DOI:10.6237/NPJ.202504_59(2).0004

淺談我國「海域覺知能力」整合-以海纜安全為例

Study on the Coordination of ROC's Maritime Domain Awareness-Taking the Security and Protection of the Connection of Submarine Communication Cables as an Example

海軍陸戰隊上校 陳明仁、海軍陸戰隊中校 曾革鈞

提　　要：

一、「海域覺知(MDA)能力」是維護我國對外海纜安全的重要措施之一，需要依賴岸際雷達、「船舶自動識別系統」、無人機和衛星等技術與能力的整合，才能完整監控海上活動目標，同時迅速識別威脅，採取行動。

二、近年來，中共對我國海纜的破壞，無論是蓄意或無意，都凸顯這些「關鍵基礎設施」的脆弱性；而面對這類「灰色地帶」挑戰，我國需要加強跨部會的合作和資訊共享、建立統一的資訊平台，並透過更多國際合作、提升「海域覺知能力」，防堵中共犯臺企圖，確保國家安全。

三、隨著中共對我國海纜的安全威脅日增，而破壞海纜亦恐成為其對「灰色地帶」手段之一；因此，本文藉分析中共對我海纜的安全威脅及我國「海域覺知能力」所面臨的限制及挑戰，期能保障海纜與其他「關鍵基礎設施」安全，讓資訊訊號傳輸順暢完整，進而維護國家利益與民生發展。

關鍵詞：海域覺知、海纜、灰色地帶、船舶自動識別系統、海洋視野、海巡

Abstract

1.China's Maritime Domain Awareness (MDA) capability is an important measure to maintain the security of China's international submarine cables. It relies on technologies and capabilities such as inter-shore radar, automatic identification system (AIS), drones and satellites, to integrate to monitor maritime activities and identify threat targets.

2.In recent years, the PRC's sabotage of ROC's submarine cables has highlighted the vulnerability of these critical infrastructures. For example, in February 2023, the submarine cable was damaged by Chinese fishing

boats and cargo ships in Matsu. In response to these gray zone challenges, our country needs to strengthen cross-departmental cooperation and information sharing, establish a unified information platform, and improve maritime domain awareness capabilities through international cooperation.

3. As the PRC's threats to ROC's submarine cables are increasing day by day, destroying submarine cables is also one of its gray zone means of dealing with Taiwan. This article will analyze the security threats posed by the PRC to ROC's submarine cables and the limitations and challenges faced by ROC's maritime awareness. It is expected to ensure the safety of submarine cables and other key infrastructure, maintain maritime information communication lines, and safeguard national interests and external international networks.

Keywords: Maritime Domain Awareness, MDA, Cable, Submarine Communication Cables, Gray Zone, AIS, SeaVision、Coast Guard

壹、前言

美國在2000年「911恐攻事件」後，基於國土安全需求，冀望建立「海域覺知(Maritime Domain Awareness，以下稱MDA)能力」，俾全面掌握海上目標，以肆應非傳統的威脅安全，俾使決策者面對全球的威脅時，能有效管理風險，並優先分配資源處理危機。[1]2002年1月，時任美國總統布希(George Bush)曾表示：「海域覺知能力的核心就是對傳統海洋邊界之外的所有船隻、貨物和人員能精確掌握的資訊、情報、監視和偵察工作。」並於2005年提出《國家海事安全戰略：實現海域覺知國家計畫》(National Plan To Achieve Maritime Domain Awareness For The National Strategy For Maritime Security)，積極提升國家軟、硬體設施，以強化整體監偵效能。[2]2020年6月，我國也將建構國家的「MDA能力」納入《2020年國家海洋政策白皮書》中，做為建立維護海事安全的參據文件及標準，期能達到有效監控管轄海域內之所有海洋活動，降低對我國家安全、海事安全及經濟與環境之衝擊。[3]

「海域覺知能力」的基礎建立在利用

註1：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47。

註2：National Maritime Intelligence-Integration Office (NMIO),National Maritime Domain Awareness Plan Strategy For The National Strategy For Maritime Security", National Maritime Intelligence-Integration Office (NMIO),January,2023, p. iii, https:// nmio.ise.gov/Portals/16/National%20MDA%20Plan%202023%20%28U%29.pdf，檢索日期：2025年1月6日。

註3：《2020國家海洋政策白皮書》(高雄市：海洋委員會)，2020年6月，頁30。

圖一：我國至馬祖海纜示意圖

資料來源：劉淑琴譯，〈華爾街日報：海纜中斷無法連網臺灣離島窺戰時可能情景〉，中央通訊社，2023年3月8日，https://www.cna.com.tw/news/aipl/202303080333.aspx，檢索日期：2025年1月5日。

岸置雷達、船隻、飛機和衛星等各種感測器，完整蒐集船舶和異常事件的原始資料，這些資料經過整合、篩選和計算後，可以轉化為有用的資訊。例如從事不法活動的船隻常會關閉「船舶自動識別系統」(Automatic Identification System，以下稱AIS)隱匿其位置，造成執法單位辨識困難；因此，識別和追踪這類「暗船」(dark ships)，需要比對大量無線電頻率和衛星影像等資料，並分析、研判與識別。又或當面臨中共大批機漁船的聚集時，研判是否成為進行「灰色地帶」(Gray Zone)衝突前的徵候，進而迅速提出相應的政策建議和應對措施。[4]任一國家要建立「MDA能力」，其實是需要跨部會的合作及資訊共享整合，才能建構「共同作戰圖像」(COP)，適時做出反應。[5]

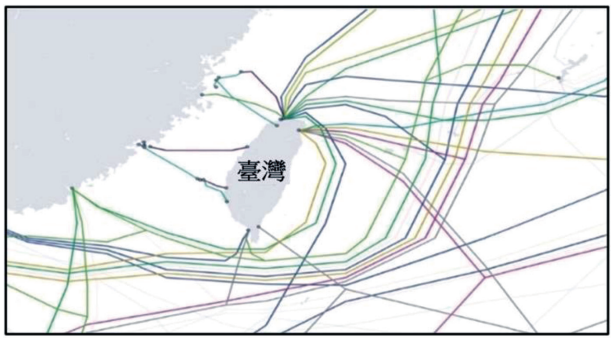
美國智庫「大西洋理事會」(Atlantic Council)研究員伊莉莎白・布勞(Elisabeth Braw)在《外交政策》(Foreign Policy)期刊中撰文表示，2023年2月發生在我國馬祖列嶼的海底電纜(以下稱海纜)切斷事件，正是中共試圖切斷我國網際網路的手段之一；[6]尤其大陸籍的拖網漁船、貨輪，更在一週內先後破壞「臺馬2號及3號」海纜(如圖一)，讓馬祖地區立即陷入斷網危機，也造成居民諸多不便。[7]面對兩岸當前對立形勢嚴峻，不排除中共可能以偽裝成貨船或漁船的間諜船，藉截斷我國周邊的海纜(如圖二)，製造「灰色地帶」之襲擾，同時引發地區紛爭與對立，達成恫嚇我國人民之目的，也加深此一問題的重要性與急迫性。因此，撰文的主要目的即是期望透過整合我國「海域覺知(MDA)能力」，適當反制中共「灰色地帶」之威脅，以維繫海底電纜正常運作，並提供相關建議，亦期讓更多國人關注此議

註4：李俊毅，〈「海域意識」在印太安全之角色〉，《國防安全雙週報》(臺北市：財團法人國防安全研究院)，第72期，2023年2月3日，頁47，https://indsr.org.tw/respublicationcon?uid=12&resid=1941&pid=3762&typeid=3，檢索日期：2025年1月15日。

