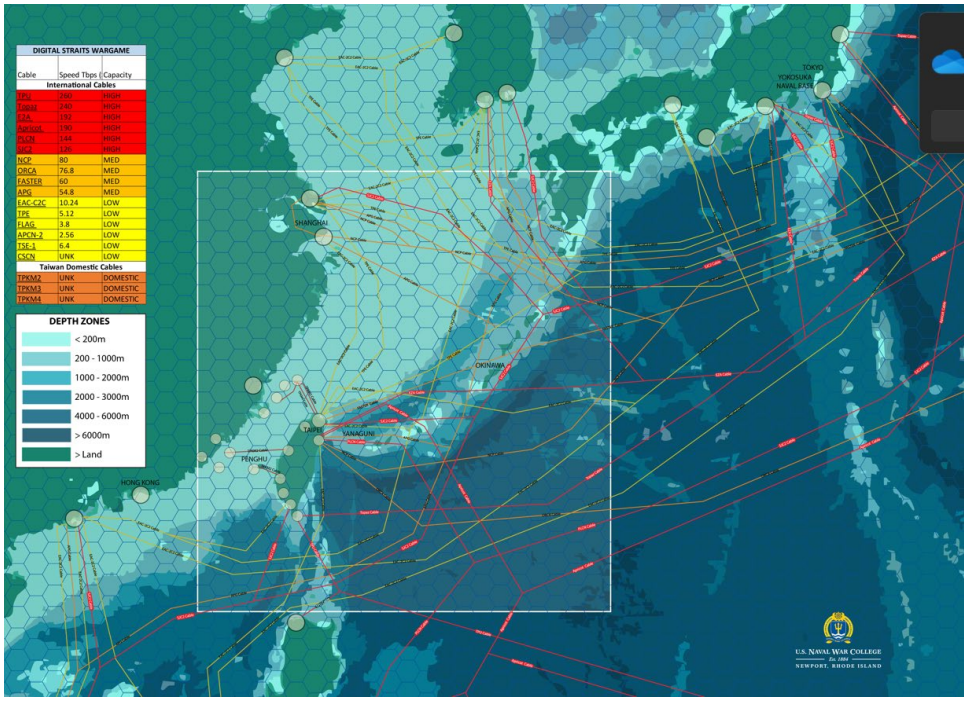
CYBER & INNOVATION POLICY INSTITUTE
U.S. NAVAL WAR COLLEGE • NEWPORT, RI



Digital Straits Wargame Report

(July 2026)

Authored by: Jason Vogt & Nina Kollars

Game Designed by the CIPI Gravely Group 25-26

Prof. Jason Vogt

Dr. Nina Kollars

LCDR Luke Millen (USN)

Maj Eric Dayhuff (USAF)

LTC Adam Gray (USAF)

MAJ Sam Harding (USA)

CAPT Brendan Sullivan (USCG)

Mr. Derek Albert (DoS)

Table of Contents

Disclaimer: Professor Vogt and Dr. Kollars are researchers who collaborate with students of Cyber and Innovation Policy Institute's Gravely Group Advanced Research Project. The opinions and views expressed are those of the authors alone and do not necessarily represent the assessments or policies of the U.S. Government, U.S. Department of War or its components, to include the Department of the Navy or the U.S. Naval War College.

I. Executive Summary

From January-March 2026, the U.S. Naval War College's Cyber & Innovation Policy Institute conducted three unclassified critical infrastructure wargames focused on defending Taiwan's commercial undersea communications cables called the Digital Straits Wargame. These games included over 50 participants from the U.S. military, Japan's self-defense forces, Australia's science and technology community, other national security experts and members of the private sector.

Teams representing the maritime security forces from the United States, Japan, Taiwan and other regional partners demonstrated that through coordinated regional action they could complicate Chinese sabotage efforts against Taiwan's international undersea communications systems in a wargame scenario based on a limited confrontation in 2030. However, Taiwan's domestic cables—particularly those connecting its outlying islands located inside the Taiwan Strait—remained acutely vulnerable. Despite sharing the same objectives, players across all three games executed different approaches to operations inside the strait based on their defensive priorities and perceived risk of escalation.

