 14, 2024, the Wacs cable off the west coast of Africa, along with three other submarine internet cables—Sat-3, Ace, and MainOne—was severed due to a suspected subsea seismic event near the Ivory Coast. This caused widespread internet disruptions across the region, including parts of South Africa. Fortunately, much of the traffic was quickly rerouted, and repairs were completed by April 30, 2024. Tech Central, Severed West African Internet Cables Repaired, April 30, 2024. *See* Duncan McLeod, "Severed West African internet cables repaired," *Tech Central,* Apr. 30, 2024, https://techcentral.co.za/west-african-internet-cables-repaired/243767/.

[51] ICPC, *Government Best Practices*, pg. 1.

[52] ICPC, Catch Fish. Not Cables, (last accessed Feb. 25, 2025), www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.iscpc.org/documents.

[53] Mick Green and Keith Brooks, "The Threat of Damage to Submarine Cables by the Anchors of Ships Underway," (last accessed April 9, 2025), https://cil.nus.edu.sg/wp-content/uploads/2011/04/Mick-Green-and-Keith-Brooks-The-Threat-of-Damage-to-Submarine-Cables-by-the-Anchors-of-Cables-Underway.pdf.

Fish Aggregation Devices (FADs) present an emerging risk to submarine cables. FADs, which are used to attract fish, can damage cables during installation or repair due to abrasion from mooring lines or when FAD anchors are placed on or drift over a cable. The industry works actively to mitigate these risks through cable awareness campaigns and close collaboration with regulators. However, stronger government support—particularly through improved regulation and enforcement—would further enhance these efforts. As novel maritime activities such as deep-sea mining expand, proactive policies will be essential to protect this infrastructure.[54]

Several mitigations are available and are being utilized to address these risks, particularly those related to accidental and intentional human activities. The most obvious measure is armoring cables for tensile and impact resistance. While all submarine cables have some degree of armoring, those in shallow waters closer to shore often have additional layers.

Beyond physical reinforcement, Automated Identification Systems (AIS) has served to prevent accidental damage as well. Initially designed as a safety mechanism for vessels to avoid collisions, it can be used to provide real time information about a vessel's identity, type, position, course, speed, and navigational status.[55] While AIS remains most useful for investigating incidents after they occur and identifying responsible parties, its real-time alerting and prevention capabilities have made a substantial impact in improving cable protection worldwide.

While AIS use is mandatory for vessels of a certain size, it does not provide perfect visibility into maritime activity. Many vessels turn off AIS to evade detection while illegally fishing in protected areas or to hide lucrative fishing spots from competitors.[56] More significantly, AIS relies on VHF transmission, which has a limited range and is prone to dropouts and dead zones, particularly in remote areas. Improved enforcement of AIS regulations, alongside the adoption of a more robust monitoring system, would help prevent accidents by alerting vessels when they are near cables.

A more advanced vessel monitoring system is needed, however. Vessel Monitoring Systems (VMS), a satellite-based tracking technology primarily used to monitor commercial fishing vessels could fulfill this function. Unlike AIS, which relies on VHF signals, VMS offers continuous, near perfect tracking through onboard transceivers that transmit vessel ID, time, and location via satellite.[57] In the United States, over 4,000 vessels are monitored this way, making it the largest national VMS fleet.[58] VMS is already used to manage protected areas, verify fishing activity, and support enforcement programs. Its capabilities make it well-suited to strengthen protections around submarine cables, especially in

---

[54] International Seabed Authority, (ISA), *Submarine Cables and Deep Seabed Mining*, Mar. 10, 2015, www.isa.org.jm/wp-content/uploads/2022/06/techstudy14_web_27july.pdf.

[55] United States Coast Guard, "AIS Frequently Asked Questions," (last accessed Feb. 25, 2025). www.navcen.uscg.gov/ais-frequently-asked-questions.

[56] Oceana, "Avoiding Detection: Global Case Studies of Possible AIS Avoidance," Mar. 2018, oceana.org/reports/avoiding-detection-global-case-studies-possible-ais-avoidance/.

[57] Northwest Atlantic Fisheries Organization, "Vessel Monitoring System," (last accessed Jun. 8, 2025), https://www.nafo.int/Fisheries/ReportingRequirements/VMS.

