專載

DOI:10.6237/NPJ.202604_60(2).0001

由海纜安全檢視海巡署在韌性防衛體系中的角色

Examining the Role of the Coast Guard Administration in a Resilient Defense Framework: A Perspective on Submarine Cable Security

黃宣凱 先生、駱韋任 先生

提　　要：

一、在全球數位化快速深化與地緣政治競逐升溫的背景下，海底電纜已由單純的通訊工程設施，轉化為攸關國家安全、經濟穩定與數位主權的關鍵基礎設施。本文以「灰色地帶」行動與數位戰略安全為視角，檢視印太地區海底電纜的發展趨勢、依賴結構與安全脆弱性，並分析其所面臨之實體破壞、網路滲透與治理失靈等複合式威脅。

二、現行國際法與區域治理機制在低可歸責性與跨境執法方面仍存有侷限性，確實難以有效回應中共「灰色地帶」行動所帶來的長期風險。本文也聚焦我國制度脈絡，除檢視「海纜七法」完成立法後的治理轉型，也說明海巡署在預警監測、海域執法、跨部會協調及韌性防衛體系中所扮演的前端支援與協調角色。

三、當前我國海底電纜安全治理應由「事後修復」導向，轉型為結合智慧科技、制度整合與區域合作的「韌性防衛」模式，方能強化我國在印太地區的數位韌性與整體安全治理能力。

關鍵詞：海纜安全治理、灰色地帶行動、印太戰略、韌性防衛、海巡署

Abstract

1.As global digitalization and geopolitical rivalry intensify, submarine cables have evolved from basic infrastructure into critical assets for national security and digital sovereignty. This paper adopts a“gray zone”and strategic security perspective to examine Indo-Pacific cable trends and vulnerabilities, analyzing multifaceted threats such as physical sabotage, cyber infiltration, and governance failure.

2.Limitations in international law regarding low attributability hinder effective responses to protracted gray zone risks. Focusing on Taiwan, this study reviews the governance transition following the“Seven Laws on Submarine Cables”and elucidates the Coast Guard Administration’s

(CGA) pivotal role in monitoring, maritime enforcement, and inter-agency coordination within the resilient defense system.
3. Taiwan's cable governance must shift from a reactive"post-damage repair"model toward a proactive"resilient defense paradigm integrating smart technology and regional cooperation. This transition is vital for bolstering Taiwan's digital resilience and comprehensive security governance within the Indo-Pacific architecture.

Keywords: Subsea Cable Security Governance, Gray Zone Tactics, Indo-Pacific Strategy, Resilient Defense, Coast Guard Administration (CGA).

壹、前言

隨著全球數位化加速與地緣政治競逐升溫，海底電纜做為國際資訊傳輸的關鍵基礎設施，已由單純的「技術工程」資產，轉化為攸關國家安全的「戰略性安全」資產。[1]依「國際電信聯盟」(ITU)與美國「國土安全部」(Department of Homeland Security)統計，全球逾九成五的跨國資料流量，係透過約500條海底電纜系統傳輸，[2]其安全性可能直接影響國家安全、經濟穩定與軍事指揮體系；然因海纜位置分布廣泛、可視性低且維修成本高昂，讓它成為「低可見度、高戰略價值」的脆弱基礎設施。

「俄烏戰爭」爆發後，波羅的海與印太地區接連出現疑似「灰色地帶」威脅，並導致海纜與能源管線受損，凸顯關鍵海底基礎設施在複合式威脅環境下的高度風險。2024年底至2026年間，歐洲多起海纜斷裂事件頻傳，案件涉及中國大陸籍貨輪與具俄羅斯背景船舶，相關國家立即採取相應措施；如芬蘭政府為落實「歐盟」(EU)《關鍵實體韌性指令》(以下稱CER)[3]，遂修正國內法制並擴大邊防與海域執法權限，政策重心由「事後修復」轉向「事前預防」與「即時攔截」，[4]凸顯出「北約」(NATO)國家正以制度化回應「灰色地帶」威脅。此外，在印太戰略格局下，海纜安全已成為「數位戰略安全」的核心議題；尤其我國位居「第一島鏈」樞紐，也是區域重要的數位連結節點。加上近年臺

註1：Lionel Carter, Douglas Burnett, Seana Drew, Graham Marle, Lennard Hagadorn, Debbie Bartlett-McNeil, and Nigel Irvine, Submarine Cables and the Oceans: Connecting the World (Cambridge: UNEP-WCMC, 2009), p.8。

註2：U.S. Department of Homeland Security, "Critical Infrastructure Security and Resilience: Undersea Cable Systems," (Washington, DC: DHS Office of Cyber and Infrastructure Analysis, 2020), pp.1~2。

註3：「關鍵實體韌性指令」(Directive【EU】2022/2557 - Directive on the resilience of critical entities)核心目標為強化歐盟境內關鍵基礎設施實體(Critical Entities)的「物理韌性」與「持續運作能力」，以防範自然災害、恐怖攻擊、破壞行為與混合威脅。

註4：林于棠，〈從波羅的海「海底電纜事件」看關鍵基礎設施防護〉，國防安全研究院第899期，2026年1月5日，https://indsr.org.tw/focus?typeid=27&uid=11&pid=2994，檢索日期：2026年1月30日。

海周邊發生多起具「中」資背景船舶涉嫌損害海纜，顯示傳統分工模式已不足以因應日益複雜的「複合式威脅」。

本文以「複合式威脅」與數位戰略安全為分析視角，探討印太地區海底電纜所面臨之威脅與治理缺口，並檢視現行國際與區域安全治理架構之限制；另方面，聚焦我國制度脈絡，分析「海岸巡防署」(以下稱海巡署)於跨部會「韌性防衛體系」[5]中，可扮演之功能定位與發展潛能。亦期望能補強對非軍事海域治理與關鍵數位基礎設施防護之討論，為我國在區域海上安全合作與數位韌性治理中之制度設計與實務運作，提供具體且可行的政策參考，這也是撰文主要目的。

貳、海底電纜體系的發展趨勢與脆弱性

鑑於海纜處於關鍵基礎設施的重要地位，有必要針對其發展趨勢與依賴性、結構脆弱性等層面切入，分析全球海底電纜體系的戰略演變、產業變遷與高度依賴所衍生之風險，俾做為後續治理與安全討論之基礎。臚列說明如后：

一、全球海纜現況與發展趨勢

(一)隨著雲端運算、5G與「人工智慧」(AI)等數位科技快速發展，跨境資料傳輸對高速、低延遲與高可靠性的需求持續攀升，讓海底電纜的重要性由單純的通訊技術層次，進一步上升至國家安全與地緣政治競逐的核心議題；若從電纜鋪設路徑、登陸站(Cable Landing Stations)選址到投資結構的變化，可反映出主要國家與跨國企業在數位主導權與資訊韌性上的戰略布局。近年來，美國、日本、澳洲與印度等國，推動的「自由開放的印太」(Free and Open Indo-Pacific，FOIP)戰略，透過海底電纜建設強化區域互聯與通訊安全；相對地，中共則藉由「數位絲綢之路」擴展海纜與雲端基礎設施，企圖展現其在全球數位秩序中的影響力。