註5：曾國政，〈海軍建置「協同作戰能力」(CEC)與現行數據鏈路之研究〉，《海軍學術雙月刊》(臺北市)，第56卷，第6期，2022年12月1日，頁89。

註6：Elisabeth Braw, "China Is Practicing How to Sever Taiwan's Internet", Foreign Policy, February 21, 2023, https://foreignpolicy.com/2023/02/21/matsu-islands-internet-cables-china-taiwan/，檢索日期：2025年1月15日。

註7：許靜之，〈水面下的臺海危機？海底電纜：中國灰色地帶戰略新章〉，公視新聞網，2023年8月5日，https://news.pts.org.tw/projects/taiwan-submarine-cable/，檢索日期：2025年1月18日。



圖二：我國對外國際海纜示意圖

資料來源：參考TeleGeography, “Submarine Cable Map”, TeleGeography, November 28, 2023, https://www.submarinecablemap.com/，檢索日期：2025年1月6日，由作者彙整製圖。

題，進而確保國家的安全。

貳、海纜安全面臨之挑戰

海纜的主要威脅因素有人為、天然環境和生物等因素，如發生在2006年恆春外海的地震，就引發海底土石流，造成恆春海溝附近13條國際海纜斷裂，直接影響東南亞地區的網路暢通達一個月之久，此為典型的天然環境因素造成之損壞；[8]但綜觀海纜的安全威脅，主要仍集中在人為因素，而破壞敵人的海纜可實現的目標，包含在衝突的早期階段做為切斷軍事或政府通信手段，使其無法正常運用網路；或是透過竊取海纜中的資訊，以進行間諜或特殊目的等活動。[9]

由於此類破壞行為，目前在國際法和監管作為上，仍相對的不足，《聯合國海洋法公約》(The United Nations Convention on the Law of the Sea，UNCLOS，以下稱《公約》)雖然有提供一些保護措施，但在確保海纜安全方面仍顯不足。舉例而言，《公約》並未禁止各國在戰時將海纜視為合法的軍事目標，即使是在《公約》第113條有要求各國頒布法令，並將承平時期破壞海纜的行為定為「刑事」犯罪(Criminal)，但是國際上常見的處理方式仍是以「罰鍰」(Infringement Penalty)為主；雖然「國際電纜保護委員會」(The International Cable Protection Committee，ICPC)有提供技術和法律建議，但其決議仍缺乏具體約束力，也讓維護海纜安全面臨一定程度的急迫性。[10]以下就海纜安全所面對的威脅，分述如後：

一、海纜的重要性

(一)通訊安全

根據美國「國土安全部」所屬「國家情報總監辦公室」(Office of the Director of National Intelligence，ODNI)的研究指出，商業海纜的通訊占全球電子通訊的百分之九十七以上；而各國政府目前均大量依賴海纜設施進行通訊，外交和軍事電文與通聯等，主要也透過這些海纜得

註8：邱捷芯，〈臺灣海纜數量三年內再增三條 結合盟友串出「護國圍牆」〉，中央廣播電台，2020年12月17日，https://www.rti.org.tw/news/view/id/2087065，檢索日期：2025年1月20日。

註9：Colin Wall and Pierre Morcos, “Invisible and Vital: Undersea Cables and Transatlantic Security”, CSIS. org, June 11, 2021, https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security，檢索日期：2025年1月19日。

註10：Rishi Sunak MP, “Undersea Cable Indispensable, insecure”, Policy Exchange. org, Nov, 2017, p. 17, https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf，檢索日期：2025年1月20日。

附表：近年國際間海纜遭破壞一覽表

日　期	事　件　概　要
2022 0926-27	波羅的海連接俄羅斯及德國的「北溪1、2號」天然氣管線遭到不明原因炸毀。
2023 0202、08	馬祖「臺馬2、3號」海纜先後遭中國大陸籍的拖網漁船勾斷及貨輪下錨破壞。
2023 1007-08	波羅的海香港籍貨櫃船「新新北極熊號」的海錨沿著海床拖行造成愛沙尼亞、芬蘭和瑞典間斷纜。
20240218	英國籍的紅寶石號被襲擊後，船錨在底部拖行，切斷多條海纜，迫使電信和科技業者不得不改變網絡傳輸路徑。
2024 1117-18	在波羅的海，瑞典與丹麥間的2條海纜疑似遭中國大陸籍的貨櫃船「伊鵬3號」下錨破壞。
20241225	在波羅的海芬蘭與愛沙尼亞間的海纜(Estlink 2)疑似遭俄國的油輪「老鷹號(Eagle S)」破壞。
20250103	基隆外海中華電信海纜疑似遭中大陸籍「順興39號」拖錨破壞。

資料來源：參考Andrius Sytasen and Anne Kauran,“Three Baltic pipe and cable incidents 'are related', Estonia”, Reuters, Oct 27, 2023, https://www.reuters.com/world/europe/three-baltic-pipe-cable-incidents-are-related-estonia-says-2023-10-27/；劉淑琴譯，〈華爾街日報：海纜中斷無法連網 臺灣離島窺戰時可能情景〉，中央通訊社，2023年3月8日，https://www.cna.com.tw/news/aipl/202303080333.aspx；高詣軒編譯，〈波海電纜受損，指向俄影子艦隊〉，《聯合報》，2025年1月14日，https://udn.com/news/story/6904/8487887，檢索日期：2025年1月25日，檢索日期：2025年1月23日，由作者彙整製表。

以正常運作。[11]2008年12月，在地中海連接埃及、義大利間的三條國際海纜，疑似因海象惡劣，當船隻在落錨固定時，造成海纜的損毀意外事件，連帶導致歐洲與中東之間百分之八十的網路訊號中斷。再者，由於要順利自歐洲至美國遠端操控無人機，至少需要頻寬500MBs，方能順利進行飛行操作，此狀況使得當時美國在伊拉克上空執行各項軍事任務的無人機架次，從每天數百架次，急劇銳減到僅數十架次，足見海纜通訊傳輸之良窳，影響訊號傳輸至鉅(近年遭破壞海纜，如附表)。[12]

(二)關鍵基礎建設

「美國海軍研究院」(U.S. Naval Institute)在2023年《議事錄》(Proceedings)期刊專文〈海岸警衛隊應該帶頭保護海纜〉(The Coast Guard Should Lead to Protect Undersea Cables)中就指出，若中共利用「灰色地帶」的手段，以漁船無意切斷我國與國際連接的海纜後，再運用其機漁船及海上民兵阻礙企圖修復的民間海纜維修船，將會使我國對外的網路基礎設施、通訊和金融貿易中斷，[13]此作法不僅造成國內金融秩序崩壞及國內民心士

註11：Madison L. Long,“Information Warfare in the Depths: An Analysis of Global Undersea Cable Networks”, Proceedings Magazine (U.S. Naval Institute, Annapolis, MD), Vol. 149, (May, 2023), https://www.usni.org/magazines/proceedings/2023/may/information-warfare-depths-analysis-global-undersea-cable-networks，檢索日期：2025年1月17日。

註12：同註10, pp. 21~22。

註13：Lieutenant Andrew Niedbala and Ensign Ryan Berry,“The Coast Guard Should Lead to Protect Undersea Cables”, Proceedings Magazine (U.S. Naval Institute, Annapolis, MD), Vol. 149, (August, 2023), https://www.usni.org/magazines/proceedings/2023/august/coast-guard-should-lead-protect-undersea-cables，檢索日期：2025年1月19日。

