

# 論海事「定位、導航及定時」 (PNT)之武器化發展

Position, Navigation, and Timing Weaponization in the Maritime  
Domain: Orientation in the Era of Great Systems Conflict

作者：佐里(Diane M. Zorri)為安柏瑞德航空大學安全研究助理教授。

凱斯勒(Gary C. Kessler)為智庫「大西洋理事會」(Atlantic Council)客座高級研究員。

譯者：劉宗翰中校。

本篇取材自美國《聯合部隊季刊》(Joint Force Quarterly)，2024年第一季，本文屬公開出版品，無版權限制。

## 提 要：

- 一、21世紀不容忽視的海上安全威脅之一，係「定位、導航及定時」(PNT)功能遭人為操弄，以混淆指揮者的認知判斷，並逐漸朝「武器化」發展之趨勢；而「全球衛星定位系統」(GPS)與「自動辨識系統」(AIS)的PNT功能受操弄案例，近幾年來更屢見不鮮，意味這個警訊已不容忽視。
- 二、本文以案例研究與文獻分析法，指出GPS存在訊號干擾、訊號欺騙、系統故障三項弱點，凸顯美國在GPS因應與配套措施並不完善；至於船舶AIS資料與軌跡偽造，並不需要高科技能力就能辦到，而中共、俄羅斯經常在AIS上出現偽造作法，政府高層與海事當局不能輕忽這種現象帶來的影響。
- 三、GPS與AIS問題的重要性逐漸升高，錯誤判斷無疑將引發衝突事件；鑒此，本文作者也提出各項精進作法，供華府與海事當局參考。「他山之石，足以攻錯」，我國相關單位與軍方，也應參考擬定相應作法，才能捍衛海疆安全，並提升海事韌性。

關鍵詞：全球定位系統、自動辨識系統、定位、導航、定時

## 壹、前言

現代戰爭中的欺敵、混淆及避實擊虛等手段，與古代戰爭的手段運用並無不同，<sup>1</sup>同理，戰爭虛實也被探討數世紀之久

；惟理解究竟何者為「實」仍是人類的一項挑戰，並應學會如何看穿欺騙的迷霧。人的認知反應來自於心理接受外在感受的回饋，而現代社會則充斥著各項改變認知的科技，戰場上亦復如此；誠如孫子所言

註1：Sun Tzu, The Art of War (New York: Simon & Schuster, 2004)。

表一：美國戰略學者馬漢之思想內涵簡介

理論 架構	以約米尼(Antoine Jomini)《戰爭藝術》的理論做為架構，主張以殲敵、制海為目的，也就是以優勢海上力量控制海洋，利用公海向海外投送兵力，確保海上航運安全，並建立稱霸的海軍。
知名 著作	他一生著作共20本專書、137篇論文，著名著作為《海權對歷史的影響》、《海權對法國大革命和帝國的影響(1793-1812)》及《海軍戰略論》。
重要 論述	◎主張集中海軍主力放在近海水域來確保本土安全，並以小規模艦隊繼續統轄遠洋水域。 ◎海軍為支持敵人戰略點的關鍵基礎，攻擊敵海軍成為最有效之攻勢，所以艦隊應用於攻擊敵主力艦與交通線，而不是防禦性工具。 ◎海上戰略的四項重要原則： ★集中：勿在同一時間內，追逐2個目標，而且當遭遇敵兩艘戰艦時，要集中火力合攻1艘。 ★中央位置：擁有位置適中、形勢強固、資源豐富的海軍基地，海戰時就可居於先天有利地位。 ★內線：從中央位置，向一個或數個據點延伸，用以阻止敵軍會合中心位置，用劣勢兵力牽制一面之敵；另以主力集中攻擊他面之敵。 ★交通線：補給線與聯絡線總稱，為大軍作戰命脈，來自海軍基地的後勤補給不間斷，才能維持海上作戰行動。

資料來源：參考廖麒林，〈馬漢「海軍戰略論」要義對我之啟示〉，《海軍學術雙月刊》(臺北市)，第46卷，第1期，2012年2月1日，頁25-34；〈馬漢海權論與海軍戰略論簡介〉，Blogger，2008年2月12日，[https://neko1789.blogspot.com/2008/02/blog-post\\_5467.html](https://neko1789.blogspot.com/2008/02/blog-post_5467.html)，檢索日期：2024年5月2日，由譯者彙整製表。

：「兵者，詭道也」。<sup>2</sup>戰略學家長期以來認為，在建立全球影響力方面，掌控海軍優勢與制海權至關重要；<sup>3</sup>美國「海權之父」馬漢(Alfred Thayer Mahan)指出，海軍在保護全球海洋貿易與交通線方面扮演重要角色(如表一)，而且一支小型海軍兵力，可藉由鎖定對手關鍵弱點，以壓倒性之姿，戰勝一支強大的海軍。

當一個國家的海上資產遭受攻擊時，將對地緣政治、軍事及經濟產生深遠影響，如1898年美艦「緬因號」(USS Maine)，因誤觸水雷導致爆炸沉沒，同年4月底就爆發「美西戰爭」(美國與各獨立勢力共同對抗西班牙帝國)；1915年英國皇家郵輪「盧西塔尼亞號」(RMS Lusitania)在愛爾蘭南方海域遭德國「U-20號」潛艇

擊沉，進而改變「一戰」的走向，並為後來美國參戰添加助力；及1964年美艦「麥達克斯號」(USS Maddox)與「特納·喬伊號」(USS Turner Joy)在東京灣北部遭北越魚雷快艇攻擊(即東京灣事件)，隨後引發美國介入「越戰」(1955-1975年)。

美國海軍係世界上最強大的遠征艦隊，當前正面臨心懷不軌國家、小型艦隊及非常規之敵人等運用新興科技，襲擾海上交通線或攻擊海軍艦船，這些惡意行為者採「以小搏大」方式，操弄系統中的關鍵組成子系統；<sup>4</sup>而21世紀海上安全最嚴重的持續性威脅，為對手操縱「全球定位系統」(Global Positioning System，以下稱GPS)與船位「自動辨識系統」(Automatic Identification System，以下稱

註2：同前註。  
註3：Alfred T. Mahan, The Influence of Seapower Upon History, 1660-1783, 12th ed. (Boston: Little, Brown and Company, 2004), pp.12-16。  
註4：Jeffrey Engstrom, Systems Confrontation and System Destruction Warfare: How the Chinese People’s Liberation Army Seeks to Wage Modern Warfare (Santa Monica, CA: RAND, 2018)。

AIS)兩項科技中的「定位、導航及定時」(Position, Navigation, Timing, 以下稱PNT)功能,進而影響美軍對周遭環境的「狀況覺知」(Situational Awareness)。<sup>5</sup>

美國國家安全戰略應提升海上領域的重要順位,因為國家九成進出口貿易係經由航運,而且海運體系每年貢獻國庫5.4兆美元(約新臺幣171.4兆),約占「國內生產毛額」(GDP)的四分之一。「海上運輸體系」(Maritime Transportation Network)是由航運通道、港口、運河船閘、碼頭、船塢、海路等交織而成的貿易網絡,比其規模更大的「全球海上運輸網絡」(Global Maritime Transportation Network),目前有將近九成的跨國貿易與運輸係依賴海運,不僅組成複雜且各部分相互依存,其重要性與關鍵基礎設施「不相上下」,但當國家在檢視全球經濟與戰略安全的重要組成面向中,海運網絡的重要性往往被低估。<sup>6</sup>