[58] NOAA Fisheries, "Enforcement: Vessel Monitoring," (last accessed Jun. 8, 2025), https://www.fisheries.noaa.gov/topic/enforcement/vessel-monitoring.

remote or AIS-blind zones, by enabling real-time alerts when vessels approach sensitive routes. Importantly, VMS data can help identify vessels involved in damaging activities, whether accidental or intentional.

To enhance accountability, likeminded governments should explore requiring all vessels to activate VMS when entering their Exclusive Economic Zones. This would establish a clear expectation of visibility and create legal liability for vessels that disable tracking and cause harm to undersea infrastructure. When combined with AIS, physical protection, and emerging fiber sensing technologies, VMS can significantly bolster global efforts to safeguard critical subsea cables.

Recommendations: 15-17

II. Physical Security of Cable Landing Stations

Of the 1.5 million kilometers of submarine fiber-optic cables laid around the world, all are connected to land at least two of an estimated 1,400 cable landing stations (CLS).[59] These shoreline facilities serve as the link between subsea and terrestrial telecommunications infrastructure – such as satellite links, fiber optic cables, and microwave towers – which deliver information to data centers or end users.

As with submarine cables and other types of terrestrial critical infrastructure, CLS facilities are vulnerable to damage from natural hazards such as hurricanes, storms, wildfires, and earthquakes. While they face lower risk of damage from accidental human activity compared to submarine cables, CLS facilities face similar risks from malicious actors. A 2017 report, entitled Threats to Undersea Cable Communications, sponsored by the United States Department of Homeland Security (DHS) and Office of the Director of National Intelligence (ODNI), highlights threats to CLS facilities, noting that "landing stations are the most accessible and impact-rich targets."[60]

While the capacity coming into the CLS cannot be rerouted, in most circumstances internet traffic can bypass the CLS and submarine cable entirely by being rerouted via terrestrial cables to other facilities and subsea cables. However, damage to a CLS facility may cause broader service disruptions if it connects multiple submarine cables, as is the case with most modern facilities.[61] CLS facilities inherently represent a shared risk, and responsible network builders prioritize resilience by deploying multiple cables and diverse connections.

Due to the relative ease of implementing physical protections and establishing jurisdictional oversight, protection of CLS facilities is more straightforward and more mature than that of submarine cables. Standard industry practice includes a variety of mitigation measures for CLS

---

[59] Niva Yadav, "What is a cable landing station?" *Data Center Dynamics,* Sept. 2, 2024, www.datacenterdynamics.com/en/analysis/what-is-a-cable-landing-station/.

[60] CRS, *Protection of Undersea Telecommunication Cables*, pg. 6.

[61] Data Center Dynamics, "What is a cable landing station?"

facilities, such as physical security protocols like surveillance systems, access controls, and intrusion detection. Additionally, ensuring the resilience of these facilities against natural disasters and potential disruptions to supporting infrastructure, such as energy supply, is a key part of their protection strategy.

Recommendations: 18

III. Interception of Data on Cables or at Landing Stations

Given the technical complexity of this type of espionage, the theoretical risk is unlikely to be implemented in practice at this time for three reasons. Firstly, it takes significant resources both to access the cable and siphon off that volume of data at scale. Secondly, the volume of data generated would create a 'needle in a haystack' problem for the adversary in which decryption, categorization, and identification of relevant information is all but impossible. Thirdly, even if those challenges could be solved by a highly resourced nation state actor, the act of 'tapping' a cable itself would have an anomalous impact on the cable, likely making it detectable.

Pre-Deployment Tampering: Before cables are laid, there is a theoretical risk that vulnerabilities could be introduced during the manufacturing process. Similarly, cable repair components stored in depots, often with less stringent security than cable landing stations, could, in principle, be targeted for tampering. For example, one of the largest cable depots serving the Asia-Pacific region is the Wujing Depot, located in China. While there is currently limited public evidence of exploitation, the long-term storage of components in jurisdictions of strategic concern warrants continued vigilance and mitigation of any supply chain risks.