氣低迷，更會有利中共達成奪島的企圖，同時為其「統一大業」奠基。

(三)難以取代的網路頻寬

我國目前對外的國際網路主要是依賴海纜和衛星通信為主，其中海纜的頻寬流量最大，卻也容易受損或遭破壞；因此，多被視為國家重要「關鍵基礎設施」(Critical Infrastructure，CI)保護項目之一。至於衛星及微波部分則可做為備援。「數位發展部」官員即形容海纜就像是高速公路，衛星則像是鄉間小路；若高速公路受損，是無法靠其他道路取代原本的使用流量。[14]由於海纜的頻寬是以TB計算(電腦的容量單位)，微波通訊則是以GB計算；[15]若海纜受損，僅能以現有的高軌道同步衛星和類似「俄烏戰爭」期間大出風頭的「星鏈系統」(Starlink)或是英國的「One Web」公司的低軌衛星提供備援手段，雖然頻寬僅能確保通訊不會完全斷訊，卻無法提供完整與即時的資訊；[16]因此，缺乏完善之備援機制，將更加凸顯海纜傳輸安全所扮演的角色。

二、人為的破壞

(一)英國前參謀總長海軍上將托尼・拉達金(Admiral Sir Tony Radakin)在2020年1月時曾表示，近20年來俄羅斯的潛艦活動有明顯增加的趨勢，研判其已具備威脅鄰近海域海纜安全及竊取資訊的能力；他也進一步指出，蓄意破壞他國海纜的舉動將視為「戰爭行為」(Act of War)。[17]如運用漁船在淺水海域對海纜實施破壞、或故意沿著海床拖行船錨、扯斷電纜，偽裝成一般意外事件，此一手法與2023年2月發生在我國馬祖海域的海纜遭截斷事件，幾乎「如出一轍」；況且，維修海纜的費用更是驚人，以「中華電信股份有限公司」而言，維修一次就高達新臺幣1,500萬元，確實十分可觀，[18]同時也凸顯海纜安全問題之嚴重性。

(二)2024年11月28日美國媒體《華爾街日報》(Wall Street Journal)報導指出，在同月17、18日北歐波羅的海的海纜遭中國大陸籍貨輪「伊鵬3號」(Yi Peng-3)破壞，背後疑為俄國情報機構幕後主使；

註14：朱乃瑩，〈軍事衝突下如何保障海纜？數位部韌性建設司長鄭明宗：增加國際海纜、發展隱匿登陸〉，沃草有限公司，2023年5月16日，https://watchout.tw/reports/bcTqVDtgtyC0q4IV4Wmd，檢索日期：2025年1月20日。

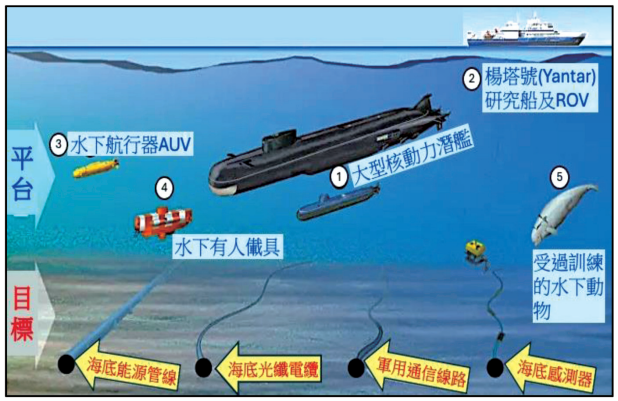
註15：有線通訊的頻寬是Tera級(TB，10的12次方，即兆)，行動網路是Giga級(GB，10的9次方，即十億)，衛星僅有Mega級(MB，10的6次方，即百萬)，彼此差距達100萬倍，如果我國聯外海纜被摧毀，很難靠衛星頻寬替代海纜，https://watchout.tw/reports/bcTqVDtgtyC0q4IV4Wmd，檢索日期：2025年1月20日。

註16：江明晏、蘇思云，〈中華電強化網路韌性 海纜、微波、衛星互為備援〉，中央通訊社，2023年4月9日，https://www.cna.com.tw/news/afe/202304090016.aspx，檢索日期：2025年1月20日。

註17：DAVID WILKES, "How Putin could black out Britain: Top military man warns Russian sabotage could wreck undersea cables that supply our internet and $10 trillion of financial deals a day", Daily Mail, January 10, 2022, https://www.dailymail.co.uk/news/article-10388139/How-Vladimir-Putin-target-undersea-cables-devastating-international-trade.html，檢索日期：2025年1月19日。

註18：同註9。

並指出俄國研究船「楊塔」(Yantar)號當時即在附近海域活動，不僅行踪不定，且目的不明。[19]該船所以被認定是對地區海纜的威脅，因為她能夠攜帶2艘深海作業的小型潛艇，並可在水深達6公里的海底作業，結合船上裝備有液壓切割機功能的「遙控潛水器」(ROV)，能夠快速切斷或監聽電纜；再加上這艘研究船的活動範圍，通常集中在關鍵但難以到達的布纜海域周邊，屆時將讓造成損壞的電纜更難以修復(如圖三)。[20]



圖三：俄國破壞水下目標的方式示意圖

資料來源：參考H I Sutton, "5 Ways The Russian Navy Could Target Undersea Internet Cables", Naval News, April 7, 2021, https://www.navalnews.com/naval-news/2021/04/5-ways-the-russian-navy-could-target-undersea-internet-cables/，檢索日期：2025年1月21日，由作者彙整製圖。

三、資訊竊取的威脅

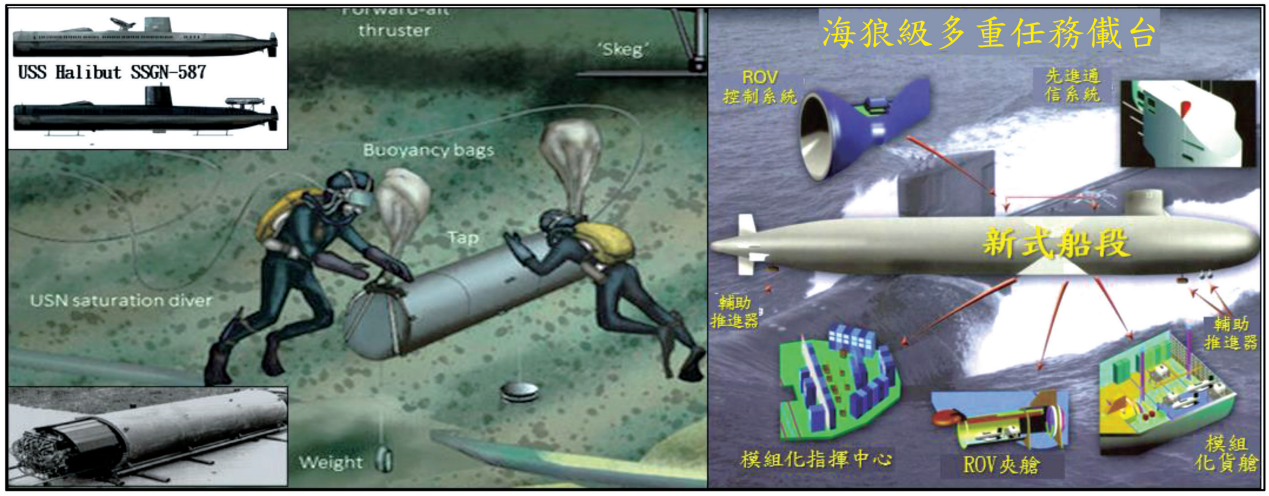
(一)海纜的竊聽行為早有前例可循，美國在1971年的「冷戰」時期，就曾派遣改裝後的「大比目魚號」核子潛艦(USS Halibut SSN-587)執行代號「常春藤鐘聲(Operation Ivy Bells)」的特種任務，前往北極圈鄂霍次克海(Okhotskoye More)周圍尋找蘇聯的通訊海纜。由於西伯利亞海岸線上本就有禁止下錨的標誌，這反而節省該艦搜尋的時間，最終在蘇聯領海內水深120公尺處，找到直徑僅5英吋的通訊海纜，並由潛水員裝上能自動脫落又不破壞海纜的監聽器，才得以順利分析錄音並破解其加密訊息，此舉措直到1981年才被蘇聯發覺。[21]