眾多研究文獻皆指出,海運良窳將影響國家的食物、能源、財政,甚至是國家安全與美軍的全球兵力投射。<sup>7</sup>鑒此,本文以案例研究與文獻分析方式,聚焦探討

GPS、AIS中的「定位、導航及定時」(PNT)功能如何為人所操弄,並混淆人的判斷與認知,最終一步步朝「武器化」(Weaponization)發展之趨勢,同時提出相關精進作法,供政府與相關當局參考。

## 貳、全球定位系統(GPS)

世界上的海運系統依賴美國「全球定位系統」(GPS)、歐盟「伽利略」(Galileo)、中共「北斗」與俄羅斯「格洛納斯」(GLONASS)等四大「全球導航衛星系統」(Global Navigation Satellite Systems, 以下稱GNSS),為船艦導引方位、路線及海上周遭環境的「狀況覺知」,並提供「定位、導航及定時」(PNT)功能,不僅用於陸地、海上及空中,而且也能用於關鍵基礎設施的精確定時(如表二)。再者,精確定時的重要性無庸置疑,若GPS定時訊號中斷或受損,將影響電信、金融服務、交通及電力系統網的正常運作,甚至還會引發其他如安全層面的問題。

GPS提供的定位資訊,其準確度可達3呎(約91公分)以內範圍,<sup>8</sup>雖然在遠洋海域可能較不需要這種精確定位;但在沿岸地

註5：Chris C. Demchak, "Achieving Systemic Resilience in a Great Systems Conflict Era: Coalescing Against Cyber, Pandemic, and Adversary Threats," The Cyber Defense Review Vol. 6, No. 2, Spring 2021。

註6：Cyber Strategic Outlook: The United States Coast Guard's Vision to Protect and Operate in Cyberspace (Washington, DC: U.S. Coast Guard, August 2021)。

註7：David Alderson, Daniel Funk, and Raluca Gera, "Analysis of the Global Maritime Transportation System as a Layered Network," Journal of Transportation Security, November 28, 2019, pp.1-35；Gary C. Kessler and Steven D. Shepard, Maritime Cybersecurity: A Guide for Leaders and Managers, 2nd ed. (Kindle Direct Publishing, September 2022)；Jason Ito, "Cyber at Sea: Protecting Strategic Sealift in the Age of Strategic Competition," Modern War Institute, May 10, 2022, <https://mwi.usma.edu/cyber-at-sea-protecting-strategic-sealift-in-the-age-of-strategic-competition/>, 檢索日期：2024年5月8日。

註8：Pratap Misra and Per Enge, Global Positioning System: Signals, Measurements, and Performance, rev. 2nd ed. (Lincoln, MA: Ganga-Jamuna Press, 2021)。



表二：各國全球導航衛星系統簡介

國家	系統名稱	衛星數量	建置年	精度(公尺)	壽期	軌道高度(公里)
美國	全球定位系統第二代(GPS II)	31	1997-2016	1.8(開放)	7-10年	20,180
	第三代(GPS III)	32	2018-2034	0.5	15年	20,180
歐盟	伽利略系統	30	2020	1(開放) 0.1(加密)	12年	23,222
中共	北斗2號系統	16	2008-2012	25(開放) 0.1(加密)	12年	21,500-35,800
	北斗3號系統	35	2015-2020	6(開放) 0.1(加密)	12年	21,500-35,800
俄羅斯	格洛納斯系統	24	1982-2014	2.8	10年	19,130

資料來源：參考林柏州，〈從美國升級GPS看全球導航系統發展〉，《國防安全週報》(臺北市)，第18期，2018年10月19日，頁16，由譯者彙整製表。

區或穿越狹窄扼制點或關鍵節點，如荷莫茲、麻六甲、波斯普魯斯海峽或巴拿馬、蘇伊士運河等，PNT功能卻扮演重要角色。<sup>9</sup>在GNSS中，由於GPS的準確性與精準度表現突出；因此，成為全球使用最廣泛的導航系統(如表三)。<sup>10</sup>不過，其仍存在訊號干擾、訊號欺騙、系統故障等三項弱點，分述如下：

一、訊號干擾

(一)指接收器因受附近的無線電傳輸干擾，導致無法偵測GPS訊號。由於訊號係由高度約2萬200公里的衛星所發射，功率約50瓦，訊號到達地球表面僅剩下幾毫瓦；因此，惡意行為者會以數瓦功率在GPS頻率上廣播，進而壓制接收器獲取GPS訊號所提供的正確PNT。<sup>11</sup>

(二)訊號干擾最初是為軍事用途而開發，且造價便宜的干擾器已經可在黑市上購買，這種不合法的使用現象已超過10年以上。早期為人所知的案例發生在2013年美國「紐瓦克自由國際機場」(Newark Liberty International Airport)，因有人使用干擾器擾亂飛航作業而遭罰款。當前全球各地也不斷發生猖獗的GPS干擾，尤其挪威機場受到的影響最為嚴重；另根據該國情報單位分析指出，2018年於挪威舉行的「北約」(NATO)「三叉戟聯合軍演」(Trident Juncture Exercise)期間(「冷戰」後最大規模)，該區域的GPS干擾活動較先前明顯增加。此外，中共、北韓及俄羅斯長期以來都有干擾他國GNSS的不良紀錄。<sup>12</sup>

註9：Gary C. Kessler and Diane M. Zorri, Cross Domain IW Threats to SOF Maritime Missions: Implications for U.S. SOF (MacDill Air Force Base, FL: Joint Special Operations University Press, 2021)。

註10：Bill Bostock, “Downed Russian Fighter Jets Are Being Found With Basic GPS ‘Taped to the Dashboards,’ UK Defense Minister Says,” Business Insider, May 10, 2022, <https://www.businessinsider.com/russia-su34-jets-basic-gps-receivers-taped-to-dashboards-uk-2022-5>，檢索日期：2024年5月10日。

註11：Tom Nardi, “Teardown: Mini GPS Jammer,” Hackaday, September 8, 2020, <https://hackaday.com/2020/09/08/teardown-mini-gps-jammer/>，檢索日期：2024年5月12日。

註12：Tegg Westbrook, “The Global Positioning System and Military Jamming: The Geographies of Electronic Warfare,” Journal of Strategic Security Vol. 12, No. 2, 2019), pp.1-16。

表三：美國「GPS」系統簡介



基本由空中衛星群、地面控制站、使用者接收器組成

- ◎美國國防部在「冷戰」時為軍事用途所設計並部署的計畫，主要目的在協助飛彈導引、軍事偵察及地形勘查，後來擴大應用於通訊、運輸、電網、金融等，都依賴GPS提供準確定時。
- ◎由「太空軍」負責管理地球軌域的衛星導航系統，可以為地表絕大部分地區提供準確的定位、測速和高精度的標準時間。
- ◎目前有32枚衛星，配置於6個不同軌道上，接收衛星訊號分為軍用P碼（精度小於1公尺並不對外開放）、民用C/A碼（精度為10公尺左右）及導航電文（檢視衛星是否正常使用）。

資料來源：參考曾智揚、游高、崔國強，〈淺談北斗衛星影響臺灣測繪產業發展〉，《測量工程》（宜蘭市），第58卷，2019年6月，頁1-17；How Does GPS Work?, National Aeronautics and Space Administration(NASA), <https://spaceplace.nasa.gov/gps/en/>，檢索日期：2024年5月11日，由譯者彙整製表。

