DOI:10.6237/NPJ.202608_60(4).0006

中共混合威脅下我國海底電纜安全與防護策略

Taiwan's Submarine Cable Security and Protection Strategies under Hybrid Threats from China

曾敏禎　小姐

提　　要：

一、我國海底通訊電纜承載外、離島民生、金融、政務與國防通信，更成為中共「灰色地帶襲擾」的重要目標；近年，國內海纜受外力破壞事件顯著增加，馬祖地區更數度因大陸籍漁船或貨輪蓄意破壞造成斷纜而多日斷網，連帶凸顯我國關鍵基礎設施的脆弱性。

二、中共對我國海纜破壞似呈現系統化樣態，包括以盜砂船與漁船在敏感海域作業，藉民事活動掩護政治目的；或動用商船於禁錨區下錨破壞並偽裝為意外，更運用「權宜輪」降低可歸因性，再加上海纜切割技術研發，讓此一威脅由近岸延伸至深海，影響不容小覷。

三、鑒於海纜安全已成為國安核心議題，更攸關我國通訊韌性與民生穩定，故本文提出可行的監控、防護與國際協作對策，並依「預防、偵測、回應與修復、嚇阻」架構，強化巡弋與智慧監測能力，俾建立跨部會指揮與修復機制。另方面，透過執法與追責，提升威懾效果，期望有助政府前瞻性政策制定與國防安全規劃參考。

關鍵詞：海底電纜安全、灰色地帶襲擾、通訊韌性與國安

Abstract

1.Taiwan's submarine cables carry critical civilian, financial, governmental, and defense communications, especially to outlying islands. Recently, incidents of external damage rose, with repeated disruptions near Matsu highlighting their high vulnerability.

2.China's attacks on Taiwan's submarine cables exhibit systematic patterns, including the use of sand dredgers and fishing vessels in sensitive waters under the guise of civilian activities to achieve political objectives; deploying commercial vessels to anchor in prohibited zones to damage cables while disguising the acts as accidents; employing auxiliary vessels to reduce attribution risk; and developing cable-cutting tech-

nologies capable of extending the threat from coastal areas to the deep sea.
3.In light of submarine cable security having become a core national security issue, this paper seeks to propose feasible measures around the framework of prevention, detection, response & recovery, and deterrence, it aims to strengthen patrol and intelligent monitoring capabilities, establish cross-agency command and repair mechanisms, and enhance deterrence through law enforcement and accountability. These efforts are intended to provide forward-looking references for policymaking and national defense planning.
Keywords: Submarine Cable Security, Gray Zone Operations, Communication Resilience and National Security

壹、前言

海底通訊電纜承載全球約九成以上的國際數據流量，被視為是當代數位經濟的核心命脈，也是國家關鍵基礎設施中最脆弱、也卻最不可或缺的節點。[1]近年來，我國海底電纜（以下稱海纜）系統面臨的風險，已由傳統的自然損害與意外事故，逐漸轉變為人為干擾與蓄意破壞並存的複合威脅；這些威脅包含商業船舶拖錨、漁業活動、關鍵節點偵蒐，以及疑似具戰略意圖的切斷與干擾行為等。在地緣政治競爭升高與「灰色地帶襲擾」常態化的情勢下，海纜似已成為大國競逐中能被低成本操作、卻能產生高戰略影響的關鍵標的；致其安全風險從單一技術層面擴展至跨域整合的國安挑戰，其安全韌性更直接影響我國在區域體系中的穩定與可信賴度。

在此背景下，我國的海纜安全已不僅是工程維護問題，更與國家安全、區域資訊基礎設施穩定及印太戰略格局緊密相連。因此，本文將聚焦分析中共近年針對我國可能採取之海纜相關混合威脅手法，內容涵蓋「灰色地帶襲擾」、關鍵節點破壞及資訊作戰整合運用等面向；亦進一步檢視我國現行防護機制之限制與缺口。本文也提出包含預警、監偵、法制強化、公私協力及國際合作等多層次安全強化措施，期能回應新興威脅態勢，並為我國未來通訊安全韌性建構與國家整體戰略部署，提供具體政策建議，這也是撰文主要目的。

貳、我國海纜現況

海纜安全不僅攸關國內離島民生、政

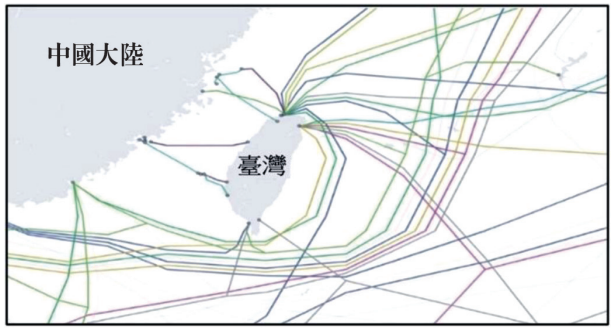
註1：Henri van Soest and Harper Fine, “Vital Yet Vulnerable: Undersea Infrastructure Needs Better Protection,” RAND Commentary, March 11, 2024, https://www.rand.org/pubs/commentary/2024/03/vital-yet-vulnerable-undersea-infrastructure-needs.html，檢索日期：2026年4月17日。

務與日常通信，更深度嵌入國際通訊網路與地緣戰略布局。面對中共「灰色地帶襲擾」升高背景下，有必要系統性檢視其重要性與風險現況，以及我國於亞太海纜網路中的戰略角色轉變。以下就國家海纜現況，分述如後：

一、通訊海纜的重要性與風險

(一)我國屬典型的海島型國家，對於本島與外島間的數位連結高度仰賴海纜。目前，國內的海纜主要負責連結本島與外、離島，以確保民生、政務、醫療、金融與軍事等關鍵通信不中斷。且其與國際海纜「多路由、多落點」的分散式架構不同；國內海纜多為雙路由設計，彼此互為備援(如圖一)，以減少單一斷纜造成通信中斷的風險。故行政院於2024年已核定，將海纜正式納入關鍵基礎設施範疇，凸顯政府對離島通訊安全與韌性的重視。

(二)回顧2019至2023年間，我國海纜共發生36起外力破壞或推擠受損案件，其中2023年就高達12件。[2]依「中華電信股份有限公司」(以下稱「中華電信公司」)數據指出，過去5年臺灣與馬祖間的海纜中斷事故超過20次，[3]顯示馬祖為國內斷纜風險最高區域。2023年2月，大陸籍漁船



