Testimony before the
U.S.-China Economic and Security Review Commission

"Part of Your World: U.S.-China Competition Under the Sea"

A Testimony by:
Jason Hsu
Senior Fellow, Hudson Institute, Former Legislator, Taiwan

March 2, 2026

Chair Price, Vice Chair Schriver, distinguished members of the Commission, I am honored to share my views on the critical and urgent topic of China's targeting of undersea cable infrastructure in the Taiwan Strait and the broader Indo-Pacific region. The views expressed in this testimony are my own. As a former member of the Taiwanese Legislature and current Senior Fellow at the Hudson Institute, I have spent years focusing on technology, defense, and cross-strait relations. The vulnerability of subsea cables to Chinese sabotage remains a crucial factor in Taiwan's ability to function as a connected, democratic society and in the United States and its allies' efforts to maintain a free and open Indo-Pacific.

In my testimony, I will address the strategic importance of subsea cables to Taiwan and the Indo-Pacific, China's sabotage campaign and its integration into Beijing's gray zone warfare strategy, evidence of coordination with Russia, the development of purpose-built cable-cutting technologies, the role cables would play in a potential military conflict, options for backup connectivity including satellite alternatives, and recommendations for Congressional action. I hope this testimony will be of use to the Commission as it considers what policy recommendations to make to Congress.

The Strategic Importance of Undersea Cables to Taiwan and the Indo-Pacific

Subsea fiber-optic cables are the backbone of the modern global economy. They carry an estimated 97 to 99 percent of all intercontinental internet traffic, enabling financial transactions, military communications, cloud computing, and the digital activity of billions of people.[1] There are approximately 597 submarine cables, stretching roughly 1.3 million kilometers across the world's ocean floors, most laid by four companies: SubCom of the United States, Alcatel Submarine Networks of France, Nippon Electric Company of Japan, and HMN Technologies of China.[2] Despite the popular image of a wireless, satellite-connected world, the reality is that virtually all international data flows through thin glass fibers resting on the seabed.

As an aside, subsea cables represent an industry where Beijing is actively seeking to expand its market share. China's HMN Technologies, formerly Huawei Marine Networks, remains the world's fourth-largest and fastest-growing subsea cable builder over the past decade, having

[1] TeleGeography, Submarine Cable Map, accessed February 2026, https://www.submarinecablemap.com/.

[2] Recorded Future, Submarine Cables Face Increasing Threats Amid Geopolitical Tensions and Limited Repair Capacity, accessed February 2026, https://www.recordedfuture.com/research/submarine-cables-face-increasing-threats

completed more than 100 projects across 78 countries and regions.[3] Across the Indo-Pacific, HMN Technologies was involved in 16 undersea cable projects worth $1.6 billion.[4] Under the Digital Silk Road initiative launched in 2015, Beijing has pursued an ambitious goal of capturing 60% of the global fiber-optic cable market. China is now more than halfway there as its four leading fiber-optic cable companies, YOFC, Hengtong, FiberHome, and Jiangsu Zhongtian Technology, now control more than 35% of the global market.[5] Unlike cutting-edge semiconductors, where U.S. export controls have constrained China's progress, China possesses all the necessary technology to build and deploy subsea cables independently. For U.S. allies and partners, allowing China to dominate subsea cable construction and ownership in emerging markets would increase the risk that Beijing could conduct surveillance, intercept data, or deliberately disrupt networks.

Taiwan is connected to the global network through just 24 undersea cables, namely 14 international and 10 domestic inter-island cables.[6] The international cables link Taiwan to Japan, South Korea, the Philippines, Singapore, and the United States, while the domestic cables connect the main island to the Penghu, Kinmen, and Matsu island groups. These cables come ashore at approximately eight landing stations concentrated near New Taipei City in the north and Kaohsiung in the south. The system is designed with built-in redundancy to account for both geopolitical and geological risks. Apart from the threats posed by mainland China, Taiwan sits by the Eurasian and Philippine tectonic plates and regularly experiences earthquakes and typhoons that can damage submarine cables. Between 100 and 200 cable faults occur worldwide each year, caused by natural and accidental factors.[7] For instance, in December 2006, a 7.0-magnitude earthquake off Taiwan’s southwest coast cut eight of eleven submarine cables due to underwater landslides. This blocked 98% of communication to some regions and took weeks to repair.[8]

Since that natural disaster, Taiwan’s digital connectivity has only grown, creating a profound national security vulnerability. A disruption to Taiwan's digital connectivity would not only inconvenience its 23 million citizens but also paralyze financial markets, disrupt the semiconductor manufacturing that underpins the global technology supply chain, and sever critical military and government communications at precisely the moment they are most needed. Taiwan's semiconductor industry depends on reliable international data connectivity for everything from design file transfers to supply chain coordination to real-time manufacturing oversight. And while there are some redundancies in place meant to reduce the risk of a cable cut, one cable loss can still be disruptive, especially if that cable connected the main island with the smaller island chains.