Post-Deployment Tampering: The complexity of cable tapping operations is high. It is far simpler to interfere with cables at their connection points with CLS facilities than underwater. Despite this, some security experts have raised concerns that nation-state actors could tamper with cables at sea. Recently, U.S. officials have warned that vessels operated by S.B. Submarine Systems (SBSS) – a state-controlled Chinese company that repairs submarine cables – have been deactivating their AIS transponders while operating off the coasts of Taiwan, Indonesia, and other Asian countries.[62] Additionally, concerns have been raised about the recent travel by a Chinese research vessel, Tan Suo Yi Hao, along Australia's western and southern coastlines, with mapping of the routes of Australia's cables a likely objective.[63]

---

[62] Daniel Runde et. al., *Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition*, CSIS, Aug. 2024, pg. 4., www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition.

[63] Samantha Dick and Stephen Dziedzic, "Dutton says Chinese research ship is collecting intelligence, mapping undersea cables," *ABC News,* Mar. 31, 2025, www.abc.net.au/news/2025-04-01/dutton-says-chinese-research-ship-mapping-undersea-cables/105122068.

Tapping an undersea cable requires resources that, likely, can only be marshalled by a nation-state. Because of the depth of the cable, such an operation would require a submarine or similar pressure-tolerant diving equipment. Additionally, the amount of data from even a small tap would likely require a storage system on the scale of a major data center as modern cables can transmit data at 320 Tbps. Moreover, any attempts to tamper with the cable undersea would likely create anomalies in the light passing through the cable, which would be captured by the modems. While tapping an undersea cable is not impossible, such an effort would require significant resources and risks easy detection, such that the efforts of adversarial nation states would likely be directed toward more accessible targets.

Further traffic traveling across modern subsea cables is largely encrypted. Concerns over the security of encrypted traffic have been raised due to the concept of "harvest now, decrypt later" operations.[64] Such an operation involves a malicious actor, most likely a nation-state, collecting large amounts of encrypted data that rely on traditional encryption protocols, rather than post-quantum cryptography (PQC). The actor stores this data until a quantum computer cable of breaking the encryption becomes viable. The storage capacity needed to retain up to 320Tb of data per second travelling across submarine cables, however, would overwhelm the resources of even the most well-resourced actors.

Furthermore, mitigations can be implemented to protect against manipulation or exfiltration of data from terrestrial and submarine cables. For example, to protect against "harvest now, decrypt later" operations, data owners should ensure appropriate encryption protocols are in place to encrypt data in transit, potentially including a plan to transition to quantum-resistant algorithms. The responsibility for protecting the confidentiality and integrity of data should reside with data owners to ensure that data is protected wherever it is in transit, not just when transiting subsea cables, and to avoid creating a systemic single point of failure. This ensures that even if a malicious actor gains access, decoding that data would be significantly more difficult.

Ultimately, however, given the vast resources required and without a clear path to generating usable information the risk associated with cable 'tapping' remains very low.

Recommendations: 19-21

IV. Emerging Detection Capabilities

While the previous sections focus on potential risk to subsea cable technology, an emerging technology - fiber sensing - can also play a role in improving real-time incident detection. Fiber sensing leverages the optical transmission technology used by modern fiber-optic cables to send information between endpoints. In these cables, data is transmitted through the optical fiber core

[64] K. F. Hasan *et al.*, *A Framework for Migrating to Post-Quantum Cryptography: Security Dependency Analysis and Case Studies,* IEEE Access, Feb. 16, 2024, pg. 23431, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10417052.

by a modulated laser that generates an electromagnetic field. The oscillation direction of the electric field, known as the State of Polarization (SOP), changes as the light propagates. The SOP is sensitive to external stimuli, such as the pressure and physical movements experienced by the fiber, which causes it to fluctuate. Fiber sensing technologies integrated into modems can monitor and detect variations to the SOP. By analyzing these changes, operators can gain valuable insights into the physical movements or disturbances affecting the cable, enabling real-time detection of tampering or damage.[65]

Beyond detecting damage to cables after they have gone offline, fiber sensing can provide insights into underwater activity in the vicinity of submarine cables. This could improve investigations, support attribution of incidents, and ultimately increase accountability, thereby enhancing deterrence. Additionally, fiber sensing can serve as an early warning system for natural hazards. For example, changes in the SOP of a particular submarine cable caused by an underwater earthquake could provide information to early warnings of tsunamis, allowing governments to mitigate harms to populated areas.

