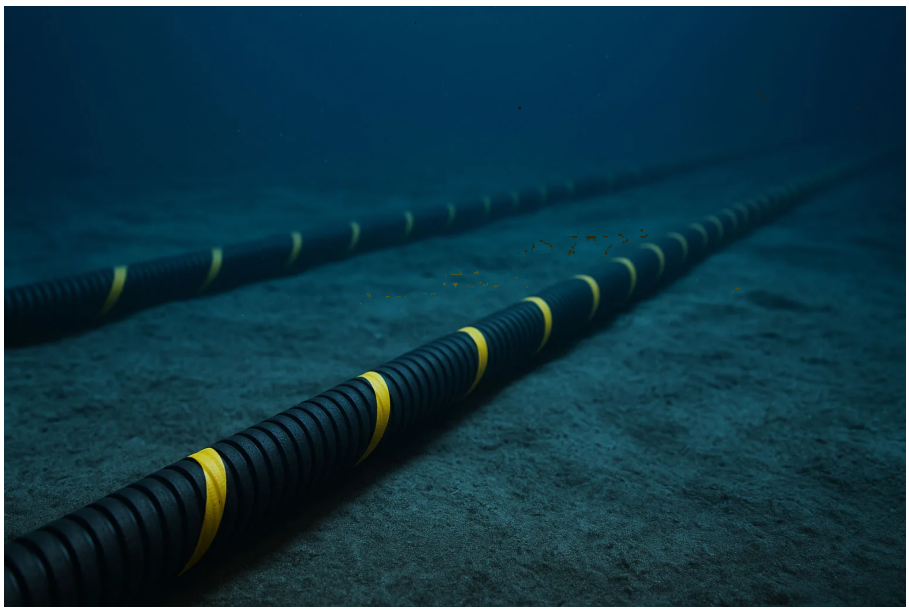

Risk of Undersea Cable Sabotage: Companies Launch New Solutions in the Indo-Pacific

Published on 28/04/2025

Taiwanese authorities accused this month the Chinese captain of the cargo ship *Hong Tai 58* of damaging an undersea communication cable connecting the island to the Penghu archipelago, located near the Chinese coast.

This case is a clear example of how undersea cable sabotage — a difficult activity to prove — has become an integral part of "gray zone" tactics, aimed at identifying and exploiting opponents' weaknesses.

The Taiwanese coast guard had already detained the *Hong Tai 58* — a Togo-flagged ship with a Chinese crew — at the end of February. A similar incident occurred north of Taiwan in January, involving a Hong Kong-owned commercial vessel.

This year, Taiwan has already recorded five cases of undersea cable damage, compared to the three annual cases recorded in both 2023 and 2024. In response, the coast guard has compiled a blacklist of about 100 suspect ships, all with ties to China.



The cargo ship Hong Tai 58, detained by the Taiwanese coast guard in February 2025 ©taipeitimes.com

A Growing Threat

Despite official denials from Beijing, some observers believe these sabotages are part of China's coercive strategies against Taiwan.

During a hearing of the *House Armed Services Committee* in the United States, Senator *Jacky Rosen* (D-Nev.) denounced China's "reckless, coercive, and aggressive activities," pointing to undersea cable sabotage as a "particularly alarming tactic."

At the same hearing, Admiral *Samuel Paparo*, commander of the U.S. Navy's Indo-Pacific Command (INDOPACOM), confirmed the existence of sabotage attempts around Taiwan.

A few weeks after the seizure of the *Hong Tai 58*, it emerged that the Chinese Naval Scientific Research Center had patented a deep-water device capable of cutting even the most fortified communication or power cables.

In the event of a large-scale conflict, one of China's priorities would be to isolate Taiwan, compromising civilian and military communications.

In his address to Congress, Admiral Paparo outlined two strategies to counter these sabotages:

- **Intelligence and rapid intervention**: intercept damage attempts through monitoring and targeted action.
- **Resilience**: create redundant communication networks and develop constellations of low Earth orbit satellites to ensure communication continuity.



Admiral Samuel Paparo, commander of the Indo-Pacific Command for the United States ©U.S. Navy

The Private Sector's Response

The private sector is also responding to this new threat.

Saab Australia aims to support governments in protecting undersea infrastructure through advanced mine countermeasure technologies. The company offers autonomous underwater vehicles (AUVs) and seabed sensors capable of real-time infrastructure monitoring. Among the solutions presented are the remotely operated vehicle Work-Class (wWROV), controllable via satellite up to 5,500 meters deep, and the AUV Sabertooth, capable of continuous operation thanks to an underwater docking station.

In France, the company *Exail* has secured a contract with the French Ministry of Defense to develop AUVs capable of operating up to 6,000 meters deep. These systems, expected to be delivered by 2027, will be able to autonomously reprogram ongoing missions in case of detecting suspicious activities.

Thales Australia is focusing on *Blue Sentry* technology, which uses thin-line towed arrays for detecting both surface and underwater threats. The system is designed to identify and track

anomalous contacts through a network of advanced sensors.

The remotely operated vehicle *Work-Class* (WROV), controlled via satellite and capable of operating up to 5,500 meters deep ©Saab

Maritime Surveillance and Integrated Threat Response

The protection of critical undersea infrastructure, such as communication and power cables, requires a multi-level approach based on the integration of advanced technological capabilities and a continuous and structured maritime surveillance system.

Among operational solutions, the use of automatic identification systems for naval units (AIS) represents a fundamental tool for real-time monitoring of maritime routes and activities. These systems allow for the detection of any deviations from authorized routes, immediately activating alert mechanisms and enabling rapid intervention by the competent authorities.

Strengthening maritime domain awareness is strategic for anticipating and countering anomalous or suspicious behaviors that could threaten the integrity of undersea infrastructure. An effective analysis and reaction capability allows for the prevention of hostile actions before significant damage occurs, or for timely intervention after an illicit action, ensuring coordinated incident management through international diplomatic and legal channels.

The adoption of these integrated measures is particularly relevant for island states or strategic regions with a high density of critical infrastructure, where the resilience of the information system and the protection of communications are essential elements for national security and regional stability.

News link: https://www.defensenews.com/global/asia-pacific/2025/04/25/with-indo-pacific-undersea-cables-at-risk-companies-tout-their-tech/