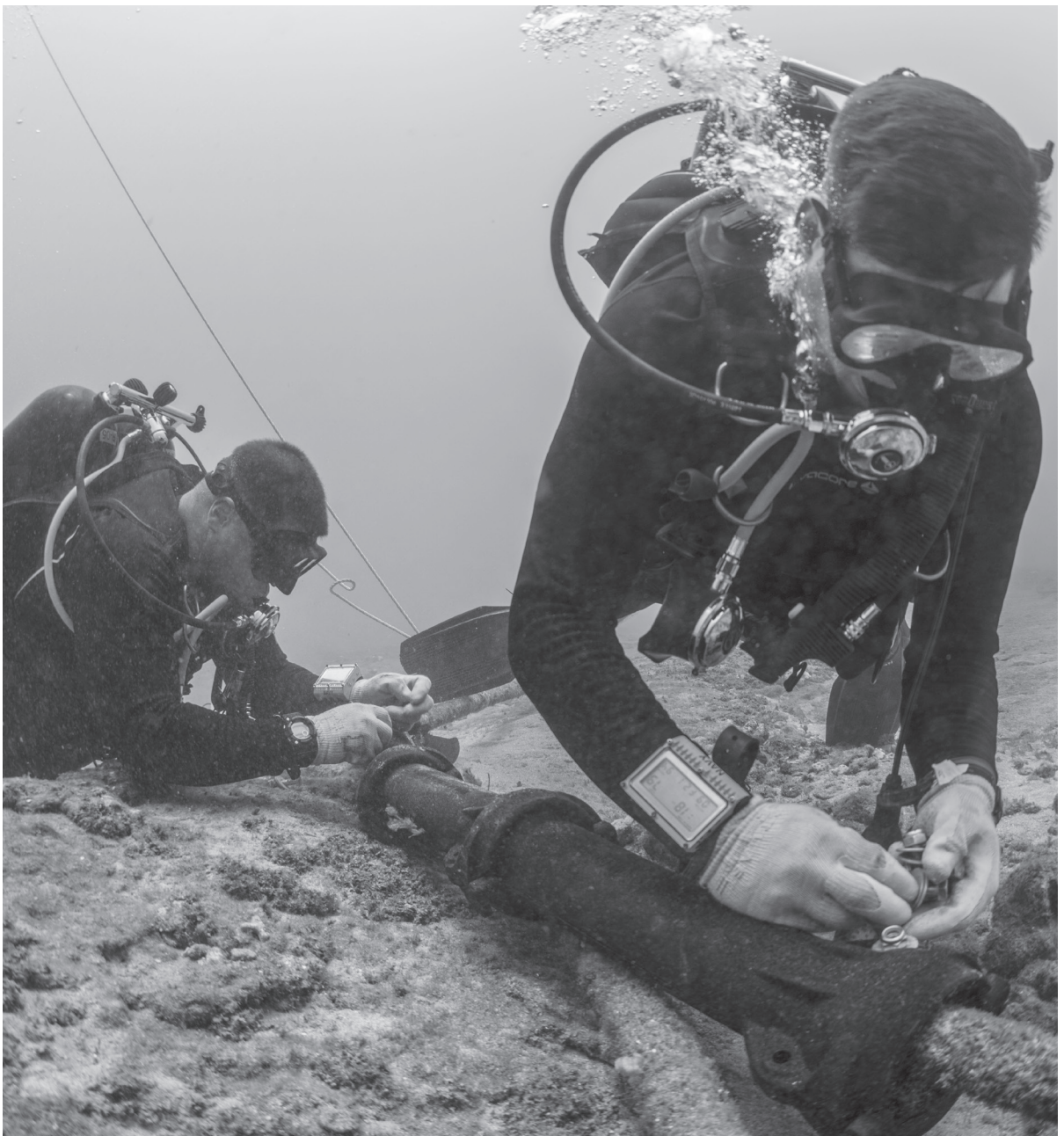


Toward Undersea Cable Resilience: The Case for Global Collaboration

Charles Mok



Escalating threats to undersea cable networks, stemming from gray-zone sabotage at vulnerable chokepoints, are receiving long-overdue attention from policymakers and the public. Recent incidents highlight the strategic vulnerability of this infrastructure, due to a lack of redundancy, limited repair capacity, and gaps in international maritime law. Despite attempts at multilateral cooperation through the G7 and the Quad, concrete actions are lagging. The US administration has not directly addressed this issue. To strengthen resilience, democracies must collaborate and invest in hardened cable designs, real-time monitoring and data sharing, routing diversity, regional repair hubs, and enhanced legal frameworks. They must work together to secure their lifeline for economic and national security and future digital-technology advancement.