The question of whether the U.S. and its partners/allies should prioritize protection of international cables over Taiwan's domestic infrastructure weighed heavily on player decisions. Several teams chose to prioritize the protection of international cable infrastructure over Taiwan's domestic cables, believing this could help control escalation with China and conserve limited repair assets for the highest priority infrastructure. However, this decision also leaves Taiwan's islands digitally isolated and the government vulnerable to additional pressure, which could further China's coercive objectives directed at Taiwan.

In two instances, players chose not to deploy U.S. naval assets into the Taiwan Strait prior to the initiation of China's cable sabotage campaign resulting in the islands being cut off from the mainland. During a third game, the U.S. and Taiwan teams flooded the strait with military, coast guard, surveillance and repair assets, which severely hampered the China's ability to conduct cable-cutting operations. While these operations were effective in this specific situation, they did place U.S. forces and repair assets at increased risk.

The threat posed by China's civilian deep-sea research vessels, which can operate in remote areas of the Pacific where undersea cables traverse, also posed substantial challenges to the players representing the U.S. and its partner nations. Some research vessels carry deployable manned submarines, remotely operated vehicles (ROVs) or autonomous underwater vehicles (AUVs) capable of operating along the sea floor.[i] These submersibles are designed to survey environmental data and collect mineral samples but could also be used to support cable sabotage operations.[ii] Monitoring and interdicting these vessels would require substantial resources, which were unavailable during the game. Prioritizing one or two high-capacity cables for surveillance, protection and repair enabled more effective use of the limited assets available.

II. Background

Taiwan's Undersea Cable Infrastructure[1]

The international undersea fiberoptic communications cable network consists of over 600 current or planned cables that stretch nearly 1.5 million kilometers. Fueled by the exponential growth of the worldwide web, these cables carry more than 90% of the globe's international internet traffic.[iii] Nearly all these cables are owned and operated by private companies, including major telecommunications providers. Increasingly, global technology firms, such as Google, Meta and Amazon have invested in cable infrastructure to connect directly to their growing data center infrastructure.[iv]

Undersea cables are produced by a handful of global providers, which are installed and repaired by an international fleet of approximately 80 vessels.[v] They are designed to operate in harsh underwater environments for at least 25 years but are frequently damaged by human activity and geological events. The International Cable Protection Committee, a non-profit organization focused on improving the security of undersea cables, estimates that between 150-200 cable faults occur globally each year.[vi] More than half of these incidents can be attributed to accidents involving fishing equipment and anchors. As geopolitical tensions have increased in Europe and Asia, analysts have identified at least nine cable cutting incidents that have involved suspicious circumstances, five of which have occurred around Taiwan. [vii]

By 2028, Taiwan will be serviced by nineteen undersea cable systems, which come ashore at ten cable landing stations.[viii] A cable landing station houses networking systems that connect undersea data traffic to the land-based internet service providers and telecommunications infrastructure. Near areas closer to shore, cables are often buried in a protective trench that can stretch for several kilometers. In areas where burying is not possible, cables can be enclosed in a protective metal sheath to help protect them from anchors and other hazards. In deeper waters, cables lay directly on the ocean floor without any additional protection.

Nearly all of Taiwan's cable systems consist of multiple cables, several of which connect to more than one landing station in Taiwan. Sixteen are international, accounting for more than 90% of Taiwan's external internet traffic. The remaining three cable systems are domestic, connecting to Taiwan's outlying islands located in the Taiwan Strait. [ix]

Since the first undersea fiberoptic cables were connected to Taiwan in the 2000's, the capacity of cable systems has increased significantly. Older systems have system wide bandwidths of less than 10 terabytes per second (TB/s), whereas some newer cables have 20 times that capacity. For example, Google's recently installed Topaz cable has a systemwide capacity of 240 TB/s,

