全球衛星導航系統的威脅與因應

杜貞儀

網路安全與決策推演研究所

壹、前言

全球衛星導航系統（Global Navigation Satellite System, GNSS）以覆蓋全球的衛星系統，透過通訊技術對全球各地提供即時且高精度的定位、導航及定時（Position, Navigation and Timing, PNT）服務。GNSS 技術發展以軍事用途為核心，但逐步拓展至民用領域。以美國之全球定位系統（Global Positioning System, GPS）為例，原先任務即是對美軍全球部署提供即時 PNT 服務，第一次波灣戰爭即是 GPS 首次大規模實戰運用，包括盟軍以 GPS 導航定位在沙漠中快速移動至戰術位置，由伊拉克軍未預料的翼側進攻；及以「聯合直接攻擊彈藥」（Joint Direct Attack Munitions, JDAM）等精準打擊彈藥（precision-guided munitions）展現其「如外科手術般精準」的打擊威力，而後採用 GPS 作為導引方式的類似武器不斷改良、精進。[1] 時至今日，GPS 幾乎是無處不在。美國防部 2000 年移除 GPS 系統民用訊號的選擇性提供（Selective Activity），不再針對民用訊號添加誤差、限制其精度範圍，民用的導航與定位等應用服務也因此得以快速增長。

由於軍民兩方對 GPS 的依賴，美國防部先進研究計畫署（DARPA）已將 GPS 視為「單點障礙」（single point of failure），一旦失效，其影響將難以估計。[2] 加上近年來軟體定義無線電

[1] Larry Greenemeier, “GPS and the World’s First “Space War”,” *Scientific American*, February 8, 2016, https://www.scientificamerican.com/article/gps-and-the-world-s-first-space-war/; “The JDAM Revolution,” *Air Force Magazine*, September 1, 2006, https://www.airforcemag.com/article/0906jdam/..

[2] Connie Lee, “DARPA Pursuing Global Positioning System Alternatives,” National Defense, May 31, 2018, https://www.nationaldefensemagazine.org/articles/2018/5/31/darpa-pursuing-global-positioning-system-alternatives.

（software-defined radio）普及，訊號生成相關軟硬體均能輕易取得，使干擾 GPS 訊號的成本大為降低，全球各地已發現多起干擾案例，不僅對航行、飛行安全形成威脅，也揭示即時、穩定、精確且無所不在的 PNT 服務，可能已不再是理所當然。

部分國家基於 GPS 仍為美軍所控制為由，為掌握技術主導權、或在衝突發生時保有作戰所需的 PNT 服務，便發展自有 GNSS 系統。其中以提供全球服務為目標者，包括俄羅斯的格洛納斯系統（GLONASS）、歐盟的伽利略定位系統（Galileo）和中國的北斗系統（Beidou, BDI）。但具備此技術能量備援的國家僅為少數，對於其他國家而言，為減少可能衝擊，實需採行降低風險作為，並在 GPS 可能中斷的情況下，預擬 PNT 服務及相關系統的持續運作方案。

因此，本文將藉由介紹 GNSS 系統組成 PNT 服務的應用範圍，評估威脅來源，並就已知威脅案例與近期替代方案發展，瞭解現行的因應作為，以對未來可能的改善方向提供建議。

貳、無處不在的GNSS系統

GNSS 系統架構各異，但基本組成均包含太空（衛星）、地面控制與使用者三大單元（見圖一）。以 GPS 為例，目前太空（衛星）單元包括至少 24 顆中地球軌道（Medium Earth Orbit, MEO）衛星，軌道高度大約為兩萬公里，持續向地球發射電磁波訊號。衛星在民用訊號共有 L1 A/C、L2C、L5 及 L1C 四種不同訊號，並接受來自地面控制單元的操作指令。

地面控制單元則是由地面監控站、地面天線傳輸站以及主控中心所構成（見圖 1）。地面監控站追蹤並監控衛星訊號，回傳至位於美國科羅拉多州的施里弗空軍基地（Schriever AFB）主控中心，計算衛星軌道資料再上傳至衛星更新。使用者單元則是 GPS 接收器，將接收到的 GPS 衛星訊號換算成位置、速度與時間。