In recent years, undersea cable resilience has moved to the front page of global discussions about economic and national security. As this infrastructure faces increasing threats of sabotage from malign actors, policymakers and the public are frequently reminded that undersea cable networks carry up to 99 percent of intercontinental data transmission. However, these networks are prone to breakages, either due to natural reasons, including seismic activities, or increasingly, man-made incidents—whether accidental or intentional.¹

In recent years, the number of undersea cable breakages has increased, particularly in key regions of the world. In the first two months of 2025, four undersea cable disruptions were reported in Taiwan, including one international system connecting externally and three other cables that connected Taiwan to the outlying islands of Matsu and Penghu.² In the Baltic Sea, telecommunications and power cables, often accompanied by gas pipelines, serve the communications and energy needs of countries such as Sweden, Finland, Germany, Estonia, and

Latvia, and have also experienced a steep rise in damage caused by vessels operating in the region.³ In 2024, the Houthi rebel group allegedly attacked at least three cables in the Red Sea, undermining connectivity between Asia, Europe, Africa, and the Middle East.⁴

Several patterns are emerging. First, these incidents are concentrated around geopolitically sensitive flash-point regions that are also congested with undersea infrastructure—regional and international chokepoints that are easy targets. Second, most (though not all) of the vessels found to be causing damage in the Baltic Sea and around Taiwan are owned or registered in Russia or China.⁵

Pain Points in Undersea Cable Repair

As cables must eventually reach land, they inevitably become more susceptible to damage near-shore, and where the sea is shallower. Most of the Baltic Sea is shallow,⁶ averaging only 55 meters,

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

2 Hahon Chia-Hung Chiang, "Countering China's Subsea Cable Sabotage," Global Taiwan Initiative, March 19, 2025, <https://globaltaiwan.org/2025/03/countering-chinas-subsea-cable-sabotage/>.

3 Katharina Buchholz, "Baltic Sea Cable Incidents Pile Up—Who Is to Blame?," *Forbes*, updated February 6, 2025, <https://www.forbes.com/sites/katharinabuchholz/2025/01/31/baltic-sea-cable-incidents-pile-up-who-is-to-blame/>.

4 Jon Gambrell, "3 Red Sea Data Cables Cut as Houthis Launch More Attacks in the Vital Waterway," AP News, updated March 4, 2025, <https://apnews.com/article/red-sea-undersea-cables-yemen-houthi-rebels-attacks-b53051f61a41bd6b357860bbf0b0860a>.

5 Mithil Aggarwal, "When American Allies' Undersea Cables Are Severed, Suspicion Falls on Russia and China," NBC News, January 14, 2025, <https://www.nbcnews.com/news/world/undersea-cables-are-cut-suspicion-falls-russian-chinese-vessels-rcna187105>.

6 "Baltic Sea," Wikipedia, https://en.wikipedia.org/wiki/Baltic_Sea.

and the Taiwan Strait⁷ averages only 150 meters, leaving the majority of these waters within reach of modern deep-sea dredging or anchoring activities. Both regions, as well as the Red Sea, are active and busy maritime regions, making patrolling and rapid response by authorities after any incidents even more complex and demanding.

According to the UN Convention on the Law of the Sea (UNCLOS),⁸ a coastal nation has sovereignty in its territorial waters (up to 12 nautical miles, 22.2 km, or 13.8 miles from its shore), where it may establish local laws to arrest, prosecute, and punish any perpetrators. There is, however, much less that coastal nations can do for incidents outside of their territorial sea. While a nation can exercise its rights to maintain and repair undersea cables in its 200-nautical-mile exclusive economic zone, once an incident occurs in international waters, there is little the nation can do to hold the perpetrators responsible for any damage or liability.⁹ Jurisdiction is given to the country that the perpetrator's vessel is registered to, or the perpetrator's country of citizenship, leaving the owners of damaged infrastructure limited means of redress. This often gives rogue actors a free pass to damage.¹⁰

While damage and cuts to undersea cables can usually be repaired, the repair process is complicated, expensive, and potentially lengthy. The plumbers and bricklayers of undersea infrastructures do not occupy a particularly lucrative part of the undersea cable business; only a handful of companies make, lay, and repair fiber-optic-based communications cables. As companies race to build new cable systems around the world to satisfy growing demand from internet usage and artificial intelligence (AI), the industry has been stretched thin to fulfill the needs of the less profitable repair business¹¹ with an aging repair fleet, where most ships are already over twenty or thirty years old.¹² As a result, it can take weeks or months to repair damaged cables.