## 二、訊號欺騙

（一）訊號欺騙係混淆GPS接收器，讓其認知錯誤的位置。2012年，「德州大學

」奧斯汀分校的團隊首次向美國「國土安全部」（Department of Homeland Security）展示訊號欺騙，他們用錯誤的GPS訊號誤導一架無人機，使其無法正確判讀所在位置高度；2013年，該團隊又以同樣方式成功欺騙長65公尺、排水量1,643噸，造價不斐的豪華遊艇「德拉赫斯白玫瑰號」（White Rose of Drachs），使它在地中海航行時改變航向。<sup>13</sup>

（二）公開的大規模GPS訊號欺騙案例發生在2017年6月，「阿提亞號」（Atria）油輪停泊在俄國諾渥羅西斯克港（Novorossiysk Port）外的黑海海域，但GPS定位卻顯示位於格連吉克機場（Gelendzhik Airport），兩者相距32公里；且該油輪並非單一事件，因為至少有20多艘船同樣定位在機場上。<sup>14</sup>該事件雖非首次，但卻是公開且周知的大規模GPS欺騙，<sup>15</sup>根據美國智庫「先進國防研究中心」（Advanced Defense Studies Center）研究指出，自2016年以來有將近9,900件訊號欺騙發生在黑海、克里米亞、俄羅斯、敘利亞及其他地區等，其干擾源頭都指向俄軍。<sup>16</sup>此外，在2020年的調查報導亦指出，一艘德國研究船在2017至2018年的全球航行中，偵測到多個地點發生類似的訊號欺騙。<sup>17</sup>

註13：Mark L. Psiaki, Todd E. Humphreys, and Brian A. Stauffer, "Attackers Can Spoof Navigation Signals Without Our Knowledge. Here's How to Fight Back GPS Lies," IEEE Spectrum Vol. 53, No. 8, August 2016, pp.26-53。

註14：Dana Goward, "Mass GPS Spoofing Attack in Black Sea?" The Maritime Executive, July 11, 2017, <https://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea/>，檢索日期：2024年5月13日。

註15：同註12。

註16："Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria," Center for Advanced Defense Studies, March 26, 2019, <https://c4ads.org/reports/above-us-only-stars/>，檢索日期：2024年5月14日。



圖一：「艾克森瓦爾狄茲號」漏油事件

說明：「艾克森瓦爾狄茲號」(Exxon Valdez)油輪在1989年發生觸礁漏油，當時約4,200萬公升原油流入阿拉斯加州威廉王子灣水域，造成生態浩劫後，直接促成「AIS」的問世。

資料來源：參考Exxon Valdez oil spill, Wikipedia, [https://en.wikipedia.org/wiki/Exxon\\_Valdez\\_oil\\_spill](https://en.wikipedia.org/wiki/Exxon_Valdez_oil_spill)，檢索日期：2024年5月20日，由譯者彙整製圖。

### 三、系統故障

要讓GPS系統故障，摧毀當然是手段之一。一般系統使用超過32枚衛星，其中29枚處於全天候運作，而運行最少需要24枚。依照GPS系統設計原理，系統能因應自然故障的情況，意即若1枚衛星發生故障，它會因此脫離系統，此時另枚衛星就會接替它原本位置。鑒於俄、「中」都具備摧毀衛星的能力，例如自2012年春季以來，一提到衛星威脅議題，俄國總統普丁(Vladimir Putin)就會放話要打下美國GPS

系統的衛星；<sup>18</sup>美國智庫「國家公共政策研究所」(National Institute for Public Policy)在《各國太空能力對美國國安之影響》(Foreign Space Capabilities Implications for U.S. National Security)報告指出，共軍已可以摧毀或干擾地表上空1,900-35,000公里軌道上的500枚美國衛星，也提出在外太空引爆核武來製造電磁脈衝(EMP)，以癱瘓或破壞目標國的在軌衛星。<sup>19</sup>由於美國GPS系統目前並未具備因應遭攻擊後的復原韌性，有關當局應研擬可能的配套措施。

由於美國GPS脆弱性與面臨的威脅不僅是海事圈的問題，而且也影響當代社會的諸多層面。雖然GPS的管理者為「太空軍」，但因其為軍民兩用資產；因此，不僅需要軍事方案，同樣也要有民間方案。<sup>20</sup>再者，俄羅斯為干擾GPS的慣犯，在2014年併吞克里米亞時，就干擾烏克蘭接收GPS訊號，也曾在「北約」演習時試圖干擾衛星訊號，而「俄烏戰爭」期間又故計重施。此外，俄國還在2021年時宣稱，其最新的反衛星飛彈技術，可以炸燬GPS系統的32枚衛星，並在同年底對一枚退役的

註17：Katherine Dunn, "The Long Ocean Voyage That Helped Find the Flaws in GPS," Fortune, January 24, 2020, <https://fortune.com/2020/01/24/gps-disruption-test-voyage/>，檢索日期：2024年5月15日。


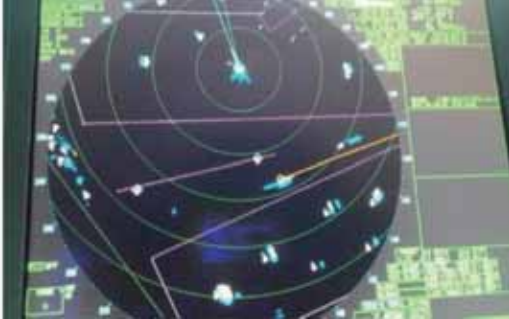
註18：Dana A. Goward and John Garamendi, "Putin Is Holding GPS Hostage. Here's How to Get It Back," Defense News, April 12, 2022, <https://www.defensenews.com/opinion/2022/04/12/putin-is-holding-gps-hostage-heres-how-to-get-it-back/>，檢索日期：2024年5月16日。

註19：Steven Lambakis, Foreign Space Capabilities Implications for U.S. National Security (National Institute for Public Policy Publishing, September 2017)。

註20：Dana A. Goward, "Get the Bullseye Off GPS," Space News, April 19, 2022, <https://spacenews.com/op-ed-get-the-bullseye-off-gps/>，檢索日期：2024年5月17日。



表四：「自動辨識系統」(AIS)簡介

	
<p>◎船舶安裝的AIS(圖上)可與鄰近船舶、AIS岸臺及衛星等設備交換電子資料，提供船舶交通管理系統辨識及定位，以避免發生海上碰撞事故。</p> <p>◎《國際海上人命安全公約》(SOLAS)要求航行於國際水域，總噸位在300噸以上船舶和所有不論噸位之大小客船，都應安裝AIS。AIS發出訊息包括獨特的識別碼、船名、位置、航向、船速，並顯示在AIS螢幕或電子海圖上(圖下)，用以追監船舶動向。</p> <p>◎AIS使用海上移動VHF波段交換資料，設備成本較雷達為低，但其可視範圍幾近於雷達，而且當地「船舶交通管理系統」(VTS)只要搭配AIS岸臺(無須安裝雷達)，就可獲得所有船舶的AIS軌跡。</p>	

