

電磁干擾、欺騙衛星偵察、導航與通訊對 島嶼防禦的威脅與因應

曾怡碩

網路安全與決策推演研究所

壹、前言

太空中的衛星與地面接收站、控制台所構成的衛星遙測、通訊、導航已然是現代生活不可或缺的一部份，對於全球運輸、貿易、金融與傳播都具舉足輕重影響。在軍事上，無論是對地偵察亦或衛星導航及通訊，均為台灣遂行防衛作戰與韌性作為之一部。近年俄烏戰爭不時傳出陸上海馬士火箭及機場導航遭干擾事件，2025年伊朗為因應美以運用長期衛星偵照空襲其核武設施，疑似祭出干擾荷姆茲海峽航船之導航、通訊，以展示其封控之意圖。最近一次則是在2025年8月31日歐盟執委會（European Commission）主席馮德萊恩（Ursula von der Leyen）專機飛越保加利亞上空時，疑遭俄羅斯干擾其座機全球定位系統（Global Positioning System, GPS）導航訊號。

鑒於烏克蘭與伊朗兩國之地緣均為臨海接陸，倘若以島嶼防禦角度而言，電磁干擾威脅會如何衝擊影響類似台灣的環海島嶼對太空資產的運用？又，島嶼防衛又能如何因應是類威脅？有鑒於此，本文藉由文獻分析方法，在簡短說明電子戰對於太空衛星與地面站的影響渠道之後，緊接探討電磁頻譜作戰對於太空衛星與地表島嶼收發感知設施，在偵察、導航、通訊之可能干擾與偽造欺騙等攻擊手段，¹以及相對的因應政策、投資與措施，冀能對敵方之太空資產

¹ 針對太空資產，電子戰手段通常包括干擾與偽造欺騙，故將欺騙一併討論。另針對太空資產還可施行網路戰手段，本篇著眼電子戰手段，於此不予討論。詳見：杜貞儀，〈全球衛星導航系統的威脅與因應〉，《國防情勢特刊》第10期，2021年7月5日，<https://reurl.cc/WOWjXy>。

遂行主動防禦，並藉由重複多重備援韌性建置，有效建構相對之嚇阻與防禦力。

貳、電磁干擾與偽造欺騙太空資產樣態

太空衛星不論遙感偵照、通訊傳播還是定位導航計時，與地面之間的控制站以及接收站均有訊息傳遞，分別為從地面站向衛星傳輸數據的上行鏈路（uplink）和從衛星向地面站傳輸數據的下行鏈路（downlink），這些鏈路在預定的頻段上運行，星系衛星之間可能還有無線電波或者光學的通聯。²囿於太空與地面距離遙遠及大氣條件（如雨、霧、電離層效應）的影響之不可抗限制因素，訊號抵達接收器之前多已衰減甚多，因此讓上行鏈路接收的衛星或下行鏈路接收之管控站或接收站容易成為惡意勢力遂行電磁干擾（jamming）或欺騙（spoofing）的目標。

干擾是故意以射頻（Radio Frequency, RF）訊號試圖屏蔽合法衛星訊號的接收——如用噪聲屏蔽接收器，或是破壞接收器運作的頻譜環境。干擾攻擊的有效性和可偵測性通常取決於干擾射頻訊號的特性，常見的干擾樣態包括：以單一頻率的恆定訊號有效瞄準特定頻段的連續波（Continuous Wave, CW）干擾、可隨時間改變頻率並破壞更寬頻訊號並繞過靜態濾波器的掃頻干擾（Chirp or Swept Jamming）、同時屏蔽多個訊號的雜訊干擾（Noise Jamming）以及間歇性高能量突發的脈衝干擾（Pulsed Jamming）。³

遭受干擾的脆弱性則可視距離與數量而定，若以高軌道同步通

² Tim Fountain, 〈太空電子戰概觀〉,《翔宇科技》,2023年7月14日, <https://www.eagletek.com.tw/event-details/tai-kong-dian-zi-zhan-gai-guan>。