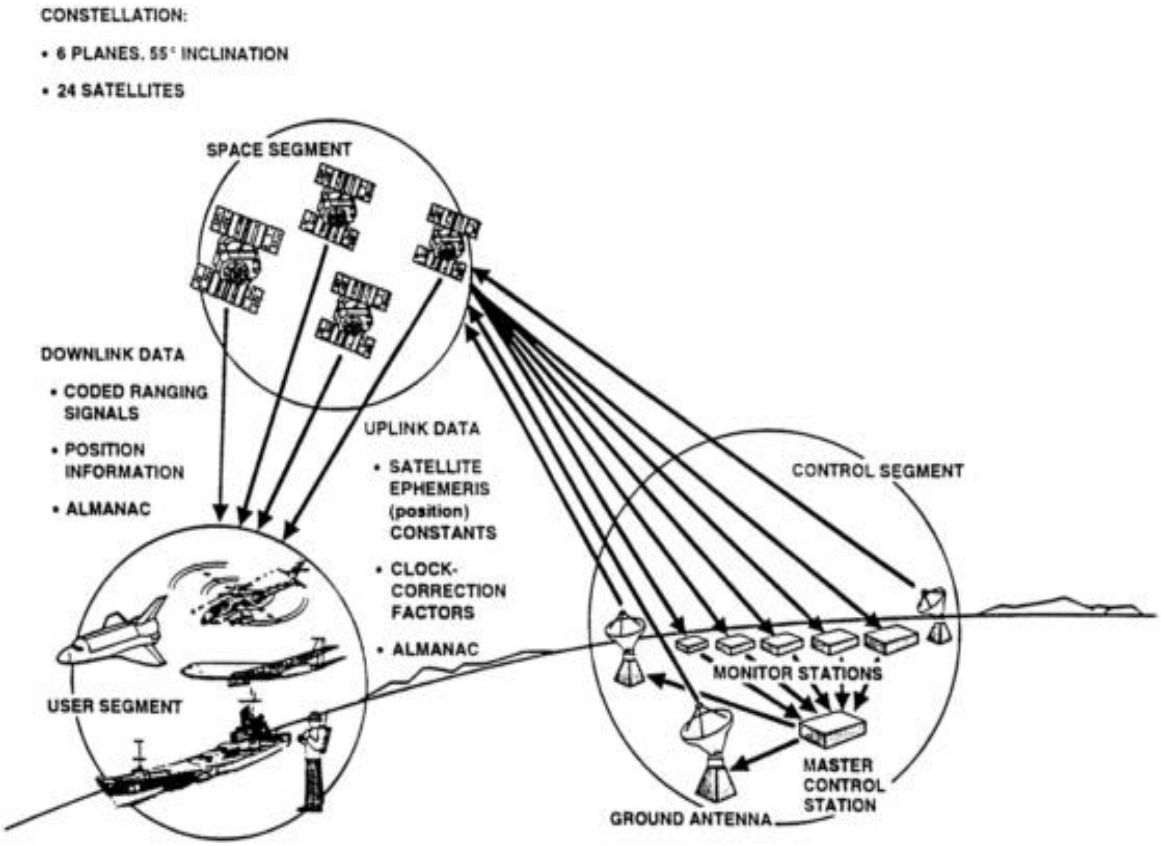

圖 1、GPS 系統基本組成示意圖

資料來源：Aerospace Corporation

基於 GPS 的工作原理，每顆 GPS 衛星皆必須在時間上完全同步，才能進行精確定位，因此在每顆 GPS 衛星上，均有至少各兩座銫/銣原子鐘，提供準確的時間與頻率訊號，又因所接收到的訊號須經過換算，GPS 接收器實際上可視為一台小型電腦，而非被動的接收訊號。若在地球上同一位置接收到三顆 GPS 衛星訊號，即能透過其訊號到達時間差進行定位，若增加至四顆，還能進一步推算出高度。[3]