(二)從產業結構面向觀察，全球海底電纜市場也出現顯著明顯轉變，過去由傳統電信商與專業製造商主導的產業格局，隨著全球網路巨擘如「谷歌」(Google)、Meta(即臉書前身)、「亞馬遜」(Amazon)與「微軟」(Microsoft)等科技公司投入自建電纜計畫而重塑。再者，雖然低軌衛星被視為潛在的通訊備援方案，但在頻寬、穩定性與成本效益上，仍難以全面取代海底電纜，且未來全球通訊架構勢將呈現以海纜為核心、衛星為輔助的多層次互補網絡。

(三)截至2025年，全球運行或建設中

註5：「韌性防衛體系」此一概念源自我國政府近年因應地緣政治情勢變化與複合式安全威脅所推動之整體戰略轉型。該詞彙於2024年逐漸成為政策論述焦點，總統賴清德先生於2024年6月19日就職滿一個月記者會中亦公開提出提出此一詞彙。

的海纜系統已增至約597條、登陸站1,712處，遠高於2016年的321條；[6]其中，由「Meta」、英國電信公司「Vodafone」與「中國移動通信集團有限公司」等投資的「2Africa計畫」[7]，預計連結歐、亞、非洲等逾30個國家，被視為數位地緣戰略工程的典範，[8]更反映海纜安全成為資料主權、經濟權力與地緣安全的新競逐場域。

(四)海纜研究也逐漸跨足環境與科學領域，氣候變遷引發的深層海流與海洋動力變化，可能影響電纜結構安全與長期穩定性，使監測技術的重要性日益提升。當前全球主要海洋觀測體系，如「全球海洋觀測系統」(Global Ocean Observing System)[9]、「亞果計畫」(Array for Real-Time Geostrophic Oceanography)[10]、「深海觀測策略」(Deep Ocean Observing Strategy)[11]及多項跨國合作計畫，均為海底電纜風險評估與環境監測提供更多關鍵數據。整體而言，全球海底電纜正朝向高度戰略化、產業多元化與跨領域整合的方向發展，成為數位時代不可或缺的核心基礎設施。

二、海纜脆弱性

(一)海底電纜承擔著全球網際網路運作與金融體系穩定的核心功能，從國際金融交易、雲端運算、社群媒體互動，到AI模型的即時運算與資料交換，皆依賴這些隱沒於深海中的光纖「數位動脈」。[12]這種深度依賴，使全球經濟運作呈現出前所未有的高度集中性與脆弱性。目前，全球僅少數跨國公司，掌握主要的海纜鋪設與維護技術，再加上登陸站點多位於地理與政治敏感區域(如新加坡、香港、日本沖繩、關島與我國等)，使得「關鍵海纜」一旦受損，就可能導致區域性資訊中斷或全球金融連動風險(我國對外國際海底電纜，如圖一)。[13]

註6：TeleGeography, Submarine Cable Map 2025(Washington, DC: PriMetrica, Inc., 2025), pp.1~3。

註7：該計畫為全球規模最大的海底光纖系統之一，透過新一代高速海纜強化非洲與歐洲、中東及亞洲的數位連結，並以約4.5萬公里的環狀架構串聯30餘國與多個登陸站，提升網路韌性與穩定性。

註8：Douglas R. Burnett, "The Strategic Dimensions of Global Submarine Cable Networks," Journal of Maritime Affairs, Vol.18, No.2, Month 2022, pp.135~138。

註9：「全球海洋觀測系統」(GOOS)是一個由聯合國主導的國際合作計畫，旨在建立一個持續、長期且全球性的海洋監測網路。

註10：「亞果計畫」(Argo)是全球海洋監測的核心計畫，透過約4,000個自動剖面浮標，隨洋流漂浮並定期在海面至2,000公尺深處巡航，它每10天傳回一次海水的溫度與鹽度數據，是科學家掌握氣候變遷、預測颱風及監控全球暖化的關鍵利器，我國也積極參與其中，由氣象署與部分大學(如臺大)負責。

註11：「深海觀測策略」(DOOS)是隸屬於「全球海洋觀測系統(GOOS)」下的國際合作框架。它專注於水深2,000公尺以下的深海區域，整合物理、化學與生物多樣性監測，旨在建立長期、系統化的觀測網絡，以應對氣候變遷、資源開發及深海生態保護等全球性挑戰。

註12：Nicole Starosielski, The Undersea Network (Durham, NC: Duke University Press, 2015), p.9。

註13：Burnett, Daniel R., "Private Networks, Public Risks: Big Tech and the New Submarine Cable Order," Telecommunications Policy,Vol.46,No.5,2022, p.3。

(二)由於多數電纜鋪設於深達數千公尺的海床，缺乏即時監控能力，也難以在短時間內進行維修；現有監測多依賴少數商業衛星與有限的海洋監測系統，其資訊回報週期長且空間解析度不足。[14]尤其在地緣政治競爭升溫的背景下，海纜不僅可能因自然災害受損，更可能成為「複合式威脅」的潛在目標。在此脈絡下，印太地區做為全球資料流的戰略樞紐，特別容易成為技術競逐與戰略干擾的前線。

參、海纜面臨的複合式安全威脅

由於海纜分布於廣闊且難以即時監控的海域，其安全風險呈現高度複合特徵，涵蓋實體破壞、地緣政治博弈、網路滲透與供應鏈脆弱性等多重面向。以下針對當前全球海底電纜所面臨的主要安全威脅類型，從實體、數位與技術治理層面，分段說明如後：

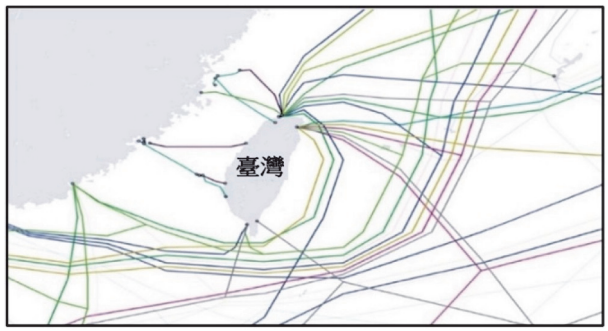
一、實體安全與地緣政治風險

大多數海底纜線均位於深海區域，不僅無法即時監控與物理保護，任何意外斷纜或惡意破壞均可能造成跨區域網路癱瘓、金融中斷及國家安全風險。有關海纜涉及的地緣政治風險，摘陳如后：

(一)實體威脅來源

1. 偶然性風險

包含「非故意損害」及「自然災害」兩類，其中非故意約占電纜故障事件的六成以上，主要源自航運與漁業活動，如下錨、底拖漁法或海底施工，均可能意外損壞纜線；加上我國周邊淺水區，如西南海域及巴士海峽，由於漁業密集，均屬高風險區域。自然災害包括環太平洋地震帶的地震、海嘯、火山爆發及海底滑坡等重大災害，可能同時摧毀多條纜線。[15]