資料來源：參考黃聰正，〈建構安全開放的海洋地球村，認識AIS船舶「自動辨識系統」〉，《海巡》，第6期，2003年，頁51-52；「自動識別系統」(AIS)，交通部航港局，<https://transport-curation.nat.gov.tw/portAuthority/ais.html>；“Automatic Identification System (AIS)：Cloaking and Consequences,” Maritime Mutual Risk Bulletin No. 16, July 2, 2019, p.1；Shilavadra Bhattacharjee, “What is Automatic Identification System-Types And Working,” Marineinsight, July 27, 2022, <https://www.marineinsight.com/marine-navigation/automatic-identification-system-ais-integrating-and-identifying-marine-communication-channels/>，檢索日期：2024年5月19日，由譯者彙整製表。

「Tselina-D」衛星進行測試。<sup>21</sup>華府相關當局短期內並未規劃強化GPS系統脆弱性的方案，也沒有研擬系統中斷的因應配套措施，這種不足之處應及早改進。

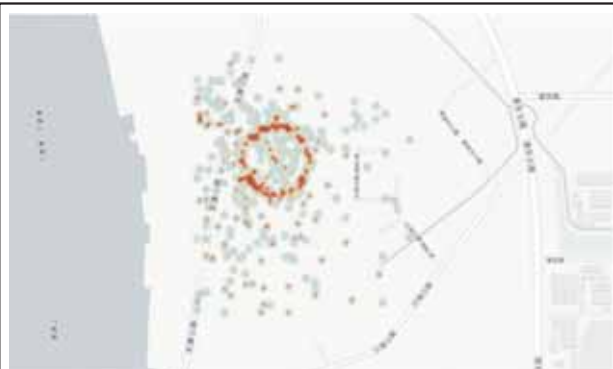
參、自動辨識系統(AIS)

一、AIS在1990年代問世時，主要是為因應油輪觸礁漏油的生態浩劫事件(如圖一)，而GPS與其他國家的GNSS不斷進步，也促成「自動辨識系統」(AIS)的發展，並成為船舶與海事機關用以維持地區船艦的交通狀況示警(AIS簡介，如表四)。

其後，世界各地的AIS數據資料，在經年累月不斷積累下，已成為可提供船艦從過去到現在的歷史移動軌跡，並對追蹤航運路線、基本產業情報及理解航運樣貌等面向，都至關重要。

二、2002年「國際海事組織」(International Maritime Organization，IMO)在修訂《國際海上人命安全公約》(International Convention for the Safety of Life at Sea，以下稱SOLAS)時，雖然將AIS列為船舶必具設備，但卻存在眾所周知的安全漏洞，諸如缺少發送者

註21：Brian G. Chow and Brandon W. Kelley, “Russian Invasion of Ukraine Reinforces the Urgency of Fixing U.S. Satellite Vulnerability by 2027,” Space News, March 8, 2022, <https://spacenews.com/op-ed-russian-invasion-of-ukraine-reinforces-the-urgency-of-fixing-u-s-satellite-vulnerability-by-2027/>，檢索日期：2024年5月18日。



圖二：GPS受干擾後呈繞圈模式

資料來源：Mark Harris, “Ghost Ships, Crop Circles, and Soft Gold: A GPS Mystery in Shanghai,” MIT Technology Review, November 15, 2019, <https://www.technologyreview.com/2019/11/15/131940/ghost-ships-crop-circles-and-soft-gold-a-gps-mystery-in-shanghai/>, 檢索日期：2024年5月24日，由譯者彙整製圖。

身分認證、訊息時間戳記、數據有效性認證及資料完整性認證。美艦都配備AIS無線電收發機，但大多數情況下不會維持廣播狀態，原因在於SOLAS公約中臚列軍艦的豁免條款，以避免行踪外洩。<sup>22</sup>有關GPS與AIS偽造的案例，摘陳如下：

(一)2019年7月，英國「史丹納帝國號」(Stena Impero)油輪在行經荷莫茲海峽時，伊朗藉口該船的AIS違反國際海事規定，命令海軍登船扣押，接著改變油輪航線進入伊朗領海；然此事件應係伊國為報復英軍陸戰隊先前在直布羅陀海峽扣押伊國油輪所致，而英國所持理由為該船違



圖三：GPS訊號欺騙集中在舊金山西北部雷斯岬附近

資料來源：Bjorn Bergman, “AIS Ship Tracking Data Shows False Vessel Tracks Circling Above Point Reyes, Near San Francisco,” SkyTruth, May 26, 2020, <https://skytruth.org/2020/05/ais-ship-tracking-data-shows-false-vessel-tracks-circling-above-point-reyes-near-san-francisco/>, 檢索日期：2024年5月24日，由譯者彙整製圖。

反歐盟制裁規定，企圖運送原油到敘利亞。<sup>23</sup>同年7月，美國貨船「麥盧卡號」(Manukai)在抵達上海港時，AIS顯示有1艘船正以7節(時速約12.6公里)速度駛進相同航道，另一艘船則先是消失，隨後又發現它竟然停在碼頭。<sup>24</sup>據美國「先進國防研究中心」研究發現，在該船回報有問題當日，約有300艘出入的船隻都受影響；且在分析AIS資料後發現，GPS受干擾後呈繞圈模式(如圖二)，並非以往將訊號導向固定地點的方式。<sup>25</sup>此外，「全球漁業監測」(Global Fishing Watch)組織與環境監

註22：Gary C. Kessler and Steven D. Shepard, *Maritime Cybersecurity: A Guide for Leaders and Managers*, 2nd ed. (Kindle Direct Publishing, September 2022)。

註23：Michelle W. Bockmann, “Seized UK Tanker Likely Spoofed by Iran,” *Lloyd’s List*, August 16, 2019, <https://lloydslist.maritimeintelligence.informa.com/LL1128820/Seized-UK-tanker-likely-spoofed-by-Iran>, 檢索日期：2024年5月21日。

註24：Mark Harris, “Phantom Warships Are Courting Chaos in Conflict Zones,” *Wired*, July 29, 2021, <https://www.wired.com/story/fake-warships-ais-signals-russia-crimea/>, 檢索日期：2024年5月21日。

註25：“Shanghai GPS Spoofing,” video, 0:42, C4ADS, 2019, for download, <https://drive.google.com/file/d/1dTWu7H9JjRyN0uQPZ9HwiUzCFd7cd5pL/view>, 檢索日期：2024年5月22日。





**圖四：我國海軍「磐石艦」AIS信號遭偽冒圖**

說明：圖片顯示該艦船位正在江蘇省南通市「陸上行舟」

資料來源：胡智凱，〈中國破解竄改我磐石艦定位「陸上行舟」〉，信傳媒，2020年3月28日，<https://www.cmmedia.com.tw/home/articles/20549>，檢索日期：2024年5月24日，由譯者彙整製圖。

察機構「天空真相」(SkyTruth)在2020年時的聯合研究發現，那時在舊金山西北部雷斯岬(Point Reyes)一帶因不明原因，集中出現這種GPS訊號欺騙與AIS資料偽造情形；而經追查後發現，訊號與船舶之間距離竟然達到1萬6,093公里遠(如圖三)。<sup>26</sup>

(二)上海港的GPS訊號欺騙案例與研究機構發現的遠距離案例，意味著混淆船艦判斷GPS訊號的影響，已可從船艦周邊擴及至全球各地；誠然中共應為上述案例的主嫌之一。因為長期以來，中共就遭外界懷疑使用偽造AIS，以藏匿「非法、未

報告、不受規範」(Illegal, Unreported and Unregulated，以下稱IUU)捕魚的漁船，並讓顯示的位置與實際距離相差數百或數千浬遠。值得注意的是，我國海軍油彈補給艦—「磐石艦」也曾出現在中共AIS偽造的行列中(如圖四)，顯見其應該找到AIS信號發射漏洞，讓其得以竄改船隻詳細資料、建立擁有相同細節的虛假船隻，以及修改助航項目等。<sup>27</sup>