在 GPS 提供的服務中，定位、導航兩項直接提供地理空間資訊，較為人所知，但定時服務的影響範圍更深遠。許多關鍵基礎設施如通訊、運輸、電網、金融等，均依賴 GPS 提供準確時間，成為「不可見的公共設施」(invisible utility)。就以網路服務的資料中心

[3] Alain L. Kornhauser, "Global Navigation Satellite System (GNSS)", in course material of *ORF 467: Transportation Systems Planning and Analysis (Fall 2007)*," https://www.princeton.edu/~alaink/Orf467F07/GNSS.pdf.

來說，連網裝置和雲端應用將各種資料整合至相互連結的資料中心，以加速各地的資料存取與交換。為了讓各地資料能有效同步，所有裝置和伺服器均需透過網路時間協定（Network Timing Protocol, NTP）與時間伺服器（time server）對時，而此伺服器則再藉由 GPS 接收器所收到、換算之衛星訊號進行校正，確認所有裝置資料時間一致、各地資料均是最新、一致的版本。換言之，雲端服務的實現，是以定時作為基礎。

另外一個常見例子，則是金融服務的時間戳記，也就是進行股票、期貨等交易時的重要依據。[4]尤其近年在金融市場中，以自動化之高頻交易賺取價差相當盛行，要求時間精度達毫微秒（nanosecond）之譜。若無 GPS 校正後之精準時間，則此交易模式將無法維繫。因此，預期未來使用 GPS 提供之校時服務的設備有增無減的情況下，其潛在威脅層面亦隨之擴大。

參、定位、導航、定時服務威脅評估

根據其特性，對 GNSS/PNT 的威脅約有三種類型。首先是不經意造成的中斷，如太陽風暴、閏秒（leap second）、設備維護意外等，多半發生於 GNSS 太空單元及地面控制單元，以 GPS 而言，此二者均為美國政府的權責範圍。蓄意造成的中斷發生在使用者單元，包括 GPS 干擾（jamming）及欺騙（spoofing）兩種，有時混合採用；再來則是系統層級的攻擊，包括網路攻擊、惡意軟體、以及供應鏈攻擊等，針對 GPS 接收器本身或是藉由外部聯網環境進行攻擊。[5]以下對蓄意中斷的各項類型進行簡要介紹：

[4] Rohit Braggs, "How resilient PNT protects global networks from attack or failure," *GPS World*, June 24, 2019, https://www.gpsworld.com/how-resilient-pnt-protects-global-networks-from-attack-or-failure/.

[5] Ernest Wong, "Responsible Use of PNT for DLT in the Financial Service Sector," *GPS.gov*, January 28, 2020, https://www.gps.gov/multimedia/presentations/2020/ATIS/wong.pdf; "Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure," Department of Homeland Security, 2020, https://us-cert.cisa.gov/sites/de

一、GPS干擾

干擾指蓄意製造無線電波增加雜訊，繼而影響 GPS 接收器的訊號處理，達成降低或阻絕（degrading or denying）接收器正常運作的效果。雖然這些干擾有部分源於 GPS 訊號微弱，容易受到太陽黑子活動、電離層以及其他訊號影響，但在 2009 年以英國領港公會（Trinity House）所屬船隻 Galatea 號進行的一項測試顯示，船上一支功率僅有行動電話千分之一的裝置，就足以在電子海圖上顯示錯誤的船位，進而顯示至附近航行船隻的自動辨識系統上，並且使船上救生系統失效，電羅經、雷達也都受到影響。不過，直接進行干擾會出現明顯的訊號源，各項儀器突然失去功能，很難不引人注意而引發警訊。[6]