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。

2. 惡意性威脅

指由國家(或代理人)或是惡意活動發起，旨在破壞、干擾或竊取資訊；此類行動通常難以偵測與歸責，常發生於深水區或主權爭議海域。世界各地近年均有相關案例，如以先進的潛艦、「水下無人儀具」(UUV)及偽裝民用船舶進行切割、干擾或植入竊聽裝置，在印太區域尤為明顯。畢竟臺海、南海及麻六甲海峽電纜密集，且位於地緣政治焦點，常成為惡意行動的

註14：同註1，頁31~33。

註15：International Cable Protection Committee,“Annual Submarine Cable Incident Report,”(London: ICPC, 2022), p.5。

目標。2025年底，芬蘭政府就在「芬蘭灣」(Gulf of Finland)海域查扣具俄國背景的權宜船「費特堡號」(Fitburg)刻意破壞海底電纜即是一例。[16]

(二)地緣政治博弈下的戰略化

1.近幾年來，海底電纜已廣泛被提升至數位戰略資產的高度，成為大國競爭的新興焦點，破壞或控制敵對國的海纜，成為一種「不對稱作戰」手段。分析其目的包括癱瘓經濟、軍事與情報系統，並在衝突前夕創造資訊優勢，常見的方式包括受國家指揮行為者或其代理船隻，以「科研」或民用活動為名，進行長時間滯留或反覆錨泊，模糊「故意破壞」與「意外事件」的界線，此種行徑亦會對執法與監控，構成制度上的挑戰。

2.「灰色地帶」行動的特點即為非軍事性與難以歸責，自然也對執法機關造成極大的挑戰。主要體現在三個面向，包含舉證困難，缺乏即時監控難以分辨故意與意外；執法敏感性高，過度回應可能被敵對國操作成為升高衝突的藉口；韌性需求大，需將海纜防護納入國家安全及數位韌性策略，才能強化海巡單位在內的非軍事執法機構角色。換言之，面對來自海上的複合式威脅，提升海巡執法能力並建構海纜防護韌性，已成為捍衛國家數位安全的「重中之重」。

二、網路與資訊安全挑戰

(一)海纜的安全風險已從傳統物理破壞延伸至網路與資訊層面。首先，登陸站與「網路管理系統」(Network Management Systems)做為關鍵節點，雖然傳輸鏈路具高強度加密，仍容易成為滲透與攔截目標。依經驗顯示，美國情報單位就曾於光纖節點實施上游攔截，並截取外交與軍事通信，凸顯海纜面臨的高度風險。[17]其次，「海纜供應鏈安全」亦是安全風險的核心議題之一，從製造、鋪設到系統更新，每一環節皆可能遭植入惡意程式，進而遭到操控。

(二)近期因有「中」方企業參與印太海纜專案而引發的「技術信任赤字」(Trust Deficit)問題，促使多國推動「可信任供應鏈」(Trusted Supply Chain)政策，以維護戰略通信安全。[18]再者，海底電纜遭受的威脅正由實體破壞向複合式數位攻擊轉變，入侵管理系統或感測網路可能造成流量重導、訊號遺失或通信中斷，使實體與資訊防護界線快速模糊。[19]此

註16：2025年12月31日，芬蘭電信公司「Elisa」連接塔林(Tallinn)的數據纜線斷裂，芬蘭當局隨即查扣具俄國背景的「費特堡號」，懷疑其在愛沙尼亞海域拖錨數公里肇事，並依法偵辦。

註17：Glenn Greenwald, No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (New York: Metropolitan Books, 2014), pp.94~96。

註18：歐錫富，〈印太海底電纜安全與灰色地帶挑戰〉，《國防情勢月報》(臺北市)，第240期，2024年4月，頁15~18。

註19：Brenden Kuerbis and Farzaneh Badiei, "Cybersecurity of Undersea Cables: A Governance Challenge," Journal of Cyber Policy, Vol.5, No.2, Month 2020, pp.248~251。

外，自然環境因素如複雜海域地形、劇烈海流亦可能導致纜線微彎曲、外露或信號衰減，均將增加通信中斷的可能性。

三、偵測、防護與復原技術發展

建構具韌性的海纜防衛體系，須依賴「偵測、防護與復原」三大技術的協同發展，加上海域執法與監控支援，方能提升系統生存能力。摘陳說明如下：

(一)偵測技術為維護海纜安全的核心基礎，其中「分散式聲學感測」(Distributed Acoustic Sensing，以下稱DAS)可將光纖轉化為沿線感測器，記錄微小振動與聲波變化，用以偵測拖網、錨擊及潛艦活動。當DAS資料與岸際雷達、「船舶自動識別系統」(AIS)及衛星監測整合後，能提供即時預警訊息，協助海巡及相關單位於干擾初期介入。此外，AI與「機器學習」(Machine Learning)、「深度學習」技術的導入，讓系統能分析船舶航跡、滯留時間及行為模式，自動辨識異常行動與「灰色地帶」威脅，提高海域監控的準確性與即時性，並促成海事監測系統與預警的智慧化發展。[20]

(二)防護技術聚焦於物理抗性與系統強化。物理層面透過加厚鎧裝及深埋海纜，提升抗磨損與抗拖曳能力，特別適用於高風險海域；系統層面的強化則透過網絡冗餘設計與多路徑環狀結構，確保單點故障不致影響整體通信，形成防護與韌性兼具的架構。

(三)復原技術強調快速維修與跨域協作，即便防護完善，斷纜仍難以完全避免；因此「維修效率」直接關乎系統韌性。故利用水下無人載具及遙控潛水器進行斷纜定位與輔助維修，可大幅縮短修復時間；同時，AI輔助資源調度與修復優先排序，亦能降低海纜中斷風險。

(四)在執法層面上，海巡單位能夠提供必要護航與現場維安支援，確保海纜修復作業得以順利進行，從而形塑科技手段與執法機制相互支持的雙軌式防衛架構，確保國家海底電纜的安全。

肆、國際與印太區域海底電纜安全治理與合作

既有的法律體系雖對海纜之鋪設、維護與破壞行為，設有一定規範，然面對新型「複合式威脅」及跨境執法困難，其規範密度與執行效能仍顯不足。有鑑於此，有必要從國際法與國內法雙重層次，檢視海底電纜保護之現行法制架構與制度缺口，做為後續韌性治理與制度強化之基礎。

一、與海纜有關的法律現況

(一)國際法層面

海纜的治理主要奠基於包括《公海公約》(Convention on the High Seas)與《

註20：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。

大陸礁層公約》(Convention on the Continental Shelf)、《海纜保護公約》(Convention for the Protection of Submarine Telegraph Cables)，及《聯合國海洋法公約》(UNCLOS，以下稱海洋法公約)，輔以「國際海纜保護委員會」(ICPC)之實務建議及「歐盟」《網路與資訊安全第二號指令》(NIS2)[21]、《關鍵實體韌性指令》與《海纜韌性建議》(Commission Recommendation on Secure and Resilient Submarine Cable Infrastructures)等多項條約規範。摘述如後：