[1] *For additional information see "Cuts Both Ways: The Geography, Technology and Strategy of Undersea Cable Sabotage in the Pacific," published by the authors in the Journal of Information Warfare in July 2026. https://www.jinfowar.com/journal/volume-25-issue-3/cuts-both-ways-geography-technology-strategy-undersea-cable-sabotage-pacific*

which means that it can carry more data than all eight cable systems connected to Taiwan prior to 2016. In the event of a conflict or natural disaster, it is possible that 2-3 high-capacity cable systems would be sufficient for Taiwan's international data needs, although this would be contingent on electrical power and land-based infrastructure also being intact.[x]

Two-thirds of Taiwan's cables connect directly to Japan, which serves as a regional cable hub. Taiwan also maintains direct connections to South Korea, the Philippines, Singapore and the U.S. territory in Guam. Eight systems connect to China, only three of which are higher capacity. [xi]

Taiwan's onshore cable infrastructure, which includes the cable landing stations, is concentrated in the northern part of the island, located close to Taipei. Several higher bandwidth cables come ashore in in the township of Toucheng, located along the eastern coast. Here the waters grow deep quickly, offering greater natural protection than those located along Taiwan's western shores.[xii] Several new cables are being installed by hyperscalers in southern portion of the island, where there are also additional data centers planned.

Taiwan's territory also includes dozens of smaller islands located inside the Taiwan Strait. There are three domestic cable systems that connect to the Kinmen, Penghu and Matsu islands to mainland Tawain. These islands are home to over 150,000 residents, who rely on cables to maintain connectivity to the mainland.[xiii] These cables sit in relatively shallow waters near China, making them particularly vulnerable to sabotage.

III. Game Overview

The Digital Straits Wargame is designed to explore how the U.S. and its regional allies/partners can protect Taiwan's undersea communications cable infrastructure from attacks and deter Chinese maritime forces from supporting cable sabotage operations. The players were divided into four teams (U.S., Taiwan, Japan and an International Team) that worked cooperatively to protect Taiwan's undersea infrastructure from a Chinese cable sabotage campaign. China's (Red Team) actions were preplanned and directed by the game's facilitators. Players were given a limited number of surface vessels, surveillance platforms and repair assets to conduct their operations. In addition to surface ships, the Red Team also had several cable sabotage platforms capable of operating at different ranges and depths. The game took ~3 hours to play and represented 48-72 hours of maritime security operations.

Game Schedule

Introduction

- 0:00-0:30- Intro Game Brief

Move 1 (Partner Nations Initiate)

- 0:30-1:00- Planning & Force Laydown
- 1:00-1:15- Red Force Reveal
- 1:15-1:45- Partner Movement and Key Interactions
- 1:45-2:00- Reposition and Repair

Move 2 (Red Initiates)

- 2:00-2:10- Red Movement
- 2:10-2:30- Partner Planning
- 2:30-2:45- Movement and Key Interactions