Gray-Zone Aggression Turning Offensive

Gray-zone activities are coercive actions that operate in the space between peace and war.¹³ Their purpose is to challenge the status quo beneath a threshold that would prompt a retaliatory response, including military action. Gray-zone activity operates just below the proverbial "red line," especially where denying involvement or intention allows actors to evade accountability. Targeting critical infrastructure—such as undersea cables—that can be easily disrupted by conventional means, and leaving the scene quickly, typically leaves no practical liability because it escapes legal accountability. A hit-and-run playbook with little liability and ample deniability suits rogue actors well.

While damage and cuts to undersea cables can usually be repaired, the repair process is complicated, expensive, and potentially lengthy.

Meanwhile, the gray-zone coercion tactics employed by China and Russia have become more aggressive. Current efforts appear to focus on gathering information on precise cable locations, practicing techniques to cut them, and instilling fear in adversaries.¹⁴ While concerns for undersea cable resilience have recently been widely reported, few international collective efforts have been taken in response.

The challenge of proving intent with respect to cable breakages has been evident for Baltic Sea riparian nations in recent years. Sweden's prime

7 "Taiwan Straits," World Atlas, <https://www.worldatlas.com/straits/taiwan-strait.html>.

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

9 Amy Paik and Jennifer Counter, "International Law Doesn't Adequately Protect Undersea Cables. That Must Change," Atlantic Council, January 25, 2025, <https://www.atlanticcouncil.org/content-series/hybrid-warfare-project/international-law-doesnt-adequately-protect-undersea-cables-that-must-change/>.

10 "United Nations Convention on the Law of the Sea," United Nations, December 10, 1982, article 113, https://www.un.org/depts/los/convention_agreements/texts/unclos/part7.htm.

11 Josh Dzieza, "The Cloud Under the Sea," The Verge, April 16, 2024, <https://www.theverge.com/c/24070570/internet-cables-undersea-deep-repair-ships>.

12 Dan Swinhoe, "The Cable Ship Capacity Crunch," Submarine Telecoms Forum, December 6, 2022, <https://subtelforum.com/the-cable-ship-capacity-crunch/>.

13 Lyle J. Morris, Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk, and Marta Kepe, "Gaining Competitive Advantage in the Gray Zone," RAND, June 27, 2019, https://www.rand.org/pubs/research_reports/RR2942.html.

14 Daniel Thomas, "Ben Hodges: Stop Treating Russian Sabotage Like a Crime Scene," Euromaidan Press, February 18, 2026, <https://euromaidanpress.com/2026/02/18/ben-hodges-stop-treating-russian-sabotage-like-a-crime-scene/>.

minister, Ulf Kristersson, wryly proclaimed in the Munich Security Conference in February 2025, “We don’t just believe in random things suddenly happening quite often.”¹⁵ However, commenting on the January 26, 2025, undersea cable damage between Sweden and Latvia, Sweden’s prosecutor could only establish that “a combination of weather conditions and deficiencies in equipment and seamanship contributed to the cable break.”¹⁶ In another incident, even when European investigators were able to board the Yi Peng 3—responsible for the C-Lion 1 cable breakage on November 18, 2024, caused by dragging its out anchor behind the vessel for an astounding day and a half, for over 180 nautical miles—as the incident took place in international waters, the investigation could only be led by the Chinese Accident Investigation Board, and interrogation of the crew was conducted in the presence of Chinese officials.¹⁷

In February 2025, Chinese vessel Hong Tai 58, registered in Togo, cut the TPKM3 cable that connects the island of Penghu with the main island of Taiwan, within Taiwan’s territorial sea. The vessel’s captain was arrested and subsequently charged in April for “intentional undersea cable damage.” The People’s Republic of China (PRC) did not play a part in the investigation. On June 12, 2025, the captain, identified only by his surname “Wang,” was sentenced to three years in prison by a court in Tainan, Taiwan.¹⁸