1.在《海纜保護公約》中即要求締約國將干擾或破壞電報電纜之行為刑罰化，為後續將光纖電纜之實體破壞與訊號干擾納入法律規制，提供重要概念基礎。《海洋法公約》第112條[22]則明確保障各國在公海鋪設與維護海底電纜之自由，並將此一權利延伸至大陸礁層[23]，同時要求各國對故意或過失損害電纜之行為，設立刑事責任與救濟制度(第113~115條)[24]。當海纜事件涉及主權爭議或國家安全因素時，由於《海洋法公約》亦設有管轄限制性例外(第297條)等條款，反而削弱國際司法機構對爭端行使強制管轄的可能性，使法律救濟機制在高度政治化或安全化的情境下，面臨適用上的侷限。

2.在區域治理層次，相關規範近年逐漸成形。「歐盟」(EU)自2023年起，透過NIS2指令與CER體系，結合《海底電纜韌性建議》，建立涵蓋資通安全與實體防護的跨部門聯防框架，強調事故通報機制、跨境協調與基礎設施冗餘投資，以降低單點失效風險。此外，2017年出版的《塔林手冊2.0》(Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations)[25]亦從UNCLOS、無害通過與國家主權等脈絡，提供對網路行動與海上活動的法律解釋指引，補充既有國際法對複合式威脅的適用空間。

3.國際間在不法行為歸責與國家責任的實務適用上，仍面臨顯著困難；畢竟海纜事件往往涉及跨境證據蒐集、快速歸因與可執行反制措施等問題。在公海或他國

註21：「網路與資訊安全第二號指令」(Directive EU 2022/2555 - Directive on measures for a high common level of cybersecurity across the Union)核心目標為建立歐盟統一的資安治理與事故通報制度，加強公共與私部門的網路防禦能力，涵蓋能源、運輸、健康、數位基礎設施(如雲端服務與海底電纜)等關鍵領域。

註22：《海洋法公約》第112條第1項：「所有國家均有權在大陸架以外的公海海底上鋪設海底電纜和管道。」

註23：《海洋法公約》第79條第1項：「所有國家按照本條的規定都有在大陸架上鋪設海底電纜和管道的權利。」

註24：《海洋法公約》第113條：「…故意或因重大疏忽而破壞或損害公海海底電纜，…，以及類似的破壞或損害海底管道或高壓電纜的行為，均為應予處罰的罪行。」第114條：「每個國家應制定必要的法律和規章，規定…在鋪設或修理該項電纜或管道時使另一電纜或管道遭受破壞或損害，應負擔修理的費用。」第115條：「…船舶所有人在其能證明因避免損害海底電纜或管道而犧牲錨、網或其他漁具時，應由電纜或管道所有人予以賠償…。」

註25：《塔林手冊2.0》是目前國際上最權威的網路軍事行動法律指南。由「北約合作網路防禦卓越中心」(NATO Cooperative Cyber Defence Centre of Excellence)召集專家編撰，旨在探討現行國際法如何適用於網路空間，該手冊雖非法律條約，卻是各國政府與法律學者判定網路攻擊是否構成「使用武力」或「戰爭行為」的重要參考基準。

大陸礁層海域的執法、扣押與舉證尤為不易；加上各國對海纜保護區的劃設標準與執法強度，亦缺乏一致性，且涉案船舶常跨越多重司法管轄，導致司法互助程序冗長，進而形成惡意破壞行為「低風險、高報酬」的結構性誘因。總體而言，海纜雖已納入既有國際法保護架構，但在複合威脅、跨境管轄與執行能力不足的情況下，仍存在明顯的規範落差、歸因困難與執行不足等問題，亟需透過更高程度的制度協調、監控整合與跨域防護策略加以補強。

(二)國內法層面

海底電纜是我國重要的關鍵基礎設施，然而在地緣政治與中共「灰色地帶」行動頻繁的背景下，「中」方藉偽裝成貨船或漁船的海上民兵船，頻繁製造「灰色地帶」襲擾，如2023年馬祖外海電纜中斷事件，引發紛爭與對立，企圖達成恫嚇我國人民之目的。[26]相關案件也暴露出我國在海纜法制的實體防護與執法權限，面臨雙重挑戰。臚列說明如下：

1. 首先是刑事責任規範不嚴，導致可歸責性不足。對於蓄意拖錨、關閉AIS進行不當作業等行為，難以產生足夠威懾，亦未將這些行為提升至國家安全或公共危險罪的範疇。其次，執法與取證限制，造成執行力不足。海巡單位針對海纜損壞案件的執法困境，包括通報時效延遲、證據鏈保全困難、法律管轄權的限制(領海外難以追訴)、情報資訊不完整(船隻偽冒或未開啟AIS)，以及執法授權與政治考量等。[27]第三，治理方式呈現跨領域、跨機關模式，影響程序效率。我國涉及海纜案件的機關橫跨資安、國防、海域執法、交通管理、涉外部會、司法機關與民間單位等，導致登陸站與實體線路的保護標準、事故分級與即時通報系統缺乏一體化設計；且海纜修復許可程序，亦因缺乏「單一窗口」機制，導致維修曠日費時。[28]

2. 我國已成功推動「海纜七法」的法制轉型，標誌著邁向海纜治理的新篇章，同時將海底電纜由一般通訊設施明確提升為「國家關鍵基礎設施」(如圖二)；其保護層級與電力、能源及水資源安全並列，不僅回應UNCLOS對海纜保護刑罰化的國際法趨勢，更重構我國海纜治理的執法架構。此外，也大幅加重故意與過失破壞海纜及相關管線之刑責，並引入犯罪工具沒收

註26：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；黃世澤，〈澎湖漁場、馬祖海纜全遭殃，中國盜砂船入侵的海峽風暴〉，報導者，2023年4月27日，https://www.twreporter.org/a/china-dredging-penghu-matsu-destruction，檢索日期：2026年2月1日。

註27：吳肇恩，〈海底電纜破壞行為之國際法歸責與我國執法權限探討〉，《政大法學評論》(臺北市)，第151期，2023年9月，頁20~24。

註28：International Cable Protection Committee, "Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables," International Cable Protection Committee, November 18, 2022, https://www.iscpc.org/publications/icpc-best-practices/, visited date:2026/1/22。