[3] CSIS, "Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition," July 16, 2025.

[4] Lowy Institute, "The Cable Ties to China's Digital Silk Road," accessed February 2026.

[5] Nikkei Asia, "China's Undersea Cable Drive Defies U.S. Sanctions," June 25, 2024.

[6] Global Taiwan Institute, "Countering China's Subsea Cable Sabotage," March 25, 2025.

[7] Al Jazeera, "As Undersea Cables Break Off Europe and Taiwan, Proving Sabotage Is Tough," March 10, 2025.

[8] Submarine Networks, “ Submarine Cables Cut after Taiwan Earthquake in Dec 2006,” March 19, 2011. https://www.submarinenetworks.com/en/nv/news/cables-cut-after-taiwan-earthquake-2006#:~:text=Eight%20submarine%20cables%20were%20cut%20after%20the,services%20in%20Asia%2C%20affecting%20many%20Asian%20countries.

Replacing a cable, while possible, can be expensive. In 2023 alone, cables connecting Taiwan and the Matsu Islands were severed 12 times, resulting in repair costs of NTD $96.4 million (approximately USD $2.9 million).[9] But repairing these cables is a complex and time-intensive process, as it may require a waiting period for repair ships, which can be delayed due to maritime conditions and weather. Taiwan's average repair times depend heavily on the severity and nature of the damage. Which could range from weeks to months,[10] For example, the damage to TPE, an international cable connecting Taiwan, Japan, and the US, was repaired within 2 weeks thanks to the timely assistance of Japan's KDDI Ocean Link.[11] However, there is no fixed timeframe for providing an average repair time, especially due to natural or political factors. This leaves Taiwan's communications infrastructure particularly vulnerable to persistent disruptions. Specifically, if this were during a blockade or contingency when allies could come to the aid in time, it would significantly delay and intensify the effects of the damage.

But the economic impact of the loss of undersea cables extends beyond repair costs. A Mercatus Center study estimated that disruption of Taiwan's digital communications alone would cost the island's economy approximately $55 million per day, or $1.69 billion per month.[12] But the ripple effects across global markets, supply chains, and allied military coordination would dwarf that figure. Japan, South Korea, the Philippines, and Australia all depend on subsea cable systems that transit waters where China asserts territorial claims or exercises growing influence. Singapore, the most connected hub in Asia with 25 subsea cable landings, serves as a digital gateway whose disruption would reverberate across all of Southeast Asia. The Indo-Pacific region leads the world in projected subsea cable investment, with spending expected to exceed $10 billion by 2026, underscoring both the region's dependence on this infrastructure and the scale of the risk.

China is well aware of the region's interconnectedness and has used its position to make demands of its neighbors. In 2023, Vietnam saw five of its cables cut, mainly due to ship anchors, fishing activities, and natural events, instead of direct sabotage. This left the country with a serious lag in website performance, with millions of Vietnamese losing digital access. Repairs took several weeks because China required cable repair ships to obtain permits to operate in the South China Sea.[13] If these cables were cut in the South China Sea to isolate Taiwan, or by a natural disaster, the resulting disruption could reverberate across the Indo-Pacific and harm regional economies.

In Taiwan, the concentration of cable landing stations in just two metropolitan areas creates additional geographic vulnerability. China can target landing stations through precision strikes, cyber operations, or even physical sabotage on land, which can achieve the same effect as cutting multiple cables at sea. Taiwan's Ministry of Digital Affairs has recognized this risk and begun

[9] Chunghwa Telecom, as cited in Global Taiwan Institute, March 2025. In 2023, cables connecting Taiwan and the Matsu Islands were severed 12 times, resulting in NTD $96.4 million (USD $2.9 million) in repair costs.
[10] Ministry of Digital Affairs (Taiwan, ROC), "海纜障礙狀況"[Submarine Cable Fault Status], 2026.
[11] The Reporter, "□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ 繫「數位生命線」的應變挑戰" [Under the Crisis of Submarine Cable Breaks, Taiwan's Challenges in Safeguarding Its "Digital Lifeline"], 2025.
[12] George Mason University, Mercatus Center, "Taiwan Strait War Could Lead to Undersea Internet Cable Cutoff, Costly Shipping Disruptions," 2022.
[13] Voice of America, "Undersea Cables Emerge as Source of Friction in South China Sea," 2024; Washington Post, "Escalating Contest over South China Sea Disrupts International Cable System," 2024.

providing subsidies to build new backup landing facilities to diversify these chokepoints, but progress remains slow relative to the pace of the evolving threat. The Commission should understand that undersea cable security is a challenge for both maritime and terrestrial environments, requiring an integrated approach.