Other evidence shows increasing use of technology by Russia and China to threaten global undersea cable infrastructure. On March 24, 2025, the *South China Morning Post* reported on “a powerful deep-sea cable cutter,” supposedly capable of cutting cables at depths of up to 4,000 meters.¹⁹ While some analysts disputed the paper’s reporting as sensationalized, since it focused on an early-stage design tested only in a shallow-water tank and without a

prototype, the story provided evidence that China’s research priorities appear to be more oriented toward disruption than cable protection.²⁰ Others noted that such research might be less about technology than “theater,” creating unease, uncertainty, and confusion about cable reliability and indirectly resulting in drastically increasing the manufacturing and operating costs of new cables, especially if, for instance, Western governments impose stringent new regulations mandating extra armoring along extended sections of the cable routes.²¹

In early April 2025, British military sources disclosed the discovery of Russian underwater sensors that are suspected of being used to spy on both British submarines and undersea cables in UK waters; the sensors allegedly washed ashore and were located by the Royal Army.²² As Dodge Billingsley writes:

*Moreover, analysts have speculated about the degree of evidence for coordination between Russia and China. China and Russia shared an interest in degrading western capabilities, and it is “highly probable” that they are complicit in such acts of sabotage against critical western infrastructure, for instance, with the Russian-captained Chinese vessel such as Yi Pang 3 that was involved in the November, 2025, undersea cable damage incident in the Nordic.*²³

AI Invulnerability Depends on Maritime and Undersea Security

As the world competes for AI supremacy, most focus has been on the building blocks of digital technologies—from memory chips to high-end graphics processing units (GPUs) that go into devices and servers that, in turn, make up the data-center and hyperscaler computing facilities where cloud services and large-language models (LLMs) run. What

15 Alexander Martin, “Sweden’s PM on Suspected Cable Sabotage: ‘We Don’t Believe Random Things Suddenly Happen Quite Often,’” *The Record*, February 15, 2025, <https://therecord.media/sweden-pm-on-suspected-russian-cable-breaks-not-an-accident>.

16 “Prosecutor Revokes Decision on Seized Ship,” Swedish Prosecution Authority, February 3, 2025, <https://www.aklagare.se/en/for-the-media/press-releases/2025/february/prosecutor-revokes-decision-on-seized-ship/>.

17 “Kina begränsade utredare—svårt bevisa sabotage,” *Aftonbladet*, April 15, 2025, <https://www.aftonbladet.se/nyheter/a/ny7EPo/inga-bevis-for-avsiktligt-kabelbrott-i-ostersjon>.

18 “Taiwan Jails Chinese Ship Captain for Damaging Undersea Cables,” *Reuters*, June 12, 2025, <https://www.reuters.com/business/media-telecom/taiwan-jails-chinese-ship-captain-damaging-undersea-cables-2025-06-12/>.

19 Stephen Chen, “China Unveils a Powerful Deep-Sea Cable Cutter That Could Reset the World Order,” *South China Morning Post*, March 22, 2025, <https://www.scmp.com/news/china/science/article/3303246/china-unveils-powerful-deep-sea-cable-cutter-could-reset-world-order>.

20 Zichen Wang, “Some Troubled Science Reporting at *South China Morning Post*,” *Pekingology*, April 4, 2025, <https://www.pekingology.com/p/some-troubled-science-reporting-at>.

21 Cynthia Mehboob, “Cutting Through the Narrative: What China’s Deep-Sea Cable-Cutter Really Signals,” *The Interpreter*, March 26, 2025, <https://www.lowyinstitute.org/the-interpreter/cutting-through-narrative-what-china-s-deep-sea-cable-cutter-really-signals>.

22 Liz Perkins, “Russian Spy Sensors Found Hidden in UK Waters,” *The Telegraph*, April 6, 2025, <https://www.telegraph.co.uk/news/2025/04/06/russian-spy-sensors-hidden-uk-waters/>.

23 Dodge Billingsley, “Damage to Undersea Cables in Baltic Hint at China–Russia Collusion,” Foreign Military Studies Office (FMSO), US Army, Training, and Doctrine Command (TRADOC) G-2, <https://oe.t2com.army.mil/product/damage-to-undersea-cables-in-baltic-hint-at-china-russia-collusion/>.

connects all these data centers are the fiber-optic land and underground cables within and across national borders, and the undersea cables that link continents across oceans. Future 6G mobile technology development will drive up demand for bandwidth of global internet's backhaul communications. It is not an understatement to say that the AI race depends on undersea cable resilience.