(三)就民間角度而言，AIS資料偽造有多種目的，如展現自身具有這種能力、掩蓋IUU捕魚、走私及其他非法活動，並將原身分洗白，以避免受偵察、制裁或檢查。<sup>28</sup>再就軍事層面而言，由於軍艦並非定期發送AIS資料，也不難發現有軍艦集體偽造AIS資料的情形，2020年9月，AIS顯示英國「伊莉莎白女王號」(HMS Queen Elizabeth)航空母艦及另5艘護衛艦正駛向愛爾蘭海，但查看衛星影像空照圖時，卻發現她們所在位置空無一物；事實上，這6艘軍艦不僅不在AIS所標定的軌跡上(如圖五)，甚至不排除她們並不在一起，或根本未開啟AIS廣播資料。<sup>29</sup>

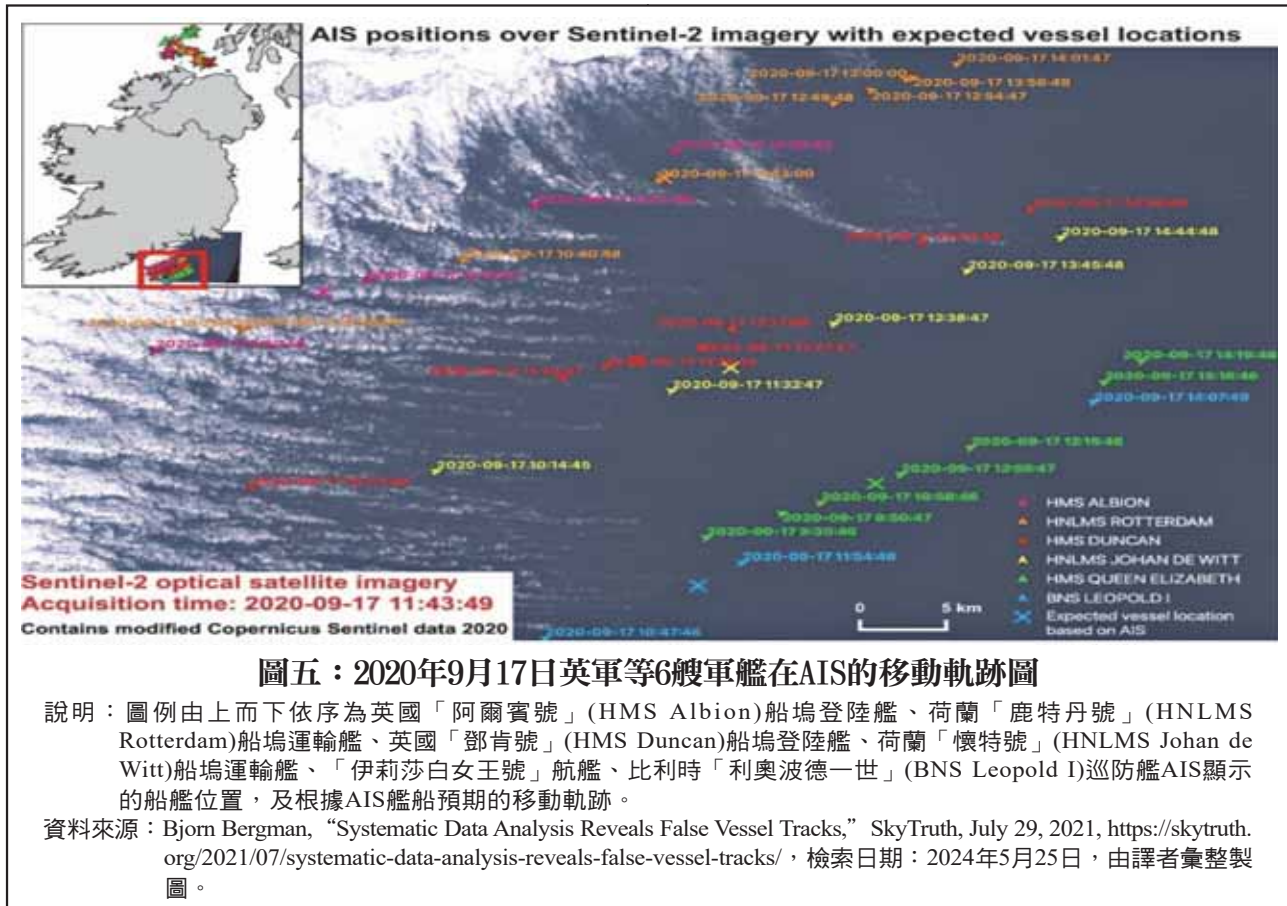
三、AIS資料偽造也有可能引發情勢升溫，如2021年6月，當「北約」(NATO)

註26：Bjorn Bergman, "AIS Ship Tracking Data Shows False Vessel Tracks Circling Above Point Reyes, Near San Francisco," Sky Truth, May 26, 2020, <https://skytruth.org/2020/05/ais-ship-tracking-data-shows-false-vessel-tracks-circling-above-point-reyes-near-san-francisco/>，檢索日期：2024年5月23日。

註27：胡智凱，〈中國破解竄改我磐石艦定位「陸上行舟」〉，信傳媒，2020年3月28日，<https://www.cmmedia.com.tw/home/articles/20549>，檢索日期：2024年5月24日。

註28：James R. Watson and A. John Woodill, "Anticipating Illegal Maritime Activities From Anomalous Multiscale Fleet Behaviors," ArXiv, October 15, 2019, <https://arxiv.org/pdf/1910.05424.pdf>，檢索日期：2024年5月24日。

註29：同註23。



艦船在黑海演習前，英國「捍衛者號」(HMS Defender)驅逐艦與荷蘭「埃弗森號」(HNLMS Evertsen)巡防艦，於18日下午抵達烏克蘭敖德薩(Odesa)，但AIS追蹤軌跡卻顯示2艦在當晚前往克里米亞塞凡堡(Sevastopol)，船位顯示距離俄國「黑海艦隊」司令部僅約3.6公里。可是從社群媒體(Youtube)影片、實況攝影機及其他證據都顯示，該2艦並未離開碼頭；再者

，當時克里米亞主權爭議仍未歇，再加上鄰近塞凡堡艦隊司令部，若「北約」艦船在未經同意下進入俄國領海，將被視為一種挑釁行為。<sup>30</sup>10天後，AIS追蹤軌跡又顯示美軍驅逐艦「羅斯號」(USS Ross)的位置靠近克里米亞，但實況攝影機卻顯示它仍泊靠於敖德薩碼頭。<sup>31</sup>

上述2021年案例，只是過往數年間許多國家軍艦AIS資料偽造事件之一，<sup>32</sup>且偽

註30：H.I. Sutton, "Positions of Two NATO Ships Were Falsified Near Russian Black Sea Naval Base," USNI News, June 21, 2021, <https://news.usni.org/2021/06/21/positions-of-two-nato-ships-were-falsified-near-russian-black-sea-naval-base>, 檢索日期：2024年5月26日。

註31：Yörük Işık, "And . . . All Fake Like HMS Defender Incident. USS Ross Is in Odesa's Cabotage Harbor!" Twitter, June 29, 2021, <https://twitter.com/yorukisik/status/1409992626477191175>, 檢索日期：2024年5月26日。

