數位經濟關鍵基礎建設海底電纜的防護: APEC新合作議題的挑戰

政治大學國際關係研究中心研究員 李瓊莉

在邁向數位經濟時代之際，APEC地區的海底電纜（以下簡稱海纜）分佈密度與區域經貿互賴程度自然是成正相關。APEC會員經濟體在2010年代初期業已經開始針對海纜的防護與韌性強化進行合作。APEC資通訊工作小組（APEC Telecommunications and Information Working Group, APEC TEL）在2011年進行了一項「海底電纜訊息共享專案」(Submarine Cable Information Sharing Project)，於2012年3月發佈了一份報告:《海纜資訊共享計畫:立法實踐與聯絡窗口》（Submarine Cable Information Sharing Project: Legislative Practices and Points of Contact），各會員經濟體同意設立聯絡窗口（points of contact），以促進海纜維修的便捷性。2013年2月APEC秘書處與政策支援小組(Policy Support Unit)在「APEC供應鏈連結架構行動計畫」(APEC Supply Chain Connectivity Framework Action Plan)項下發佈了另一份《海纜中斷的經濟影響》（Economic Impact of Submarine Cable Disruptions）報告，正視海纜對區域經濟成長的重要性，並指出馬六甲海峽、呂宋海峽、以及南中國海是海纜遭受破壞的高風險區，呼籲各會員經濟體透過政策協調提升海纜維修能力以降低風險。

除了數位經濟發展趨勢所需，當前人工智慧（Artificial Intelligence）運用已經將生活日常推向「數位世界」（digital world），資料中心（data center）成爲戰略基礎建設，然而資料中心若沒有傳輸電纜則形同囤積資料的大型倉庫，無法眞正發揮功能。根據多項估計，全球跨洲際的數位連結與大量資料傳輸有百分之九十以上透過海纜，其中更是包括敏感的金融交易資訊以及政府間的重要文件傳輸，這個趨勢似乎已經不可逆，而海纜防護也隨新科技的發展同時面臨新挑戰。APEC面對這些發展趨勢的因應動能似乎尚未成熟，本文接下來討論當前海纜防護的挑戰，以供APEC會員經濟體發展相關合作議題之參考。

一、海纜安全風險

基本上海底電纜建造應已經內建防護設計，與資訊安全領域常用的「設計確保安全」（security by design原則相同，所指的是產品在建造過程中

就應將安全防護設計在其中，而不是等成品完成後再附加上去。目前全球四大海纜供應製造商包括美國的SubCom、法國的阿爾卡特海底網路公司（Alcatel Submarine Networks, ASN）、日本的日本電氣公司（Nippon Electric Company, NEC）、以及中國的華海通信（HMN International），在建造階段已經顧及三個安全基本要件:可信賴（reliability）、堅固（robustness）、以及維修設計（repair），但電纜本身除了會逐漸老舊毀損之外，實體防護的眞正挑戰是來自海纜暴露在海域的脆弱性（vulnerability），而遭破壞斷裂的風險則可歸類爲非蓄意（unintentional）意外損壞、以及蓄意（intentional）惡性破壞。

所謂非蓄意意外損壞來源，最無助的是超乎建造時可臆測的天然災害，在APEC地區，颱風和地震頻繁，便經常造成海纜受損，使得大範圍地區對外通訊中斷，這類的天然災害損失，除透過天災保險之外，無從取得賠償。另外，漁船作業或輪船定錨時若沒有注意到處於海纜埋設區，沒有特別警覺就可能在無意間破壞海纜。這類的意外事件在處理上也沒有想像中的容易，因爲目前國際間除了「國際電纜保護委員會」（International Cable Protection Committee, ICPC）提供爭端解決最佳範例（best practice），並設定一些自願性的治理規範之外，並沒有具約束力的國際公、私法得以適用海纜事故紛爭之處置，特別是當事故發生地點的管轄權因主權爭議難以判別，或當船籍、船東、船員皆屬不同國籍時，那麼究責賠償的判定就更形複雜。