³ Will Thornton, 〈什麼是全球導航衛星系統干擾(GNSS Jamming)?〉,《吉康科技》,2025年7月11日, <https://www.gcomtw.com/mailshot/Spirent/GSS7000/2508GNSSJamming/2508GSS7000.html>。

訊或區域定位衛星而言，以 3 萬 6 千公里高度而言僅需三顆即可達全球覆蓋，而全球導航衛星系統（Global Navigation Satellite System, GNSS）理論上 3 顆可運作、⁴數學驗證上則須 5 顆方可達精準定位。⁵但相對於低軌通訊與偵察衛星、中軌道定位導航衛星，同步通訊、偵察、定位衛星與距離地面也更為遙遠，囿於電子攻擊能量限制，因此如干擾目標為特定區域內的地表接收站與空中、海上、地面機動或固定使用端，多選擇在特定頻率範圍內以屏蔽手法，達到干擾接收端上行鏈路傳遞與接收下行鏈路的目的。若針對通常位於中軌運行 GNSS 進行干擾，則除了干擾接收端上行鏈路傳遞與接收下行鏈路，也可選擇直接干擾衛星，達到阻止目標獲取定位、導航和授時資訊。⁶

偽造欺騙（spoofing）則是透過發射或注入假訊號以騙過接收端，因此可能依據射頻能量與距離，針對地表接收端發射或者注入頻譜接近的混淆射頻，將假的識別、位置與時間取代正確資訊，癱

⁴ 「……全球導航衛星系統係透過與地面接收器的通訊來計算精確位置，其運作原理基於三角測量法，該方法利用至少三顆衛星的已知位置和發送的訊號來確定接收器的位置；每顆衛星會發送一個帶有時間標記的訊號，接收器會測量這些訊號抵達的時間差，並根據光速計算接收器與每顆衛星之間的距離，當接收器獲取來自三顆或更多顆衛星的距離數據後，透過幾何計算得出其在地球上的確切位置；如果有第四顆衛星的訊號，接收器還能進一步修正時間誤差，提高定位的準確度；這種方法廣泛應用於導航、地理測繪、精準農業以及許多工業領域，以確保精準且可靠的定位服務。」引用自：〈全球導航衛星系統（GNSS）發展與未來趨勢〉，《奧創矽統科技有限公司》，2025 年 2 月 15 日，https://www.ultrontek.com/news_detail/global-navigation-satellite-system-trends。

⁵ 「……GPS（全球定位系統）技術是利用衛星發射的無線電信號搭配精準的原子鐘，提供位置和時間的資訊。導航裝置（例如手機）根據一顆以上衛星接收信號的傳輸飛行時間（time of flight）來計算距離，從而做到定位。由於接收裝置的內建時鐘不如原子鐘精準，使得百萬分之一秒的時間誤差，可能導致 300 公尺的位置偏差。因此，GPS 問題不僅是空間定位問題，也是時間定位問題。……一直以來，業界普遍認為至少需要 4 顆衛星才能解決 GPS 精準定位問題。……現今，荷蘭恩荷芬理工大學（Eindhoven University of Technology, TU/e）的布廷（Mireille Boutin）和德國慕尼黑工業大學（Technische Universität München, TUM）的肯佩爾（Gregor Kemper）證明：1、如果視線中的衛星少於 3 顆，GPS 導航沒有可信度可言。2、4 顆衛星時，獲得唯一解的概率約為 50%。3、5 顆（以上的）衛星才可在幾乎所有情況下，唯一確定接收位置。」引用自：〈數學家證明：五顆衛星才能精準導航〉，《科學人》，2024 年 12 月 17 日，<https://www.scitw.cc/posts/20241217-17673>。

⁶ 同註 2。Tim Fountain，〈太空電子戰概觀〉，《翔宇科技》，2023 年 7 月 14 日，<https://www.eagletek.com.tw/event-details/tai-kong-dian-zi-zhan-gai-guan>。