China's Gray Zone Warfare Through Cable Sabotage

China has deliberately targeted Taiwan's undersea cables as part of its expanding gray zone warfare toolkit, with a notable and alarming escalation since 2023. The U.S.-China Economic and Security Review Commission's 2025 annual report found that China has increasingly engaged in undersea cable-cutting activities as a gray-zone pressure tactic, with mounting evidence that Beijing is developing new cable-cutting technologies for potential wartime use.[14] Cable sabotage fits into their broader "Three Warfares" strategy that includes military encirclement exercises, Coast Guard harassment, cyber intrusions, economic coercion, and information operations to wear down Taiwanese resilience without triggering a conventional military response.

The pattern of sabotage incidents has been well documented in both Taiwan and the U.S. In February 2023, two cables connecting Taiwan's Matsu Islands to the mainland were severed: first by a Chinese fishing boat on February 2, then by a Chinese cargo vessel that dropped its anchor on February 8. The archipelago's 14,000 residents were left with slow internet for over 50 days, relying on a microwave backup system that provided only 2.2 gigabits per second, compared with the normal demand of 8 to 9 Gbps.[15] Though China claimed both incidents were coincidences, losing two cables in six days short of a natural disaster is not a "coincidence." Between January and February 2025, Taiwan experienced four additional incidents of submarine cable disruption: three domestic and one international.[16] In January 2025, a Tanzania-flagged vessel controlled by a Hong Kong company and crewed by Chinese nationals disabled its tracking system before dragging its anchor over the Trans-Pacific Express cable, severing a key link connecting Taiwan, Asia, and the United States. Days later, the Taiwan Coast Guard said it thwarted a second cable-cutting attempt by a Mongolia-flagged ship. In February, the Togo-flagged Hongtai 58 severed a cable connecting Taiwan's main island and the Penghu Islands.[17]

China conducts these operations using a consistent, sophisticated methodology. Saboteurs use civilian hulls, fishing trawlers, and cargo ships that are foreign-flagged but crewed by Chinese nationals. These vessels employ mechanical means such as anchor dragging or trawl gear to sever cables rather than explosives, which would be more easily attributable. The vessels frequently change names, registrations, and flags to evade identification. The Hongtai 58 had previously operated under the names Hongtai 168 and Jinlong 389 while cycling through maritime registries in Andorra, Tanzania, and Togo.[18] This systematic identity manipulation

[14]U.S.-China Economic and Security Review Commission, 2025 Annual Report to Congress, Chapter 11: Taiwan, November 2025.
[15]The Diplomat, "After Chinese Vessels Cut Matsu Internet Cables, Taiwan Seeks to Improve Its Communications Resilience," April 17, 2023.
[16] See note 6.
[17] See note 6.
[18] See note 6.

suggests a calculated effort to obscure ownership, evade responsibility, and establish a flexible "maritime shadow warrior" network for gray zone operations.

What makes subsea cable sabotage particularly effective within the gray zone context is its exploitation of the attribution challenge. As Ray Powell, director of Stanford's Sea Light project, has observed, the entire gray zone is about maintaining just enough deniability that even though the evidence overwhelmingly points to the perpetrator, affected nations cannot definitively prove intent and justify an escalatory response. Beijing has offered various explanations for cable incidents. Initially, it blamed maritime accidents, but then China's Weihai Public Security Bureau claimed that two Taiwanese nationals had been operating the Hongtai 58 as part of a smuggling operation.[19] This attribution challenge has paralyzed the international community's response. As Powell has warned, China and Russia will continue this behavior because they calculate that the consequences will not be severe enough to warrant stopping.

The attacks are notably precise, targeting cables between Taiwan and its smaller islands, particularly Matsu and Penghu, where there is far less redundancy, rather than striking at the larger international trunk cables. This targeting pattern confirms that the saboteurs possess detailed knowledge of cable routes and are deliberately selecting vulnerable links to maximize disruption while minimizing the risk of a decisive international response. So far, the cable cuts have caused significant disruption to the outlying islands, though Taiwan's main island has rerouted traffic through surviving cables. But the margin of safety is narrowing with each incident.

The sabotage campaign must be understood within the context of China's broader military pressure on Taiwan. Between 2018 and mid-2025, the People's Liberation Army conducted at least a dozen military drills in the Taiwan Strait and around Taiwan, with scale and frequency increasing annually, including exercises that encircled the island and simulated blockade operations. The Strait Thunder-2025A exercises in April 2025 deployed 135 aircraft, 38 naval vessels, and 12 other official vessels in the areas surrounding Taiwan. In December 2024, the PLA deployed nearly 90 ships in waters stretching from the East China Sea to the South China Sea in its largest military drills near Taiwan in almost 30 years.[20] Cable sabotage is not occurring in a vacuum; it is one instrument in a comprehensive campaign of coercion that spans the military, economic, diplomatic, and information domains.