In the last decade, major American tech companies—like Google, Meta, Microsoft, and Amazon—have taken over from global telecommunications firms as the biggest investors building new undersea communications cable networks. For more than ten years, Google has invested in undersea cable projects all over the world.²⁴ In February 2025, Meta announced Project Waterworth, which will connect five of the world's continents.²⁵ Telecommunications companies around the world form consortiums to co-develop and operate these undersea cable systems to lease bandwidth to their respective customers. Technology companies, however, which are relatively well capitalized, have found themselves in a strong position to control their own connectivity, bandwidth, and destiny. The largest internet service, social media, and cloud providers in the world are the largest undersea cable investors, and also among the biggest AI companies. Other major AI-related developers and investors—such as OpenAI, Nvidia, and Softbank—are also likely in the not-too-distant future to invest in undersea cable infrastructures.

This makes the stakes of undersea cable security and resilience high. Undersea cable resilience will shape the race to develop, operate, and lead the next generation of emerging technologies from AI to quantum computing and beyond. The future of AI security may, in fact, depend on safeguarding and maintaining maritime and undersea security.²⁶

Five Steps for Coordinated, Targeted Response

How can these critical systems be improved and hardened to prevent damage, and how can the overall undersea cable infrastructure be made more redundant and diversified to reduce the impact of any particular incident? Escalating potential for Russia, China, and other adversaries to pose threats

to undersea cables demands a more coordinated and coherent response from democracies, who must target and address key vulnerabilities in global undersea cable networks.

Undersea cable resilience will shape the race to develop, operate, and lead the next generation of emerging technologies from AI to quantum computing and beyond.

First, democracies should invest in new *technology innovation and development* to harden the security of the next generation of undersea cable networks. This effort should include adding protective *underwater* measures—from materials and armoring to enhanced sensing devices to detect attacks—as well as surveillance *above water*, including satellite imaging analysis to detect suspicious shipping movements, and data sharing and advanced prediction and warning systems, including using AI.

Existing technology can be more effectively used to share data and systems. For instance, the UK's Nordic Warden system is now available not only to the UK, but also to the Baltic and Nordic countries, the Netherlands, and other NATO member states.²⁷ The system utilizes AI to analyze data from multiple sources, including the Automatic Identification System (AIS) that broadcasts the positions of vessels, to predict risks and issue warnings to member nations in the Joint Expeditionary Force (JEF). This kind of technological and operational cooperation, currently undertaken only in Europe, could prove useful elsewhere, including in East Asia. For these systems to be effective, countries in other regions must be willing to share marine data.

Second, future deployment of undersea cable systems must *enhance overall network redundancy* to improve resilience. This can be done by continuing to invest more cables to connect key destinations with different routes, as well as by adding landing

24 Winston Qiu, "Complete List of Google's Subsea Cable Investments," Submarine Cable Networks, updated December 2024, <https://www.submarinetworks.com/en/nv/insights/complete-list-of-google-s-subsea-cable-investments>.

25 Sebastian Moss, "Project Waterworth: Meta Announces World's Longest Subsea Cable Project Spanning Five Continents," Data Centre Dynamics, February 14, 2025, <https://www.datacenterdynamics.com/en/news/project-waterworth-meta-announces-worlds-longest-subsea-cable-project-spanning-five-continents/>.

26 Christian Bueger, "The Hidden Maritime Frontier of Artificial Intelligence," Italian Institute for International Political Studies, January 28, 2025, <https://www.ispionline.it/en/publication/the-hidden-maritime-frontier-of-artificial-intelligence-198152>.

27 "UK-Led Nordic Warden System Activated Following Black Sea Cable Damage," DefenseMirror.com, January 8, 2025, <https://www.defensemirror.com/news/38562>.



sites. While cable investments are predominantly made by private firms and consortiums, governments could accelerate this effort by simplifying and expediting the approval process, as well as by providing co-funding or financing support.

