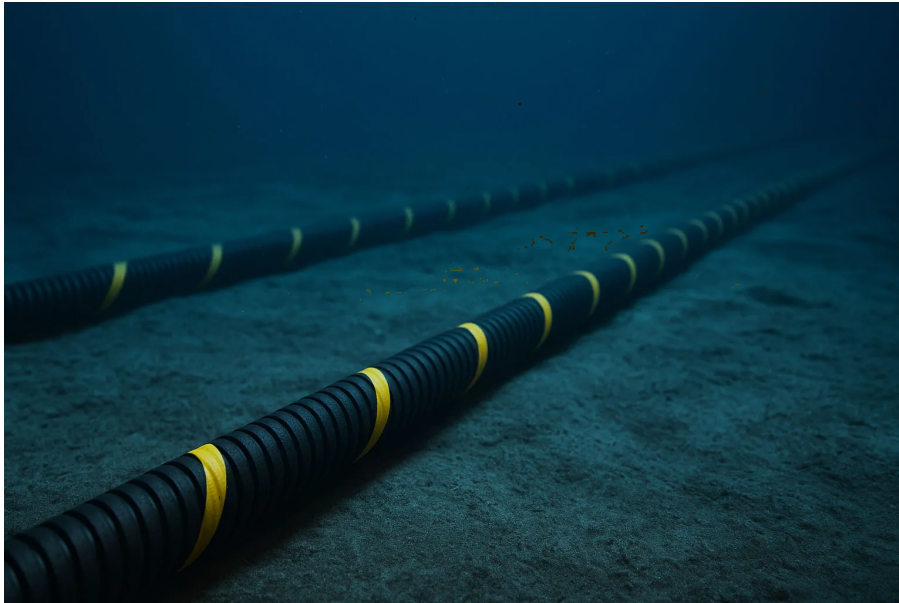




Rischio sabotaggi cavi sottomarini: le aziende lanciano nuove soluzioni nell'Indo-Pacifico

Pubblicato il 28/04/2025

Le autorità di Taiwan [hanno accusato questo mese](#) il capitano cinese della nave cargo *Hong Tai 58* di aver danneggiato un cavo di comunicazione sottomarino che collega l'isola all'arcipelago delle Penghu, situate vicino alla costa cinese.

Questo caso rappresenta un chiaro esempio di come il sabotaggio dei cavi sottomarini — attività difficile da provare — sia ormai parte integrante delle tattiche di "zona grigia", volte a individuare e sfruttare i punti deboli degli avversari.

La guardia costiera taiwanese aveva già trattenuto il *Hong Tai 58* — una nave battente bandiera togolese con equipaggio cinese — alla fine di febbraio. Un episodio simile si era verificato a nord di Taiwan in gennaio, coinvolgendo in quel caso una nave commerciale di proprietà di Hong Kong.

Quest'anno Taiwan ha già registrato cinque casi di danneggiamento dei cavi sottomarini, contro i tre casi annuali registrati sia nel 2023 che nel 2024. In risposta, la guardia costiera ha compilato una lista nera di circa 100 navi sospette, tutte con legami alla Cina.



La nave cargo Hong Tai 58, trattenuta dalla guardia costiera di Taiwan a febbraio 2025 ©taipeitimes.com

Una minaccia crescente

Nonostante le smentite ufficiali di Pechino, alcuni osservatori ritengono che questi sabotaggi rientrino nelle strategie coercitive cinesi contro Taiwan.

Durante un'audizione del *Comitato per i Servizi Armati della Camera* statunitense, la senatrice *Jacky Rosen* (D-Nev.) [ha denunciato](#) le "attività imprudenti, coercitive e aggressive" della Cina, indicando il sabotaggio dei cavi sottomarini come una "tattica particolarmente allarmante".

Alla stessa audizione, l'ammiraglio *Samuel Paparo*, comandante del Comando Indo-Pacifico (INDOPACOM) della Marina statunitense, ha confermato l'esistenza di tentativi di sabotaggio attorno a Taiwan.