但在部分區域，針對 GPS 的干擾顯然已經成為新常態。挪威北部靠近芬蘭及俄羅斯邊境的芬馬克地區（Finnmark），自從2017年始便時常發生 GPS 干擾，使通信和導航系統無法運作。特別是該區地處偏遠，許多居家醫療設施、緊急救濟服務及救護車都仰賴 GPS 地圖，GPS 干擾很可能會使面臨急難的民眾無法得到及時支援。雖然挪威情報單位分析顯示，北約在 2018 年於挪威舉行冷戰結束以來最大規模之軍事演習—「三叉戟聯合軍演」（2018 Exercise Trident Juncture）期間，針對該區域的GPS干擾比前期明顯增加（見圖2），推論干擾可能與演習有關。但該區警長則認為，此種干擾可能有各種成因，包括俄羅斯在北極圈內日益增加的軍事演習活動，但多年來，干擾持續發生，應非針對特定事件，而是企圖造成一個 GPS 無

fault/files/documents/Improving_the_Operation_and_Development_of_Global_Positioning_System_%28GPS%29_Equipment_Used_by_Critical_Infrastructure_S508C.pdf.

[6] Alan Grant, Paul Williams, George Shaw, Michelle De Voy & Nick Ward, "Understanding GNSS availability and how it impacts maritime safety," *Paper for International Technical Meeting of the Institute of Navigation*, January 24-26, 2011, https://rntfnd.org/wp-content/uploads/GNSS-Maritime-GLA.pdf.

法使用的新常態，迫使該區居民必須仰賴羅盤與紙本地圖。[7]

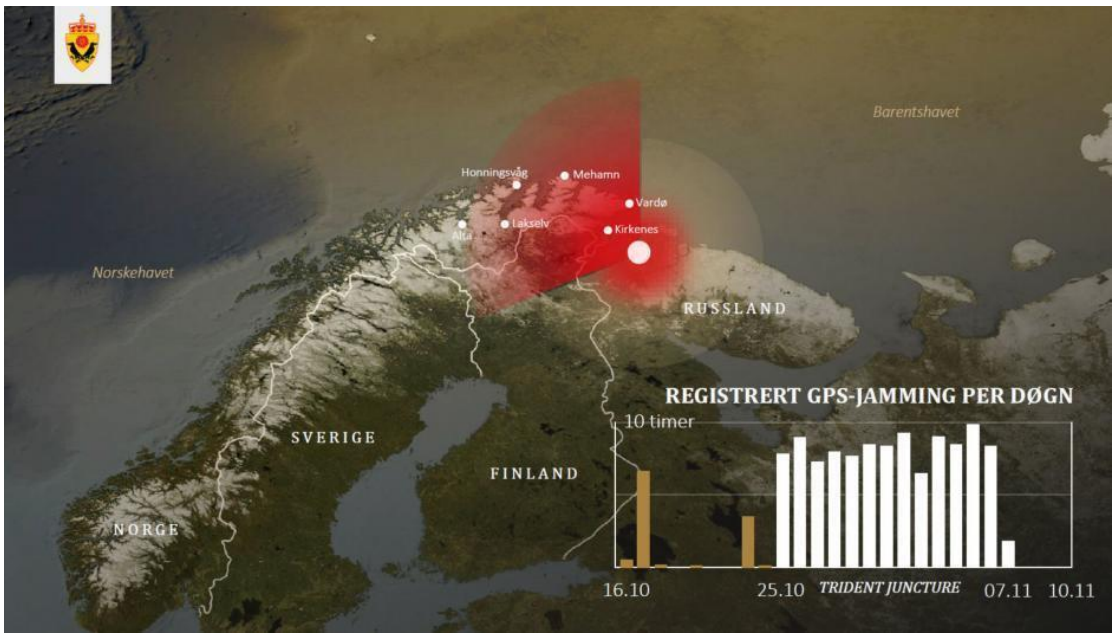

圖 2、北約「三叉戟聯合軍演」期間 GPS 干擾情形

圖片來源：挪威情報局

二、GPS欺騙

欺騙則是刻意製造假訊號以擾亂 GPS 系統，又可分量測欺騙（measurement spoofing）和資料欺騙（data spoofing）兩種。量測欺騙指偽造波形與真實 GPS 訊號類似的無線電波，使目標 GPS 接收器換算出錯誤的位置、速度與時間資訊。資料欺騙則是直接於目標 GPS 接收器引入偽造之數位資料進行換算。但無論何種欺騙形式，均可能對 GPS 造成從產生錯誤資料至接收器故障等多種影響。[8]