Both Australia and Europe offer examples of public-private partnership initiatives to improve undersea cable resilience. Since the mid-2010s, Canberra has stepped up engagement with its South Pacific neighbors, a region it views as “deeply entwined” with Australia’s future. Australian support includes investments to fund cable projects to connect with its island neighbors, and the Australian Infrastructure Financing Facility for the Pacific (AIFFP). Between 2018 and 2023, five cable projects were announced, with one completed and two under construction.²⁸

In February 2024, the European Commission published its recommendation on “Secure and Resilient Submarine Cable Infrastructures,” which included funding and financing facilitations from the European Investment Bank as well as the respective

member states’ national investment promotional banks, with other public or private investors, for cable projects verified as of “European interest.”²⁹

Third, realignment trends in global undersea cables also offer opportunities for *building better path diversity* and hence more resilience. For instance, in recent years, a significant realignment of undersea cable routes has taken place in East Asia. For decades, trans-Pacific cables connected North America with East and Southeast Asia via the major hubs of Japan, Hong Kong, and then via the South China Sea to Singapore, taking the most convenient routes that passed through major markets. Since 2020, however, the United States has blocked American companies from building new cable projects to Hong Kong, citing the Chinese government’s goal of making Hong Kong the dominant hub in the Asia Pacific region, as well as national security and cybersecurity risks.³⁰ China has also made new cable projects in disputed areas of the South China Sea almost impossible by requiring, but then delaying, approvals by PRC authorities.³¹

28 Hayley Channer, “Improving Public-Private Partnerships on Undersea Cables: Lessons from Australia and Its Partners in the Indo-Pacific,” Center for Indo-Pacific Affairs, University of Hawaii at Manoa, January 17, 2024, <https://manoa.hawaii.edu/indopacificaffairs/article/improving-public-private-partnerships-on-undersea-cables-lessons-from-australia-and-its-partners-in-the-indo-pacific/>.

29 “Commission Recommendation of 26.2.2024 on Secure and Resilient Submarine Cable Infrastructures,” Council of the European Union, February 27, 2024, <https://data.consilium.europa.eu/doc/document/ST-7087-2024-INIT/en/pdf>.

30 “Team Telecom Recommends that the FCC Deny Pacific Light Cable Network System’s Hong Kong Undersea Cable Connection to the United States,” US Department of Justice, June 17, 2020, <https://www.justice.gov/archives/opa/pr/team-telecom-recommends-fcc-deny-pacific-light-cable-network-system-s-hong-kong-undersea>.

31 Tsubasa Suruga, “Asia’s Internet Cable Projects Delayed by South China Sea Tensions,” Nikkei Asia, May 19, 2023, <https://asia.nikkei.com/Business/Business-Spotlight/Asia-s-internet-cable-projects-delayed-by-South-China-Sea-tensions>.

These developments have effectively caused new trans-Pacific cable constructions to avoid the East China Sea corridor and the South China Sea. Instead, investors of new cable systems have sought new routes, redirecting new cable projects from North America first to Guam, and then the Philippines and Indonesia, thereby skirting Chinese influence. The recent E2A system,³² expected to be completed in 2028, will connect North America with Japan and terminate in Taiwan and Korea. A “Far North Fiber” project,³³ proposed originally in 2021, and subsequently receiving funding from the EU’s Connecting Europe Facility,³⁴ will also connect Japan to Finland via the Arctic, with a “ready-for-service date” target of 2029.³⁵

Fourth, governments must *expand capacity in the cable repair industry*. Countries near high-risk choke-points or in geopolitically sensitive regions should cooperate to provide incentives to cable repair operators to establish dedicated regional support, which could ease logistical scheduling of repair vessels and reduce the wait time for repairs and maintenance. In East Asia, for example, many of the countries have robust shipbuilding industries, such as Japan and South Korea. These strengths can be leveraged to cooperate with leading undersea cable repair companies to achieve self-sufficiency, from investing in new vessels to training more skilled workers.

Fifth, in addition to regional cooperation, governments in the free world should *coordinate to act with concrete measures at the global level*. Indeed, data route diversity and redundancy were raised in the Group of Seven (G7) digital ministers’ meeting hosted by Japan in 2023.³⁶ Their declaration recognized “the importance of discussion on the role of submarine cable networks and their global development and maintenance, particularly from the security and resilience viewpoint.” It further stressed that, “with the current geopolitical situation in mind, it is urgently important for the G7 to cooperate with other like-minded partners, including those in developing and emerging economies in strengthening global connectivity by ensuring secure and resilient routes of international communication infrastructure.”³⁷

In September 2024, the Quad nations (Australia, India, Japan, and the United States) emphasized the security and resilience of undersea cables in their Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World.³⁸ The statement highlighted the importance of international cooperation to safeguard undersea cable infrastructure from physical damage, cyber threats, and geopolitical risks. The statement was subsequently endorsed by the European Union, Japan, New Zealand, Korea, Singapore, the UK, and several other countries during the 2024 United Nations General Assembly.