圖一：我國對外國際海纜示意圖

資料來源：陳明仁、曾革鈞，〈淺談我國「海域覺知能力」整合-以海纜安全為例〉，《海軍學術雙月刊》(臺北市)，第59卷，第2期，2025年4月1日，頁59。

與貨輪在短短6天內就導致兩地間海纜全斷，造成馬祖長達50天斷網，對國內民生與行政運作造成嚴重衝擊；[4]2025年初，又發生具「中」資背景的「權宜輪」-即多哥(Togo)籍「宏泰」貨輪下錨拖斷纜線事件。此類行為均屬於海上「灰色地帶襲擾」，代表中共可能藉此測試臺灣與外、離島的通訊與電網韌性，並利用通信中斷激化當地民怨、製造社會不穩，達到心理戰與輿論戰目的。

(三)為因應近年外力破壞與自然災害風險攀升，「中華電信公司」已啟動海纜新增建設計畫，預2026年陸續完工；除採用更高傳輸容量與耐用材料，並透過加強物理防護與布放深度，降低外力損害機率

註2：江明晏、蘇思云，〈臺馬海纜中斷 中華電：近5年故障逾20次 暫不確信是否遭蓄意破壞〉，中央通訊社，2023年2月17日，https://www.cna.com.tw/news/aipl/202302160241.aspx，檢索日期：2026年4月24日。

註3：Wen Lii, "After Chinese Vessels Cut Matsu Internet Cables, Taiwan Seeks to Improve Its Communications Resilience," The Diplomat, April 15, 2023, https://thediplomat.com/2023/04/after-chinese-vessels-cut-matsu-internet-cables-taiwan-shows-its-communications-resilience/，檢索日期：2026年4月30日。

註4：黃子杰、陳柏諭，〈臺澎3號海纜全斷 扣留中資背景貨輪調查〉，公視新聞網，2025年2月25日，https://news.pts.org.tw/article/739491，檢索日期：2026年4月20日。

。[5]在訊號容量方面，海纜傳輸能力約為衛星通訊的4萬倍以上、微波通訊的1,300倍以上；[6]換言之，在相同時間內，海纜所能承載的資料量，遠非衛星或微波系統所能比擬。此一數據凸顯我國外、離島通信高度依賴海纜，一旦發生長期斷纜，衛星與微波鏈路僅能提供有限的應急備援，無法滿足外、離島的通信需求。

二、國際海纜戰略布局與臺灣地位

(一)美國「印太戰略」下的臺灣樞紐化

1.近年來，美國持續深化全球通訊安全戰略上的布局，自2020年發起維護「5G乾淨網路(5G Clean Networks)」計畫後，[7]其範圍即不再侷限於行動網路基礎設施，更在同年8月擴大涵蓋包括電信服務、雲端儲存、數據中心、以及海纜等廣義通訊服務領域。其核心目的即是防堵中共資通訊供應鏈的滲透，俾確保敏感數據不致落入可能受中共控制的系統中。

2.在這一框架下，美國對連接到香港的國際海纜計畫特別審慎。以「太平洋光纜網路」(Pacific Light Cable Network，PLCN)為例，因海纜在香港的登陸站被認為可能導致數據流量暴露於中共情報部門監控，加上部分投資方的「中」資背景亦存在高度風險；最終美方否決該系統連接香港的許可申請，僅保留連接我國與菲律賓的分支線路。[8]此案例成為美國在海纜安全審查上「國安優先於經濟效益」(National security concerns outweigh economic interests)的關鍵轉折點；且自2020年以來，美國及其盟國積極推動多項新建海纜計畫，都避開敏感登陸點，並強化與盟國網路連結合作。[9]檢視這些計畫均包含我國在內，顯見臺灣在亞太區域通訊網路中的戰略地位重要(如表一)。

(二)我國海纜多點化布局

我國國內有4個海纜登陸站，其中北部3處、南部1處，在近年海纜布局上正逐步朝「東西分散布局、南北互備支援、多點登陸配置及AI骨幹網路接軌」的方向推進，俾形成強化國家通訊韌性的整體戰略矩陣。主要海纜概況如後：

註5：江明晏，〈中華電續拓「海地星空」布局 再添海纜投資〉，中央通訊社，2025年6月29日，https://www.cna.com.tw/news/afe/202506290083.aspx，檢索日期：2026年4月24日。

註6：海纜通信系統(傳輸容量約為83 Tbps)，衛星通信系統(傳輸容量約為2Gbps，僅海纜容量之1/41,500)及微波鏈路(傳輸容量約60 Gbps，僅占海纜容量3/4,150)。〈海纜與網路之未來發展政策與安全防護計畫(核定本)〉，數位發展部，2022年9月，頁19，https://www.ey.gov.tw/File/312F12CDE9C9A230，檢索日期：2026年4月21日。

註7：“The Clean Network,” U.S. Department of State, August 5, 2020, https://2017-2021.state.gov/the-clean-network/，檢索日期：2026年4月20日。

註8：Jun Zhang, “Heading in the Direction of Bifurcated Networks: Hong Kong’s Evolution Amidst the Global Submarine Cable System,” Asian Review of Political Economy, Vol. 3, No. 8, June 28, 2024, p.10。

註9：Anna Gross, Alexandra Heal, Chris Campbell, Dan Clark, Ian Bott and Irene de la Torre Arenas, “How the US is Pushing China out of the Internet’s Plumbing,” Financial Times, June 13, 2023, https://ig.ft.com/subsea-cables/，檢索日期：2026年4月17日。

表一：近年美國規劃新建海纜概況表

海纜名稱	路　　線	預計完工	特　點　與　功　能
Apricot	美國-日本-臺灣-印尼-菲律賓-新加坡	2027年底	多國節點互聯，兼具亞太區域內與跨太平洋功能。
TPU	臺灣-菲律賓-美國	2026年	Google與中華電信合作，採用先進多芯光纖(MCF)，提升跨太平洋數據運輸能力。
ORCA	美國-臺灣	2027年第1季	專為高安全性與低延遲設計，係強化臺美雙向高速訊號的骨幹。
E2A	美國-臺灣-日本-南韓	2029年	建立東北亞至北美新一代大容量通道，並提升備援能力。

資料來源：作者自行綜整製表。

1.「TPU」海纜由「中華電信公司」與「谷歌」(Google)等美商合作，連接臺灣、菲律賓與美國，採用最新多芯光纖技術，大幅提升傳輸容量與可靠性；[10]並在本島東部新建登陸站，預於2026年完工，以強化臺灣成為跨太平洋韌性新樞紐。未來「TPU」將成為我國東岸備援海纜奠定基礎，推動朝向「多登陸點、跨區互備」的國際通信架構前進。