The psychological dimension of cable sabotage should not be underestimated. China's Three Warfares strategy encompasses psychological, media, and legal warfare aimed at undermining an adversary's will to resist. When residents of the Matsu Islands endured 50 days of degraded internet, the impact extended far beyond inconvenience. Businesses suffered, government services were disrupted, and a pervasive sense of vulnerability took hold among the population. This is precisely the effect Beijing seeks. Each successful cable cut demonstrates to the Taiwanese public that their government cannot fully protect them, that China possesses the ability to isolate them, and that the international community may lack the will or the means to prevent it. On Taiwan's main island, the psychological impact of even a partial loss of internet

[19] Al Jazeera, "China Probe Finds Taiwanese Men Controlled Ship That Cut Undersea Cables," December 24, 2025.
[20] Jamestown Foundation, "'Strait Thunder-2025A' Drill Implies Future Increase in PLA Pressure on Taiwan". April 11, 2025.

connectivity could be devastating, particularly if it occurred alongside other gray zone provocations aimed at testing Taiwan's social cohesion and political resolve.

In the broader South China Sea, the cable competition takes on additional dimensions. When it comes to the South China Sea, U.S. and other firms are put at a competitive disadvantage compared to Chinese firms. The U.S., since 2020, has refused to license American companies to invest in undersea cable consortia with Chinese companies or in new cables that would connect directly to China, including Hong Kong. In response, China has withheld permits for cable projects transiting waters it claims under the nine-dash line, forcing companies to reroute at significantly higher cost.[21] Major cable projects like the Meta- and Google-owned Echo and Bifrost cables now cross the Java Sea rather than the more efficient South China Sea route.[22] Meanwhile, HMN Technologies maintains an operational advantage in deploying its own cables within contested waters, raising what analysts have described as the risk of a Chinese monopoly over subsea cables in the South China Sea. This anticompetitive act is not only geared toward promoting Chinese firms but also allows Beijing to disrupt rival states' communications while safeguarding its own data and military communications, particularly in times of conflict.

Evidence of Sino-Russian Coordination

One of the most alarming developments in this space is the growing body of evidence suggesting operational coordination between China and Russia on undersea cable sabotage. The Jamestown Foundation documented that activities of the Chinese-registered Shunxing-39 north of Taiwan and the suspicious transit of the Belize-flagged, Russian-operated Vasili Shukshin, which spent nearly four weeks from December 2024 through mid-January 2025 in commercially nonsensical movements near Taiwan's Fangshan undersea cable landing station. Their movements were described by maritime analysts as aimlessly criss-crossing the area for no apparent reason, before returning to the Russian Pacific port of Vostochnyy. These continued actions suggest possible collaboration related to the reconnaissance and sabotage of undersea cables connecting Taiwan to the outside world.[23]

These incidents were not limited to Taiwan; Europeans have also faced ongoing disruptions to sea cables, particularly in the Baltic Sea, due to suspected undersea infrastructure sabotage by Chinese merchant vessels in 2023 and 2024, with strong indications of Russian assistance and coordination. In November 2024, the Chinese vessel Yi Peng 3 severed two cables, one connecting Finland and Germany, with the other linking Sweden and Lithuania, by dragging its anchor for over 100 miles. European investigators determined that a Russian sailor was part of the crew and that Russian intelligence agencies had instructed the captain to sever the cables.[24] This mirrored an October 2023 event in which a Chinese vessel carrying Russian sailors damaged a Baltic Sea gas pipeline and an undersea cable connecting Finland. This collaboration

[21]ISEAS-Yusof Ishak Institute, "The Struggle for Subsea Cable Supremacy in Southeast Asia," Perspective No. 2025/21, February 2025.
[22]Center for Indo-Pacific Affairs, University of Hawaii at Manoa, "Entangled: Southeast Asia and the Geopolitics of Undersea Cables." & Nikkei Asia, “Taiwan's island internet cutoff highlights infrastructure risks,” May 31, 2023.
[23]Jamestown Foundation, "Strangers on a Seabed: Sino-Russian Collaboration on Undersea Cable Sabotage Operations," November 6, 2025.
[24]Washington Times, "Inside the Ring: China Ready for Undersea Cable Attacks, Congressional Report Warns," November 19, 2025.

represents what some analysts have described as a growing Russia-China gray-zone axis, perhaps moving toward a full-fledged partnership, in which Beijing can surreptitiously aid Moscow in its European fight while adding layers of deniability to its own Taiwan-focused operations.[25] The coordinated nature of these incidents, with Chinese vessels targeting European undersea assets in exchange for Russian assistance near Taiwan, suggests that the two regimes are sharing tactics, intelligence, and operational assets. This coordination means that subsea cable threats can no longer be assessed in isolation; they must be understood as part of an increasingly integrated challenge to U.S. and allied national interests.