此種威脅並不僅限於 GPS，具相同工作原理之其他 GNSS 均有可能受影響。自 2016 年始，在世界各地的港口均有發現針對衛星定

[7] Peter B. Danilov, "GPS Jamming Still Causing Problems in Finnmark," *High North News*, November 19, https://www.highnorthnews.com/en/gps-jamming-still-causing-problems-finnmark.

[8] National Cybersecurity & Communications Integration Center, National Coordinating Center for Communications, "Improving the Operational and Development of Global Positioning System (GPS) Equipment Used By Critical Infrastructure," U.S. Department of Homeland Security, https://us-cert.cisa.gov/sites/default/files/documents/Improving_the_Operation_and_Development_of_Global_Positioning_System_%28GPS%29_Equipment_Used_by_Critical_Infrastructure_S508C.pdf.

位導航的欺騙狀況。美國智庫 C4ADS 藉由其他民用衛星之 GNSS 訊號資料進行分析，發現至 2018 年 11 月止，在黑海附近有超過九千起船舶被定位至機場的案例，因而形成不正常的移動軌跡（圖 3）。此現象很可能是俄羅斯以電戰手段於境內、克里米亞等地，針對 GNSS 訊號進行欺騙。如此做法可能出於幾項原因，如保護重要人士出訪時不受未知無人機攻擊的威脅、重要政府機關防護、以及保護海外作戰基地等。[9] 種種行為均顯示，俄羅斯不吝於展現其電戰能力，並且持續將此用於海內外的各種場景中。

