Redundancy, Resiliency, and Repair
Securing Subsea Cable Infrastructure

KEY TAKEAWAYS

- Global subsea cable networks are subject to cross-cutting threats and obstacles, including accidental cuts by fishing and other commercial vessels and natural disasters, as well as permitting and regulatory issues that slow or halt the laying of new cable or the repair of damaged cable. Likewise, threats from state and nonstate actors make subsea cables subject to wider strategic and geopolitical competition. This combination of challenges and threats makes cable redundancy, resiliency, and repair critical policy priorities.
- In the United States, no single agency is currently responsible for coordinating the redundancy, repair, and resilience of subsea cables. Therefore, the private sector—including cable manufacturers, hyperscalers (tech giants like AWS, Google, Meta, and Microsoft), and owners and investors—must navigate numerous regulatory processes to obtain the necessary approvals and permits to lay, repair, or replace cables.
- The United States must prioritize the security, resilience, and modernization of subsea cables. But it cannot meet this challenge alone. Close cooperation with allies and partners will be essential to securing this vital infrastructure for the future.

By Erin L. Murphy and Thomas Bryja

BACKGROUND & CONTEXT

Subsea fiber-optic cables are the world's primary conduit for data, carrying 99 percent of data internationally, making them indispensable to both national and economic security. This infrastructure is critical for all aspects of modern daily life, providing access to the internet as well as delivering the data that underlies communications, e-commerce, financial transactions, telehealth, and e-education systems.

Moreover, the AI revolution is relentlessly driving the need for more data and increased connectivity, all of which fundamentally depends on subsea cables. Training large language models takes enormous, distributed storage to compute, and if those networks are globally oriented, they will require additional subsea capacity to connect them.

At the same time, private sector companies, the United States, and like-minded partners and allies are increasingly concerned about China's role in the industry through HMN Tech and other state-directed investments in the infrastructure, as well as China's growing ability to deploy coercive methods, such as denying permits. Suspected Chinese and Russian activity has further demonstrated the considerable risk posed to cable systems from deniable gray zone activities.

As geopolitical tensions continue to rise and digital demands grow, high regulatory barriers and disruptions to these networks carry far greater economic and security consequences than ever before.

LEGISLATIVE OR POLICY IMPLICATIONS

There are several pieces of legislation that are currently being considered in Congress related to the security of subsea cables. These include:

- H.R. 261 (Undersea Cable Protection Act): Companies that have already acquired a state or federal permit would not need to obtain an additional permit from the National Oceanic and Atmospheric Administration (NOAA) to install, operate, maintain, repair, or recover an undersea cable. This promotes interagency cooperation for subsea cable operations.
- H.R. 3479 (SECURE American Telecommunications Act): Outdated regulations governing subsea cables would be updated to better respond to contemporary threats and challenges. Penalties for damaging cables will increase; intentional damage would be classified as a Class C felony with a fine of up to $250,000 and negligent damage would be classified as a Class A misdemeanor with a fine of up to $100,000. Cable operators would be required to meet minimum physical and cybersecurity standards outlined by the Federal Communications Committee (FCC), which would be granted authority over subsea cable licensing. Cable

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

connections that pose national security risks would be blocked. This bill promotes interagency coordination and international cooperation by calling for the United States to join the International Cable Protection Committee (ICPC).

- H.R. 2503 (Undersea Cable Control Act): Foreign adversaries would be blocked from obtaining technologies that are required to build, maintain, or operate undersea cables through export controls. The United States would seek agreements with allies to implement shared export control policies.
- S. 3249 (Strategic Subsea Cables Act of 2025): U.S. government coordination and international engagement on the security, installation, maintenance, and repair of subsea fiber-optic cables would be enhanced. The president would be required to impose sanctions on individuals responsible for intentionally damaging subsea fiber-optic cables, and to establish an interagency committee to coordinate subsea cable efforts alongside industry partners. Federal agencies would develop procedures to rapidly communicate threat information with private sector subsea cable operators to improve their situational awareness and protective measures.