至於蓄意惡性破壞行爲則可能源自商業利益驅使的非法抽砂，到地緣政治競逐所引起的惡意騷擾，尤其是國家政府針對敵對政體所採取的「灰色地帶操作」（grey zone operation），後者在近幾年對海纜防護安全的風險有顯著增加。中國、俄羅斯常分別被高度懷疑是在亞洲、歐洲利用非法船隻或權宜船進行海纜破壞的元兇，但此類的指控並非沒有政治成本，可能引來的報復風險不可輕忽，因此各國在調查完整之前不宜太過武斷。然而最近「中國船舶科學研究中心」（China Ship Scientific Research Center）所研發出的先進「深海電纜斷切」技術（advanced deep-sea cable cutting technologies），結合水下無人機的操作，確實對海纜防護形成威脅。若北京不明確說明發展這類技術的戰略企圖，則提高了各國合理懷疑中國在潛在衝突海域惡意破壞海纜的正當性。

爲了降低海纜脆弱性與易損風險，在政策層次上，各國所採取的策略大致歸爲三大方向:備份（redundancy）、韌性（resilience）、修復（repair）。通常備份所指包括複製海纜、多條路線設計、尤其避開地緣政治高風險區。近來也增加建構微波（microwave）或者衛星（satellite）傳輸系統做爲替代選項，但後兩者的傳輸量遠不及海纜，多僅能用來應急。至於對實體電纜防護韌性的強化，則建立在備份的基礎上，但近年來各國關切焦點不再僅限於對海纜或其所有人的衝擊，而是擴及如何因應海纜斷訊對社會、經濟所造成的衝擊，因應策略則有賴政府各相關部會的整合協調。至於修復部分，及時偵測的能力有賴地方性資源，而在修復技術層面上則屬另一種產業，由於目前海纜修復船數量不多，有賴高度國際合作和公私協力，才能順利完成修復工作。

二、預防措施

上述三個海纜防護作爲都是屬於事故發生後的因應措施，也就是說在第一時間偵測到事故後才啓動，屬於補救措施。許多國家已發展「海纜自動警告系統」（Submarine Cable Automatic Warning System, SAWS），但即使有船舶自動識別系統

（Automatic Identification System, AIS）追蹤船跡，也很難在事故發生的當下立即確認海纜是否遭破壞。從政策層次上來看，「事後補救」不及「事前防阻」來得有效，爲達到防護保障，發展預防措施（prevention measure）更爲重要，而預防措施的設計則在於落實「嚇阻」（deterrence）與預警（early warning）這兩個重要概念。

據TeleGeography的研究顯示，非蓄意人爲意外損壞仍是海纜防護的最大威脅，因此嚇阻策略主要在於提高非蓄意破壞海纜的罰責，使得船隻在作業時必須提高警覺。從海纜經營聯盟的角度來看，若能劃設海纜保護區或事故高風險區，並強制要求船隻繞道避開保護區或禁止船舶在高風險區作業，便可以大幅降低大部分的人爲風險，甚或完全避免。海纜經營業者的建議顯然會對經營藍色經濟（blue economy）的海洋島國造成衝擊，使其在政策層次上有所保留。

相較於強制避開或禁止作業，「預警系統」的建立，對於非蓄意損壞或蓄意破壞行爲的防制都是比較折衷可行的。預警系統包括監控（monitoring）、偵測（detection）、以及回應（responding）三個次系統。同樣的，在海纜鋪設關鍵區域劃設保護區，裝設監測系統，隨時監測經過的船隻，若發現停滯過久的可疑船隻，則對其發送警告，並同步與執法單位（如海巡）合作，在有必要時加以驅離，如此一來可有效地降低蓄意破壞的風險。有些國家（如台灣）更進一步的列出可疑船隻觀察名單，積極監控，一旦發現可疑船隻出現，海巡單位便提高警覺，以防範蓄意破壞。

三、美中戰略競逐

海底電纜系統除了海纜之外，尚包括陸地接收站（landing station），主要利害關係行爲者除了具有管轄權的各國政府之外，尚包括海纜供應製造商、經營公司組成的聯盟，各方之間的協調已經具有相當難度，而當前的美中戰略競逐的國際情勢，使得海纜建造與防護都難免加上了地緣政治考量。中國在海纜深耕已久，根據TeleGeography在2025年2月的統計，全球現有海纜共570條當中中國就占了200多條，而2025至2027年全球新海纜投資金額預計可達130億美元，幾乎是2022-2024年的兩倍，使得早已開打的美中「海纜戰」可能愈演愈烈。