2.「Candle」海纜係媒體巨擘「Meta」(臉書【Facebook】前稱)與亞太多國頂尖電信業者共同打造的次世代高容量海纜，全長約8,000公里，串聯日本、菲律賓、印尼、馬來西亞及新加坡等國，超過5.8億人口，預計2028年將完工。系統採用規格與Meta目前最大容量的「Anjana海纜」同級，旨在支撐亞太地區急速成長的網路流量與AI訓練、跨國雲端運算所帶來龐大資訊流量需求，[11]並成為打造亞太地區高容量資料主幹。此案顯示大型串流影音平台業者(Over-The-Top services，OTT)正深度投入亞太通訊基礎建設，以提升區域資料流通能力，並強化關鍵節點國家的網路韌性。[12]

3.「AUG East」海纜由「中華電信公司」與新加坡、日本及韓國等亞太主流電信商，與美國「亞馬遜」旗下「Amazon Web Services」(AWS)與「微軟」等國際OTT巨頭共同參建，呈現跨國與跨產業合作新模式，預計2029年啟用。這條全長約8,900公里新海纜規劃在我國2處登陸，並延伸至東北亞與東南亞多國，並可與美方

註10：Dan Swinhoe, “Google Announces US-Taiwan-Philippines Cable with Chunghwa, Globe, and AT&T,” Data Centre Dynamics, May 26, 2023, https://www.datacenterdynamics.com/en/news/google-announces-us-taiwan-philippines-cable-with-chunghwa-globe-and-att/，檢索日期：2026年4月27日。

註11：最典型的OTT 包括Google、YouTube、Meta(Facebook、Instagram、WhatsApp)、Microsoft(Azure、Teams)、Amazon(AWS)等，上述科技巨頭需要大量國際傳輸量來支撐雲端服務、AI 訓練流量、串流影音、社交媒體、資料中心互聯；由於需求遠大於傳統電信商，業者選擇直接投資甚至自建海底電纜。

註12：“Introducing the Candle Subsea Cable, Updates to Our Asia-Pacific Connectivity Projects,” Engineering at Meta, October 5, 2025, https://engineering.fb.com/2025/10/05/connectivity/introducing-the-candle-subsea-cable-updates-to-our-asia-pacific-connectivity-projects/，檢索日期：2026年4月25日。

表二：中共對臺灣的海纜威脅矩陣

威脅模組	工具/平台	深度能力	法律掩護	成本
民用工具化	大型貨輪錨爪作業（下錨、拖曳）、慢速航行破壞。	約200公尺以內（港口、近岸海纜）	商業航運、等待進港。	低
非法經濟常態化	盜砂船（大規模抽砂）、流刺網/底拖網漁船。	50－100公尺（淺海區域）	漁業作業、砂石開採。	低
權宜輪法律漏洞	「權宜輪」或假外籍船隻、雙重船籍貨輪與油輪。	依船舶設備不同	無害通過權、第三國船籍保護。	低
軍事化威脅	拖曳式海纜及深海電纜強力切割裝置。	最深可達4,000公尺（現有國際設施可作業深度之兩倍）	軍事演訓、科研任務。	中

資料來源：作者自行綜整製表。

的「E2A」海纜相互銜接，形成通往北美資料中心的高速主幹。[13]

（三）我國在亞太海纜網路中的戰略升級

1. 由於多條海纜直接或間接以我國為轉接節點，使臺灣本島能承接東北亞-東南亞-北美之間的高速資料流動；在亞太跨區域數據量急速成長的背景下，此一樞紐化地位不僅成為資料轉運站（transit hub），更成為區域分流核心，具備在系統故障或區域風險升高時，能協助維持網路的穩定。[14]

2. 現行與規劃中的海纜路線多刻意選擇避開中國大陸沿岸高風險區域，改採「民主供應鏈環」模式，直接連接日本、韓國、新加坡、菲律賓、關島與美國等盟國。此舉除減少敏感資料免受高風險海域控制外，也讓我國成為「去中化」數位網路架構中重要節點，兼具資訊安全與國家戰略層面上的關鍵意義。

整體而言，這波以臺灣本島為重要節點的海纜建設，不僅是技術升級，更是地緣政治結構變遷具體象徵，體現美國在印太地區建構數位連結戰略布局正在落實，也代表周邊國家正在組建一條更安全、可控、可信的全球資訊通道。在此架構中，我國地位正大幅提升，除成為國際數位基礎設施鏈內不可替代樞紐外，亦擁有更高的話語權與價值。

參、近年中共破壞我國海纜樣態

由近年臺灣周邊海域海纜受損事件分析，中共對海底通訊電纜干擾已非零星個案，而是逐步發展為具策略設計與分工模式的「灰色地帶襲擾」。為釐清其行動邏輯與風險層次，以下將從非法活動、民用

註13：“Undersea Infrastructure 2.0: Asia’s Next Wave of Submarine Investments,” Telecom Review, January 30, 2026, https://www.telecomreviewasia.com/news/featured-articles/28230-undersea-infrastructure-2-0-asias-next-wave-of-submarine-investments/，檢索日期：2026年4月30日。

註14：江明晏，〈中華電：AI時代海纜頻寬需求大增 臺灣躍跨太平洋樞紐〉，《經濟日報》，2025年12月2日，https://money.udn.com/money/story/5612/9177402?from=edn_newest_index，檢索日期：2026年4月24日。

表三：中共「權宜輪」(或「中」資背景)船舶侵擾我國海纜統計表

日　期	船　名	船　籍	涉及事件與造成損失	背　景　分　析
2022.5.14	外籍貨輪	不明	「臺馬2號」海纜疑遭損害斷纜。	開始出現非中共旗幟船舶破壞紀錄。
2023.2.2	不明漁船	大陸（疑）	臺馬2號「淡水-東引」區段斷纜，疑遭漁船下錨勾損。	與隨後2月8日事件形成連鎖斷網。
2023.2.8	不明貨輪	大陸（疑）	臺馬3號「草漯-南竿」區段斷纜，馬祖萬戶對外通訊全斷。	造成「斷網危機」，改由微波通訊支應。
2025.1.3	順興39	喀麥隆/坦尚尼亞	於野柳東北方海域拖斷國際海纜「跨太平洋快線」(Trans Pacific Express Cable System)。	2024年12月8日起，即在北部海域交錯航行，船員皆為陸籍。
2025.1.12	寶順號	蒙古	在石門外海徘迴甚久意圖不明，且一度接近基隆海纜區。	聲稱故障，但在海纜重疊區異常繞行。
2025.2.24	長順輪/新田30	蒙古/巴拿馬	滯留屏東枋山海纜區形跡可疑，隨即海委會發布監控警示。	雖未直接斷纜，但其低速徘徊被視為破壞行動演練。
2025.2.25	宏泰58	多哥	於臺南將軍西北方海域拖斷「臺澎3號」國內海纜。	海巡署登檢押回，船員均為陸籍，被列入黑名單之「FOCs」。
2025.4.16	先鋒輪(原長順輪)	不明	再度於枋山海纜區慢速航行，疑似進行海底地形偵測。	顯示「FOCs」具備頻繁改名或船旗，以掩護行動。