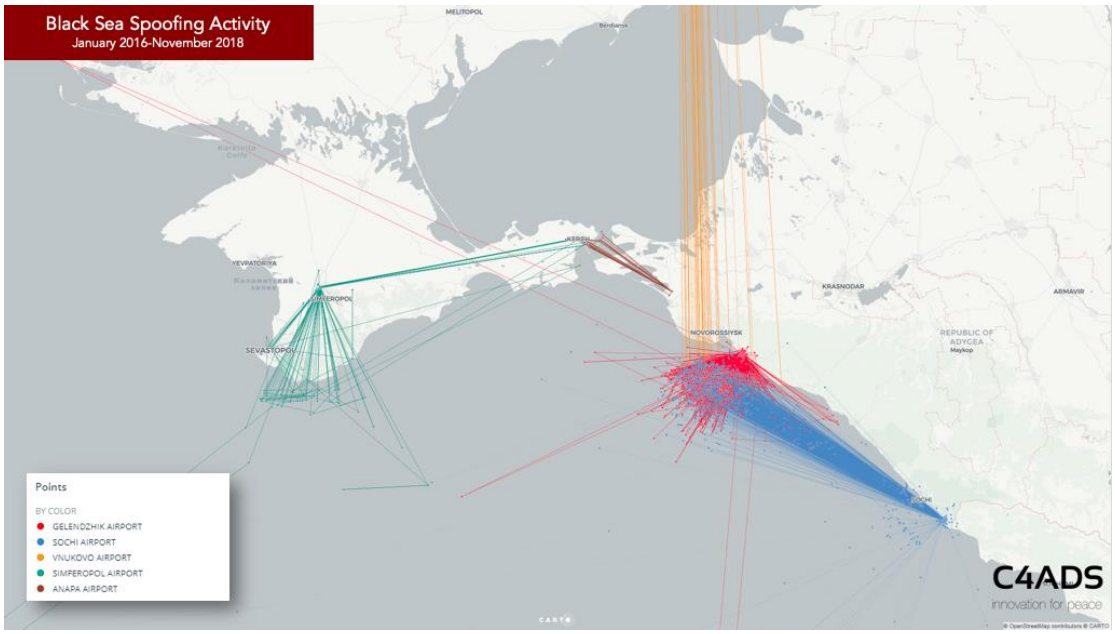

圖 3、黑海附近的 GNSS 欺騙狀況

圖片來源：C4ADS

三、系統性攻擊

針對 GPS 接收器的系統性攻擊，包括網路攻擊、惡意軟體、以及供應鏈攻擊等，以往並非 GPS 威脅所關注的重點，但 2020 年 8 月，GPS 裝置與服務大廠台灣國際航電（Garmin）遭勒索軟體攻擊，顯示除了訊號干擾與欺騙外，GPS 接收器作為小型電腦，傳統

[9] "Above Us Only Stars: Exposing GPS Spoofing in Russia," C4ADS, 2019, https://www.c4reports.org/aboveusonlystars.

網路安全的議題也應受到重視。[10] 在 Garmin 事件中，對方僅要求贖金，但已凸顯 GPS 相關服務的脆弱，容易攻破，亦有可能自內部破壞系統與資料完整性，造成更進一步的損害。

就定時而言，網路上的設備透過網路時間協定（Network Timing Protocol, NTP）與時間伺服器對時，此一協定亦有漏洞，攻擊者能藉此發送放大的流量，形成分散式阻斷攻擊（DDoS）癱瘓目標網路服務。[11] 而網路設備韌體設計缺陷，亦可能使單一時間伺服器以 NTP 重複查詢而癱瘓，使與其相接的 GPS 接收器的校時資料，無法透過網路提供服務。因此網路設備的供應鏈安全，也是維持定時服務的一項重點。[12]

肆、GPS威脅之風險管理與替代方案

由以上實例可以看出，針對 GNSS 的威脅已經相當普遍，並不僅限於 GPS。近期改進並部署之 GPS III，在軍用碼（M Code）亦已提升其抗干擾能力。[13]美國國家標準和技術研究院（National Institute of Standards and Technology, NIST）為協助 PNT 服務供應與使用者評估自身風險，提高維運韌性，提出基於網路安全框架（Cybersecurity Framework, CSF）的《NIST 基礎 PNT 剖析》（*NISTIR 8323 Foundational PNT Profile*），從 CSF 五大構面—識別、保護、偵測、回應與復原（Identify, Protect, Detect, Respond and Recover）來評估風險，並提供落實風險管理的行動目標。[14]

---

[10] Brian Barrett, “The Garmin Hack Was a Warning,” *WIRED*, August 1, 2020, https://www.wired.com/story/garmin-ransomware-hack-warning/.

[11] “NTP amplification DDoS attack,” Cloudflare, https://www.cloudflare.com/zh-tw/learning/ddos/ntp-amplification-ddos-attack.

[12] 此為 2006 年丹麥網路管理者與台灣友訊科技之爭議，詳見 John Leyden, “D-Link settles dispute with ‘time geek’,” *The Register*, May 11, 2006, https://www.theregister.com/2006/05/11/d-link_time_dispute_settlement/。

[13] Theresa Hitchens, “GPS Anti-Jam M-Code Takes Two Steps Forward,” *BreakingDefense*, August 7, 2020, https://breakingdefense.com/2020/08/gps-anti-jam-m-code-takes-two-steps-forward/.

[14] “NISTIR 8323 Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services,” National Institute of Standards and Technology, February, 2021, https://csrc.nist.gov/publications/detail/nistir/8323/fin