Development of Purpose-Built Cable-Cutting Technologies

Beyond the gray zone sabotage conducted through civilian vessels, China is actively developing purpose-built technologies for large-scale cable destruction in a military conflict. They are moving beyond improvised anchor-dragging toward systematic wartime capability. Chinese researchers at PLA-linked institutions have been filing patents for cable-cutting devices for over a decade. In 2013, the PLA Navy's Institute of Communication Application patented a deep-sea optical cable shear and retrieval device, which appears designed for covert operations, given its military origin. In 2022, the PLA Naval University of Engineering patented a cable-retrieval system that incorporates tools to sever and secure both ends of cut cables simultaneously. Finally, Zhuhai Yunzhou Intelligence Technology secured a patent in January 2025 for an undersea cutting device and towed cutting system.[26]

China has since increased its innovation in deep-sea technology. In early 2025, the U.S.-sanctioned China Ship Scientific Research Center published a design for an electric cutting device capable of operating at depths exceeding 13,000 feet.[27] In mid-2025, China unveiled a new ship designed to cut undersea cables, equipped with a six-inch diamond-coated grinding wheel spinning at 1,600 rpm and capable of breaching the most fortified reinforced sheaths at depths of 4,000 meters. Originally designed for deep-sea mining, the device gives Beijing plausible deniability while enabling strategic disruption at depths exceeding most cable infrastructure.[28] Given the PLA’s involvement in researching and advancing civilian cable technology, these innovations present a red flag over the country’s capabilities and potential involvement in future cable cuts.

The Role of Subsea Cables in a Potential Military Conflict

In any military conflict involving Taiwan, Chinese military doctrine dictates that subsea cable infrastructure would be among the very first targets before invasion. The Mercatus Center obtained a Chinese database listing strategic points of interest in Taiwan, including numerous undersea cable landing stations, indicating that the PLA has conducted extensive intelligence

[25]The Diplomat, "China's Undersea Cable Sabotage," January 28, 2025.
[26]Jamestown Foundation, "Creative Destruction: PRC Undersea Cable Technology," July 22, 2025.
[27] Washington Times, "Inside the Ring: China Ready for Undersea Cable Attacks, Congressional Report Warns," November 19, 2025.
[28]CSIS, "China's Underwater Power Play: The PRC's New Subsea Cable-Cutting Ship Spooks International Security Experts," July 16, 2025.

preparation of the battlefield.[29] The PLA is expected to sever undersea cables around Taiwan to crush the island's communications before an invasion. If China is successful in severing all cables, it would paralyze government and military communications and create widespread panic among the general public.

Taiwan's defense forces will have a harder time coordinating defensive operations due to a lack of communication, which will disrupt military command and control. It would also paralyze financial markets and government operations, creating economic chaos that could undermine the public's will to resist. Worse, it would sever Taiwan's ability to communicate with the international community, preventing the kind of real-time information sharing that has been so critical to Ukraine's diplomatic campaign against Russia in the aftermath of the invasion. If the U.S. or other allies intervened in this conflict, these cable cuts would disrupt coordination between Taiwan's forces and allied reinforcements, complicating U.S. and allied military responses during the critical first hours and days of a crisis.

The PLA Navy does not need to cut all of Taiwan's cables; by severing as few as three key cable clusters near the Bashi Channel, the PLA could theoretically reduce Taiwan's bandwidth by 99%. This would create a digital blockade complementary to a naval quarantine.[30] Combined with cyber operations targeting remaining communications infrastructure and potential jamming of satellite alternatives, this approach represents a comprehensive information-denial strategy from space to the seabed. Cable systems linking Taiwan, the Philippines, and the United States, including the Pacific Light Cable Network, Trans-Pacific Express, FASTER, and the E2A system, would all be at risk, with cascading effects on global financial markets, cloud computing services, and internet connectivity across the Indo-Pacific.[31]

Repair would be effectively impossible during active hostilities. The global cable repair fleet is severely limited; average repair times already exceed 40 days under normal peacetime conditions.[32] Taiwan lacks its own cable repair ships, and the highly sought-after international repair vessels often have packed schedules. In a conflict scenario involving multiple simultaneous cable cuts in a contested maritime environment, no repair ship or crew would be able to restore capacity quickly, let alone operate unimpeded by the PLA Navy.

Taiwan's Response and the Need for U.S. Support

In response to China's growing assertiveness and gray zone warfare, Taiwan has taken several important steps to counter sea cable cuts. Within the private sector, operators like Chunghwa Telecom shift traffic onto surviving international systems and activate lower-capacity backups, including microwave and satellite links, to keep service functioning until repairs are completed. The Taiwanese government has also shifted its approach to protecting sea cables by prosecuting and detaining crews suspected of sabotage. Most notably, in February 2025, Taiwan detained the Hongtai 58 and subsequently sentenced its Chinese captain to three years in prison for sabotage,