(二)時至今日，美軍最新型的「海狼」級(Seawolf class)核子潛艦「吉米卡特號」(USS Jimmy Carter SSN-23)，就有設計竊取海纜資訊的特殊能力，更能深潛到600公尺的海底，利用遙控潛水器(ROV)在海纜上安裝特殊設備，以截取機密資訊(如圖四)，也正凸顯美國藉由偵知主要敵對國動態及掌控全球資訊的企圖。[22]

註19：翁世航，〈《華爾街日報》：波羅的海電纜遭中國貨輪破壞，疑俄羅斯情報機構幕後主使〉，中央通訊社，2024年11月28日，https://www.thenewslens.com/article/245484，檢索日期：2025年1月21日。

註20：Nadia Schadlow and Brayden Helwig, "Protecting undersea cables must be made a national security priority", Defense News, July 2, 2020, https://www.defensenews.com/opinion/commentary/2020/07/01/protecting-undersea-cables-must-be-made-a-national-security-priority/，檢索日期：2025年1月21日。

註21：美國「國家安全局」員工羅納德·佩爾頓(Ronald Pelton)於1981年向蘇聯出賣「常春藤鐘聲」行動，以3萬5,000美元(約118萬5,800臺幣)的價格出售秘密，被捕後結束了近十年的間諜活動，後來被定罪並被判處終身監禁，而當時蘇聯人發現的原始竊聽器則陳展在莫斯科「克格勃博物館」中。Matthew Carle, "The Mission Behind Operation Ivy Bells and How It Was Discovered", Military. com, February 7, 2017, https://www.military.com/history/operation-ivy-bells.html; Jack Brown, "Operation Ivy Bells", Military. com, February 7, 2017, https://www.navalorder.org/national-history-day-winner-2021-operation-ivy-bells，檢索日期：2025年1月22日。



圖四：美軍「常春藤鐘聲」任務(圖左)及「海狼級」潛艦儀台(圖右)示意圖

資料來源：參考Jack Brown, "Operation Ivy Bells", Navy Order, 2021, https://www.navalorder.org/national-history-day-winner-2021-operation-ivy-bells/，檢索日期：2025年1月19日，由作者彙整製圖。

參、海纜的安全威脅

鑒於中共對我國海纜產生的破壞，無論是蓄意或無意，都凸顯相關「關鍵基礎設施」(CI)的脆弱性；針對這些「灰色地帶」的挑戰及威脅，我國更需要加強跨部會的合作和資訊共享、建立統一的資訊平台，並透過更多國際合作，提升MDA能力，確保海纜安全。以下就國際海纜及我國海纜概況，分述如后：

一、國際海纜概況

(一)波羅的海區域

自從2022年俄羅斯通往德國的「北溪」(Nord Stream)天然氣管線在波羅的海遭到破壞後，不僅顯示海纜和管線的脆弱性，此外，於2023年10月7及8日，同樣在波羅的海有連接愛沙尼亞與芬蘭到瑞典間的兩條海纜也遭到破壞，加上先前兩國天然氣管線也受到外力造成損壞，讓地區國家對海纜等水下管線安全的憂心日益增加。事件後，愛、芬兩國經比對「船舶動態」(Marine Traffic)及AIS訊號後，將行經該海域的香港籍貨櫃船「新新北極熊號(Newnew Polar Bear)」列為主要調查對象(如圖五)，[23]初判肇因係該船沿著海床拖行海錨所造成的損壞，但兩國調查人員尚

註22：National Interest Newsletter, "The Mystery of the USS Jimmy Carter and Mission 7", National Interest Newsletter, March 11, 2021, https://nationalinterest.org/blog/reboot/mystery-uss-jimmy-carter-and-mission-7-179811；和風漫談，〈海底光纜是如何鋪設的？那麼多光纜，會不會被船隻、漁網刮斷？〉，壹讀網，2019年6月18日，https://read01.com/KDEADyP.amp，檢索日期：2025年1月22日。

註23：Andrius Sytasen, "Estonia focuses on Chinese vessel in investigation into underwater cable damage", Reuters, Oct 26, 2023, https://www.reuters.com/world/europe/estonia-focuses-chinese-vessel-investigation-into-underwater-cable-damage-2023-10-25/，檢索日期：2025年1月23日。

圖五：波羅的海的天然氣管線和海纜受損示意圖

資料來源：參考Andrius Sytas and Anne Kauranen, "Three Baltic pipe and cable incidents 'are related', Estonia", Reuters, Oct 27, 2023, https://www.reuters.com/world/europe/three-baltic-pipe-cable-incidents-are-related-estonia-says-2023-10-27/; Andrius Sytas, "Estonia focuses on Chinese vessel in investigation into underwater cable damage", Reuters, Oct 26, 2023, https://www.reuters.com/world/europe/estonia-focuses-chinese-vessel-investigation-into-underwater-cable-damage-2023-10-25/，檢索日期：2025年1月22日，由作者彙整製圖。

無法判定係蓄意或意外導致，同時已向中共外交部請求法律援助，協助調查該船隻及其船員，以釐清責任。[24]

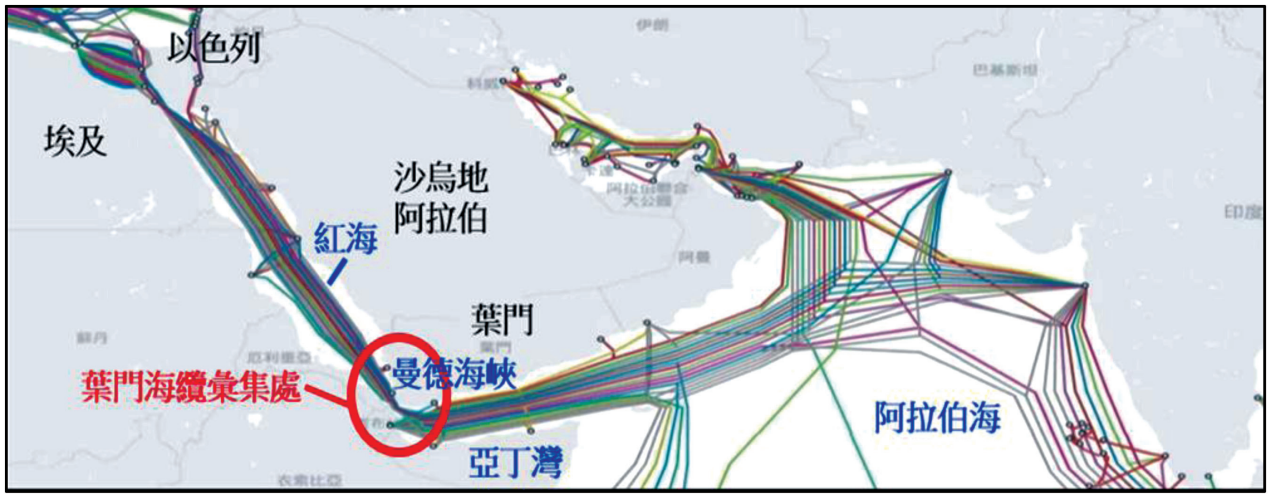
(二)紅海區域

1.2023年「以哈戰爭」發生後，葉門的「胡塞武裝組織」(Houthi)就曾於2024年2月5日在社群媒體-「Telegram」上發布紅海地區的海纜地圖，暗示該國所處的戰略位置，其中曼德海峽正位居國際海纜交會處(如圖六)；該國「葉門電信公司」(TeleYemen)對此則譴責此一組織以海纜做為目標，造成國際電信聯盟擔憂恐怖組織介入海纜的運作，陸續拒絕與其合作，進而影響紅海地區的通訊效能。[25]