Poche settimane dopo il sequestro del *Hong Tai 58*, è emerso che il Centro di Ricerca Scientifico Navale cinese aveva brevettato un dispositivo per acque profonde, in grado di tagliare anche i cavi di comunicazione o alimentazione più fortificati.

In caso di conflitto su vasta scala, una delle priorità della Cina sarebbe isolare Taiwan, compromettendo le comunicazioni civili e militari.

Nel suo intervento al Congresso, l'ammiraglio Paparo ha indicato due strategie per contrastare questi sabotaggi:

- **Intelligence e intervento rapido:** intercettare i tentativi di danneggiamento attraverso il monitoraggio e l'azione mirata.
- **Resilienza:** creare reti di comunicazione ridondanti e sviluppare costellazioni di satelliti in orbita terrestre bassa per garantire la continuità delle comunicazioni.



L'ammiraglio Samuel Paparo, comandante del Comando Indo-Pacifico per Stati Uniti ©U.S. Navy

La risposta del settore privato

Anche il settore privato sta rispondendo a questa nuova minaccia.

Saab Australia si propone di supportare i governi nella protezione delle infrastrutture sottomarine attraverso tecnologie avanzate di contromisure contro le mine. L'azienda offre veicoli sottomarini autonomi (AUV) e sensori da fondale in grado di monitorare le infrastrutture in tempo reale. Tra le soluzioni presentate figurano il veicolo comandato a distanza [Work-Class \(wWROV\)](#), controllabile via satellite fino a 5.500 metri di profondità, e l'[AUV Sabertooth](#), capace di operare in maniera continuativa grazie a una stazione di attracco subacquea.

In Francia l'azienda *Exail* ha ottenuto un contratto con il Ministero della Difesa francese per la realizzazione di AUV in grado di operare fino a 6.000 metri di profondità. Questi sistemi, previsti in consegna entro il 2027, saranno in grado di riprogrammare autonomamente le missioni in corso in caso di rilevamento di attività sospette.

Thales Australia punta invece sulla tecnologia *Blue Sentry*, che utilizza array rimorchiati a linea sottile per il rilevamento di minacce sia in superficie sia subacquee. Il sistema è progettato per identificare e tracciare contatti anomali grazie a una rete di sensori avanzati.

Rischio sabotaggi cavi sottomarini: le aziende lanciano nuove soluzioni nell'Indo-Pacifico - brigatafolgo

Il veicolo operato a distanza *Work-Class* (WROV), controllato via satellite e in grado di operare fino a 5.500 metri di profondità ©Saab

Sorveglianza marittima e risposta integrata alle minacce

La protezione delle infrastrutture sottomarine critiche, come i cavi di comunicazione e di alimentazione, richiede un approccio multilivello fondato sull'integrazione tra capacità tecnologiche avanzate e un sistema di sorveglianza marittima continuo e strutturato.

Tra le soluzioni operative, l'utilizzo dei sistemi di identificazione automatica delle unità navali (AIS) rappresenta uno strumento fondamentale per il monitoraggio in tempo reale delle rotte e delle attività marittime. Tali sistemi consentono di rilevare eventuali deviazioni dai percorsi autorizzati, attivando immediatamente meccanismi di allerta e permettendo un rapido intervento da parte delle autorità competenti.

Il rafforzamento della consapevolezza del dominio marittimo è strategico per anticipare e contrastare comportamenti anomali o sospetti che potrebbero minacciare l'integrità delle infrastrutture sottomarine.

Un'efficace capacità di analisi e reazione consente di prevenire azioni ostili prima che si verifichino danni significativi, oppure di intervenire tempestivamente dopo un'azione illecita, assicurando una gestione coordinata dell'incidente anche attraverso canali diplomatici e giuridici internazionali.

L'adozione di queste misure integrate è particolarmente rilevante per Stati insulari o regioni strategiche ad alta densità di infrastrutture critiche, dove la resilienza del sistema informativo e la protezione delle comunicazioni rappresentano elementi essenziali per la sicurezza nazionale e la stabilità regionale.

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