資料來源：作者自行綜整製表。

工具化、制度漏洞與軍事威脅四個面向(如表二)，臚列分析如後：

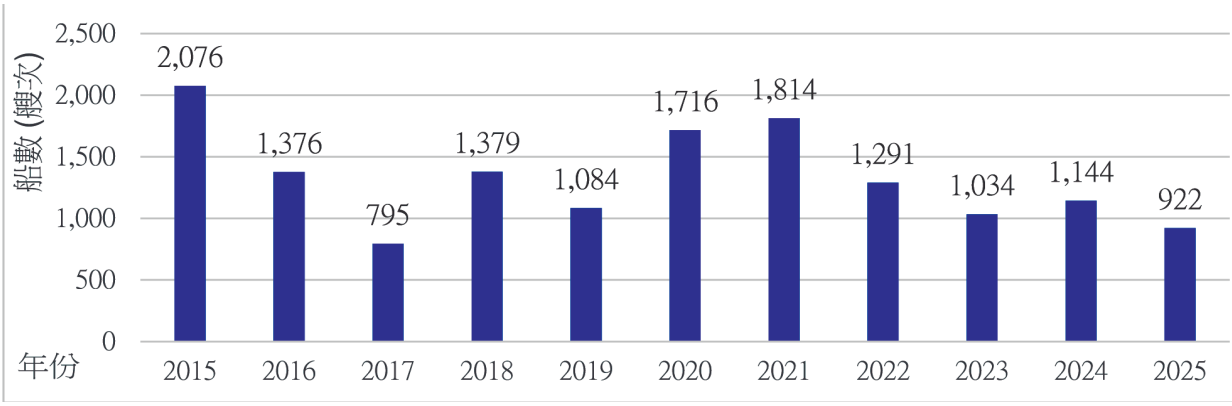
一、非法經濟活動常態化

(一)根據「海巡署」統計，2016年7月至2026年4月間，我方共取締大陸籍盜砂船近20艘次(沒收16艘次)，查獲盜採砂量逾2萬5,000公噸，[15]尤其集中出現在我馬祖與澎湖周邊海域。此類盜砂船大規模抽砂作業，導致海底淺灘快速流失，破壞原有沉積層，造成被掩埋的海底通訊電纜外露，在惡劣海況或船舶作業時更易受損，2022年3~4月間，馬祖海纜接連損壞就是一例(如表三)。[16]

(二)近十年，我政府驅離非法越界大陸籍漁船高達1萬3,000多艘次(如圖二)，大陸籍漁船在我國周邊進行長距離的海底拖動漁具，更對海纜造成直、間接的機械拉扯與切割風險。2023年2月，馬祖地區民眾通信與網路中斷數週的元凶，即為大陸籍漁船勾斷所致。這些非法經濟活動雖名義上屬於民事範疇，但其效果包括頻繁活動導致我方海底基礎設施長期處於高風險環境，製造持續性壓力；加上行為可被包裝為經濟或漁業操作，難以在國際場域上直接定性為軍事挑釁。畢竟此類破壞不只僅限於通訊中斷，還波及當地經濟、社

註15：〈取締違法大陸抽砂船成效〉，行政院海洋委員會海巡署，2026年2月10日，https://www.cga.gov.tw/GipOpen/wSite/ct?xItem=139485&ctNode=11298&mp=marine，檢索日期：2026年6月20日。

註16：蘇思云，〈NCC：臺馬海纜遭中國漁船勾斷 年底將備援達平時通訊水準〉，中央通訊社，2023年2月16日，https://www.cna.com.tw/news/aipl/202302160263.aspx，檢索日期：2026年4月22日。



圖二：2015年-2025年大陸籍漁船越界活動統計圖

資料來源：參考〈114年海巡統計年報〉，海洋委員會海巡署，2026年4月14日，https://www.cga.gov.tw/GipOpen/wSite/ct?xItem=167513&ctNode=13480&mp=999/，檢索日期：2026年4月21日，由作者綜整製表。

會穩定與外島防務通訊，影響層面廣泛，不容輕忽。

二、民用工具化

(一)至2024年9月，「中」方擁有船隊總規模已達4.3億載重噸，市占率占比約為百分之十九，穩居世界前列。[17]且由近年事例可證，中共正利用其在全球航運市場龐大船隊優勢，透過商船活動在臺灣周邊進行高隱匿性、低成本「灰色地帶」襲擾。這些陸籍貨輪在港口外錨泊等待或進行航道調整時，其錨爪就可直接對海底通訊基礎設施造成物理威脅；[18]2025年2月「宏泰58」貨輪異常Z字形航行與隨意下錨造成切纜行為，[19]即明白彰顯此類事件並非偶發，而是具備行動一定模式特徵，包括偽裝為正常商業航運操作，藉港口擁塞或氣候因素，以掩飾其長時間滯留與下錨行跡。

(二)檢視此類破壞行動無需額外專業裝備，即可透過改裝或直接使用現有錨具，達成切斷海纜之效果，其執行門檻與成本極為低廉，行動後更可表達係「航行意外」或「操作疏失」，俾在「國際法」與商業保險體系中，大幅規避責任歸屬與究責難度。[20]相較傳統軍事攻擊，此種手段具備高度可否認性，且能有效迴避《聯合國海洋法公約》(The United Nations Convention on the Law of the Sea，UN-

註17：王辰陽，〈我國擁有海運船隊總規模已達4.3億載重噸〉，新華網，2024年10月15日，https://www.news.cn/fortune/20241015/4885242493d9427fa3a7eba9b628cb17/c.html，檢索日期：2026年4月22日。

註18：John Dotson, "The Chinese Communist Party's Political Warfare Directed Against Taiwan: Overview and Analysis," GTI "Counter Ideological Work and Political Warfare" Research Series: Paper #1, May 2024, pp.11~13。

註19：邵心杰，〈「宏泰」貨輪Z字形移動、釋放錨爪勾斷海纜線 檢方起訴大陸籍船長〉，聯合新聞網，2025年4月11日，https://udn.com/news/story/7320/8667764，檢索日期：2026年4月17日。

註20：Gahon Chia-Hung Chiang, "Countering China's Subsea Cable Sabotage," Global Taiwan Brief, Vol. 10, No. 6, March 2025, p.7。

CLOS)與國際通訊規範中對武力使用與敵對行為的明確界定。尤有甚者，透過民用船舶、漁船或工程船遂行破壞行動，實質上已將民用海事活動轉化為「非軍事化破壞工具」，更模糊戰時與平時、軍事與非軍事之界線，使受害方在政治回應與安全升級上，陷入進退兩難。