癱導航與目獲系統。⁷不同於阻斷訊號的干擾作為，偽造欺騙（spoofing）則是透過發射或注入假訊號以騙過接收端，使接收端接收標記與回報錯誤的時間與位置，不僅影響導航、航管協調、監視系統，還會進一步導致整個態勢感知的錯亂。⁸

參、電磁干擾欺騙太空資產對島嶼防禦的威脅與局限

一、太空資產與島嶼防禦

島嶼四面環海，倘若軍需、糧食與能源仰賴進口，即有遭致封鎖之風險。更重要的是，在面對敵封控供應生命線之際，除須獲知敵部署動態以調整安全航道與護航布置，還須提防對外聯繫之大宗載具海底纜線具有遭致敵惡意切斷的潛在可能。因此，太空中的偵察衛星與通訊衛星、加上地面固定與機動接收、轉換設施作為島嶼防禦必要或備援手段，其重要性不言可喻。

二、電磁干擾太空資產對島嶼防禦的影響

島嶼防禦若從衝突升級進程而言，電磁干擾太空資產除了前述封控階段的隔絕對外通訊、增加布建與護航困難度之外，倘若偵照衛星遭到上行或下行干擾，將不易掌握敵方集結動態，從而限制防守方因應行動進程，除可能因此無從佐證信號情報與人員情報，也可能因此喪失先制打擊集結船團的時機。其次，對於集中火力殲敵於渡海登陸前或殲登陸敵軍於灘際，倘若導引防守方的攻擊無人機蜂群、攻船飛彈及精準長程火箭的導航計時衛星遭遇干擾，恐將因為失去準頭而無法殲敵造成海峽煉獄或海灘煉獄景況。最後，一旦敵軍登陸與守軍陸戰或城鎮戰，在干擾太空資產之外，製造欺騙信號讓防守方軍民無所適從，將助於製造不確定與恐懼氛圍，加速消耗防守方民心士氣與抵抗意志。

⁷ Jakub Steiner，〈探討航空領域中的 GNSS 偽造攻擊脆弱性〉，《吉康科技》，2025 年 8 月 19 日，<https://www.gcomtw.com/mailshot/Spirent/GSS7000/2509GNSS/2509GSS7000.html>。

⁸ Jakub Steiner，〈探討航空領域中的 GNSS 偽造攻擊脆弱性〉。

三、電磁干擾太空資產對於島嶼作戰之侷限

電磁干擾欺騙太空資產之功率決定於頻譜、電力、距離與方位，對於攻島作戰而言，難度相對較陸地作戰高出甚多。即使是在太空軌道中迫近防守方所運用之偵照或通訊衛星，仍顯高難度且難以持久。若要從海中或空中干擾防守方於島嶼中部署之固定或機動接收裝置，必須冒險接近目標，倘若要具相當功率得以在一定範圍外遂行電戰干擾遮蔽，則自身勢必在外觀尺寸與電波探測上都是明顯目標而易於戰時遭攻擊摧毀。另一方面，如果借鑒烏克蘭「蜘蛛網」無人機攻擊事件，在俄羅斯境內以貨櫃車機動至所暗藏無人機攻擊半徑內對目標發動攻擊時，並以俄境內之網路進行進行指管及回傳畫面，接續進行戰果評估與心戰宣傳。⁹如果是以陸上部署或以掛載電戰夾艙之大型無人機遂行電戰干擾，鑒於在台灣可施展電戰干擾的選擇有限，陸上部署易遭偵測予以破壞，運用空中無人機則限於奇襲前置攻擊干擾，或者在島嶼周遭甚至島內預先部署大量電戰無人機，否則也將是難以為繼。

肆、結語：因應建議

島嶼防守方的預置或者因應作為也會減弱攻擊方干擾作用，甚至使之失效。關鍵在於多軌道多層次布建導航、監視、偵察、通訊衛星體系，建立國際與國內公部門與私部門合作夥伴關係，並通過國際專業組織渠道，最大化太空資產韌性，讓敵電戰干擾效果折扣或者難持續，達到消耗敵軍令其電戰打擊失去預期作用的目的。