法律	修正重點	保護對象
《電信管理法》	增列犯罪工具、船舶或機械設備可沒收處置	通訊海纜與登陸站
《電業法》	保護範圍納入海底電力電纜；新增過失犯罰則；可沒收犯罪工具、船舶	海底電力電纜
《天然氣事業法》	保護納入海底輸氣管線；新增過失犯罰則；可沒收犯罪工具、船舶	海底輸氣管線
《自來水法》	保護納入海底送水管線；新增過失犯罰則；可沒收犯罪工具、船舶	海底送水管線
《氣象法》	強化氣象設施防護；新增過失犯罰則；可沒收犯罪工具、船舶	蒐集地震、颱風等資料的海底電纜
《商港法》	滯留船舶三個月內須離港或移泊；偽冒船舶或無正當理由未離港者可沒入	規範船舶入港、滯留與驅離措施
《船舶法》	強制船舶維持AIS正常運作並發送正確資訊	船舶自動識別系統（AIS）、船舶管理

圖二：我國「海纜七法」修正重點與保護對象示意圖

資料來源：李書瑜，〈行政院通過「海纜七法」修正草案，黃勝雄：三大風險威脅臺灣命脈〉，關鍵評論，2025年9月24日，https://www.thenewslens.com/article/259062，檢索日期：2026年1月15日。

、強制船舶維持AIS正常運作等制度設計，有效避免「權宜輪」、「幽靈船」及「灰色地帶」行動所造成的執法真空。

3. 相關法律亦明確授權執法機關得於海纜保護區內，對異常滯留、低速徘徊或身分不明船舶，採取預警性驅離、攔查與扣留措施，讓治理模式由「事後修復」轉向「事前阻斷」。在此脈絡下，海巡署被定位為「通訊韌性防衛體系」的第一道防線，其影響包括強化破壞海底電纜犯罪之偵察與即時處置法源；解決涉案船舶扣留與港區安全之實務困境；透過強化船舶識別資訊揭露義務，提升監控與裁罰效能。修法亦促使海巡署建立標準化的「事件－證據－司法互助」流程，同時整合海事與資安情報，進一步推動跨部會與跨領域常態化的演訓要求。

簡言之，「海纜七法」不僅補齊過去刑責不足與權限模糊的制度漏洞，更透過法制化整合科技監測、行政協調與海上執法能量，使海纜安全上升為國家戰略層次的數位韌性議題，為我國因應複合式威脅，奠定長期且具正當性的治理基礎。

二、國際與印太區域海纜治理機制

海底電纜在國際社會及印太地區均被視為「戰略連通性」(strategic connectivity)與「數位主權」(digital sovereignty)的核心載體，各國並透過此「基

礎設施外交」，強化區域互信；[29]對我國而言，這不僅是數位安全課題，更是提升國際能見度與突破外交侷限的契機。身處印太鏈結樞紐位置，我國實可藉海纜安全治理參與多邊合作體系，同時接軌國際規範，融入區域「海上韌性防衛網絡」的合作架構。[30]參與作法如後：

(一)印太區域治理的雙層架構

1.戰略框架層面－從倡議到制度化行動

自2024年以來，印太主要國家及多邊組織已將「安全且具韌性的海底電纜連通」(Secure and Resilient Submarine Cable Connectivity)納入政策主軸，如「四方安全對話」(指美、日、澳、印四國，以下稱Quad)推動設立「電纜連結及韌性中心」(Cable Connectivity and Resilience Centre)以強化區域國家的法規制度、維修能量與監測技術，以及推動印太海纜網路的安全治理。[31]2024年3月，「七大工業國組織」針對安全數位通訊網路海纜達成的戰略共識亦指出，海纜承載全球絕大多數的國際數據流量，而確保連線安全與基礎設施韌性已成為全球數位治理的核心目標。[32]區域組織-「東協」(ASEAN)亦在2024年《新加坡宣言》(Singapore Declaration)中，提出「建構安全、多元且具韌性的海底電纜網絡」，[33]顯示該議題已成為印太區域國家合作的新焦點。

2.技術與治理層面－標準化與程序協調

「國際海纜保護委員會」與「國際電信聯盟」則持續推動跨國技術規範，包括「海纜事故通報格式」(Cable Incident Reporting Template)與登陸站韌性指標，為各國建立共同海纜治理指引。[34]如星國在《電信法》中劃設法定「電纜保護區」，並由「資訊通信媒體發展局」建立跨部

註29：Chien-Er Wu, “Taiwan’s Participation in Indo-Pacific Digital Connectivity Governance: Legal and Policy Perspectives,” Taiwan International Review,Vol.19,No.2, Month 2023, pp.58~63。

註30：Shih-Keng Yeh, “Maritime Diplomacy and Taiwan’s Role in Indo-Pacific Resilience Networks,” Journal of Asia-Pacific Security Studies, Vol.11, No.1, Month 2025, pp.105~108。

註31：湯姆・阿布克(Tom Abke)，〈印太國家強化防衛海底電纜，防範漏洞湧現〉，Indo-Pacific Defense Forum，2024年9月18日，https://ipdefenseforum.com/zh-hant/2024/09/印太國家強化防衛海底電纜，防範漏洞湧現/，檢索日期：2026年2月2日。

註32：G7 Italia, “Joint Statement on Cable Connectivity for Secure and Resilient Digital Communications Networks,” (Rome: Government of Italy, 2024), p.1。「七大工業國組織」(G7)是由全球七個發達經濟體組成的非正式論壇，成員國包含美、日、德、英、法、義大利及加拿大，主要討論全球經濟治理、國際安全與能源政策等重大議題。

註33：Association of Southeast Asian Nations (ASEAN), “The 4th ASEAN Digital Ministers’ Meeting Singapore Declaration: Building an Inclusive and Trusted Digital Ecosystem,” Association of Southeast Asian Nations, February 2, 2024, https://asean.org/wp-content/uploads/2024/02/ADGMIN4-Singapore-Declaration-Final.pdf, visited date: 2026/1/31。

註34：International Cable Protection Committee, “Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables,” International Cable Protection Committee,November 25, 2024, https://www.iscpc.org/publications/icpc-best-practices/,visited date: 2026/1/31。

會協調機制；日、澳兩國則在「Quad」框架下推動「電纜連接與韌性夥伴關係」(Quad Partnership on Cable Connectivity and Resilience)[35]，並於澳洲坎培拉設立「電纜連接與韌性中心」(Cable Connectivity and Resilience Centre，以下稱CCRC)[36]，整合印太國家的技術培訓、維修許可標準化與情資分享，進而推進「技術、作業、執法」三位一體的韌性防禦體系。以上這些措施，不僅縮短跨境修復時間，亦可建立因應「灰色地帶」行動的制度性防護基礎。

(二)我國的外交介面與治理參與

1.以技術合作切入

依我國國情現況，可透過「非正式」與「技術性」途徑間接進入海纜治理的國際合作體系，初期先以觀察員身分參與「國際海纜保護委員會」活動，提供事故資料與研究成果，強化專業能見度。在實際操作上，包含由「國家通訊傳播委員會」、海巡署共同與澳洲CCRC簽訂技術交流備忘錄，參與訓練與演練，或以外離島斷纜事件做為區域韌性案例，以提供共享教材；透過這種「專業外交」與「技術外交」模式，彼此可在不觸及主權爭議下，強化我國在印太數位治理的參與度。