2.中東地區智庫「波灣安全論壇」(Gulf International Forum，GIF)在2024年的報告中指出，「胡塞武裝組織」擁有威脅航運安全的快艇與飛彈等武器，但海纜之所以能正常安全運作，是因為該組織目前仍缺乏破壞海纜的水下作業能力。

註24：Mark Trevelyan, "Russian firm says Baltic telecoms cable was severed as Chinese ship passed over", Reuters, Nov 8, 2023, https:// www.reuters.com/world/europe/russia-says-telecoms-cable-damaged-last-month-just-before-nearby-baltic-gas-2023-11-07/，檢索日期：2025年1月23日。

註25：Patrick Wintour, "Houthis may sabotage western internet cables in Red Sea, Yemen telecoms firms warn", The Guardian, Feb 5, 2024, https:// www.theguardian.com/world/2024/feb/05/houthis-may-sabotage-western-internet-cables-in-red-sea-yemen-telecoms-firms-warn，檢索日期：2025年1月24日。



圖六：葉門地區的海纜彙集處示意圖

資料來源：參考勞家樂，〈Three Baltic pipe and cable incidents 'are related', Estonia〉，香港電台網站新聞，2024年3月4日，https://news.rthk.hk/rthk/ch/news-programmes/this-episode.htm?cmsid=103&episode_id=938643&livetime=20240304000000&segment_id=2&share=facebook，檢索日期：2025年1月23日，由作者彙整製圖。

[26]2024年2月，該武裝組織擊沉英國「紅寶石號」(Rubymar)貨輪，致其海錨在海底拖行並切斷地區15條海纜中的4條，估計當時影響歐亞間整體網路流量的百分之二十五；[27]甚至，葉門政府就提出警告，指在伊朗政府支持下，該武裝組織除會攻擊以色列籍船隻外，同樣有可能會破壞海纜。這些都讓地區海纜安全議題持續登上國際版面，更顯示維護海纜的重要性。[28]

(三)亞太區域

1. 對美國而言，同樣擔心國內各地區的海纜登陸站(Cable Landing Point)等「關鍵基礎設施」(CI)，有可能成為中共竊取資料的目標；因此，其「國土安全部」在2020年就以國家安全為由，拒絕中共「鵬博士集團」和「谷歌」(Google)及「臉書」(Facebook)等公司共同投資一條長達1萬2,800公里、連接美國和香港的「太平洋光纖網路海纜」的建設；[29]也就是間接認定在香港的中共情報和安全部門，將會從中竊取美國公民的個資，並從中獲取其他國家的數據資訊。

2. 正因為「中」資企業所投資參與的海纜建設，在美、韓、日和我國皆有設立

註26：王光磊，〈葉門憂「青年運動」破壞紅海海底電纜〉，《青年日報》，2024年2月6日，https://tw.news.yahoo.com/葉門憂-青年運動-破壞紅海海底電纜-160000887.html，檢索日期：2025年1月24日。

註27：陳律安編譯，〈紅海危機波及電信傳輸 業者資料傳送被迫改道〉，聯合新聞網，2024年3月17日，https://udn.com/news/story/6811/7836229，檢索日期：2025年1月25日。

註28：David Gritten, "Crucial Red Sea data cables cut, telecoms firm says", BBC NEWS, March 5, 2024, https://www.bbc.com/news/world-middle-east-68478828，檢索日期：2025年1月24日。

註29："US-China row moves underwater in cable tangle", BBC, June 18, 2020, https://www.bbc.com/news/world-asia-53088302，檢索日期：2025年1月22日。

海纜登陸站，亦可由系統的後門程式，監控所有通過登陸站的資訊，這也代表海纜的鋪設公司也有能力破壞海底設施；同時在未來可能的軍事衝突中，海纜登陸站更容易成為受攻擊的目標。[30]換言之，中共對海底基礎設施的控制，可視做廣義的數據戰爭，讓海纜鋪設既是一門生意，也是另一個截取資訊的戰場。[31]

二、我國海纜概況

(一)國際海纜囿於跨國管轄權結構和跨司法區域的性質，也使得各國難以對其完全掌控。美國「海軍戰爭學院」(Naval War College)學者詹姆斯・霍爾姆斯(James R. Holmes)就指出，切斷敵人的海纜是長久以來的一種作戰策略，遠在「一戰」期間，英國即曾截斷德國的電報海纜；而「冷戰」時期，美國也曾四處搜尋蘇聯的海纜。所以近期在北溪天然氣管線遭到破壞，開啟將破壞海底的「關鍵基礎設施」(CI)做為「灰色地帶」手段的先例，也證實攻擊我國的海纜，可能成為中共的手段之一。[32]

(二)「北約」(NATO)的學者在2024年的「布拉格國際資安大會」(Prague Cyber Security Conference 2024)上就曾指出，屬於CI的海纜對惡意攻擊者格外具有吸引力的原因之一，在於它的脆弱性使其成為易受攻擊的目標，也因為海纜的位置通常是公開的，攻擊者可以相對容易找到並標定位置。以英國為例，即使海纜圖資沒有公開，但在承包商內部仍然可以獲得相關資訊，惡意攻擊者自然知道由何處下手，同時也具有能力定位這些電纜並進行破壞。[33]因此，從我國海纜分布概況，即能發現海纜安全維護實屬不易，如何透過「海域覺知能力」整合，確保海纜安全，成為未來重要之課題。

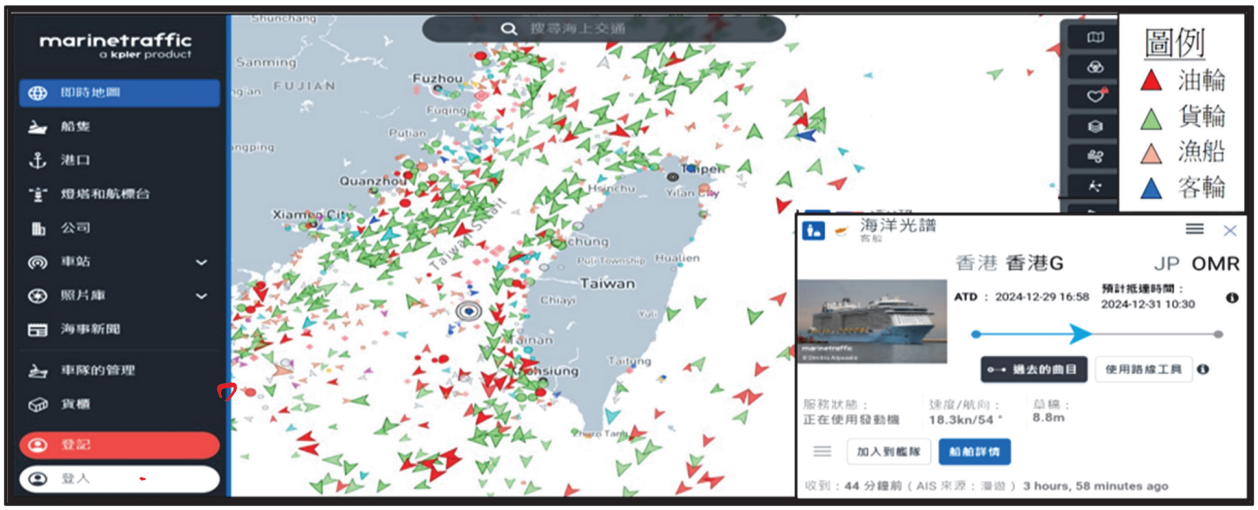
肆、我國海域覺知的現況

我國在「海域覺知(MDA)能力」的現況與構建，主要係指具備對管轄海域的監控及執行任務的能力，透過多種技術手段和跨部門合作來進行，以確保國家安全和海上活動的正常運行。有關我國在MDA能力現況的分析，臚列如后：