Post-Game Discussion

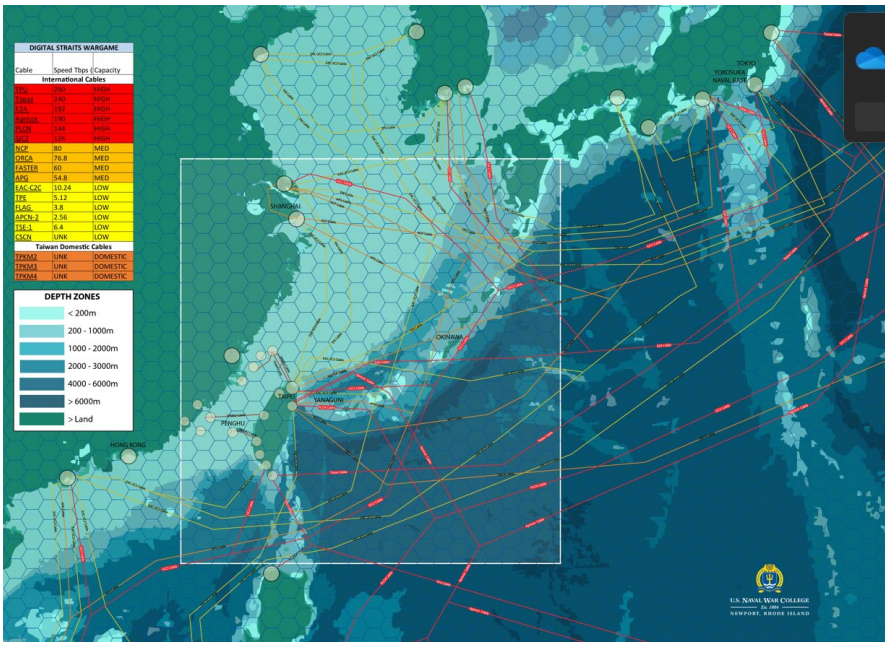
- 2:45-3:00- Facilitated discussion

Game Introduction

Players were pre-recruited based on regional or technical expertise. They were divided into four teams (U.S., Taiwan, Japan and International) with 3-5 personnel on each team. Prior to the start of the game, players were provided an overview brief that describes Taiwan's unclassified undersea communications cable infrastructure, the game board, scenario, objectives, constraints, friendly order-of-battle/capabilities, enemy order of battle/cable sabotage capabilities, and the game schedule.

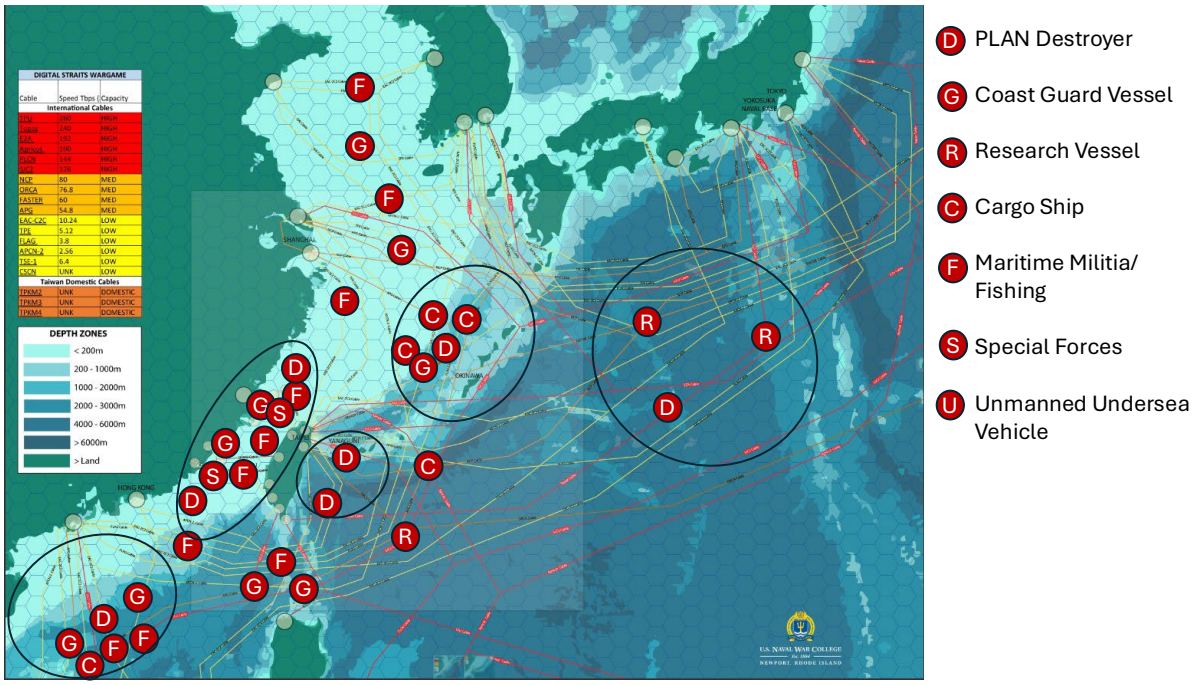
Move 1 (Partners Initiate)

During the first move, players were provided detailed maps of Taiwan's unclassified undersea communications infrastructure and game tokens representing their given order-of-battle. The teams were asked to study the infrastructure and develop a cooperative maritime security plan to protect it. This is done prior to any Chinese assets being placed on the game board. At the end of the planning stage, all partner nation teams placed their assets on the game board.