表 1、《NIST 基礎 PNT 剖析》評估項目與目標

CSF 項目	目標
識別（Identify）	● 識別企業/營運環境及組織任務 ● 識別所有資產，包括依賴 PNT 資料的各項應用 ● 識別提供 PNT 資訊的來源與基礎設施 ● 識別可能造成具體威脅的弱點、威脅與衝擊以評估風險
保護（Protect）	● 保護組成、傳輸與運用 PNT 資料的系統，基於應用需求支持所需之完整性、可用性與保密性（integrity, availability and confidentiality） ● 透過依從資安原則，包括了解 PNT 來源、資料等各種訊息的基本特性與服務、管理系統開發生命週期、以及部署所需之訓練、授權與接取控制來保護 PNT 服務部署與運用 ● 透過認證的回應與復原計畫，在可能產生威脅的情境下，保護仰賴 PNT 的用戶與服務，以維持足夠營運層級 ● 就企業與營運需求，保護仰賴 PNT 服務與資料的組織
偵測（Detect）	● 透過監控與持續檢查確保偵測進行 ● 建立部署與處理偵測之異常與事件的處理程序
回應（Respond）	● 以經認證之回應步驟控制 PNT 事件 ● 與 PNT 資料用戶、應用與利益攸關者溝通 PNT 資料事件的發生及其影響 ● 發展回應與減低已知或預期威脅及/或弱點的程序 ● 基於來自事件的經驗逐步發展回應策略與計畫
復原（Recover）	● 以經認證之復原步驟將依賴 PNT 服務之系統回復至適當的工作狀態 ● 與 PNT 資料用戶、應用與利益攸關者溝通 PNT 服務復原行動與住況 ● 基於來自事件的經驗逐步發展復原策略與計畫

資料來源：作者整理自 *NISTIR 8323 Foundational PNT Profile*

《NIST 基礎 PNT 剖析》也建議使用 PNT 服務的單位，將替代 PNT 來源整合進企業架構，確保在 PNT 服務中斷時，可進行故障轉

al.

移（failover）持續運作。對於各種仰賴 GPS 進行定位、校時等服務的關鍵基礎設施而言，整合 GPS 替代方案（GPS Alternative）以提升服務韌性，已經是刻不容緩的任務。在軍事應用部分，美國 DARPA 在近十年曾就各種替代方案進行研究。[15]而美陸軍為了在未來大國競爭下的大規模作戰行動中，保有 PNT 運作，取得資訊及決策的雙重優勢，已於 2020 年 9 月成立 PNT 現代化專案辦公室與研究室，尋求如以偽衛星（pseudolite）小型地面收發站建立區域定位系統等方式，來降低目前對 GPS 的依賴。[16] 民用系統部分，由於科技進展使舊有羅遠系統（Long Range Navigation, LORAN）有新的突破，成為可靠、安全的 GPS 替代方案。

羅遠以地基無線電發射站為基礎，運用雙曲線進行定位以導航，並在後續持續演進至第三代 LORAN-C。尤其技術改進後的增強式羅遠系統（enhanced LORAN, eLORAN，以下簡稱「e 羅遠」），誤差約可達 10 公尺以內，工作範圍則約達 2,200 公里，並且使用 90 至 110 千赫的低頻段，運用地面發射站其訊號強度可達 1 百萬瓦，大大提高訊號干擾所需功率，不僅提升干擾難度，亦能提供無人載具應用，改善因 GPS 訊號太弱無法定位的問題。[17]

若將 e 羅遠系統各站點以光纖連結，並結合 IEEE 1588-2008 精確時間協定（Precision Time Protocol, PTP），即可形成分散且不易受無線電波干擾的 PNT 服務網路。[18] 目前已有許多國家進行類似的 e

[15] "Adaptable Navigation Systems (ANS) (Archived)," DARPA, 2017, https://www.darpa.mil/program/adaptable-navigation-systems; "Micro-Technology for Positioning, Navigation and Timing (Micro-PNT) (Archived)," DARPA, 2017, https://www.darpa.mil/program/micro-technology-for-positioning-navigation-and-timing.

[16] Caitlin O'Neill, "Beyond GPS: PM PNT team test Pseudolite characterization and performance, " U.S. Army, November 7, 2017;,Nathan Strout, "US Army launching new PNT Modernization Office and Open Innovation Lab," *C4ISRNET*, September 10, 2020, https://www.c4isrnet.com/battlefield-tech/2020/09/10/army-launching-new-pnt-modernization-office-and-open-innovation-lab/.