2.建構跨部會「海上韌性防衛網絡」

(1)在印太區域海纜與關鍵海上基礎設施防護的脈絡下，以「跨部會、跨層級」的聯合治理模式，逐步建構具整合性的「海上韌性防衛網絡」。在此架構中，除相關主管機關之制度設計外，海巡署與海軍應依其法定職掌與實務能量，形成分工明確、協調順暢的協作關係，共同支撐韌性防衛體系運作。海巡單位可於平時與低強度「灰色地帶」情境中，結合海軍既有海上與空中感知能量，參與跨國巡護行動，並透過AIS、雷達、海事監控系統等資料的協作共享，逐步推動「全海域感知」與「情資共構」機制，提升對異常活動、可疑船舶與潛在風險的即時辨識能力。

(2)在海纜維運或修復期間，可由海巡單位於必要時負責海上執法與作業安全維護，並結合海軍於外圍警戒、海域態勢掌握與必要支援能量，建立臨時但具彈性的安全管制與作業協調機制。另在不涉及軍事衝突升高的前提下，海巡署亦可與海軍共同參與或協同規劃與友邦之情境式演練與能力交流，並聚焦於拖錨破壞、無人載具干擾、「灰色地帶」干擾行動等混合式風險，同時藉此累積平時合作經驗，為必要時的平戰轉換奠定制度與實務基礎。

註35：「電纜連接與韌性夥伴關係」係由Quad發起，旨在強化印太海底電纜的安全與韌性。透過技術支援、政策協作與培訓，提升關鍵設施的復原力，確保數位連接在面對災害或人為威脅時仍能穩定運行。

註36：CCRC係於2024年宣布成立，主要目的是強化印太區域國家的海底電纜安全、監測與維修能力，並促進盟國間在電纜治理與技術標準上的協調。

此作法除有助將海事執法功能延伸至關鍵基礎設施保護層面外，並透過與海軍的制度化合作，強化我國參與區域海上韌性治理的實質能力。

3.以知識外交建構軟實力

可透過外交部與教育部共同推動之學、研合作機制，與日、澳及星國等理念相近國家，建立具制度化架構的聯合研究中心，並將海纜與關鍵海上基礎設施治理納入「知識外交」的重要議題。此類合作不僅聚焦於「AI監測技術」與海域風險預警模型的研發，亦可結合「危機通訊演練」與跨國協調機制設計，強化在突發事件下的資訊透明與政策回應能力；另在學術上，可透過比較與制度分析，推動海纜防護相關之法制整合研究，以促進治理原則與最佳實務的跨國擴散。再者，透過學術研究與政策實務並行的合作模式，應能形塑跨國政策社群與專業網絡，積累我國在印太區域海上韌性治理中的知識影響力及規範話語權，進一步轉化為具持續性的「軟實力」。

(三)挑戰與風險

1.印太地區橫跨多重主權與法律體系，各國對於海纜鋪設、修復許可、執法權限與通報程序之規範差異甚大，缺乏統一標準。當海纜受損事件發生時，往往需同時面對沿岸國、船旗國與營運國等多方管轄權交錯，導致修復程序延宕，讓通訊中斷風險由單一國外溢至整個區域。

2.近年針對海纜的威脅多以「低於武裝衝突門檻」的方式進行，並偽裝成意外事故、科研活動或商業作業，刻意模糊故意破壞與意外損壞之界線，此類行動樣態，在國際法上難以即時歸責，亦缺乏明確的反制手段，導致受害國在政治、法律與安全回應上，往往陷入進退失據的困境。

3.海纜維修高度依賴少數具專業能力的維修船隊與技術人員，而印太地區可即時投入的維修能量本就有限，一旦發生多點、同步的斷纜事件，不僅將拉長修復時程，也可能造成跨國通訊與金融系統的重大中斷，再度放大經濟與安全層面的連鎖衝擊。

4.多數國際海纜由跨國電信商或科技企業以聯合投資方式建置與營運，其決策邏輯以商業效率與成本控管為核心，相關資訊往往受到商業機密保護。此一結構使政府在風險評估與危機管理上，難以即時掌握完整路徑與脆弱點，造成公共治理與國家安全決策的資訊「不對稱」。

5.在美、「中」科技競逐加劇的背景下，電纜路徑、設備來源與系統標準的選擇，逐漸帶有「陣營化」色彩，迫使部分國家在合作對象上必須承擔政治風險，進一步提高國際協作與制度協調的複雜度。

此外，我國在海纜治理上除面臨上述共通風險外，尚受限於非聯合國會員身分

、地緣政治敏感性及內部跨部會協調機制，仍待整合等結構性因素；若未能建立一致且前瞻的「海纜外交與治理策略架構」，將不利於在多邊場域中爭取制度參與與話語空間，亦難以應對高度複雜化的海纜安全風險，值得注意。

伍、海巡署在海纜韌性防衛體系中的角色與潛能

在海底電纜逐步被納入國家關鍵基礎設施與數位安全治理核心的情況下，海域執法機關的功能定位，成為當代海洋安全研究的重要議題。以下就海巡署在海纜韌性防衛架構中的角色定位與發展潛能，概述如後：

一、海巡署的角色與定位

在印太地緣政治競逐日益激烈，海底電纜成為「戰略通信中樞」的背景下，我國面臨的不僅是傳統海上安全挑戰，更包含數位基礎設施的韌性防衛問題。海巡署做為國家海域治理的核心執法機關，其職權與組織功能在海纜安全與防護體系中，具有潛在的戰略價值與制度優勢。[37]以下就其法定職責與治理潛能，說明如下：

(一)法定職責與關鍵基礎設施的守護

海巡署依《海岸巡防法》的法定職權與能夠持續部署、執法的艦船資源，在海纜治理上展現出高度的「功能整合性」優勢。其任務涵蓋海域治安維護、海洋權益保障及海難救助，並依《電信管理法》對電信設施(含海底電纜)之保護規範與損壞罰則，進行調查、蒐證與司法移送等職權。再者，鑑於海纜係支撐我國資訊流通、金融體系與國際通信運作之關鍵命脈，其安全已屬國家關鍵基礎設施範疇；故海巡於執行相關任務時，亦負有確保關鍵設施穩定運作之法定責任，讓其角色由傳統海上治安維護，延伸至國家數位韌性與資通防衛的重要支援環節。[38]

(二)法律地位與應對行動

1. 相較於軍事力量，海巡艦船在法律定位與行動屬性上，具有較低的衝突敏感性，所屬人員也隨時得在不升高安全對抗門檻的前提下，積極處理不明漁船干擾、民用船舶可疑活動、情報蒐集行為或偽裝施工等「灰色地帶」行動。此特性，使海巡機關不僅能於前端偵測與初步應處階段，發揮戰略緩衝與彈性回應的功能，亦有助於降低敵對勢力以非軍事、民用手段干擾或破壞海纜可能造成的安全衝擊。