(U) Game board depicting Taiwan's undersea communications infrastructure

Following the initial laydown, Chinese assets were placed onto the game board, revealing the initial stages of a cable sabotage campaign focused on the Taiwan Strait. The Red Team used Chinese maritime militia and commercial cargo vessels to conduct cable cutting operations supported by People's Liberation Army (PLA) Navy and Chinese coast guard assets. Their game objective is to sever cables connecting Taiwan's islands from the mainland. The game scenario also included suspected PLA maritime Special Operations Forces (SOF) deployments near Taiwan's islands, which could be used to plant explosives on cable infrastructure. Additionally, China deploys suspected cable sabotage platforms in the East China Sea and South China Sea. Several PLA Navy destroyers are positioned near Taiwan's eastern coast, and multiple deep-sea research vessels are operating in the Philippine Sea in the vicinity of cable infrastructure.



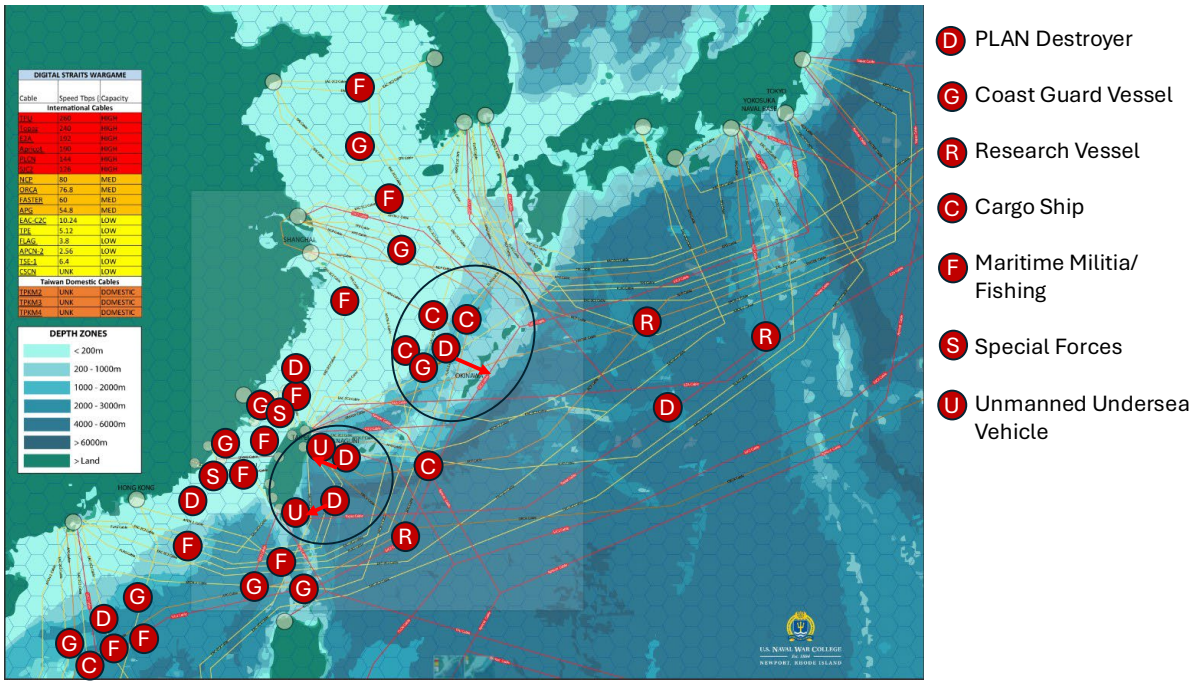
(U) China Laydown Move 1

Once Chinese forces are revealed, the teams are asked to describe their initial force laydown and reactions to the Red strategy. Teams then reposition assets to interdict or deter Chinese cable-cutting operations. They can also deploy cable repair platforms. Key interactions are discussed as a group. At the end of the turn, the facilitators determine which cables have been severed, along with its impact to Taiwan's overall connectivity.