Global coordination also means addressing the lack of legal accountability for damage to undersea infrastructure and related difficulties in enforcement.

While these efforts acknowledge the threats and identify a need for nations to work together, concrete policy implementation has lagged. Meanwhile, the pattern of gray-zone attacks suggests a need for urgency in protecting undersea cable infrastructure; coordinating strategies to improve redundancy, monitoring, and intelligence-sharing; and facilitating new investment. The 51st G7 Summit, hosted by Canada in 2025, failed to make meaningful progress on infrastructure resilience, in spite of the fact that the key focus areas of the Summit—global economic stability, digital transition, and international security—all depend on infrastructure resilience.

Global coordination also means addressing the lack of legal accountability for damage to undersea infrastructure and related difficulties in enforcement. Doing so would require changes in global governance regimes and international law, such as the previously mentioned UNCLOS, which has

32 “E2A,” Submarine Cable Network, March 25, 2025, <https://www.submarinenetworks.com/en/systems/trans-pacific/e2a>.

33 “Far North Fiber,” Wikipedia, https://en.wikipedia.org/wiki/Far_North_Fiber.

34 “Far North Fiber Takes a Major Step Forward—Cable Route Study Started,” Far North Fiber, April 11, 2024, <https://www.farnorthfiber.com/news>.

35 Far North Fiber, <https://www.farnorthfiber.com/>.

36 “Results of G7 Digital and Tech Ministers’ Meeting in Takasaki, Gunma,” G7 2023 Hiroshima Summit, April 30, 2023, https://www.soumu.go.jp/joho_kokusai/g7digital-tech-2023/en/topics/topics_20230430.html.

37 “Ministerial Declaration: The G7 Digital and Tech Ministers’ Meeting, 30 April 2023,” G7 2023 Hiroshima Summit, April 30, 2023, https://www.soumu.go.jp/joho_kokusai/g7digital-tech-2023/topics/pdf/pdf_20230430/ministerial_declaration_dtmm.pdf.

38 “Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World,” US Department of State, September 26, 2024, <https://2021-2025.state.gov/joint-statement-on-the-security-and-resilience-of-undersea-cables-in-a-globally-digitalized-world/>.

remained largely unchanged since 1884.³⁹ While difficult, these changes would benefit not only developed regions in Europe and Asia, but other areas of the world, from Africa to South and Central America, and the Middle East to the Pacific Islands.

Resilience Cannot Be Achieved Alone

The second Trump administration has taken steps to recognize the importance of undersea cable resilience. An executive order on “Restoring America’s Maritime Dominance,” issued on April 9, 2025, focused on ensuring the security and resilience of the United States’ maritime industrial base, mainly with respect to shipbuilding.⁴⁰ A second executive order that month, “Unleashing America’s Offshore Critical Minerals and Resources,” addressed the importance of deep-sea exploration and seabed mineral development.⁴¹ Both are indirectly related to undersea cable resilience. In early August, the Federal Communications Commission (FCC) finalized and adopted new rules on undersea cable buildout and security—the first time in over two decades that relevant rules have been revised.⁴²

The new rules focus on measures to protect undersea cables against foreign adversaries, such as China, Russia, and Iran, by limiting these actors’ involvement in cables owned by US entities or that connect with the United States. By applying a presumption of denial for certain foreign adversary-controlled license applicants, restricting capacity leasing agreements to such entities, and prohibiting the use of equipment from such entities, the rules intend to exclude firms such as Huawei and HMN Technologies—formerly Huawei Marine Networks, spun off from Huawei, now the fourth-largest undersea cable construction company in the world—from US-related cable business.⁴³ The new rules also require approved projects to submit cybersecurity plans, satisfy physical security requirements, and ensure that no companies from adversary countries are involved in the cable supply chain.