[29]George Mason University, Mercatus Center, "Submarine Cables and Container Shipments: Two Immediate Risks to the US Economy if China Invades Taiwan," 2022.
[30]EditorialGE, "China Taiwan Blockade Strategy 2026," January 14, 2026.
[31]Pacific Forum, "Underwater Frontlines: China's Cable-Cutting Threat in the South China Sea," June 2, 2025.
[32]Recorded Future, as cited in Techzine Global, "Risk of Sabotage of Undersea Internet Cables Increases," July 18, 2025.

the first time Taiwanese authorities imposed serious criminal penalties for damaging undersea cables.[33] Taiwan's Coast Guard now conducts around-the-clock patrols near critical cable routes, maintains a watch list of 96 China-linked vessels blacklisted for suspicious activity, and uses alert systems to detect vessels approaching cables at low speeds.[34]

Additionally, Taiwan's National Communications Commission amended the Telecommunications Management Act in 2023 to increase penalties for damaging communications infrastructure. The Ministry of Digital Affairs followed suit in 2024 by designating ten domestic submarine cables as critical infrastructure, ensuring heightened security measures and government oversight. Finally, Taiwan has launched the RISK initiative, which stands for Risk Mitigation, Information Sharing, Systemic Reform, and Knowledge Building, to take a whole-of-society approach to protecting submarine cable networks.[35]

Despite these commendable efforts, Taiwan cannot adequately deter or defend against cable sabotage without support from the United States and the broader international community. The scale of China's threat, which exploits international maritime law and involves vessels crewed by Chinese citizens, exceeds any single nation's capacity to address alone. Without a meaningful deterrent signal from the United States, China will continue to conduct these cable cuts, threatening the broader regional economy.

Ensuring Backup Connectivity: The Satellite Alternative

There are very few alternatives to these cables, as they are cost-effective and efficient at transmitting data worldwide. However, in an emergency, low-Earth orbit satellites are the most viable alternative to subsea cables for ensuring continuity of critical services. Satellites are harder to eliminate than cables, quicker to deploy, and do not present the same geographic chokepoints. Satellites have been used effectively in Ukraine, leading to the assumption that they can fully replace cable connectivity during a conflict. The reality, however, is that Ukraine's western regions remained connected through terrestrial cables to Poland and other European neighbors; satellite communications primarily supported critical military and government operations in contested areas.[36] Taiwan, as an island without terrestrial cable connections to friendly neighbors, faces a fundamentally more acute challenge.

Even the most advanced satellite constellations, like SpaceX's Starlink or Astranis' MicroGEO, cannot match the bandwidth of fiber-optic cables. Submarine cables provide over 100 terabits per second of internet bandwidth to Taiwan, while satellite systems can only provide a small fraction of that capacity.[37] Satellite connectivity should therefore be understood as an emergency complement that ensures continuity of critical government, military, and financial communications, but it will not completely replace cable infrastructure. SpaceX's Starlink, which

[33]Global Taiwan Institute, "China's Undersea Cable Sabotage and Taiwan's Digital Vulnerabilities," June 4, 2025.
[34]Indo-Pacific Defense Forum, "Taiwan Strengthens Patrols Against China's Undersea Cable Sabotage," September 27, 2025.
[35]Taiwan's Management Initiative on International Undersea Cables (RISK), standing for Risk Mitigation, Information Sharing, Systemic Reform, and Knowledge Building.
[36]Taiwan Insight, "The Most Critical Resilience Questions of Them All: Taiwan's Undersea Cables," October 2, 2024.
[37]Subsea Cables, "Why the World Still Depends on Cables, Not Satellites," February 2026.

proved critical in supporting Ukraine's military communications, is effectively unavailable to Taiwan. Negotiations broke down over Taiwan's legal requirement that foreign entities in communications ventures form a joint venture with a local partner maintaining majority ownership.[38] Additionally, SpaceX is compromised given Elon Musk's multiple business ventures in mainland China. Elon Musk has acknowledged that Chinese officials told him not to launch Starlink in China, which, given Beijing's position, must include Taiwan. But even if Starlink were available to Taiwan, Chinese researchers have concluded that jamming it over an area the size of Taiwan is technically feasible, though it would require more than 900 synchronized airborne platforms.[39]

With Starlink not a viable option, Taiwan is pursuing multiple alternatives. Our Space Agency plans to launch six satellites starting in 2026, with an investment of $1.23 billion, though we would need hundreds of satellites to create a system providing uninterrupted backup access.[40] The government has additionally partnered with OneWeb, which secured a commercial service license in Taiwan after completing a ground station in Thailand in 2024, and is in discussions with Amazon's Project Kuiper.[41] Taiwan has established approximately 700 satellite communications hotspots across the island for emergency use, a capability that proved valuable during a magnitude 7.4 earthquake in April 2024. These communications hotspots are designated by Taiwan's Ministry of Digital Affairs to be used for critical services: government agencies, the military, hospitals, and financial institutions, instead of for the general public.[42]