However, while fiber sensing may significantly enhance situational awareness and cable protection, its deployment raises important legal considerations. Adding fiber sensing to a cable may reclassify it from a purely telecommunications cable to a measurement device. This distinction has implications under UNCLOS, as non-telecommunications cables do not enjoy the same freedoms related to installation and maintenance. To enable the widespread use of fiber sensing on cables crossing such jurisdictions, further clarification of UNCLOS provisions will be necessary to avoid regulatory conflicts and ensure continued compliance with international law.

Recommendations: 22-23

[65] Brian Lavallee, "Detecting Undersea Earthquakes with Cross-Industry Collaboration," *Ciena*, Feb. 22, 2024, https://www.ciena.com/insights/articles/2022/detecting-undersea-earthquakes-with-cross-industry-collaboration.

LEGAL & INSTITUTIONAL FRAMEWORKS

Legal and institutional frameworks play a critical role in reinforcing risk mitigation and deterrence. If designed effectively, these frameworks can serve as a catalyst for security and resilience measures by promoting awareness of risks, enhancing multi-stakeholder coordination, reducing instances of unintentional disruption, and adequately deterring acts of aggression.

A particular challenge for the governance of the submarine cable ecosystem is its inherently cross-border and multi-stakeholder nature. The 2Africa cable, for example, lands in 33 countries, travels through the EEZ of others, and traverses the High Seas, where no single country has jurisdiction. This makes for a uniquely complex jurisdictional environment for ensuring the protection of the cable as a whole. It necessitates both coordination at an international level, and consistent implementation of best practices at a national level.

Likewise, private sector prevalence across the ecosystem necessitates a multi-stakeholder approach to security and resilience. As of December 2020, 81% of cables were owned solely or partially by private companies.[66] Effective institutional frameworks for the submarine cable ecosystem must ensure private sector participation. These frameworks can be broken out to promote three distinct objectives:

1. Ensuring that domestic laws and policies are sufficient to address risks; and
2. Promoting collaboration among international partners to identify and respond to threats that exist outside of any single jurisdiction; and
3. Facilitating and intensifying coordination with non-governmental stakeholders to promote more efficient regulatory processes, trusted vendor awareness of opportunities and threats and the private sector implementation of security best practices.

I. Domestic Legal Frameworks

Firstly, it is important to recognize that the submarine cable industry already treats submarine cables and associated infrastructure, such as cable landing stations, as critical infrastructure. Owners and operators proactively implement robust risk assessment, mitigation, and recovery strategies as standard practice. Rather than imposing additional layers of oversight, what is most needed from governments is collaborative engagement and flexibility to support continuous improvement in industry-led security mitigation efforts.[67]

---

[66] Justin Sherman, *Cyber Defense Across the Ocean Floor: The Geopolitics of Submarine Cable Security*, The Atlantic Council, Sept. 2021, pp. 22. www.atlanticcouncil.org/wp-content/uploads/2021/09/Cyber-defense-across-the-ocean-floor-The-geopolitics-of-submarine-cable-security.pdf.

[67] The U.S. Department of Homeland Security recently issued a whitepaper signaling such an intention to seek deeper collaboration with the private sector on submarine cables. *See* DHS, Priorities for DHS Engagement on Subsea Cable Security & Resilience; Similarly, the EU issued a Recommendation recognizing the private sector's role in deployment and seeking to improve the permitting and financing environments for submarine

To that end, governments can play a constructive role by enhancing transparency around national security priorities. For example, publishing clear guidance on high-risk countries, prohibited equipment, and entities and countries of concern would help infrastructure operators make informed decisions and align with broader national security objectives. This type of partnership-oriented approach, grounded in information sharing and strategic alignment, can strengthen collective resilience without adding unnecessary regulatory layers. While countries such as the U.S., U.K., Australia, and Singapore have acknowledged the importance of submarine cables in their critical infrastructure frameworks, others—particularly in Europe—could further support the industry by adopting similarly collaborative, guidance-driven models.