These are welcome developments, but they only apply to FCC-licensed cable systems and cable-landing licensees that involve landing in US territories or doing business with US firms. Currently, the FCC is seeking comment on additional measures that would incentivize use of American undersea cable repair and maintenance ships and trusted technology abroad. Because undersea cables almost inevitably connect to overseas territories, these steps are long overdue. Globally there are more cable systems that are not connected physically with the United States but would affect the global resilience of the internet. In the end, US policies cannot be about only the interests of US companies, or limited to only those connections into US territories.

The United States also needs to work more closely with its allies to mitigate adversary gray-zone tactics. In 2015, Canada and Taiwan signed an agreement to share data about illegal shipping vessels and to collaborate to use dark vessel detection technology, which employs satellites to track “dark ships.”⁴⁴ Similar technology and data sharing, along with the deployment of a patrol and surveillance fleet in Europe by NATO countries, have also proven effective in protecting cable systems in the Baltic.⁴⁵ US connectivity to Europe is dependent on cable system safety in Europe, and US connectivity to the Indo-Pacific region depends on cable resilience in East Asia, including Taiwan. American interests extend far beyond just those cables that come to its shores. For its own interests and benefits, the United States should not be absent in this global cooperation.

There is also clear room for improvement in coordination on the cable supply chain among democratic allies. The Japanese government recently announced an investigation into whether Japanese firms involved in the installation and maintenance of undersea cables procure any critical components from China.⁴⁶ The United States would benefit from leading alongside its allies in future undersea cable planning, investment, development, deployment, protection, and rule-setting, for its own economic and national security.

39 Paik and Counter, “International Law Doesn’t Adequately Protect Undersea Cables.”

40 “Restoring America’s Maritime Dominance,” The White House, executive order, April 9, 2025, <https://www.whitehouse.gov/presidential-actions/2025/04/restoring-americas-maritime-dominance/>.

41 “Unleashing America’s Offshore Critical Minerals and Resources,” The White House, executive order, April 24, 2025, <https://www.whitehouse.gov/presidential-actions/2025/04/unleashing-americas-offshore-critical-minerals-and-resources/>.

42 Ryohei Yasoshima, “US to Shut Out China from Undersea-Cable Supply Chains,” Nikkei Asia, August 22, 2025, <https://asia.nikkei.com/spotlight/supply-chain/us-to-shut-out-china-from-undersea-cable-supply-chains>.

43 HMN Technologies, November 30, 2020, <https://www.hmntech.com/enPressReleases/37764.jhtml>.

44 Steven Chase, “Canada Lends ‘Dark Vessel’ Detection Gear to Help Taiwan Track Covert Ship Activity,” *The Globe and Mail*, August 21, 2025, <https://www.theglobeandmail.com/politics/article-canada-taiwan-china-dark-vessel-detection-technology/>.

45 Clement Ngu, “NATO Effective in Patrolling Baltic Undersea Cables, Says Commander,” Nikkei Asia, August 25, 2025, <https://asia.nikkei.com/politics/international-relations/nato-effective-in-patrolling-baltic-undersea-cables-says-commander>.

46 Kiu Sugano and Ryuto Imao, “Japan to Investigate Undersea Cable Supply Chains for China Exposure,” Nikkei Asia, September 15, 2025, <https://asia.nikkei.com/business/telecommunication/japan-to-investigate-undersea-cable-supply-chains-for-china-exposure>.

Global communications, international business and finance, and American leadership in emerging technologies, from AI to quantum computing, are not possible without a safe, secure, and resilient global undersea cable ecosystem. True resilience for a globally connected, secure, and resilient undersea cable network can only be achieved through collaboration among like-minded governments and stakeholders from free countries.

Charles Mok is a research scholar at the Global Digital Policy Incubator of the Center on Democracy, Development, and the Rule of Law at Stanford University. He is also a member of the Board of

Trustees of the Internet Society, and formerly an elected member of the Legislative Council in Hong Kong, representing the Information Technology functional constituency, from 2012 to 2020. As an entrepreneur, in 1994 Charles cofounded HKNet, one of the earliest internet service providers in Hong Kong. He holds a BS in computer and electrical engineering and an MS in electrical engineering from Purdue University.

Stanford University, Stanford, CA, USA, email: cpmok@stanford.edu.

Image: Pacific Missile Range Facility Barking Sands, Hawaii, United States by Petty Officer 1st Class Charles White.⁴⁷

⁴⁷ For the image, see <https://www.dvidshub.net/image/2710068/uct-2-performs-undersea-cable-maintenance-off-kauai>.