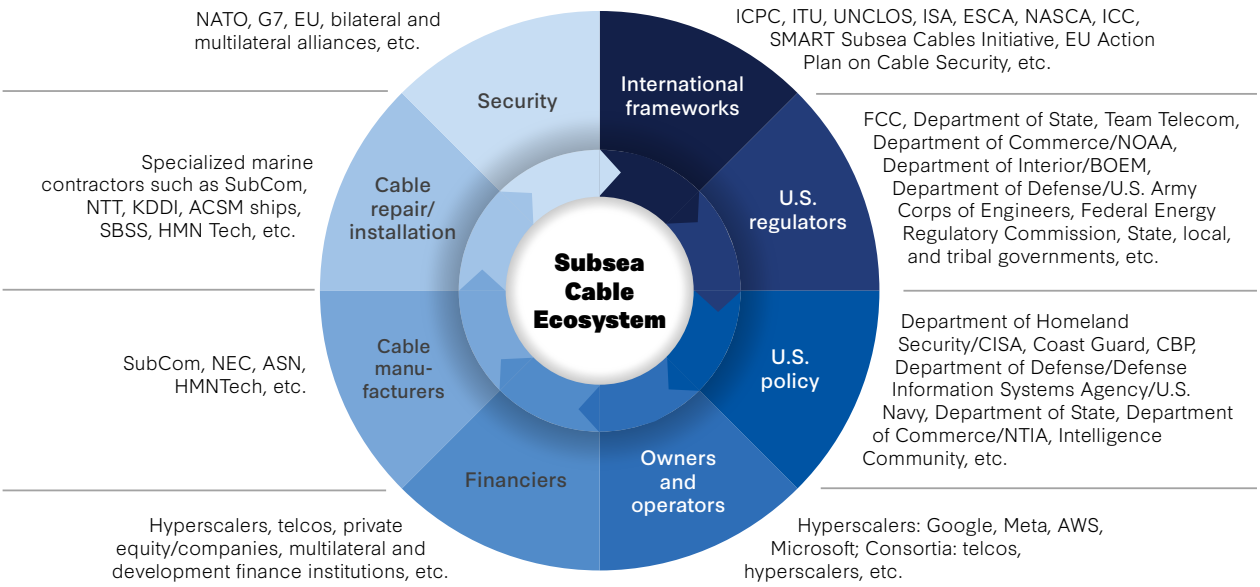
CHALLENGES & RISKS

- The majority of cable damage is caused by dropped anchors from commercial and fishing vessels that scrape across the ocean floor. Natural disasters, although rarer, can cause catastrophic breaks as well. Less likely, but of concern to policymakers, is intentional sabotage or interference by state and nonstate actors.
- Collectively, manufacturers and hyperscalers are dependent on access to specialized ships, with unique equipment that can lay and bury the cables, and the skilled crews and technicians necessary to manufacture, lay, repair, and test the cables. Only 62 vessels worldwide are actively installing and maintaining undersea telecommunications cables. Over half of all cable ships are based in Asia, and at least 12 percent are owned by China.
- Cable stakeholders must navigate a complex planning, permitting, and financing environment to support new projects and repair existing cables. The primary challenge for the private sector is navigating the complex patchwork of international, federal, and state-level approvals. Multiyear permitting processes with changing standards and timelines deter investment and slow capacity expansion. Even excluding international and state-level bodies, there is still a plethora of federal agencies involved, including: FCC, DHS, DOS, Team Telecom, DOC, Army Corps of Engineers, Coast Guard, NOAA, and more. The foundational U.S. regulatory structure on subsea cables also has not been updated in over 100 years.

RECOMMENDATIONS

- Streamline and clarify permitting and regulatory processes, designating a lead federal agency for cable coordination policy at both the federal and state levels.
- Update 100-year-old maritime laws to reflect today's realities: Establish protocols on anchorage incidents and increase penalties for cable damage.
- Expand repair surge capacity via retrofitted naval ships or through funding the construction of more cable repair ships for emergency purposes.
- Use development finance tools to support strategic financing, particularly for cable projects in emerging markets or countries with geostrategic importance that may not reach the threshold for commercially viable cable projects.
- Partner with foreign governments and the private sector to collaboratively develop best practices and to enhance information sharing and collaborative efforts to better understand the threats and challenges facing each other.

GRAPHICS/CHARTS



Source: CSIS research.

Additional Resources and Contact Information

- The Strategic Future of Subsea Cables: Ireland Case Study
- The Strategic Future of Subsea Cables: Japan Case Study
- The Strategic Future of Subsea Cables: Singapore Case Study
- The Strategic Future of Subsea Cables: Egypt Case Study

For more information, contact: **Chloe Himmel** at 202.775.3186 or **chimmel@csis.org**.