Secondly, ratifying and implementing national obligations under 1884 and UNCLOS. Article II of the former states that it's "a punishable offence to break or injure a submarine cable, willfully or by culpable negligence, in such a manner as might interrupt or obstruct telegraphic communication, either wholly or partially."[68] Article 113 of UNCLOS, meanwhile, requires countries to adopt laws to punish people or ships under its jurisdiction for damaging or breaking submarine cables on the high seas, whether "done willfully or through culpable negligence."[69] Moreover, Article 21 of UNCLOS, allows (but does not require) states to implement laws governing their territorial waters for "the protection of cables and pipelines."[70]

While on the surface this provides a robust enforcement framework, in reality it is highly dependent upon states implementing and enforcing laws for protecting cables within their territorial waters, which many do not. It's also dependent upon states taking legal action against people or ships that breach cables on the high seas, which they may not where the victim is a geopolitical adversary. Efforts to address the latter challenge through a more robust international governance framework are discussed in the section below. States can and must, however, address the former challenge in a timely fashion.

Thirdly, enforcing IMO-required use of Automatic Identification Systems (AIS). AIS is required to be fitted and used by "ships of 300 gross tonnage and upwards engaged on international voyages, cargo ships of 500 gross tonnage and upwards not engaged on international voyages and all passenger ships."[71] Yet according to a recent study, "enforcement of AIS laws is generally poor, and

---

cables. *See* European Commission, "EU Improves Submarine Cable Security and Resilience," Mar. 16, 2024, https://ec.europa.eu/newsroom/cipr/items/822835/.

[68] *1884 Convention for the Protection of Submarine Telegraph Cables*, Mar. 14, 1884, p. 2, https://cil.nus.edu.sg/wp-content/uploads/2019/02/1884-Convention-for-the-Protection-of-Submarine-Telegraph-Cables-1.pdf.

[69] UN, *Convention on the Law of the Sea*, pg. 64.

[70] Ibid., pg. 31.

[71] International Maritime Organization (IMO), "AIS Transponders," (last accessed May 23, 2025), www.imo.org/en/OurWork/Safety/Pages/AIS.aspx#:~:text=The%20regulation%20requires%20AIS%20to%20be%20fitted,and%20all%20passenger%20ships%20irrespective%20of%20size.&text=Ships%20fitted%20with%20AIS%20shall%20maintain%20AIS,provide%20for%20the%20protection%20of%20navigational%20information

… sanctions are not severe enough to act as deterrents."[72] With limited global enforcement of requirements, however, many deactivate AIS to evade detection while illegally fishing in protected areas or to avoid revealing lucrative fishing areas to competitors.[73]

Finally, governments should ensure coordinate use of the territorial seabed. This can be done by mandating educational programs for maritime employees via local marine and fishing authorities, to ensure they are aware of key cable pathways, charting requirements, and measures to avoid accidental disruption. These programs should include training on how to properly use nautical charts issued by government hydrographic offices in line with International Hydrographic Organization (IHO) recommendations. By enhancing familiarity with these tools and reinforcing their use, mariners can better navigate around sensitive infrastructure. Where fishing vessels are negligent in applying these measures, penalties should be enforced—even in cases of accidental disruption—to promote accountability and incentivize adherence to best practices. As offshore wind farms and other interests enter territorial waters, governments should balance protection of communications cables with the other interests.

Due to the inherently cross border nature of submarine cable infrastructure, the implications of implementing these best practices - or failing to do so - have implications for other countries. Thus, it's important not only that like-minded governments enforce them domestically but encourage, and support from a technical perspective, the implementation by partner governments at a domestic level. Beyond the implementation of legal frameworks, this must include penalties for non-compliance that are sufficient to deter such behavior.

Recommendations: 24-29

II. International Collaboration

In addition to establishing legal frameworks and prosecuting criminal activity, effective deterrence necessitates the ability to monitor, intercept, and penalize vessels that may cause disruption within the territorial sea. The challenge, however, is that the cable ecosystem covers such vast territory that it would require an unfeasible number of resources for countries to patrol individually.

Likeminded governments should leverage existing security mechanisms such as NATO or the Quad to establish a multilateral mechanism for conducting patrols, focused in particular on high-risk areas. These include regions that are experiencing acute geopolitical instability (e.g. Baltic Sea), have cables that are more physically exposed (e.g. Red Sea), or are key fulcrums for the global ecosystem (e.g. Straits of Malacca).