三、「權宜輪」的法律漏洞

(一)「權宜輪」(Flags of Convenience，以下稱FOCs)係指本屬某國船隻，但特意去他國註冊，然後懸掛第三國旗幟，造成船旗國與懸掛其旗幟之船舶缺乏「真實聯繫」(genuine link)，致無法對其行為有效規範與管理。[21]「中」方運用「權宜輪」預期達到之效果，至少有以下三項：

1.來源隱匿化-由於第三國籍船舶非屬敵對勢力，形式上享有「無害通過權」（right of innocent passage），中共遂透過此一法律身分，掩護其行動來源。

2.行動合法外觀化-近年中共更系統性於非洲與中、南美洲地區取得船齡老舊、價格低廉且待拍賣之「權宜輪」，經改裝後轉化為具特殊作業能力之「假外籍」船舶，強化其行動之合法外觀。

3.國際反應遲滯化-透過在國際法「灰色地帶」運作，使相關行為難以即時被界定為違法或敵對行動，進而阻礙受害國即時防衛與執法。

「中」方正是透過是類「假外籍」船舶，才得以隱匿於全球商業航運流量之中，並堂而皇之在臺海周邊進行基礎設施的破壞行動。

(二)在發生多起海纜斷裂事件後，我國已將超過50艘中共「權宜輪」列入黑名單，並以在我國領海停留天數等，標記其中高度、中度與一定程度威脅；[22]另結合「國家海洋研究院」分析近百艘黑名單「FOCs」的行動樣態發現，此類船舶主要活動於我國西部商港周邊，而高風險船舶航跡更多集中在基隆以北海域。[23]換言之，「權宜輪」已呈現高度針對性與區域集中行動特徵，並可能以關鍵港口與海纜節點為主要活動目標，更顯示其不單負有航運任務，更潛藏特定戰略意圖與「灰色地帶」運用價值。

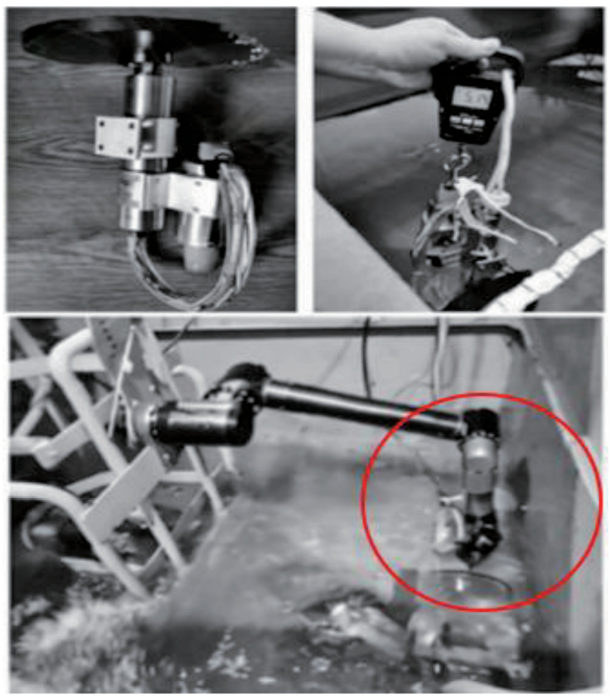
四、軍事化威脅

(一)中共「船舶科學研究中心」及其附屬的「深海儀人裝備國家重點實驗室」，在2025年開發一款深海電纜強力切割裝置，是現有海底通訊基礎設施最大作業範圍的兩倍。[24]該裝置極輕、僅5.14公斤重

註21：楊瀅陵，〈概論公海船旗國管轄制度〉，《海巡雙月刊》(臺北市)，第45卷，2010年6月，頁23。

註22：劉怡廷，〈臺灣海底電纜2個月斷4次 灰色侵擾警戒升高有哪些人為斷纜樣態？〉，公視新聞網，2025年2月28日，https://news.pts.org.tw/curation/135，檢索日期：2026年4月25日。

註23：黃瑀喬，〈加強監控96艘黑名單權宜輪 海委會：北部暫無高威脅船舶滯留〉，公視新聞網，2025年3月15日，https://news.pts.org.tw/article/742275，檢索日期：2026年4月25日。



圖三：中共深海電纜切割裝置

說明：裝置實體及重量(圖上)、電纜切割動作(圖下)。

資料來源：參考李向陽、程皓楠，〈聲稱能在4000公尺深海操作 中國公開「電纜殺手」〉，自由亞洲電台，2025年3月24日，https://www.rfa.org/cantonese/world/asia/2025/03/24/china-undersea-cable-cutter/，檢索日期：2026年4月25日，由作者調整製圖。

，能搭載於各類民用船隻或遙控潛水器(Remotely Operated underwater Vehicle，ROV)，輕易偽裝成無害通過；技術上則演進為能精準切斷60㎜鎧裝海纜，此種「外科手術式」切割，能確保百分百的成功破壞率(如圖三)。

(二)該類海纜切割裝置作業深度，已由近岸淺海逐步延伸至4,000公尺的深海區域，其對關鍵通信節點的破壞能力已不再是線性，而是倍數級放大效應；這已意味海纜安全威脅已從原本集中於地緣政治高度敏感沿岸與島鏈周邊，外溢至跨洲、跨洋全球海底基礎設施網路，讓長期被視為「相對安全」的深海主幹海纜成為潛在風險。由於深海區域監測成本高昂、即時反應能力有限，攻擊行為更容易被包裝為技術事故或自然損壞，大幅提高責任歸屬的判定困難度，進而削弱國際社會對此類行為的嚇阻與回應能力。

面對中共深海作業平台、無人載具與海洋感測技術持續整合，其對全球資訊通信骨幹中「高價值、低防護」節點的辨識與鎖定，將趨於系統化與精準化，凸顯海纜安全正日益受到重視。

肆、我國海纜安全強化措施

近年中共於臺灣周邊海域對海纜之干擾行為，已由過往零星、難以歸因之個案，逐步演變為具備戰略意圖、行動節奏與多元工具整合之行動樣態，不僅直接威脅我國對外通訊之穩定性，更可能在平時即累積關鍵基礎設施之脆弱點，於危機或衝

註24：2020年5月，中共浙江「麗水學院」申請一種拖曳式海底電纜切割裝置及其電纜切割方法專利，該裝置類似帶有切割刀的錨，可直接在海底**鉤**住電纜並快速切斷電纜，無需額外動力供電。因成本低，重量小，使用方便快速，加上團隊在期刊發表的《深海纜線電動切割裝置設計》論文試驗影像，凸顯這套系統已經從實驗室的技術概念，演進到具備實戰能力的原型機測試階段。Stephen Chen, "China Unveils a Powerful Deep-sea Cable Cutter that Could Reset the World Order," South China Morning Post, March 22, 2025, https://www.scmp.com/news/china/science/article/3303246/china-unveils-powerful-deep-sea-cable-cutter-could-reset-world-order，檢索日期：2026年4月25日。