一、我國海域覺知資源概述

(一)我國在「海域覺知能力」上，係透過海軍及海巡等部隊使用岸際雷達、紅外線、光電、攝影機、「船舶自動識別系統」(AIS)、漁船監控系統(VMS)、無人機

註30：同註11。
註31：同註20。
註32：薛小山，〈中國入侵之手伸向海底電纜 臺灣如何守住信息生命線？〉，美國之音，2023年3月22日，https://www.voacantonese.com/amp/undersea-cables-china-s-new-frontier-to-exploit-taiwan-20230321/7015481.html，檢索日期：2025年1月24日。
註33：鄭欣明、闕河鳴、鄒博全，〈2024年布拉格資安大會出國報告書〉，公務出國報告資訊網，2024年6月19日，頁19，https://report.nat.gov.tw/ReportFront/ReportDetail/detail?sysId=C11300918，檢索日期：2025年1月25日。



圖七：我國周邊「船舶動態」顯示圖

說明：「船舶動態」顯示包含系統選單、圖示及船舶數據等內容。

資料來源：參考Marine Traffic網站，2024年7月23日，https://www.marinetraffic.com/en/ais/home/shipid:6267943/zoom:6，檢索日期：2025年1月23日，由作者彙整製圖。

、機艦偵巡等科技手段，以監控海上活動、識別潛在的威脅，並進行及時的應處。常見的「船舶動態」(Marine Traffic)系統就提供諸多AIS數據(如圖七)，並以船舶的動態為核心，透過AIS追踪船舶所在位置及歷史紀錄等，同時提供航行目的地、預計抵達時間等資訊，讓使用者可據以進行船舶管理、貨櫃追踪、航行歷史等資料蒐集，同時能監控的船舶是否遵守海事法規、法律等。[34]至於衛星監控的部分，亦可藉由國軍各級情報單位提供資訊，讓掌握的海域範圍更寬廣。

(二)透過「海域覺知能力」確保我海纜安全的同時，國際海纜也已納入我國「關鍵基礎設施」之中；尤其在經歷波羅的海及馬祖海域的斷纜事件後，我國將更加重視海纜等設施的安全。[35]

二、跨部會的角色與合作

(一)跨部會合作強化海域覺知

「海域覺知能力」必須仰賴政府各個不同部門的合作，而且需要整合來自海軍、海巡署、漁業管理部門、情報機構等多方面的情報資源，以建立一個統一的共同圖像平台，俾形成全面的海域監控網絡，確保面對海上威脅時能快速反應，以應對各種突發事件。除了執法和主權行使外，國家MDA能力的核心在於資訊掌控和跨部門合作，為有效應對海事威脅，執行單位

註34：巫柏蕙，〈擴充「國際海運資料庫」數據源之探討〉，交通部運輸研究所，2024年3月28日，頁7-8，https://www.iot.gov.tw/uploads/asset/data/66610e590857771c11b3a486/擴充國際海運資料庫數據源之探討報告.pdf，檢索日期：2025年1月23日。

註35：王承中，〈金門快艇案 陸委會：陸方應加強管理三無船舶〉，中央通訊社，2024年3月4日，https://www. cna.com.tw/news/acn/202403030117.aspx，檢索日期：2025年1月25日。

必須充分掌握相關資訊，結合跨部門合作和信息共享機制，如此便能讓所有機構共同存取和使用資料和數據，進而達到有效監控之目的。

(二)共同資訊平台整合提升情資處理效能

1.建立完整「海域覺知(MDA)能力」的資料庫確有其必要，且在維護我國海域安全及主權的共同目標下，這些非機敏資料、數據庫和即時情資整合，將有助於執法人員面臨突發狀況時，能在共同圖像的基礎上，做出最佳的應變決策。[36]換言之，基於維護我國的海洋安全和利益，政府各部門有必要透過充分的資訊掌控和跨部會的合作，實現此一目標。

2.其次，在整合資訊方面，以「內政部」管理的「海域資訊整合平臺」而言，目前在電子海圖資訊的部分，就已發展並彙整海域地形、海岸線、海上交通、海纜、沉船、海洋科學調查及海洋資源等數據與圖資，並利用不同的底圖切換及套疊，提供各類海洋地理資訊系統(GIS)訊息與應用服務，除可獲得即時情資外，亦可及早預警接近我海纜所在限制水域的船隻，並迅速應處以確保安全。[37]因此，國軍相關單位倘能善用相關資源，有效分享資訊，強化情蒐、監偵及數據處理能力，更容易達成確保海域安全之目的。

三、海域覺知技術的挑戰

(一)海上目標的識別

臺灣海域內的海纜是全球通信的重要組成之一，承載著大量國際網路和電信流量，儘管有先進的監測技術，但我國在MDA能力方面仍面臨許多挑戰，例如「灰色地帶」襲擾、「三無」船舶(無船名、無船舶證書、無船籍登記)的識別、[38]海底地形複雜、海域偵知的設備部署及設備的效能與維護成本、亦有其侷限性；尤其監偵與雷達操作人員素質與訓練，更是攸關「海域覺知能力」的良窳。發生在2024年6月9日的中國大陸籍快艇非法入侵我淡水河口事件，就是因為雷達站的操作員雖在淡水外海已發現該目標，卻誤判為一般返港漁船，即使有通報相關部門協助目標識別，但仍未能及時調派海巡艇攔查，導致該快艇能長驅直入淡水河，此點值得有關單位省思改進。[39]

(二)海域覺知的管理(制)能力

註36：沈楷勛，〈110年參加美國海岸防衛隊國際海域意識班〉，公務出國報告資訊網，2021年9月13日，https://report.nat.gov.tw/ReportFront/ReportDetail/detail?sysId=C11000149，檢索日期：2025年1月25日。

註37：地政司，〈海域資訊整合平臺〉，內政部，2024年7月26日，https://ocean.moi.gov.tw/3DMap/，檢索日期：2025年1月27日。

註38：李志強，〈淺析強化關鍵基礎設施保護法案修正重點〉，《清流雙月刊》(臺北市)，2024年1月，第49期，https://www.mjib.gov.tw/FileUploads/eBooks/3ee2bc4248cf429cb5906735175c9334/Section_file/2bf31ddad7d445c2a1dc45babd955fd1.pdf，檢索日期：2025年1月27日。

註39：〈6月9日大陸人士於淡水非法入境案策進作為〉，海洋委員會海巡署，2024年6月12日，https://www.cga.gov.tw/GipOpen/wSite/ct?xItem=160647&ctNode=650&mp=999，檢索日期：2025年1月27日。

1.「海域覺知(MDA)能力」不僅是要監控「看得到」，還要執法「抓得到」，才算是具備完整的能力，由於海纜登陸站位置容易受人為破壞及漁業、錨泊、抽砂船等海上作業影響，加上，距離中國大陸東南沿岸較近之登陸站，面對中共「灰色地帶」的襲擾(如抽砂船、暗船等)，相關單位反應時間更為緊迫，有必要加強資訊整合及人員判讀能力，以提升預警及反應時間。