基於安全風險管控，美國拜登政府時期就已經著手降低中國在海纜供應鏈可能產生的危害。2019年美國將「華海通信」的前身「華爲海洋」與「華爲技術」列入限制取得部分產品與技術的「實體名單」。2020年4月美國國務院進一步提出「乾淨網路倡議」（Clean Network Program），禁止美國新造海纜直接連接香港與中國。在避開中國海纜供應鏈的同時，美國也加強與盟友合作，推進「非紅供應鏈」。2024年9月，美國要求越南預計在2030年前新建的10條海纜，避免使用包括「華海通信」在內的中國供應商；同時透過「四方安全對話」（Quad），邀請日本、澳洲及印度合作投資印太地區海纜。

竄升的海纜戰略重要性也反映在爭取承建國際海纜標案的案例裡，常被提到的是「東南亞—中東—西歐六號海纜」（South East Asia–Middle East–Western Europe 6, SeaMeWe-6），這是一條連接馬來西亞、孟加拉、印度、斯里蘭卡、馬爾地夫、巴基斯坦、吉布地、沙烏地阿拉伯、埃及、希臘及義大利等國，行經歐洲西海岸、地中海、紅海、以及印度洋，總長1.92萬公里的海纜，取得這個跨洲際線路海纜建造權形同掌握半個地球的一條重要數位生命線。當時中國「華海通信」幾乎已經以低價奪標，但美國政府出手影響SeaMeWe-6沿岸的16家私企組成的經營集團，最後2022年2月由美國SubCom

得標並開始興建，預計2026年完成。原屬於集團成員的中國電信（China Telecom）和中國移動（China Mobile）兩家經營公司則隨後退出，似乎出現了「去紅」的趨勢。

爲了降低地緣政治干擾資訊傳輸之風險，科技巨頭已經紛紛加入投資海纜供應鏈，建造專屬的海纜。2025年2月Meta宣布「Waterworth」海底電纜計畫，建造一條橫跨五大洲，全長5萬公里的海纜，預估耗資數十億美元，是目前全球最長的海纜開發案。Google至今已投資超過30條海纜，2025年7月宣布最新案「Sol」，將橫跨大西洋，連接美國、百慕達、亞速群島與西班牙。亞馬遜（Amazon Web Services, AWS）在2025年11月宣布第一個全資海底電纜計畫「Fastnet」，連接美國馬里蘭州東岸與愛爾蘭科克郡（Cork County），預計2028年啓用。

結語

亞太地區海纜供應鏈結構在近期也有新樣貌。2016年啓用的亞太直達海纜（Asia Pacific Gateway, APG）於2009年5月開始建造，當時經營聯盟包括菲律賓的PLDT、台灣的中華電信、中國的中國電信和中國Unicom、南韓的KT Corp、日本的NTT、馬來西亞的Telekom Malaysia、以及越南的VNPT，選擇日本的NEC承建，連接中國、香港、日本、韓國、馬來西亞、台灣、泰國、越南、和新加坡，此案受到地緣政治的干擾似乎不大。而2021年新建的杏子海纜系統（the Asia Pacific Route Incorporating Cognitive Optical Transport （APRICOT） subsea cable system）則不同，APRICOT連結日本、台灣、關島、菲律賓、印尼、以及新加坡，總長1.2萬公里，選擇的建造商是美國SubCom，經營公司集團則包括日本的NTT、台灣的中華電信、菲律賓的PLDT、Google 以及Meta，除了有科技巨頭加入之外，值得注意的是沒有中國廠商參加。然而即使是沒有涉及中國，仍存在許可核准問題，原預計2024年啓動，但受印尼許可審查延誤，預計在2027年之後才能啓用。

APEC的組織特質有利發展新興區域治理議題，雖然會議形式是不具約束力的論壇模式，但實質討論內涵卻具有一定影響力。一方面透過非正式領袖峰會以及部長級會議的政策揭示，對區域合作有由上而下的驅動力；另一方面透過工作小組集結產官學研的專業探討，由下而上建立折衷可行的政策共識，這樣的合作動能對降低地緣政治衝擊有所幫助。目前APEC能源部長會議視海纜爲能源基礎建設，在區域電廠整合連結有其重要性，防護合作成爲重要議題。雖然能源傳輸電纜有別於資料電訊傳輸電纜，但仍可作爲海纜安全防護合作模式的參考。■

參考資料

1.Submarine Cable Networks, https://www.submarinenetworks.com/en/
2.TeleGeography, https://www2.telegeography.com/
3.International Cable Protection Committee, https://www.iscpc.org/
4.2025 Pacific Prospects Conference: Strengthening the Resilience of Submarine Cables, Conference Proceeding, November 26, 2025, Taipei: Howard Plaza Hotel, https://sites.google.com/view/2025-pacific-prospects