突時，形成「先期癱瘓」效果。當前海纜已不僅是通訊設施，更是攸關國家韌性與戰略持續力的核心節點；其安全性與備援能力，正面臨前所未有之壓力與考驗。「歐盟」(EU)2025年2月發布的《有關強化海底電纜安全與韌性的聯合通告》(Joint Communication to Strengthen the Security and Resilience of Submarine Cables)，內容即針對當前海纜面臨的威脅與挑戰，提出包括預防(Prevention)、偵測(Detection)、回應修復(Response & Recovery)以及嚇阻(Deterrence)等應對措施；[25]故我國可參考「歐盟」作法，強化海纜安全措施，同時構築更具前瞻性與跨域整合能力之制度架構。分述如后：

一、預防作為

(一)針對以漁撈、抽砂為名的非法經濟活動，政府應於重要海纜節點與登陸區周邊劃設「海纜保護警戒專區」，透過公告禁限制航與作業行為，明確劃出高風險管制空間。同時結合海巡署與海軍之定期與不定期巡邏，提高執法能見度與即時攔查能力，以實質減少可疑船舶進入與長時間停留的機率，[26]降低海纜遭破壞風險。

(二)再者，對「民用工具化」存在的風險，政府應同步強化航行秩序管理與船舶行為透明度，整合衛星、岸基雷達與光電監偵設備進行多源情資比對，建立異常航跡與高風險行為的早期辨識機制，使任何可疑船舶於接近海纜保護區前，即被即時標示、通報並要求改道，以提前介入方式，阻斷破壞行動的發生機率。[27]

(三)執法單位應落實執行2025年公布《商港法》與《船舶法》相關修正條文，對違規船舶久置港口、不按規定離港及隱匿船舶身分等行為，以高額罰鍰、強制移離乃至沒入處分等手段，建立具強制力之港口與航行管理追踪及處置機制。[28]此舉不僅可封堵灰色空間，降低民用船舶被工具化的風險，也強化國內制度與國際海事規範的銜接性。

(四)由於關鍵海纜深埋於海床之下，故在建置時應採用高強度護套或多層防護材料，以提高物理抗破壞能力；同時規劃

註25：Joint Communication to the European Parliament and the Council, “EU Action Plan on Cable Security,” European Commission, February 21, 2025, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025JC0009，檢索日期：2026年4月27日。

註26：〈立法院第11屆第2會期外交及國防委員會第27次會議紀錄〉，立法院議事暨公報資訊網，2025年1月16日，頁278，https://ppg.ly.gov.tw/ppg/sittings/2025011024/details?meetingDate=114%2F01%2F16，檢索日期：2026年4月17日。

註27：Giovanni Soldi, Domenico Gaglione, Simone Raponi, Nicola Forti, Enrica d’ Afflisio, Pawel Kowalski, Leonardo M. Millefiori, Dimitris Zissis, Paolo Braca, Peter Willett, Alain Maguer, Sandro Carniel, Giovanni Sembenini, and Catherine Warner, “Monitoring of Critical Undersea Infrastructures: the Nord Stream and Other Recent Case Studies,” IEEE Aerospace and Electronic Systems Magazine, Vol. 38, No. 10, October 1, 2023, pp.7~8。

註28：國土安全辦公室，〈海纜七法：強化海纜保護、確保民生服務、提升國家安全〉，行政院院會議案，2025年9月18日，https://reurl.cc/6b5xeO，檢索日期：2026年4月25日。

多路由網路設計，增加登陸站數量及備援機房的地理分散性，確保單一海纜或登陸站遭受破壞時不會形成致命斷點。透過物理防護與系統冗餘並行，可有效降低敵對行動對國家及區域資訊骨幹的影響。

二、偵測作法

(一)空中監測可以「合成孔徑雷達」(Synthetic Aperture Radar，SAR)衛星與「自動辨識系統」(Automatic Identification System，AIS)衛星為核心，同時扮演「鷹眼」角色；[29]不僅止於影像監測，更導入AI航跡分析系統，針對禁錨區內的低速漂移或突發停船等可疑動態進行高頻分析；[30]另透過SAR的全天候觀測技術，能完整辨識刻意關閉AIS訊號之「幽靈船」，加上由AI進行自動化識別比對，能形成全域監控(如圖四)。[31]此外，系統可進一步整合「國際海事組織」(International Maritime Organization，IMO)船籍資料與黑名單，將商業背景納入交叉比對平台，達成情資融合，確保對高風險「權宜輪」能發出早期預警。

(二)海面監測則由浮標系統組成，是連接天空與水下的關鍵中繼站，這些浮標搭載聲學感測器、高解析相機與環境監測儀，能對特定海域進行24小時不間斷即時監控。相較衛星，海面浮標優勢在於「在地化」精準度，能有效補強衛星偵測盲區；當衛星發現異常動態時，海面設施可就近提供細節判讀，確認船隻威脅程度。此外，浮標也是數據傳輸節點，能將偵測到的環境變化與可疑目標資訊即時回傳，大幅提升監控系統的在地應變能力與判讀準確性。

(三)水下監測扮演海洋防衛預警體系的前哨角色，核心在於推廣搭載聲納與震動模組之「智慧電纜」(Smart Cables)，[32]透過整合「分散式聲學感測」(Distributed Acoustic Sensing，DAS)技術，系統能持續監控海纜周遭聲學訊號，並對外力擾動、切割或異常振動進行即時偵測。[33]當系統警示，隨即派遣遙控水下無人載具