Move 2 (China Initiates)

During Move 2, two PLA Navy destroyers located off Taiwan's eastern coast launch unmanned undersea vehicles (UUV) capable of laying mines or other explosives. These UUVs travel along the seafloor to areas where there are clusters of high-capacity cables that originate at the landing stations in Toucheng and Dawu. These UUVs, which are ascribed to potentially reach depths up to 6000 meters, allow them to target locations where the cables lay on the seafloor unprotected.[xiv]

Separately, a group of Chinese military, coast guard and suspected cable sabotage vessels operating in the East China Sea, attempt to move into the shallow waters near Okinawa to conduct cable cutting operations. Teams are given an opportunity to reposition their forces in response to these new threats. The round concludes with a discussion of these key interactions.



(U) Red Laydown Move 2

IV. Findings

Regional Cooperation Can Reduce Risks to <u>International</u> Cable Infrastructure

Teams representing the maritime security forces from the United States, Japan, Taiwan and other regional partners demonstrated that through coordinated regional action they could complicate Chinese sabotage efforts against Taiwan's international undersea communications systems. By focusing their forces along the southern Ryukyu islands, Japan was able to deter Chinese attacks along the island chain and prevent China from exploiting the seam between Japan's territory and northern Taiwan where multiple high-bandwidth cables traverse. Similarly, by deploying forces in the gap between Taiwan and the Philippines, partner nation teams prevented Chinese sabotage operations against Taiwan's most important southern cable infrastructure.

Although cable infrastructure located closer to China in the South China Sea and East China Sea remained exposed, almost all these cables were lower bandwidth. If they were severed, it would not have a significant impact on Taiwan's international communications. Across all three games, Taiwan was never in danger of losing all its international data connectivity.

Taiwan's Domestic Cables Remain Vulnerable – "To Protect or Not to Protect?"

Taiwan's domestic undersea cables—particularly those connecting its outlying islands located inside the Taiwan Strait—remained acutely vulnerable due to limited resources made available. Despite sharing the same objectives, players across all three games executed different approaches to operations inside the Taiwan Strait based on their defensive priorities and perceived risks of escalation. The question of whether to prioritize protection of international cables over Taiwan's domestic infrastructure weighed heavily on player decisions, with several teams choosing to prioritize the protection of international cable infrastructure over Taiwan's.

Teams representing Taiwan consistently deployed their assets with the goal of protecting their domestic cables in the Taiwan Strait; however, they did not possess sufficient assets to deter the China's cable cutting operations independently. In two iterations, U.S. teams chose not to deploy naval assets into the strait prior to the initiation of China's cable sabotage campaign. This could help control escalation with China and conserve limited repair assets for the highest priority infrastructure. However, it also leaves Taiwan's islands digitally isolated and its government vulnerable to pressure, which could further China's coercive objectives against Taiwan.

Several players stated that sending U.S. destroyers into the strait was too provocative and that they did not want to risk escalation to protect Taiwan's domestic cables. During these games, Taiwan's islands were cut off from the mainland. Once the cables were severed, teams then had to choose whether and how to respond to the incidents.

In one iteration, partner teams responded forcefully, deploying U.S. surface assets, Explosive Ordnance Disposal (EOD) and repair assets into the strait to reassure Taiwan and restore connectivity. In the second game, players chose to only deploy EOD and military repair assets under Taiwanese escort, raising questions about the U.S. and Taiwan's capability to coordinate security for these types of assets. Both decisions carry substantial risks, particularly if China attempts to challenge or disrupt the repair operations.