2.鑑此，對具MDA管理(制)人員的養成至關重要，其中雷達操作與監偵人員的專業、經驗尤為關鍵。以2024年7月19日「胡塞武裝組織」使用伊朗製造的「Samad-3」無人機，襲擊以色列第二大城特拉維夫為例，這架無人機採取非直線的飛行路徑，經紅海、埃及，從地中海的西邊接近，由於路徑及空中管制的失誤，使雷達操作員未能及時識別並攔截。事後以國軍隊對此誤失，增加雷達操作人員和空巡次數，避免再生類情。上述案例同樣可適用於我國海域訊跡的管理，相關專業人員第一時間之應變，將大大影響海軍、海巡單位後續的應對與處置。

綜上，儘管北部地區的海纜恐為敵破壞的主要目標，惟東部位置之海底電纜，遭受攻擊的風險亦須被重視。近期美國媒體《華爾街日報》(Wall Street Journal)報導，中共海纜船及研究船航經我國東部海域時，經常會隱匿其無線電及衛星追踪信號，[40]初步比對其航行路徑與我國海纜位置相當接近，凸顯海纜安全威脅不可輕忽。故我政府相關部門應即針對重點防衛地區之登陸站及海纜安全，建構有效之防護機制。

伍、強化海域覺知之建議

隨著中共對我國海纜的安全威脅日增，而破壞海纜亦恐成為其對「灰色地帶」手段之一；因此，運用先進技術保障我國海纜與其他關鍵基礎設施安全應為首重。再者，藉持續與國際間交換各式海纜攻擊態樣的情報，審視自我防護措施、提早因應，同樣不可輕視。[41]有關確保我國際海纜安全，具體建議如后：

一、加強跨機關合作，整合資訊與共享

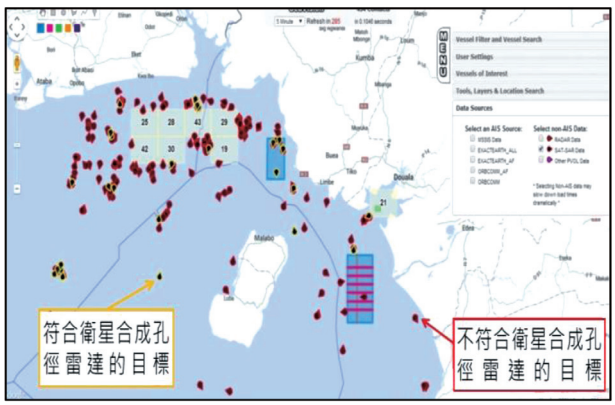
(一)提高「海域覺知(MDA)能力」有助確保海纜和其他關鍵基礎設施的安全，再透過加強投資先進的監測設備和技術，強化對海上活動目標的偵測能力，同時藉由建立一個跨部門的共同圖像共享平台，讓資訊的傳遞更加即時、有效。另外，透過國際技術合作亦可升級我國的「海域覺

註40：邱國強、陳鎧妤，〈美官員：中國海纜維修船經常匿蹤 當心搞破壞〉，中央通訊社，2024年5月19日，https://www.cna.com.tw/news/acn/202405190172.aspx，檢索日期：2025年1月28日。

註41：同註38，頁45。

知能力」，如與美國、日本、菲律賓等國進行情報交換，不僅可獲得更多的情報、技術支持，亦有助於強化區域內的整體海纜安全。

(二)我國可參考美國貫徹「海域覺知(MDA)能力」所使用的「海洋視野」(Sea Vision)平臺的資訊整合設計功能(如圖八)，除彙整各種來源的AIS資料，據以追踪海域內船隻位置及移動資訊，還可過濾並搜尋大數據，同時串連「衛星合成孔徑雷達」(Satellite Synthetic Aperture Radar)影像的船舶資料、擷取「國際海事安全及安保資訊系統」(Maritime Safety and Security Information System)、「人造可見紅外線成像資料」、岸置雷達、電子光學偵照、無線電射頻信號(主要針對未顯示AIS信號的船隻)等資料，進行交叉及關聯性比對，並藉由視覺化的地圖即時顯示、更全域性的監偵系統，加上自動查詢目標及解除限制(不明)因素，並對出現異常徵候的船隻目標發出警報，或大幅度增強識別目標之能力。[42]



圖八：美國「海洋視野」的海域資訊整合平臺示意圖

說明：本平台可以透過高端的MDA能力自動串連、比對海上目標的雷情、AIS、衛星影像及船籍資料等，以利操作者能迅速識別可疑目標。

資料來源：參考“SeaVision A web-based maritime situational awareness tool”,United States Department of Transportation, https://info.seavision.volpe.dot.gov，檢索日期：2025年1月28日。由作者彙整製圖。

二、建立海纜備援系統，鼓勵國際合作

(一)透過加強國際海纜的共同開發及合作案，加強與鄰國和國際組織的密切鏈結，如爭取「谷歌」、「臉書」、「微軟」(Microsoft)等國際雲端或資料處理中心在我國設置系統中心，除了可以獲取更多的資訊和海纜船的技術支援外，也能將我國國際海纜的受威脅與被破壞，升級成為國際或跨國事件，提高惡意破壞者在攻擊目標選定時的複雜性與難度；另將海纜的鋪設路線多樣化、增加網路節點，以提供調節流量的機會。畢竟一條海纜的頻寬可達200TB以上，當連到我國周邊的國際海纜越多，則對外的網路頻寬就越大，代表相互調度支援的流量也就越餘裕；[43]而藉國際資料中心的設置，必將帶來更多海纜的鏈結，間接讓我國的對外通信網路也

註42：“SeaVision A web-based maritime situational awareness tool”, United States Department of Transportation, https:// info.seavision.volpe.dot.gov，檢索日期：2025年1月28日。

註43：吳元熙，〈斷線、Lag都跟「它們」有關！藏在臺灣深海的網路護國神山—海底電纜〉，數位時代，2020年12月17日，https://www.bnext.com.tw/article/60585/taiwan-submarine-cable，檢索日期：2025年1月29日。

越安全。

(二)設置多重的海纜登陸站確實可避免蓄意的破壞，也增加海纜在登陸地區的韌性與安全性；此外，另需制定詳細的應急預案，方能以其他備援手段迅速恢復基本通信和其他關鍵服務的能力。受限於頻寬的考量，最佳備援方案仍是以國內、外海纜傳輸為主，非必要才使用微波或衛星通信等手段來維持通信。再者，要建立我國自主維修海纜的能力，避免受限於國際合作的海纜維修船船期，亦可降低因國際情勢升溫，造成外國維修船無法按計畫前來修護的窘境。

三、設置海纜專屬保護區，加強海域監管

(一)在政策和治理層面，我國需要不斷更新和提升「海域覺知(MDA)能力」，改進現有監控設備，以應對複雜多變的海上安全環境。例如在重要的海纜沿線設置聽音器或聲納偵測器等，以提供對海纜威脅事件的早期預警，若有不明的水面目標或水下載具接近時，確保能夠在海纜可能遭受破壞威脅等緊急情況下，及時向主管機關或海巡執法單位發出警報情資，進而予以適處。

(二)此外，亦可研究配合無人機的定期偵巡運用，協助提升海域及岸際目標辨識、機動巡邏偵察與違規案件的蒐證取締、輔助海域及岸際搜救能量等，再透過聯合海巡艦艇攔檢惡意或「三無」船舶對海纜的威脅。至於海巡單位原採購的旋翼型無人機，囿於抗風力限制，加上導控距離過短等限制；因此，在後續訓練及採購上可繼續做出精進，[44]俾滿足我國在MDA能力的急迫需求。

(三)當然，我國亦可仿效澳洲與紐西蘭在現有海纜周圍設置「海纜保護區」(Cable Protection Zone)方式，禁止或限制這些區域的海事活動，[45]並結合雷達的目標識別或艦艇執法的驅離警戒等，強制任何進入「海纜保護區」的船隻都需要透過通報或申請核准後才得以進入，以保護通信「關鍵基礎設施」，免遭漁業或拋錨等海事活動影響，同時亦可集中有限的海域偵知資源在專屬的海纜保護區內，達成有效監管海纜的目標。