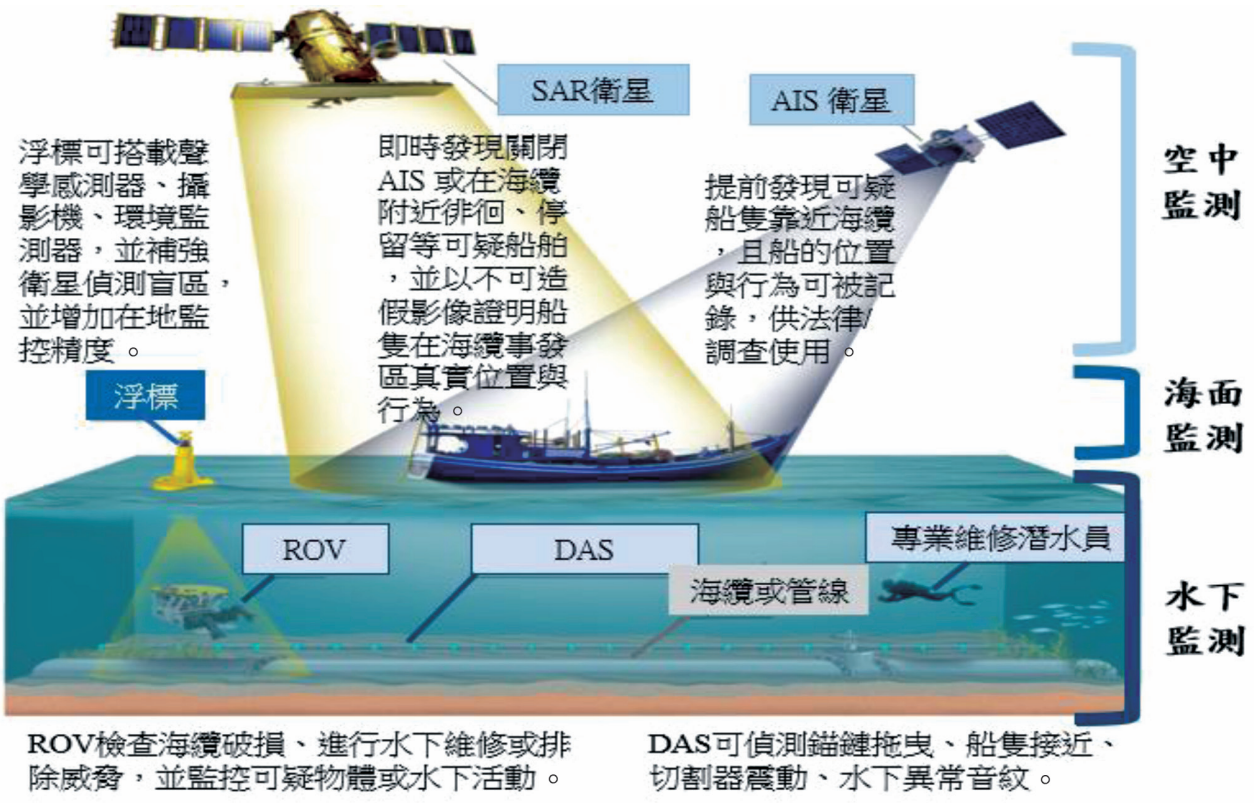
註29：陳明仁、曾革鈞，〈淺談我國「海域覺知能力」整合-以海纜安全為例〉，《海軍學術雙月刊》(臺北市)，第59卷，第2期，2025年4月1日，頁70~71。

註30：Konrad Wolsing, Linus Roepert, Jan Bauer and Klaus Wehrle, "Anomaly Detection in Maritime AIS Tracks: A Review of Recent Approaches," Journal of Marine Science and Engineering, Vol. 10, No. 1, January 2022, p.112。

註31：鄭義達，〈「人工智慧」(AI)應用於船舶辨識淺析〉，《海軍學術雙月刊》(臺北市)，第59卷，第5期，2025年10月1日，頁123~124。

註32：“Connecting Europe Facility (CEF) - Multiannual Work Programme 2024-2027,” European Commission, October 9, 2024, https://digital-strategy.ec.europa.eu/en/library/connecting-europe-facility-cef-multiannual-work-programme-2024-2027，檢索日期：2026年5月10日。

註33：Erick Eduardo Ramirez-Torres, Javier Macias-Guarasa, Daniel Pizarro-Perez, Javier Tejedor, Sira Elena Palazuelos-Cagigas, Pedro J. Vidal-Moreno, Sonia Martin-Lopez, Miguel Gonzalez-Herraez, Roel Vanthillo, "Vessel Detection and Localization Using Distributed Acoustic Sensing in Submarine Optical Fiber Cables," arXiv, September 15, 2025, https://arxiv.org/html/2509.11614v1，檢索日期：2026年4月22日。



圖四：針對海纜設施全域監控概念圖

資料來源：參考Giovanni Soldi, Domenico Gaglione, Simone Raponi, Nicola Forti, Enrica d' Afflisio, Pawel Kowalski, Leonardo M. Millefiori, Dimitris Zissis, Paolo Braca, Peter Willett, Alain Maguer, Sandro Carniel, Giovanni Sembenini, and Catherine Warner, "Monitoring of Underwater Critical Infrastructures: the Nord Stream and Other Recent Case Studies," IEEE Aerospace and Electronic Systems Magazine, Vol. 38, No. 10, October 2023, p.5，由作者彙整製圖。

(Remotely Operated underwater Vehicle，ROV)執行精確檢查並排除威脅，或派遣專業維修潛水員負責修復作業。[34]水下監測的核心是針對「觸碰、破壞與潛水活動」進行防護，不僅檢查海纜是否損壞，還能針對可疑水下物體進行監控，確保能源與資訊通道在深海環境中，能絕對安全並穩定運作。

三、回應與修復程序

(一)為完備跨部會協調機制，應由相關單位(如漁業署、港務公司、數位發展部、國家通訊傳播委員會及海軍、海巡署等)共同組建常設事故指揮中心，統一指揮通報、處置與資源調度流程，避免形成多頭馬車，影響應變效率與決策一致性，反而延誤關鍵處置時機、擴大損害範圍。

註34：“Recommendation on the Security and Resilience of Submarine Cable Infrastructures,” European Commission, February 21, 2024, https://digital-strategy.ec.europa.eu/en/library/recommendation-security-and-resilience-submarine-cable-infrastructures，檢索日期：2026年4月16日。

[35]再者，透過即時情資共享與明確分工，一旦發現海纜異常或可疑船舶，即可迅速執行驅離、管制與現場應變，並啟動修復與備援機制，以縮短海纜中斷時間，亦降低對民心、社會的衝擊。

(二)透過建立危機快速攔截程序，明訂AIS出現異常後的標準化攔截時限與作法，建立清楚的通報、判斷與出動流程，避免決策遲滯，影響到海纜安全。[36]此外，海纜密集與高度敏感海域則應預先部署快速反應艇或高速巡防能量，以縮短反應距離與抵達時間，確保執法單位能在第一時間介入查證、驅離或管制可疑船舶，提高現場應處效率與實質嚇阻效果。

(三)標註辨識的可疑船舶，執法單位應立即依執法SOP，啟動標準應對處置程序，包括海上攔查、航行限制、臨時扣押或調查等措施，並明確分工各相關單位的權責。[37]透過制度化流程與事前授權，確保執法行動迅速、合法且可回溯追踪機制，既能有效阻斷潛在威脅，也可提升國內、外對我國海域管理能力的信心與威懾力。