2. 海巡業務範疇廣泛，亦長期累積跨部會協調與情報整合之實務經驗，更具備

註37：Tsung-Yen Yeh and Ming-Hsien Wu, “Maritime Governance and Hybrid Threats in the Indo-Pacific: Taiwan’s Coast Guard as a Resilience Actor,” Journal of Maritime Policy and Security Studies, Vol. 12, No. 2, Month 2023, pp.52~55。

註38：Chung-Lien Tsai, “Legal Framework and Governance Potential of Taiwan’s Coast Guard in Critical Maritime Infrastructure Protection,” Ocean Policy Review, Vol. 19, No. 3, Month 2021, pp.95~98。

參與資訊整合與協作平臺的制度優勢。在主管機關統籌下，可與通訊監理機關、航港單位及數位治理部門等，建立海纜保護區之聯合監測與通報機制，結合電信業者回報、岸際雷達、AIS航跡資料及其他海域感知資訊，即可強化對異常行為的即時辨識、協調處置與後續復原作業，形塑多元參與的風險應處流程。

3. 在整體國家防衛與韌性治理思維下，海巡署正由傳統海上執法機關轉化為海纜韌性防衛體系中的重要支援節點，透過科技升級與智慧海域監測系統的整合，平時強化預警與巡護，在突發事件發生時，協助初級應變與跨機關協調，並於必要時協請海軍艦艇支援，或共同處理後續復原作業。

基於海巡署在我國海纜安全維護中的價值，並非建立於單一核心地位，而是在跨部會聯合治理架構下，憑藉其法定職責與實務能量，提供穩定而具彈性的戰略需求。此一定位不僅回應印太區域對關鍵海上基礎設施保護的治理趨勢，亦有助強化我國整體數位韌性與區域合作的能力。

二、海纜處理實務與多層韌性防衛體系建立

(一)事件概況

1. 2025年2月發生的海纜破壞事件，被視為我國海纜治理與通訊安全法制的重要轉折點，亦為我國司法史上首起因破壞海纜而遭判處有期徒刑的指標性案件。事件發生於臺南將軍漁港西北方約6浬海域，涉案船隻為具「中」資背景之「多哥籍」權宜輪「宏泰58號」，調查顯示，該船於海纜敏感區內滯留近54小時，並以極低速進行異常「Z字型」往返航行並實際下錨，且在海巡署與港口單位7次廣播警告均未回應，亦拒絕離開禁錨區，其船名與AIS資訊亦多次變換，顯示高度規避查緝之意圖(如圖三)。[39]該事件凸顯海纜在「灰色地帶」行動下的高度脆弱性，並直接促成後續「海纜七法」的制度性修法，對我國海纜治理產生深遠影響。

2. 該案的海纜斷裂，嚴重影響我國本島與澎湖間之通訊，並造成「中華電信公司」近新臺幣1,900萬元之經濟損失。2025年6月，經法院認定該船長明知海纜位置，仍從事高風險操作，構成毀壞犯意，依法判處3年有期徒刑，正式成為破壞海纜之刑事司法先例。[40]整體而言，該案件不僅展現跨機關偵防與司法應處能力，也加速我國海纜安全法制與主動防護機制的建構，成為國際高度關注的重要案例。

(二)多層次韌性防衛體系建立

1. 第一層-事前防護與智慧監測

註39：蔣宜婷，〈臺灣海底電纜首宗刑事案：中國籍船長判囚三年，庭上細節能釋除北京「灰色作戰」疑雲嗎？〉，BBC NEWS中文，2025年6月12日，https://www.bbc.com/zhongwen/articles/cdd2jjjn9n4o/trad，檢索日期：2026年1月30日。

註40：同註39。

圖三：「宏泰58號」案件位置示意圖

說明：海巡人員整裝待發(小圖下)、船舶接近「宏泰58號」(小圖上)。

資料來源：參考海巡署資料及蔣宜婷，〈臺灣海底電纜首宗刑事案：中國籍船長判囚三年，庭上細節能釋除北京「灰色作戰」疑雲嗎？〉，BBC NEWS中文，2025年6月12日，https://www.bbc.com/zhongwen/articles/cdd2jjjn9n4o/trad，檢索日期：2026年1月30日，由作者綜整製圖。

鑑於海纜鋪設於近海至外海、平均水深約1,000至3,000公尺之間，傳統巡邏艦艇難以長時間、全面性監控，相關機關亟需導入科技輔助治理工具。目前海巡署已與「國家通訊傳播委員會」(NCC)、「數位發展部」及交通部航政單位合作，要求電信業者強化海纜防護作為，包括部署自動告警系統，即時監控海纜周邊船舶動態，並整合AIS、雷達監測、航港局及海軍相關資料庫，形成多源感知監控網絡；未來再導入AI驅動的海洋監測系統，透過機器學習分析船舶航跡、滯留行為、拖錨或異常航行模式，將有助及早辨識潛在「灰色地帶」行動所衍生的實質破壞。

2. 第二層-動態指揮與即時應變機制

海巡署已針對突發海纜損壞事件建立「標準作業程序」(SOP)，在接獲電信業者通報後，得即時回放雷達與航跡資料，研判可疑船舶動向，並同步通報地檢署依法偵辦，並在可辨識目標且海象條件許可時，立即執行登檢、帶返調查，必要時協請海軍支援攔截。此一機制除能確保行政執法與司法偵辦的即時銜接，同時也為後續的跨部會協調與國際通報奠定基礎。

3. 第三層-案件調查、蒐證與證據鏈管理

為確保海纜破壞行為能有效進入司法程序，海巡機關已就海纜案件訂定明確蒐證重點，包括查驗船舶外觀、船錨或漁具是否留有損壞海纜之痕跡，是否攜帶或使用水下儀具、海纜切割器等特殊設備；並藉調閱航程紀錄儀(VDR)、航海日誌及海圖標示，以確認船長是否明確知悉海纜位置。此外，所有登檢與執勤過程均須全程錄影錄音，以維持證據鏈完整性；故當可疑船舶拒檢或逃離我方管轄海域時，海巡單位即報請檢察官後，透過外交、航政及司法體系，通報次一目的港或相關國家協助攔查，必要時啟動司法互助程序；若涉及刑事責任，則依法進行偵辦。

4.第四層-跨域資料整合與決策支援

跨域資料整合係支撐海纜整體安全的重要基礎。「資訊孤島」(Information Silo)[41]長期被視為海纜安全治理的結構性弱點，業管機關應建構「海纜安全資料交換平台」，整合電信業者的預警系統[42]、國防情資、衛星遙測與海洋環境資料，形成跨領域的「海洋數據湖」(Maritime Data Lake)[43]。透過AI模型長期學習不同季節、氣候條件與海域活動型態，建立可持續優化風險預測與態勢研判能力，俾從「事後反應」轉向預測型、前瞻型的安全管理。[44]