在公私協力運用國際組織部分，我國交通部通過成立民間的「國際電信開發股份有限公司（ITDC）」名義加入專事以衛星進行

⁹ 蔡鏡銘，〈烏克蘭「蜘蛛網」的密技〉，《中時新聞網》，2025年7月15日，<https://tw.news.yahoo.com/%E7%83%8F%E5%85%8B%E8%98%AD-%E8%9C%98%E8%9B%9B%E7%B6%B2-%E7%9A%84%E5%AF%86%E6%8A%80-201000085.html>。

搜救的組織 Cospas-Sarsat，由該公司結合交通部航港局、運安會以及漁業署參與國際衛星輔助搜救系統運作，除了在低軌衛星遭受干擾與遞延時，得以運用中軌衛星進行更加即時的定位更新，有效縮短搜救時間及提升搜救效率，另藉由中軌衛星搜救系統即可透過國際合作模式建立良好的搜救互助機制，確保海空運輸的安全。¹⁰

最後，在軌道部署上，日本作為島國，其做法值得我國因應參考。在通訊衛星方面，除運用美國 Space-X 的星鏈低軌衛星外，為因應日益複雜的戰場通訊與衛星干擾風險，日本防衛省除在過去 X 波段外，導入 Ka 波段以添韌性之外，還提出建構「多層次通訊體系」，部署高空平台作為即時通訊備援，並整合低軌、中軌、高軌同步等多軌道星座體系。¹¹此外還在準天頂軌道部署多枚自力發展的準天頂衛星（QZSS），而且該衛星還配備光學使其成為軌道中的太空防禦感知平台。在偵察衛星方面，日本除運用準天頂同步軌道的 QZSS，還要包括眾多日美共同構建的低軌衛星星座。

本文作者曾怡碩為美國喬治·華盛頓大學政治學系博士，現為財團法人國防安全研究院網路安全與決策推演研究所副研究員。主要研究領域為：軍隊與網路安全、兵推設計、認知作戰、中國數位監控。

¹⁰ 〈航港局中軌道衛星輔助搜救系統獲國際搜救組織正式驗測通過 有效提升搜救效能〉，《交通部航港局》，2022 年 12 月 8 日，<https://www.motc.gov.tw/ch/app/data/view?module=news&id=14&serno=202212080003#>。

¹¹ 蘇治宏，〈日本衛星產業加速發展，迎戰新興商業需求〉，《科技新報》，2025 年 5 月 7 日，<https://technews.tw/2025/05/07/japans-satellite-industry-accelerates-development-to-meet-emerging-commercial-needs/>。

Threats and Countermeasures of Electromagnetic Interference and Satellite Deception to Island Defence, Navigation, and Communications

Yisuo Tzeng

Division of Cyber Security and Decision-Making Simulation

Abstract

The electromagnetic spectrum has evolved from a military support function to the decisive battlespace of modern warfare. As commercial 5G/6G deployment and IoT proliferation saturate available frequencies, the traditional assumption of exclusive military spectrum access has become untenable. The Russia-Ukraine War demonstrates this reality: Ukraine's monthly loss of 10,000 drones due to jamming has catalyzed the development of "spectral maneuver" concepts integrating emission control, tactical coordination, and dynamic frequency management.

This article examines spectrum operations across three dimensions: technological competition driven by AI-enabled spectrum management outpacing military acquisition; operational innovation exemplified by U.S. EMBM-J and NATO DIANA initiatives transforming spectrum management from static allocation to dynamic maneuver; and geopolitical contestation where China's spectrum standardization efforts systematically challenge NATO interoperability.

Drawing on Ukraine's battlefield experience and analyzing NATO innovation mechanisms, the study argues that spectrum superiority requires accelerated dual-use technology integration, coordinated allied action in international regulatory forums, and investment in cognitive radio and AI-driven management systems. In an era where electromagnetic dominance determines operational capability, spectrum superiority has

become the prerequisite for all-domain operations and the decisive factor in strategic competition.

Keywords: Space Electronic Warfare, Island Blockade, Electromagnetic Interference and Deception, Satellite Communications, Navigation, Reconnaissance