

JONATHAN WALBERG // ASSOCIATE DIRECTOR

ETHAN CONNELL // RESEARCH TEAM LEAD

6 MARCH 2025

RELEASE

STRATEGIC RISKS TO TAIWAN'S UNDERSEA CABLE INFRASTRUCTURE

Synopsis: Taiwan relies on undersea cables for internet access and connectivity. Recent attempts to disrupt Taiwan's submarine cable infrastructure demonstrate this network's vulnerabilities. At the same time, the PRC appears to be developing new cable cutting capabilities.

Background

Undersea fiber-optic cables carry over 95% of global internet traffic. [1] These cables are a critical part of the global telecommunications infrastructure. The Indo-Pacific region hosts extensive undersea networks, but these cables are vulnerable to natural disasters, accidental damage, and sabotage. [2] Recent disruptions in the Taiwan Strait and the South China Sea underscore the PRC's interest in disrupting this network. [3]

Undersea Cables in Taiwan: Incidents

15 submarine cables, which come ashore at 7 cable landing sites, provide internet service to Taiwan. Recent attempts to sabotage these cables include (but are not limited to):

- On January 3, 2025, the Chinese-crewed ship "*Shunxin39*" damaged the TPE cable north of Taipei [5]
- The next month, two separate cable cutting incidents led to the complete disruption of internet access to the Matsu Islands [6]
- On February 25th, 2025, the Chinese-crewed ship *Hong Tai 58* damaged the TPKM-3 undersea cable. [7]

The map below shows the locations of all undersea cables connected to Taiwan and notes the location and date of these incidents.



Figure 1: A map of cable incidents created by TSM researchers Ethan Connell and Chris Dayton

China's Role

The PRC is developing new techniques and capabilities to disrupt submarine cable communications. The diagram below depicts an anchor-like device developed by researchers at China's Lishui University. This device, developed to fulfill a "need for a fast, low cost cutting apparatus for submarine cables," is designed to sever cables by dragging along the sea floor behind a vessel. [8] China appears to have also used this technology appears in the Baltic Sea as well. In a November 2024, the Chinese vessel *Yi Peng 3* severed two submarine cables, cutting data communications between Finland and Germany. [9]



Figure 2: A diagram of the cutting apparatus created by researchers at Lishui University.

Implications

The internet blackout in the Matsu Islands demonstrates the degree to which Taiwan depends on its undersea communications infrastructure. The loss of connectivity negatively impacted banking, commerce, and government operations. [10]

Communications infrastructure also plays a key role in both peacetime resilience and conflict preparedness. Disruptions to undersea cables, whether accidental or intentional, could serve as a gray-zone tactic to pressure governments and populations without escalating to open conflict. [11] If left unaddressed, adversaries could exploit these vulnerabilities to isolate key regions, creating economic damage and sowing widespread confusion and uncertainty.

Given that military and diplomatic communications also rely on these networks, any disruption could hinder crisis management and defense coordination. Taiwan does not operate its own submarine cable repair vessels, [12] resulting in repair times of anywhere between 6-8 weeks and several months. [13] Strengthening cable security is therefore important for Taiwan's resilience and readiness. [14]