註32：同註23。



造AIS資料並不難。本文作者之一凱斯勒 (Gray Kessler) 也實際做了AIS軌跡偽造示範(如圖六)，在2021年8月2日讓俄國「莫斯科號」(Moskva)飛彈巡防艦進入美國佛羅里達州東岸的卡納維拉爾港(Canaveral Port)。<sup>33</sup>

## 肆、地緣政治風險與影響

### 一、歷史相似性借鑑

(一)2021年黑海AIS資料偽造事件，不排除是俄羅斯預先設計的策略，事後藉此發布抹黑或渲染「北約」的言論，儘管世界上大部分的人都理解AIS的軌跡可能造假；但俄國人民卻有可能認為NATO意圖侵略為真。從俄國總統普丁的立場而言，

他需要的是願意相信的國內人民，而不在乎世界其他國人民是否相信。儘管我們無法確定俄國的伎倆是為了測試相關能力，或是意圖做為開戰的理由；如果是後者，則應特別關注後續偽造海上電子訊號的類案，因為這恐將成為提供俄國發動武裝衝突的理由。

(二)再回顧一下1964 年的「東京灣事件」，當時美國驅逐艦「麥達克斯號」(USS Maddox)為蒐集信號情報，在北越東京灣海域執行「德索托巡邏(DeSoto Patrol)計畫」時，遭到北越3艘俄製「P-4」魚雷快艇攻擊，該艦除立刻予以還擊外，後續配合空中「F-8」戰機，最終摧毀北越快艇，自身僅遭到單顆14.5mm機槍彈

註33：Gary C. Kessler, “AIS Spoof of a Warship,” video, 2:13, August 22, 2021, [https://www.garykessler.net/gck/202108\\_MOSKVA\\_spoof.mp4](https://www.garykessler.net/gck/202108_MOSKVA_spoof.mp4), 檢索日期：2024年5月26日。



擊中，這是東京灣第一次攻擊事件。2天後，麥艦與「特納·喬伊號」(USS Turner Joy)又在雷達上發現北越巡邏艇，此時雷達與聲納又偵測到魚雷攻擊前兆，2艦便果斷開火反擊，但不管是軍艦或飛機都未目視敵船，且真假撲朔迷離，<sup>34</sup>這是東京灣「第二次攻擊事件」，並導致美國國會通過《東京灣決議案》(Tonkin Gulf Resolution)，讓美軍得以在日後介入中南半島事務。<sup>35</sup>

(三)檢視第二次攻擊事件的調查報告指出，當時美艦周遭可能確實有船隻，但並非是攻擊艇，也沒有魚雷發射徵兆，但卻歸結出誤判來自雷達與聲納的「信號情報」(Signals Intelligence)，導致在無敵情情況下做出攻擊反應；不過，在當時政治氛圍下，軍艦急於下判斷是受到默許的。畢竟2天前北越才剛對美軍發動挑釁攻擊，這種現象也導致「信號情報」未能被仔細檢查其真偽，<sup>36</sup>凸顯假訊號混淆認知判斷並非難事。

## 二、影響與對策

當具敵意的他國軍艦接近我方艦隊時，確實存在巨大風險，且當操作人員可以故意改變「信號情報」與導航數據資料，

以混淆對方「狀況覺知」判斷時，情況會更加危險；而意圖偽造或干擾訊號可視為是挑釁行為，還會引發不良後果與深遠影響。略述如下：

(一)當GPS或他國的GNSS遭到干擾或破壞，會造成船艦航行不確定性、延誤及供應鏈效率低落，況且還可能在沿岸、近岸水域、狹窄海峽和國際扼控點等地方引發事故。由於這些地點的操作容錯率很低，只要一發生事故，將造成一定程度的影響與損失，不可不慎。值得注意的是，造假的AIS軌跡可以成為爭議論述的支持者，進而威脅美國盟邦與夥伴國之利益。此外，敵對者也可以用偽造AIS資料，佯裝成一支大型艦隊或是改變船艦的航行軌跡，況且這類威脅程度根本不可能引發《北大西洋公約》第五條的集體防禦機制；因為，只有在具攻擊性情況下，成員國才會願意共同反制，公約第五條並未規定成員國有宣戰或反擊之義務；<sup>37</sup>且迄今只啟動過一次，也就是2001年9月11日美國的「911事件」(恐怖分子挾持客機衝撞紐約世貿中心和國防部等建築)。

(二)正由於GPS訊號欺騙與AIS資料偽造的難度不高，對我們所處的海上環境安

註34：Robert J. Hanyok, "Skunks, Bogies, Silent Hounds, and the Flying Fish: The Gulf of Tonkin Mystery, 2-4 August 1964," *Cryptologic Quarterly* 19/20 (Winter 2000/Spring 2001), pp.4-10。

註35：Dale Andrad? and Kenneth Conboy, "The Secret Side of the Tonkin Gulf Incident," *Naval History Magazine* Vol. 13, No. 4, August 1999。

註36：同註32。

註37：Cassia Sari, "Cyberattacks Can Invoke NATO Defence Clause," *The Organization for World Peace*, April 25, 2022, <https://the-owp.org/cyberattacks-can-invoke-nato-defence-clause/>，檢索日期：2024年5月28日。

全將面臨挑戰，任何美國的潛在對手，諸如中共、伊朗、北韓和俄羅斯等國家，都有能力運用該手段，欺敵混淆作戰指揮官之用兵判斷；且若發動對GPS與AIS之攻擊，顯然會影響航行正常運作與對周遭環境的「狀況覺知」，影響層面可大可小。雖然有些人會爭論對GPS與AIS之攻擊，在本質上是否與網路安全有關？歸類為「網攻」是否適當？但本文認為，我們本來就應致力於防護資訊與其他數據資料之保密性、完整性、可用性、真實性、實用性和擁有權；<sup>38</sup>列入網路安全防護之一環，可藉此提升當局關注與重要性。值得注意的2020年7月底，我國也曾發生GPS網攻事件，知名穿戴式裝置大廠「臺灣國際航電公司」(Garmin)傳出遭駭消息，除生產線停工2日外，許多運用該公司導航系統的產業也受到影響。<sup>39</sup>

(三)海上網路安全在當前的重要性不容忽視，我們也不能排除俄羅斯會如法炮製，且俄國不無可能會用「北約」侵犯邊

界為名，就像前述以「NATO」軍艦在黑海的案例，向周邊其他國家發起挑釁或侵略行為。<sup>40</sup>此外也有大量證據指出，俄國在「俄烏戰爭」期間對GPS系統發動攻擊，擾亂烏軍許多依賴該系統所進行的空中鎖定、砲兵瞄準定位、通信系統及其他軍事設施的「定時」功能。<sup>41</sup>報導也指出，俄國干擾波的強度有時連自身的「格洛納斯」(GLONASS)系統也受到影響；至於其備用方案係使用名為「海鷗」(Chayka)的陸基無線電導航系統，<sup>42</sup>其功能堪比美國的「長程無線電導航系統」(Long-Range Navigation，或稱「羅遠」【LORAN】系統)。

(四)當前大多數GPS訊號欺騙與干擾的反制策略，都是短期的臨時應對措施，舉例而言，許多商用「全球導航衛星系統」(GNSS)的接收器可以偵測傳入主要衛星的訊號來源是真或假；另在遇到問題情況下，接收器能切換到其他的替代衛星系統，但美國當前並無可靠的GPS替代方案。