---

[72] Priyal Bunwaree, *The Illegality of Fishing Vessels 'Going Dark' and Methods of Deterrence*, Cambridge University Press, Jan. 11, 2023, pg. 191, www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/illegality-of-fishing-vessels-going-dark-and-methods-of-deterrence/8E5D5C30A15C91BF17423ED1EF6EE0E2.

[73] Oceana, "Avoiding Detection Global Case Studies."

Supporting these efforts, governments should establish or expand mechanisms for intelligence-sharing with trusted partners to pre-empt potential attacks, adapt patrol activities accordingly, and to support the evidentiary body needed to convict saboteurs. While the private sector has proven itself adept at ensuring continuity of service during past outages, only governments working in partnership with industry can conduct the kind of operational activities needed to deter acts of international negligence or aggression.

Beyond operational collaboration, there are critical gaps in the existing international legal architecture for submarine cables. Even if likeminded countries enforce their obligations under 1884 and UNCLOS at a domestic level, state actors can opt not to impose penalties on ships bearing their flag that engage in sabotage on the High Seas. As we enter an increasingly hostile geopolitical environment, governments must seek to address this vulnerability if we are to prevent its exploitation.

As recent disruptions in the Baltic Sea and Taiwan Strait have demonstrated, existing legal frameworks in many countries make it highly challenging to intercept, investigate, or prosecute security incidents, even where governments suspect intentional foul play.[74] This is in part due to the remote nature of the infrastructure, in part due to the failure to implement domestic legal frameworks which are fit for purpose. Whether these incidents are deemed to be accidental or intentional acts of sabotage, our inability to address acts of sabotage if and when they occur reduces our ability to deter such behavior. Governments must develop multilateral legal frameworks sufficient to deter or punish both accidental and intentional disruptions, by implementing the following measures.

The most likely avenue for doing so however, may not be through an amendment to UNCLOS, the process for which remains untested and would likely face obstruction from China or Russia. Rather, likeminded countries should consider other plurilateral mechanisms for doing so.

Given that all countries rely upon uninterrupted operation of global submarine cable infrastructure to meet their connectivity needs, there should be broad international support for the prevention and prosecution of sabotage. Even if certain major powers declined to participate in such negotiations, it would nevertheless set an important global norm which could be enforced by signatories.

We should, however, be realistic about the timeline for completion of such an international agreement. UNCLOS took 15 years to negotiate[75] and, while a narrowly tailored agreement should be more efficient, it's nevertheless a medium- to long-term objective.

---

[74] Miranda Bryant, "Sweden says China denied request for prosecutors to board ship linked to severed cables," The *Guardian*, Dec. 23, 2024, www.theguardian.com/world/2024/dec/23/china-refused-investigation-into-ship-linked-to-severed-baltic-cables-says-sweden.

[75] Gabriele Goettsche-Wanli, "The United Nations Convention on the Law of the Sea: Multilateral Diplomacy at Work," United Nations, Dec. 28, 2014, www.un.org/en/chronicle/article/united-nations-convention-law-sea-multilateral-diplomacy-work.

Recommendations: 30-31

III. Multi-Stakeholder Coordination

Government and industry stakeholders have a shared interest in promoting the security and resilience of submarine cable infrastructure. Yet, in most countries, formal mechanisms for public-private coordination remain limited. This misses an opportunity to ensure that stakeholders are well-informed about threats and opportunities and are aligned with national security objectives. To remedy this, governments should take steps to formalize their private sector engagement. These efforts should initially focus on three areas:

Establish a Single Point of Contact (SPOC) for private sector engagement: As discussed above, in most governments, multiple agencies have responsibility for some aspect of submarine cable resilience. Their remit may cut across environmental, strategic, commercial, or security considerations. Their authorities may encompass new cable approvals, repair and maintenance activities, or critical infrastructure protection.