(四)為降低海纜損壞造成的影響，政府應預先部署可於短時間內抵達事故海域的海纜維修船與相關設備，以加速損毀點定位與修復作業，縮短通訊中斷時間；[38]同時啟動衛星、微波等替代性通訊鏈路，做為緊急備援手段。不僅應確保政府指揮體系、金融交易與關鍵基礎設施之通訊不中斷，亦能降低突發破壞對國家運作與社會穩定所造成的影響。

四、嚇阻機制

(一)透過「海纜七法」正式立法，我國已明確將蓄意破壞、重大過失致損及協助破壞海纜之行為，納入刑事責任範疇，[39]政府藉清楚界定構成要件與責任主體，不僅可補足現行法制對「灰色地帶襲擾」規範內容之缺口，亦有助執法機關在蒐證、扣押與司法追訴上取得明確法源依據，

註35：鄭永泩，〈美國海域覺知計畫對我海上安全之啟示〉，《海軍學術雙月刊》(臺北市)，第48卷，第4期，2014年8月1日，頁55~56。

註36：〈立法院第114卷 第92期(5385)公報〉，立法院議事暨公報資訊網，2025年11月25日，頁476，https://ppg.ly.gov.tw/ppg/publications/official-gazettes/114/92/01/details，檢索日期：2026年4月27日。

註37：黃宣凱、駱韋任，〈由海纜安全檢視海巡署在韌性防衛體系中的角色〉，《海軍學術雙月刊》(臺北市)，第60卷，第2期，2026年4月1日，頁21。

註38：英國「國家安全戰略聯合委員會」(Joint Committee on the National Security Strategy, JCNSS)建議(Recommendation, Paragraph 72)，政府應在2030年前購買一艘真正自主的電纜維修船。和平時期，該船可以以優惠條件租賃給相關行業，危機時期則可供政府使用。UK Joint Committee on the National Security Strategy "Subsea Telecommunications Cables: Resilience and Crisis Preparedness," UK Parliament, September 19, 2025, https://publications.parliament.uk/pa/jt5901/jtselect/jtnatsec/723/report.html，檢索日期：2026年4月20日。

註39：「海纜七法」包括《電信管理法》、《電業法》、《天然氣事業法》、《自來水法》、《氣象法》、《商港法》及《船舶法》，同註37，頁15；〈政院通過「海纜七法」修正草案 強化海纜保護、確保民生服務、提升國家安全〉，行政院，2025年9月18日，https://www.ey.gov.tw/Page/9277F759E41CCD91/198a86cd-efd1-4393-8249-0f107b1c85ee，檢索日期：2026年4月25日。

方能將法律規範轉為具實質嚇阻效果之執行能力。[40]

(二)有關機關應建立針對破壞我國海纜之違規船舶完整紀錄與持續觀察名單，並透過正式管道通報國際保險與再保機構，提高其投保門檻與保費成本，[41]俾在多重經濟與名譽壓力下，削弱「權宜輪」持續營運誘因。另方面，結合「國際海事組織」(IMO)等多邊機制共同施壓，使屢犯或高風險船舶面臨航行限制、港口檢查加嚴與保費鉅增等影響，[42]透過此類經濟負擔與名譽損失的雙重作用，形成跨國層次的實質嚇阻效果。

(三)針對經過或長時間停留於海纜路徑與關鍵節點附近之船舶，除加強行為辨識、軌跡分析與即時通報機制外。尤為關鍵的是國際合作，特別是透過友我國家間建立常態化情資交換機制，[43]針對臺灣海峽等關鍵航道及海纜密集區域進行聯合監控與風險評估，以降低關鍵通訊基礎設施遭受「灰色地帶襲擾」之風險。尤其是與美、日、澳等理念相近國家，定期進行海纜保護、水下監偵與反潛巡邏等聯合演練，並整合水下聲納、無人載具與海空協同能力，[44]以強化對敵方水下載具及相關破壞行動之偵蒐能力與攔截效能。

咸信政府透過常態化與公開化操作，加上強化實際執法與應變能力，應能對潛在威脅方釋放明確之戰略訊號，同時展現共同維護水下關鍵基礎設施安全的意志與行動決心。

伍、結語

面對中共透過「非法經濟活動化」、「民用工具化」、「國際制度漏洞化」及「軍事化威脅」等多重混合手段，對我國海纜造成的系統性風險；政府亟須建構一套橫跨空中、海面至水下的多層次、多感測來源監控網路，透過即時監測與情資整合，在威脅尚未升級前即完成識別、通報與干預。此外，整合海纜破壞之歷史事件資料與現行海纜脆弱點，納入系統性風險評估模型之中，以強化預警準確性，並做為資源優先配置與防護部署之決策依據。

海底電纜已成為典型的混合威脅目標，其風險特性涉及多層次因素，包括代理

註40：Douglas R. Burnett, “Submarine Cable Security and International Law,” International Law Studies, Vol. 97, 2021, p.1672。
註41：同註38。
註42：同註26，頁279。
註43：美國國會議員於2025年7月9日提出《臺灣海底電纜韌性倡議法案》(Taiwan Undersea Cable Resilience Initiative Act)，並於2026年1月29日通過。“S.2222 - Taiwan Undersea Cable Resilience Initiative Act 119th Congress (2025-2026),” Congress.Gov, July 9, 2025, https://www.congress.gov/bill/119th-congress/senate-bill/2222/text，檢索日期：2026年4月30日。
註44：Federica Bagna, “Undersea Cables at Risk: Lessons from the EU and Taiwan,” Institute for Security & Development Policy, February 2, 2026, https://www.isdp.eu/undersea-cables-at-risk-lessons-from-the-eu-and-taiwan/，檢索日期：2026年4月20日。

勢力於「灰色地帶」環境下所發動的干擾與制度漏洞，以及可能的軍事破壞行為，我國亦須同步強化法制、技術、監控與快速修復能力，並深化國際合作，以降低威脅。另方面，應與美、日、歐、澳等友我夥伴共享高風險船舶名單、水下儀具活動資訊、聲學感測資料與修復能量，以建立常態化的聯合巡防與威脅通報機制；海軍與海巡等執法單位更應透過定期聯合演練與跨國交流合作，進一步提升我國在海纜防護及快速反應能力上的整體韌性。 ⚓

作者簡介：

曾敏禎小姐，國立政治大學亞太研究英語碩士學位學程(IMAS)、國防部情報參謀官97年班，現服務於財團法人國防安全研究院暨國立政治大學博士生。

左營軍區的故事

自勉新村

陸戰隊指揮部旁的自勉新村，是一個小而美的村子，整齊筆直的巷道，花木扶疏的前庭，是這個村子的特色，自勉新村為民國83、84年社區發展工作考評甲等績優社區，成為每一位自勉人的一段佳話。(取材自《鎮海靖疆-左營軍區的故事》)

自勉新村自治會舊照