During the third game, teams flooded the Taiwan Strait with military vessels, coast guard ships, surveillance platforms and pre-positioned repair assets, prior to the start of Chinese sabotage operations. This severely hampered China's ability to conduct cable-cutting operations. These players acknowledged the risk of escalation but decided that deterring China was a higher priority. During a real-world crisis, the decision to deploy U.S. military assets into the Taiwan Strait would be contingent on multiple factors not represented in this wargame, including diplomatic activities and economic considerations.

China's Deep-Sea Research Fleet is a Challenging Threat to Mitigate

The threat posed by China's civilian deep-sea research vessels, which can operate in more remote areas of the Pacific, also posed substantial challenges to cable protection operations. Several high-capacity cables that connect Taiwan to Japan traverse the Philippine Sea, an area that is too vast to patrol with the limited assets available during this game. Players suggested that long-range surveillance assets, such as multi-purpose reconnaissance aircraft or long-range drones, could be used to monitor these vessels and publicly expose their activities.

One player suggested prioritizing one or two high-capacity cables for surveillance, protection and repair, which would enable more effective use of the limited assets available. This concept would require partner nations to identify specific cables pre-conflict and to load civilian repair ships with spare cables from these systems to enable more rapid repair. Multiple airborne and sea-based surveillance platforms would then be deployed to monitor the cables. Maritime security vessels would also patrol the cable route, with the goal of responding swiftly to any suspected cable sabotage operations.

V. Conclusion

The Digital Straits Wargame has served to highlight the complex coordination and cooperation challenges surrounding Taiwan's undersea communication infrastructure. The wargames demonstrated that coordinated action between the United States, Japan, Taiwan, and other regional partners can complicate and deter Chinese sabotage of international cables. However, Taiwan's domestic cables within the Taiwan Strait will likely remain vulnerable. This reality, coupled with the critical and unresolved question of whether to risk escalation by deploying U.S. naval assets for their protection, presents an immediate and pressing strategic dilemma.

References

[i] Cranworth, N 2025, 'China's deep-sea exploration advances with Jiaolong and Fendouzhe success', *Marine Technology Review*, 2 January, viewed 24 April 2026
[ii] Martinson, R. 2018, "China maritime report No. 3: China's distant-ocean survey activities: Implications for US national security", US Naval War College.
[iii] TeleGeography. "Submarine Cable FAQs." Accessed early 2025. https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions
[iv] Forlini. PCMag. "Inside Meta's Effort to Build the World's Longest Underwater Cable." December 3, 2025. https://www.pcmag.com/news/inside-metas-effort-to-build-the-worlds-longest-underwater-cable?test_uuid=04IpBmWGZleS0I0J3epvMrC&test_variant=B
[v] Recorded Future. "Insikt Report." 2023. https://assets.recordedfuture.com/insikt-report-pdfs/2023/ta-2023-0627.pdf
[vi] Carter L., Burnett D., Drew S., Marle G., Hagadorn L., Bartlett-McNeil D., and Irvine N. (2009). Submarine Cables and the Oceans – Connecting the World
[vii] Recorded Future. "Insikt Report." 2023. https://assets.recordedfuture.com/insikt-report-pdfs/2023/ta-2023-0627.pdf
[viii] TeleGeography. "Taiwan." Submarine Cable Map. https://www.submarinecablemap.com/country/taiwan
[ix] TeleGeography. "Taiwan." Submarine Cable Map. https://www.submarinecablemap.com/country/taiwan
[x] Submarine Networks."Topaz." https://www.submarinenetworks.com/en/systems/trans-pacific/topaz
[xi] TeleGeography. "Taiwan." Submarine Cable Map. https://www.submarinecablemap.com/country/taiwan
[xii] TeleGeography. "Taiwan." Submarine Cable Map. https://www.submarinecablemap.com/country/taiwan
[xiii] City Population. "Taiwan: Administrative Division." Accessed on 11 February, 2026. https://www.citypopulation.de/en/taiwan/reg/admin/
[xiv] Fedasiuk, Ryan. "How China is Militarizing Autonomous Underwater Vehicle Technology." The Maritime Executive, August 22, 2021.