Additionally, in a significant development, Chunghwa Telecom signed a deal in April 2025 with Astranis for a dedicated MicroGEO satellite, which is expected to launch soon.[43] This layered approach, combining indigenous satellite development, partnerships with OneWeb and Amazon, and dedicated MicroGEO capacity, represents Taiwan's best path toward communications resilience. However, as one analyst has cautioned, relying on a single provider exposes future risks; diversification across multiple satellite partners remains essential.[44]

I mention satellites as a partial alleviation to sea cables, as the United States should also consider the broader regional dimension of backup connectivity. Allied nations throughout the Indo-Pacific face similar cable vulnerabilities, as several, such as the Pacific islands, are connected by a single cable that can leave them isolated if it is cut.[45] A comprehensive U.S. strategy for Indo-Pacific communications resilience should address not only Taiwan's specific needs but also the broader allied and partner network, ensuring that no single act of sabotage, or even a natural disaster, can sever a nation from the global information ecosystem. Pre-positioning satellite

[38]CNN, "Developing Taiwan's Own 'Starlink' Crucial for Island-Wide Communication," May 5, 2024.
[39] Domino Theory, "Taiwan Tech Firm Sees Military Uses for Its New Satellite," November 25, 2025.
[40] See note 38.
[41]CommonWealth Magazine, "Choosing OneWeb Over Starlink: Can Taiwan Build Communications Resiliency?," December 11, 2024.
[42]The Strategist, ASPI, "Wary of Cable Sabotage, Taiwan Looks to Satellites as Back-ups," February 18, 2025.
[43]Astranis, "Chunghwa Telecom and Astranis Sign Strategic Agreement to Launch Taiwan's First Dedicated Satellite," 2025.
[44] See note 41.
[45] Recorded Future, Submarine Cables Face Increasing Threats Amid Geopolitical Tensions and Limited Repair Capacity, accessed February 2026, https://www.recordedfuture.com/research/submarine-cables-face-increasing-threats

terminals and ground stations, investing in microwave backup systems, and developing rapidly deployable mobile communications platforms should all be part of this layered approach.

Emerging Trends

Several trends warrant the Commission's close attention. First, the development of purpose-built cable-cutting ships and the proliferation of PLA-linked patents represent a qualitative shift from improvised gray zone tactics toward preparations for systematic wartime destruction. Second, the growing bifurcation of global subsea cable networks along geopolitical lines risks fragmenting the global internet, as Chinese firms are prioritized for preferential cable routes, while the U.S. excludes Chinese networks, potentially leading to two largely separate digital ecosystems. Third, China's use of shadow fleet networks and sophisticated identity manipulation poses a growing challenge to maritime domain awareness, requiring new surveillance approaches. Fourth, as artificial intelligence and data center expansion drive unprecedented demand for bandwidth, the strategic importance of subsea cables will only intensify. Fifth, the limited global capacity for cable repairs, with average response times exceeding 40 days and only a handful of capable repair vessels worldwide, means that any large-scale disruption would have effects lasting weeks or months.[46]

While China's growing use of gray zone warfare is worth monitoring, the Commission should also monitor its expanding presence in the global cable repair market. U.S. officials have expressed concern that Chinese cable repair ships could compromise the security of U.S. cables in the Pacific by placing taps on undersea cables and conducting reconnaissance on U.S. military communication links under the pretext of conducting repairs. The dual-use nature of cable repair vessels, which require detailed knowledge of cable routes and access to the physical infrastructure, makes them potential instruments for intelligence collection. As the United States works to reduce Chinese involvement in cable construction, it must also address the risks posed by Chinese participation in cable maintenance and repair.

In addition to gray zone activities, as part of the Belt and Road Initiative, China has substantially expanded its influence from Southeast Asia to the Middle East and Europe. State-linked companies such as HMN Tech and China Unicorn operate as commercial firms and instruments of state strategy. Their accelerated implementation of the ASEAN Digital Master Plan 2025 has provided member states, especially Laos and Cambodia, with subsea cable infrastructure, job opportunities, and broader national development. In the Middle East and Europe, the Pakistan and East Africa Connecting Europe (PEACE) cable links China to Africa and Europe via Pakistan, Djibouti, and Egypt. HMN Technologies partially built this and was deliberately designed to circumvent Western jurisdictions, reflecting geopolitical considerations.[47] China's increased market presence can displace U.S. and allied companies as preferred partners, thereby providing the Chinese government with improved opportunities for espionage.

Recommendations for Congressional Action

[46] Recorded Future, as cited in Techzine Global, "Risk of Sabotage of Undersea Internet Cables Increases," July 18, 2025.

[47] Raghvendra Kumar, Securing the digital seabed: Countering China's underwater ambitions, *Journal of Indo-Pacific Affairs* 6, no. 8 (2023): 74-90.

Based on my analysis of the subsea cable threat environment, I respectfully offer the following recommendations for Congressional consideration.