5.第五層-區域合作與聯防機制

由於海纜韌性防衛不應侷限於國內治理，而須延伸至印太區域，因此海巡機關可與「日本海上保安廳」(JCG)、「美國海岸防衛隊」(USCG)、「澳洲邊境部隊」(ABF)等單位，建立資料互通與聯合演訓機制，不僅提升我國在國際安全議題中的能見度，也能強化區域數位基礎設施的整體防護網。

由於多層次海纜韌性防衛體系的永續運作，最終仍有賴制度化的科技治理與專業人員培育，故我國可參照「美國海岸防衛隊」，設立「海洋科技創新實驗室」(Maritime Technology Innovation Laboratory)[45]，專責AI模型訓練、資料治理與情境模擬演練；並與國際科研單位合作，建立具系統性的「智慧海洋防衛課程體系」。咸信透過科技與人力的雙軌投入，方能為我國海纜安全與通訊韌性，奠定長期穩固的基石。

陸、建議-代結語

全球海底電纜體系正迅速成為地緣政治競逐、科技治理與國家安全交會的關鍵場域；尤其海纜已不再僅屬於電信或工程技術議題，而是深度牽動關鍵基礎設施防護、跨域治理能力與國際法秩序的綜合性安全挑戰。我國位處「第一島鏈」前沿，兼具區域資料節點與高度地緣敏感性，故海纜安全議題可視為印太安全結構轉型的具體縮影。以下建議，期能有助深化我國對海纜安全之風險認知，釐清治理主體之功能分工，並提供具制度韌性的海纜安全

註41：「資訊孤島」係指組織內部系統或單位間數據無法互通共享，資訊被鎖在特定範疇中，導致數據冗餘、協作低效且難以支援整體決策。

註42：以「中華電信公司」為例，已由傳統事後搶修模式，轉型建構以科技、法制與跨機關協作為基礎的「主動式海纜破壞預警體系」。其核心架構係以SAWS海纜自動示警系統為中樞，整合AIS與AI船舶行為分析模型，即時掌握低速航行、異常滯留或疑似拖錨等高風險行為，並於破壞行為發生前即通報海巡單位介入應處。

註43：「海洋數據湖」是一種集中式的大數據儲存架構，能整合並保留來自AIS、衛星遙測、聲學感測及氣象等各類原始、異質資料。

註44：同註20。

註45：係「美國海岸巡防隊」唯一的專業科研機構，專責「研究、開發、測試與評估」。其核心任務是將先進科技轉化為實際執法能量，協助決策者評估技術可行性與風險，是確保海域任務執行效率與技術領先的戰略樞紐。

治理政策與實務層面的參考。

一、我國做為亞洲資訊鏈的重要節點，亦嚴重暴露於中共「灰色地帶」威脅下，目前有10條國內海纜與14條國際海纜，約九成九的網路頻寬都仰賴這些「數位生命線」；[46]再從「興順39號」[47]至「宏泰58號」等事件觀察，此類風險並非偶發事故，而呈現具重複性與系統性的特徵，現行治理模式仍偏重技術維修與事後復原，而前端預警、情資整合與制度化協調仍略顯不足。至於在國際法層面，UNCLOS及《海底電纜保護公約》對低強度、可否認性高的威脅行動，仍存在歸責與執行上的限制；故海纜安全實難僅以產業或技術管理因應，更須積極納入國家安全與數位治理的核心政策框架，此點值得政府高度重視。

二、在印太地區的安全實踐中，中共長期運用科研船、漁船及無人載具執行海底測繪與情資蒐集，其行動具備模糊性、低可歸責性與高策略效益，意在測試區域防禦反應並逐步塑造新常態；在此常態下，海纜防護並非單一機關可獨力承擔之任務，必須形成軍事、執法與民用治理的分工合作。海巡署憑藉平時執法的合法性與常態化的海域部署，得以在低敏感度情境下，彈性執行監控、登檢及海底電纜保護等任務；海軍則可在情勢升高或涉及軍事風險時，提供情監偵、海上態勢感知與必要的戰略嚇阻支援，形成層級分明、相互補位的安全架構，凸顯兩者在既有基礎上繼續緊密合作，確實至關重要。

三、在科技治理與韌性防衛層面，海纜安全防護需由被動修復轉向智慧預警與系統韌性建構。透過整合「分散式聲學感測」(DAS)、AIS航跡分析、衛星影像與水下無人載具等多源資料，結合AI異常行為辨識與風險分級，則可強化對拖錨、非法錨泊或可疑水下活動的即時掌握。此類系統的建置不僅有助於縮短中斷復原時間，更可做為跨部會共同使用的態勢感知基礎，支撐政策決策與分工協調，故政府應高度重視並主動提供必要協助，才能賡續強化智慧預警系統功能。

四、在制度設計上，海巡署的角色宜定位為「前端支援與協調節點」，而非海纜治理的單一核心機關，其法定職掌使其適合承擔海上異常行為的第一線監測、初步執法與即時通報；並在事件發生時，與國防部(海軍)、交通部、數位發展部及電信業者啟動聯合應處機制。此一跨部會治理模式，除了避免權責集中所帶來的制度風險，亦能真正做到提升國家海纜整體應變效率與合法性。

五、海纜防護本質上具有跨國性，難

註46：同註39。

註47：方瑋立，〈年初斷纜逃逸順興39號 8月現踪釜山外海〉，《自由時報》，2025年12月27日，https://news.ltn.com.tw/news/politics/paper/1737513，檢索日期：2026年1月30日。

以由單一國家獨力維持，當前美、日、澳等國家已逐步推動區域層級的電纜韌性合作，涵蓋資訊共享、維修能量調度與標準化管理；因此，我國可在非軍事、低敏感框架下，透過既有盟友、海巡與軍方交流管道，深化與區域夥伴的資訊交換與演訓合作，並建立多邊、非軍事導向的海纜事件通報與協調平臺，才能顧及國家通信安全需求。

總結而言，海底電纜安全已清楚揭示21世紀區域安全結構的轉變，尤其戰略競逐已由傳統軍事衝突，延伸至數據、網路與關鍵基礎設施領域；對我國而言，海纜韌性即為數位主權的重要延伸，其防護成效取決於跨部會協同、軍民分工與制度韌性是否得以有效整合。未來，透過海巡署的前端支援與協調功能、海軍的戰略支援角色，以及科技治理與國際合作的制度化推進，我國方能在國家安全前提下，建構兼具穩定性與回復力的海纜安全治理體系，確保國家通資訊網路整體安全。 ⚓

作者簡介：

黃宣凱先生，中央警察大學水上警察學系59期，中央警察大學水上警察研究所碩士。國立中山大學中國與亞太區域研究所博士候選人。曾任行政院諮議、海巡署臺中艦艦長、海巡署隊長、海洋委員會海域安全處專門委員、處長，現服務於海巡署艦隊分署。

駱韋任先生，中央警察大學水上警察學系83期，國立臺灣大學國家發展研究所碩士，曾任海洋委員會海巡署艦隊分署科員、專員，現服務於海巡署艦隊分署。