四、重視人員培訓，建立AI操作能量

(一)鑑於近期「以哈戰爭」及「中」方快艇侵入我國淡水河事件經驗，當前雷達操作及人員與裝備整合，加上「海域覺知(MDA)能力」設備的操作及判讀，確實需要經驗的累積與長期訓練，是以對相關

註44：《NAO-112-12 海洋委員會海巡署旋翼型無人飛行載具試辦計畫執行情形專案審計報告》(臺北市：審計部，2023年12月)，頁23~24，https://www.audit.gov.tw/p/405-1000-9329,c90.php?Lang=zh-tw，檢索日期：2025年1月29日。

註45：Jill C. Gallagher and Nicole T. Carter, “Protection of Undersea Telecommunication Cables: Issues for Congress”, Congressional Research Service, August 7, 2023, p. 29, https://crsreports.congress.gov/product/pdf/R/R47648，檢索日期：2025年1月28日。

人員培訓仍應進行長期投資，同時藉由發展「人工智慧」(AI)系統設備的協助篩選，判讀可疑或具威脅的海上目標，相信可以減輕人員負擔及應變突發狀況。

(二)另方面，擴大各層級施訓範圍，並且在教育訓練部分持續向下紮根，以建立及培養各級幹部維護臺海主權及利益的觀念與共識。此外，一直進行中的我國海軍及海巡等機關交流，更應持續深化第一線操作人員間的任務訓練默契，俾有助在事件發生時機，迅速提供專業及經驗的諮詢，結合跨部會與機關間的支援與支持，達成維護海洋安全之共同目標。

陸、結語

美國「海軍戰爭學院」所屬「中共海事研究所」(China Maritime Studies Institute)曾發表的第26號報告—《超越對臺首戰》(China Maritime Report No.26: Beyond the first battle for Taiwan)中，研判中共在入侵我國前的聯合封控行動中，就會在初期的導彈和空襲中針對關鍵基礎設施，如衛星地面站和海纜登陸站等長途通信設施進行攻擊，接著使用「反太空技術」(Counterspace)干擾或破壞我國通信衛星，後續則持續攻擊移動和備用通信裝置，並利用「軟、硬殺」手段以達到資訊封鎖，進一步削弱我國對外的通信能力，此研究內容值得重視。[46]

觀察報告內容，在在顯示海纜安全不容輕忽，況且倘我國與友盟國家及世界各國的聯繫管道遭切斷，將會影響我國爭取外援的窗口，政府有關單位不能不預做準備。[47]基此，2024年3月14日，由民間公司舉辦的「2024TTX區域安全兵推」中，就已將「通訊網路與海底電纜堅忍能力」項目納入，同時指出我國目前共有14條國際海纜，雖不會全部同時中斷；倘若被破壞時，也會藉由衛星及微波中繼到第三方國家對外解決通訊，所以也建議政府應將國際海纜的安全提升至國安層級，咸信此議題的重要性，當下已「毋庸置疑」。[48]

總體而言，我國在「海域覺知(MDA)能力」方面雖然已經逐步建立相對完善的系統，但面對日益複雜的海上安全環境，還是需要持續加強與升級改進。嗣後透過

註46：Lonnie D. Henley, “Beyond the first battle for Taiwan”, Asia Times, March 11, 2023, https://asiatimes.com/2023/03/beyond-the-first-battle-for-taiwan/，檢索日期：2025年1月29日。

註47：曾敏禎，〈美中海纜戰持續升溫 強化同盟與另起爐灶〉，《國防安全雙週報》(臺北市：財團法人國家安全研究院)，2023年7月7日，https://indsr.org.tw/respublicationcon?uid=12&resid=2970&pid=5083，檢索日期：2025年1月29日。

註48：張曜麟，〈海底電纜遭破壞恐釀臺海危機，前國防部副部長曝目前臺灣應變、TTX兵推給新政府建議〉，風傳媒，2024年4月15日，https://tw.news.yahoo.com/%E6%B5%B7%E5%BA%95%E9%9B%BB%E7%BA%9C%E9%81%AD%E7%A0%B4%E5%A3%9E%E6%81%90%E9%87%80-%E5%8F%B0%E6%B5%B7%E5%8D%B1%E6%A9%9F-%E5%89%8D%E5%9C%8B%E9%98%B2%E9%83%A8%E9%95%B7%E6%9B%9D%E7%9B%AE%E5%89%8D%E5%8F%B0%E7%81%A3%E6%87%89%E8%AE%8A-ttx%E5%85%B5%E6%8E%A8%E7%B5%A6%E6%96%B0%E6%94%BF%E5%BA%9C%E5%BB%BA%E8%AD%B0-125003814.html，檢索日期：2025年1月29日。

「加強跨機關合作，整合資訊與共享」、「鼓勵國際海纜合作，建立海纜備援系統」、「設置海纜專屬保護區，加強海域監管」、「重視海域覺知(MDA)能力」人員培訓，建立共同操作能量」等面向的努力與整合，將可保障我國重要基礎設施之安全。另方面經由跨部會的合作、運用技術創新和國際合作，更能有效地維護我海域海纜的安全，保障國家利益和對外國際網絡的穩定，共同反制中共「灰色地帶」襲擾，俾維繫我國海上資訊交通線暢通，從容應對任何海域安全的挑戰。 ⚓

作者簡介：

陳明仁上校，中正理工學院88年班、海軍指揮參謀學院100年班、國立中央大學歷史研究所碩士106年班。曾任海軍陸戰隊登陸戰車大隊中隊長、大隊參謀主任、陸戰隊指揮部兵參官，現服務於國防大學海軍指揮參謀學院。

曾革鈞中校，海軍軍官學校93年班、國立中山大學海洋生物科技暨資源所碩士96年班、美國陸戰指揮參謀學院109年班。曾任海軍三軍聯訓基地裁判官、海軍陸戰隊指揮部外事連絡官、國防大學海軍指揮參謀學院學員隊隊長，現服務於國防大學海軍指揮參謀學院。

左營軍區的故事

海軍子弟學校

海軍子弟學校，為今高雄市永清國小及高雄市立海青工商前身，舊址位於左營大路西側桃子園(約為今海青工商現址)。

民國38年政府遷臺後，前總司令桂永清上將鑒於軍眷清苦貧困，為解決軍眷子弟教育問題，特選定桃子園日本海軍舊庫房位置為海軍子弟學校復校預定地(原海軍子弟學校民國37年由前總司令桂永清上將於南京創校)，並指派安世琪先生為第 1 任校長，在老舊庫房及荒蕪平坦的土地上，帶領全校師生一磚一瓦修建校舍與教室。

海軍子弟學校初期僅招收軍眷子弟，不對外招生，學費全免，內設有初小(一至三年級)及高小(四至六年級)及初中，另於自立新村設有初小分校，國小部名稱為「海軍總司令部附設高雄小學」(海總附小)，初中部名稱為「海青中學」，校內師生衣服均為海軍官兵衣服汰換後，由學校師生接收，因此，初期常可看到學生穿著水兵服及軍鞋就學。

民國55年，國防部將子弟學校移交地方政府接辦，「海總附小」移至左營大路東側現址，並為了紀念學校創辦人前總司令桂永清上將，因而命名為「永清國小」；海青中學其後陸續增設高中部與高職夜間部，於民國70年由高雄市政府接辦，更名為「高雄市立海青工商職業學校」。(取材自《鎮海靖疆-左營軍區的故事》)