註38：Donn B. Parker, "Toward a New Framework for Information Security?" in Computer Security Handbook, 6th ed., ed. Seymour Bosworth, Michel E. Kabay, and Eric Whyne (Hoboken, NJ: John Wiley & Sons, Inc., 2015)。

註39：周峻佑，〈臺灣知名GPS及穿戴式裝置大廠遭網路攻擊，因部分系統被加密導致線上服務中斷〉，iThome，2020年7月29日，<https://www.ithome.com.tw/news/139094>，檢索日期：2024年5月28日。

註40：Michael Klipstein and Tinatin Japaridze, "Collective Cyber Defence and Attack: NATO's Article 5 After the Ukraine Conflict," European Leadership Network, May 16, 2022, <https://www.europeanleadershipnetwork.org/commentary/collective-cyber-defence-and-attack-natos-article-5-after-the-ukraine-conflict/>，檢索日期：2024年5月29日。

註41：Jake Thomas, "They're Jamming Everything: Putin's Electronic Warfare Turns Tide of War," Newsweek, June 3, 2022, <https://www.newsweek.com/theyre-jamming-everything-putins-electronic-warfare-turns-tide-war-1712784>，檢索日期：2024年5月29日。

註42：Olivier Chapuis, "En guerre en Ukraine, la Russie brouille la navigation par satellites et utilise le syst?me Loran, Voiles et Voiliers," March 19, 2022, <https://voilesetvoiliers.ouest-france.fr/equipement-entretien/electronique-embarquee/gps/en-guerre-en-ukraine-la-russie-brouille-la-navigation-par-satellites-et-utilise-le-systeme-loran-cfd085fa-a6ac-11ec-969a-2a6df02632f3>，檢索日期：2024年5月30日。

以往在GPS系統尚未被廣泛運用前，美國與國際海事圈主要依賴陸基型「羅遠」(LORAN)系統，但美國「國土安全部」(Department of Homeland Security)在2010年時將該系統除役時，並未考慮GPS系統若遭人破壞時的替代方案；<sup>43</sup>如今許多船員並不理解如何使用「LORAN」系統，或是該系統在航海圖上的註記。

2018年川普政府曾要求美國交通部長須為GPS建立一套備用的陸基定位與定時系統，<sup>44</sup>當時所提的「增程型羅遠」系統(eLORAN)計畫案，卻無後續下文。<sup>45</sup>另一個提案為運用「量子感測器」(Quantum Sensing)來實現「定位、導航及定時」(PNT)功能，但研究人員仍力有未逮，尚無法實現該計畫。此外，還有幾個提案是用以保護「自動辨識系統」(AIS)，但國際間各國不僅在認定標準上不一致，而且在規劃與執行方面，也無法取得共識，最終同樣無疾而終。<sup>46</sup>

## 伍、精進作法

GPS訊號欺騙與AIS資料偽造在過去幾

年間，已從單純能力展示，升級成為真正危險情況，這意味著錯誤的認知判斷，恐引發重大衝突。鑒於攻擊面向逐漸多元化，非軍事之手法已可對軍事資產進行打擊，<sup>47</sup>美國國安與國防單位應採取以下作法來減低系統脆弱性，分述如下：

### 一、強化訓練與認知能力

首先，海事操作員與艦橋軍官(海軍指航行值更官)應充分理解船上的資訊科技與作業系統，以及各系統間的關聯性、交互影響及弱點所在；而資訊安全檢查官與船上偵測系統的業務也應納入海事人員與管理體系。其次，航行操作員與船橋人員(指航海官、航海士官)須有能力判斷AIS所顯示資料的真偽，而天文導航技術、海洋慣性學、雙曲線導航系統等知識，都應納入人員的教育訓練課程中，才能具備相關能力來驗證真偽。最後，海上軍事演習應將GPS與AIS系統中斷的科目想定納入，以測試相關人員在無科技協助下，還具備多少應變能力；另外，演習也要測試我方網路的防禦能力，並檢視是否可有效反制敵人的網攻。

註43：Terminations, Reductions, and Savings: Budget of the U.S. Government, Fiscal Year 2010 (Washington, DC: Office of Management and Budget, 2009)。

註44：Frank Liobondo Coast Guard Authorization Act of 2018, Public Law 115-282, 115th Cong., 2nd sess., December 4, 2018, <https://www.congress.gov/115/plaws/publ282/PLAW-115publ282.pdf>，檢索日期：2024年6月1日。

註45：Aaron Martin, “Senate Bill Would Require Establishment of Land-Based Alternative to GPS Satellite Timing Signals,” Homeland Preparedness News, December 19, 2017, <https://homelandprepnews.com/stories/25836-senate-bill-require-establishment-land-based-alternative-gps-satellite-timing-signals/>；“PNT ExCom Backs eLoran as a Step to Full GPS Backup System,” Inside GNSS, December 10, 2015, <https://insidegnss.com/pnt-excom-backs-elor-an-as-a-step-to-full-gps-backup-system/>，檢索日期：2024年6月1日。

註46：同註21。

註47：同註9。



### 二、GPS精進作法

(一)政府高層與海事機關應理解，若短期內無法研擬因應GPS系統中斷的有效方案，此類威脅有可能會擴大為國安等級，並導致災難性後果；且涉及使用PNT功能的相關單位，如軍方、政府機關或民間企業，都將無一倖免。中共與俄羅斯在「北斗」與「格洛納斯」(GLONASS)系統中斷時，已設置陸基導航系統做為因應，但美國在GPS中斷時的配套措施並不完善，這意味著敵人已先期取得戰略優勢。<sup>48</sup>

(二)「美國國家太空『定位、導航及定時』諮詢委員會」(National Space-based PNT Advisory Board)並未建議在短期內恢復「羅遠」系統，反而是建議先強化當前GPS系統並做現代化的更新；至於未來長期方案為持續研發不依賴GPS的「量子感測」PNT系統，目前相關進程尚未達到可運用階段。<sup>49</sup>另一方案為將「美國國家航空暨太空總署」(NASA)旗下「噴射推進實驗室」的「差分全球衛星定位系統

」(Global Differential GPS，以下稱GDGPS)，與美國國安機構和關鍵基礎設施進行整合，GDGPS是利用放置於基站(已知點)之GPS衛星接收器所接收的觀測資料，計算其虛擬距離差分或相位差分修正量，再將此差分修正量利用無線電即時傳送至移動站或待測站，與放置於移動站之衛星接收器所接收觀測資料合併計算，以獲得較高精度定位。<sup>50</sup>

(三)由於華府並未指定專責機構針對「量子感測」PNT系統進行規劃、執行及監管，遑論未來整體方向；至於GDGPS整合案除需編列預算外，也要各單位相互溝通協調，才能擬定整體規劃。此外，一些專家認為中共在PNT能力上擁有領先實力，美國應將長期的PNT能力強化列為國家層級戰略；<sup>51</sup>政府高層應認知PNT功能對國家安全至關重要，並應致力改善其能力，包含低軌衛星、太空衛星、陸基導航、慣性導航、量子感測、「羅遠」系統及天文導航，唯有強化子系統，才能強化全系統

註48：Dana Goward, "China Expanding Loran as GNSS Backup," GPS World, October 12, 2020, <https://www.gpsworld.com/china-expanding-loran-as-gnss-backup/>, 檢索日期：2024年6月2日。