[17] Jeff Shepard, "eLORAN a terrestrial alternative to GPS," *MICROCONTROLLER TIPS*, October 26, 2020, https://www.microcontrollertips.com/eloran-a-terrestrial-alternative-to-gps/.

[18] Marc Weiss, Patrick Diamond and Dana A. Goward, "A Resilient National Timing Architecture," Resilient Navigation and Timing Foundation, October 16, 2020, https://rntfnd.org/wp-con

羅遠系統部署規劃，積極發展太空事業的英國，亦有 e 羅遠測試部署以分散風險。[19] 自 2010 年起 GPS 訊號曾多次遭北韓干擾的南韓，多年來持續更新維護其 LORAN-C 系統，並陸續升級至 eLORAN，其以 eLORAN 為核心技術之一的海上 PNT 服務，預計將在 2021 年 6 月 1 日開始試點，由韓國海洋警察艦艇進行測試，再陸續推廣至漁船、商船等民用船隻，以替代系統降低北韓透過 GPS 干擾造成的海上安全風險。[20]

伍、結語

由 GNSS 提供的 PNT 服務，具有廣泛的軍民應用，尤其眾多關鍵基礎設施運作，均仰賴準確的定位、導航與時間，干擾 GNSS 的潛在影響範圍極為深遠。在干擾成本已隨技術進展逐漸降低的今日，從俄羅斯近期於芬馬克、克里米亞等地的作為、以及北韓的事例可看出，透過影響 PNT 服務造成混亂，不僅能直接衝擊民眾日常生活，若在衝突情境下，可藉此大大影響敵方判斷與決策。衡量目前國際情勢，未來針對 GNSS 的威脅將有增無減，甚至亦應預期恐有服務長期中斷的新常態。為因應可能之威脅情境，使用端及服務提供者除可強化使用者單元的設計與網路安全規劃，並運用 NIST CSF 架構進行 PNT 服務風險管理、妥善使用外，政府亦可也思考以 e 羅遠等替代系統佈建 PNT 服務網路，平時與衛星系統互補，在衛星訊號因故中斷時進行備援，以降低 PNT 服務中斷所帶來的衝擊。

本文作者杜貞儀為國立臺灣大學海洋所理學博士，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助理研究員。

tent/uploads/Resilient-National-Timing-Architecture-16-Oct-2020.pdf.

[19] "UK Government Supporting E-LORAN," *MARITIMEJOURNAL*, February 16, 2018, https://www.maritimejournal.com/news101/onboard-systems/navigation-and-communication/uk-government-supporting-e-loran.

[20] Dana Goward, "South Korea partners with broadcaster on eLoran and 10-cm GPS," *GPS World*, November 23, 2020, https://www.gpsworld.com/south-korea-partners-with-broadcaster-on-eloran-and-10-cm-gps/; Lim Chang-won, "Terrestrial navigation system ready for use in S. Korea to cope with jamming and electric warfare ," *Aju Business Daily*, April 1, 2021, https://www.ajudaily.com/view/20210401091701262.

Threats to the Global Navigation Satellite System and the Response

Chen-Yi Tu

Assistant Research Fellow

Abstract

The Global Navigation Satellite System (GNSS) is a satellite system that covers the world and provides instant and high precision Position, Navigation and Timing (PNT) services to locations around the world through communications technology. The widely-use system is Global Positioning System from U.S.. Due to the high GPS dependence by both military and civilians, and fact that many critical infrastructures utilize these GPS related services, GPS has become a “single point failure” which would have profound impact when the service disrupts. With prevalence of GPS jamming, and only a few countries possessing the capability to establish indigenous GNSS as backup, risk mitigation should be in place along with formulating a continuous operation plan for PNT service in advance. This paper will discuss the threat to GNSS, including jamming, spoofing and systematic attack, by demonstrating the threat trends from recent case studies. The final part of this paper includes the risk management framework for PNT service providers and users, together with the current solution of alternative GPS.

Keywords: Global Navigation Satellite System, Position-Navigation-Timing, GPS jamming, GPS spoofing, Alternative GPS