Governments can reduce these inefficiencies, while continuing to meet desired security outcomes, by appointing a SPOC responsible for engaging companies as they navigate regulatory processes. Their role would not prevent direct engagement with individual agencies. Rather, this office would serve as the primary external liaison to private entities and internally drive maximum efficiency and transparency of the process. Singapore, for example, has addressed this issue by designating its telecoms regulator, the Infocomm Media Development Authority (IMDA), as the point of contact for submarine cables, even if other government bodies have ultimate responsibility for a particular issue.[76]

Establish two-way threat intelligence sharing with private stakeholders: The prevalence of private companies in deploying, delivering, maintaining, and securing critical infrastructure assets necessitates multi-stakeholder threat intelligence sharing. This enables public and private organizations to benefit from information, analysis, and context that they would not be privy to individually and provides an early warning system against potential threats. Beyond direct information about tactics, techniques and indicators of compromise, such organizations enable the development of a common understanding of the threat environment and what steps need to be taken to mitigate risks.

For this reason, it has become best practice for governments or industry collectives to establish threat information sharing organizations across critical infrastructure sectors. Governments that do not have such mechanisms in place should establish them, collect threat information from the private sector and, to the extent possible, use governments' own understanding of the threat environment to enrich and share out to trusted stakeholders critical threat intelligence.

---

[76] ICPC, *Government Best Practices*, p. 6.

Enhance transparency around trusted vendors: Within telecommunications infrastructure untrusted vendors have persistent success in winning contracts to manufacture, deploy and manage critical network infrastructure. While this is less acute in submarine cable networks than in Radio Access Networks, organizations like HMN continue to leverage significant Chinese government subsidies to undercut bids from competitors by up to a third.[77] For example, HMN was initially selected in early 2020 to manufacture and lay the South East Asia–Middle East–Western Europe 6 (SeaMeWe-6) cable, which will connect a dozen countries as it extends from Singapore to France. The SeaMeWe-6 cable would have been HMN's largest project to date, solidifying the expanding reach of three Chinese telecom firms that had planned to invest in it.[78] However, due to U.S. government concerns over potential Chinese espionage on these critical communications cables, the contract was granted to US-based SubCom.

China has since countered these developments with a $500 million investment into the PEACE (Pakistan and East Asia Connecting Europe) cable, a direct competitor to SeaMeWe-6. With over 15,000 km already in operation and plans to extend beyond 25,000 km, PEACE promises even greater bandwidth to participating nations.[79] These developments demonstrate the escalating geopolitical tensions over subsea cable infrastructure, as both powers seek to expand their influence.

While matching these bids dollar-for-dollar may not be a feasible long-term solution, like-minded governments can reduce the strategic advantage of untrusted vendors by publishing clear guidance on high-risk equipment, entities of concern, and trusted suppliers. This transparency would help infrastructure operators make informed procurement and partnership decisions early in the planning process and ensure alignment with broader national security objectives. Such guidance can also deter the use of untrusted vendors by signaling potential risks and consequences, while supporting trusted vendors in producing competitive, security-aligned bids.

---

[77] Joe Brock, "US and China wage war beneath the waves - over internet cables," *Reuters*, Mar. 24, 2023, https://www.reuters.com/investigates/special-report/us-china-tech-cables/.

[78] Saf Malik, "All Aboard SEA-ME-WE6," *Capacity*, May 19, 2023, www.capacitymedia.com/article/2boihe41ommbeopfcmvb5/big-interview/all-aboard-sea-me-we-6.

[79] Azhar Azam, "The Geopolitics of Cables: The US and China's Subsea War," *Fair Observer*, Dec. 17, 2024, www.fairobserver.com/politics/the-geopolitics-of-cables-us-and-chinas-subsea-war/.

Establish 1.5 track dialogues within existing regional and security dialogues: Leveraging existing security and regional groupings, including the Quad, transatlantic security alliances, the United States and allied governments should integrate submarine cable security and resilience into its international discussions bringing trusted industry partners into the fold for these dialogues where feasible. The Quad Partnership for Cable Connectivity and Resilience is an obvious vehicle for this, along with Australia's Indo-Pacific Cable Connectivity and Resilience Program focused on commissioning technical and policy research, sharing best-practice frameworks, and providing essential technical assistance. Embedded within this strategy, formal 1.5 track dialogues with trusted industry partners will be instrumental in harmonizing insights, aligning security protocols across diverse regions, and enhancing threat intelligence sharing.

Recommendations: 32-34