註49：「量子感測」(QS)為以高精度量子時鐘為基礎，透過量子衛星取得衛星與地面間傳遞糾纏光子對之時間差，以確定地面用戶座標。Michael J. Biercuk and Richard Fontaine, "The Leap Into Quantum Technology: A Primer for National Security Professionals," War on the Rocks, November 17, 2017, <https://warontherocks.com/2017/11/leap-quantum-technology-primer-national-security-professionals/>, 檢索日期：2024年6月2日；王綉雯，〈中共量子技術之作戰應用〉，《國防安全雙週報》(臺北市)，第69期，2022年12月16日，頁30。

註50：Christine Bonniksen, "Global Differential GPS (GDGPS) System Future," National Aeronautics and Space Administration, Space-Based Position Navigation and Timing National Advisory Board Meeting, July 1, 2020, <https://www.gps.gov/governance/advisory/meetings/2020-07/bonniksen.pdf>；〈差分全球定位系統〉，國家教育研究院，<https://terms.naer.edu.tw/detail/2b75fabbb5dd5f0ae78d538bee4739a4/>，檢索日期：2024年6月3日。

註51：Dana Goward, "China Leads World with Plan for 'Comprehensive' PNT," GPS World, November 15, 2019, <https://www.gpsworld.com/china-leads-world-with-plan-for-comprehensive-pnt>; David H. Millner, Stephen Maksim, and Marissa Huhmann, "BeiDou: China's GPS Challenger Takes Its Place on the World Stage," Joint Force Quarterly 105 (2nd Quarter 2022), pp.23-31。

表五：PNT評估表

項 目	執 行 目 標
識 別	◎識別所有資產依賴PNT的各項應用。 ◎識別可能造成具體威脅的弱點、威脅與衝擊，以利評估風險。
保 護	◎保護組成、傳輸與運用PNT的系統，以及規劃所需之訓練、授權與存取控制來保護PNT之使用。 ◎擬定因應與復原計畫，俾在可能產生威脅情境下，保護仰賴PNT的用戶與服務，並維持最低運作需求。
偵 測	◎持續進行監控與檢查，以確保偵測正常運作。 ◎建立因應偵測異常事件的處理程序。
回 應	◎與 PNT用戶與利益攸關者說明PNT事件的發生及其影響。 ◎擬定因應已知或預期威脅或弱點的計畫，並透過事件經驗，逐步修正既有計畫或策略。
復 原	◎擬定復原步驟將依賴PNT功能之系統回復至工作狀態。 ◎與PNT資料用戶與利益攸關者，說明PNT功能的復原情形與進度。

資料來源：參考杜貞儀，〈全球衛星導航系統的威脅與因應〉，《國防情勢特刊》(臺北市)，第10期，2021年7月5日，頁19，由譯者彙整製表。

的韌性。

### 三、AIS精進作法

在制定AIS安全方案過程中，商業界也會藉此獲致正向收益，而且AIS的競爭投標案內容，應整合各種安全措施如公鑰(Public Key)、不對稱加密、數位簽章、以及在商業應用、電腦或手機上常見的身分認證機制。<sup>52</sup>此外，在保護AIS安全方面，尚需兩個國際組織之間的協調合作，一個是負責《國際海上人命安全公約》(SOLAS)的「國際海事組織」(International Maritime Organization)，另一個是負責AIS無線電協議事務的「國際電信聯盟」(International Telecommunication Union)，<sup>53</sup>如此才能共同制定明確的願景，並走上正確的道路。

### 四、落實PNT評估表

美國「國家標準暨技術研究院」(National Institute of Standards and Technology)為強化PNT功能與協助使用者評估風險，提出基於網路安全架構的評估表(如表五)，該檢查表可做為PNT使用單位所用，各單位也應按自身條件或狀況，調整成適合本身執行的內容，才能強化韌性。

## 陸、結論

GPS與AIS系統中的「定位、導航及定時」(PNT)武器化發展已然成形，這類威脅所帶來的破壞力將不容忽視，甚至應預期PNT功能中斷後的各種連鎖效應。政府高層與海事當局不僅需瞭解相關風險與威脅影響範圍，也應及早擬定對策與反制之道，才能強化海事的韌性；另鑒於美國潛

註52：Garath Wimpenny et al., "Securing the Automatic Identification System : Using Public Key Cryptography to Prevent Spoofing Whilst Retaining Backwards Compatibility," Journal of Navigation Vol. 75, No. 2, 2022, pp.333-345。

註53：同註21。

在對手在PNT能力上具備領先實力，有關單位更應挹注資金發展PNT強化方案與配套措施，才能提升GPS與AIS系統的防護能力。儘管將「所費不貲」，但這是攸關國家重要資產的防護，不能不做投資，否則未來一旦面臨敵人發動此類攻擊，將會毫無應變能力。

### 柒、譯後語

戰場欺敵同樣是用兵之道，從古至今亦然。科技發展本意是改善人類生活，但在人性惡念驅使下，也會朝向惡的方面發展，讓科技成為敵人欺敵的最佳工具。本文指出「定位、導航及定時」(PNT)這項科技正成為敵人在海事上的欺敵手段，其影響層面「可大可小」，小的部分可能是為展示自身能力或意在躲避追蹤、查察；大的部分則可能被用來當成發動挑釁或侵略行動之藉口。作者同時也呼籲政府與海事當局應重視相關案例的出現，及早擬定因應之道，並認為該項科技運用應納入網路安全領域管制，更不應為權責問題，而爭論不休。

鑑於我國也曾發生「臺灣國際航電公司(Garmin)」GPS訊號遭駭與「磐石號」軍艦AIS資料遭偽造事件；所以我們面對PNT武器化發展趨勢自然不能置身事外。因此，本文所提精進建議，可供我國政府

與海事單位參考，藉此強化我國海事韌性。當前有關海事的假訊息、假影片、假照片及假AIS軌跡等，往往會在網路上不斷流通，企圖混淆群眾認知，這些都是認知作戰之一環，政府與軍方都應宣導相關情事真相；另一方面，強化人民與官兵的媒體「識讀」能力，避免讓敵人以資訊操作達成目標。再者，因應這類威脅，單一國家的努力往往不夠，如何能建立國際合作機制，與友好國家共享情報、協調政策和合作研究，才能有助提高整體抵抗能力，進而確保亞太區域整體的海事安全。<sup>54</sup> 📌

#### 作者簡介：

佐里(Diane M. Zorri)為美國安柏瑞德航空大學(Embry-Riddle Aeronautical University)安全研究助理教授，並在西點軍校現代戰爭研究所與聯合特種作戰大學擔任客座研究員。

凱斯勒(Gary C. Kessler)為美國智庫「大西洋理事會」下轄「網路治國術倡議」(Cyber Statecraft Initiative)客座高級研究員，創立同名公司「Gary Kessler」(位於佛州奧德蒙海灘【Ormond Beach】)，該公司承接諮詢、研究及訓練業務；亦在「Fathom Five」公司(承接海洋數位科技服務)擔任首席顧問。

#### 譯者簡介：

劉宗翰中校，國防大學管理學院93年班、政治大學外交系戰略所碩士104年班。曾任排長、《國防譯粹月刊》主編，現服務於國防部政務辦公室暨軍事譯著主編。

註54：〈【社論】強化媒體識讀能力，反制認知作戰〉，《青年日報》，2024年2月27日，<https://www.ydn.com.tw/news/newsInsidePage?chapterID=1655087>，檢索日期：2024年6月4日。