Pass and fund the Taiwan Undersea Cable Resilience Initiative Act (S. 2222). This legislation would establish a framework for advanced monitoring and detection capabilities, rapid-response protocols for cable repair, intelligence-sharing mechanisms with Taiwan, and cable-hardening measures, including deeper reinforced burial and more resilient materials.[48] Its provisions to counter China's gray-zone tactics through joint drills, intelligence-sharing platforms, and collaborative surveillance deserve urgent attention.[49]

Fund an Indo-Pacific Undersea Cable Surveillance Network. Congress should appropriate funding for a comprehensive surveillance capability that integrates existing naval assets, new sensor deployments, satellite imagery, and allied intelligence to provide persistent monitoring of critical cable routes. This should include bilateral data-sharing agreements with Japan, South Korea, the Philippines, and Australia, building on the Quad Partnership for Cable Connectivity and Resilience launched in May 2023.

Invest in cable repair capacity. Congress should authorize procurement of cable-laying and repair vessels through the NEPTUNE Act and beyond, positioning both military and commercial repair capabilities in the western Pacific. Taiwan's lack of indigenous repair ships remains a critical vulnerability that the United States can help address.

Update the international legal framework. Congress should direct the State Department to pursue a modernized international agreement replacing the 1884 Convention for the Protection of Submarine Telegraph Cables. A new framework should establish clear norms, mandatory investigation and reporting requirements for cable damage, mechanisms for flag-state accountability, and enforcement provisions adequate to the challenge posed by state-sponsored sabotage through commercial proxies.

Mandate enhanced sanctions authority. Congress should create authority to sanction vessel owners, operators, flag state registries that facilitate sabotage, and entities that provide material support for cable-cutting operations, regardless of whether the sabotage targets U.S. cables directly.

Fund Taiwan's satellite communications resilience. Through existing security assistance frameworks, Congress should support Taiwan's indigenous satellite development and facilitate partnerships with non-Chinese satellite operators such as OneWeb and Amazon's Project Kuiper, including pre-positioning of satellite terminals for emergency deployment.

Direct an unclassified intelligence assessment. Congress should direct the intelligence community to produce an unclassified assessment of Sino-Russian coordination on maritime infrastructure sabotage. This would inform allied planning and build international consensus on the scope of the threat.

[48]S.2222, Taiwan Undersea Cable Resilience Initiative Act, 119th Congress (2025-2026).
[49]S.2222, Section 4, "Countering China's Gray Zone Tactics."

Support FCC implementation. Congress should ensure full and timely implementation of the FCC's updated submarine cable landing license rules, adopted in late 2025, which effectively bar Chinese and Russian entities from cable projects that touch U.S. territory.[50]

Execute freedom of navigation operations and joint drills. The United States should conduct freedom-of-navigation operations across the Taiwan Strait and work with the Taiwanese Coast Guard on rapid-response drills to deter ongoing sabotage. Making clear that systematic attacks on allied subsea infrastructure will be treated as attacks on critical infrastructure with proportionate consequences is essential to changing Beijing's calculus.

Additionally, I recommend that Taiwan establish a Standing Subsea Infrastructure Task Force, modeled after the CECC, to coordinate. The Task Force should include the Ministry of Defense, the Ministry of Transportation and Communications, the Ministry of National Defense, the Coast Guard, private telecommunication firms such as Chunghwa Telecoms, and our intelligence services. This Task Force would have the mandate to coordinate critical actions, such as direct repair of sea cables (when necessary), intelligence sharing on high-risk or suspicious vessels, and unified incident response. This would remove the bureaucratic seams that allow gray-zone warfare tactics to be effective.

I also recommend that Taiwan build indigenous cable-repair capabilities, such as a repair boat on standby for future cuts. This can be an initiative with Japan to ensure the collective defense of critical infrastructure, given that Japanese sea cables are also at risk from China’s gray-zone warfare. This can ensure cables can be repaired within a matter of days and alleviate pressure on international repair vessels, which may not be able to fix these cuts for weeks or even months.

Conclusion

The subsea cable threat from China is not a hypothetical concern for the future; it is a present and escalating danger. Since 2023, the pace and sophistication of cable sabotage incidents around Taiwan have increased markedly, and China is investing in purpose-built technologies that signal preparation for far more devastating attacks in a military scenario. The emergence of Sino-Russian coordination adds another dangerous dimension. Taiwan has taken important defensive steps, but it cannot address this threat alone.

The long-term solution lies in developing layered alternatives, including low-orbit satellite constellations and hardened cable routes, that cannot be easily disrupted by an adversary operating beneath the waves. But in the near term, the United States must make clear through both word and action that systematic attacks on allied subsea infrastructure will carry real consequences. The United States has a narrow window to strengthen deterrence, build resilience, and shape the international response before a major crisis occurs. I urge Congress to act with urgency. Thank you for the opportunity to testify, and I welcome your questions.

[50]Federal Register, "Review of Submarine Cable Landing License Rules and Procedures," October 27, 2025.