

編輯報告

當代戰爭的面貌正在發生根本性的轉變。過去被視為軍事行動支援功能的電磁頻譜，如今已無可辯駁地演變為決定勝負的主戰場。烏克蘭前線每日因電子干擾而損失上萬架無人機的殘酷現實，到強權國家在國際標準組織中為下一代通訊頻段展開的激烈地緣政治博弈，一個清晰的結論浮上檯面：掌握並主宰此看不見的領域，就能掌握未來衝突的主動權。

本期《電磁頻譜作戰》特刊，聚集國內七位長期浸潤此領域的專家，從宏觀的戰場環境分析、特定國家的能力評估，到前瞻性的武器技術剖析，為讀者呈現一個全面、深入且具前瞻性的戰略圖像。本特刊的目標不僅是梳理現況，更是為台灣在日益複雜的電磁作戰環境（EMOE）中，探尋一條強化韌性、建立優勢的道路。

本期特刊由國防安全研究院研究員杜貞儀博士的〈複雜電磁環境下的頻譜管理與機動〉一文揭幕。該文宏觀且精闢地指出，隨著5G/6G與物聯網等商業技術的爆炸性發展，傳統由軍方獨佔頻譜的假設已不復存在；同時以俄烏戰爭為鑑，深入剖析烏克蘭如何從慘痛的戰損中，催生出「頻譜機動」的全新作戰概念，將頻譜管理從靜態的分配，轉變為整合偵、指、打、評的動態核心作戰環節。她進一步分析美軍 EMBM-J 與北約 DIANA 等創新機制，如何藉由 AI 與軍民合作，加速從「煙囪式系統」走向真正的一體化作戰，為我國應對頻譜作戰的技術與組織轉型，提供極具價值的參照。

本院研究員曾怡碩博士的〈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〉，則將電磁威脅進一步聚焦於台灣的島嶼防衛場景；本文深刻闡述島嶼防禦對太空資產（偵察、通

訊、導航衛星)的絕對依賴，並詳細分析敵方如何藉鏈路干擾與欺騙(Jamming/Spoofing)，癱瘓我早期預警、精準打擊與指管韌性，製造戰場混亂。面對此等威脅，本文務實提出以多軌道、多層次的公私協力夥伴關係，建立太空資產韌性，並借鑒日本建構準天頂衛星(QZSS)等「多層次通訊體系」的經驗，為我國指出強化太空防禦韌性的具體方向。

高志榮研究員的〈美空軍電子戰整備對我制空作戰之啟示〉，則將前述宏觀作戰概念，聚焦於制空權爭奪核心領域。該文詳盡梳理了美空軍從 EC-130H、EA-37B 到 EA-18G 等主力電戰機的性能優勢與作戰運用，並特別點出第 350 頻譜作戰聯隊如何在短時間內，完成電子戰數據的更新與回傳，成為美軍戰力倍增的關鍵。文章更務實地為我國在攻勢與守勢制空作戰中，如何規劃電子戰運用提出了具體想定，並就籌建裝備、訂定支援協議與強化情資交換等面向，提供了清晰的政策建議。

舒孝煌博士的〈美國陸軍電子戰發展現況〉一文，聚焦川普第二任期的軍事改革與部隊轉型，尤以陸軍電戰能力為核心；在美軍發布新《聯合電磁頻譜作戰》後，陸軍開始新興「多領域效應排」的實際演訓，並與多領域任務部隊在實際演訓上進行配合，同時嘗試共同投入電磁頻譜管理與運用，將電磁頻譜作戰實際與任務所有細節融合。從陸軍多領域效應營的整體能力建構，明確將多領域與新興科技納入整體作戰中心能力建構，並依此採購、獲取所需編裝以利任務進行。同時，陸軍仍在尋求新一代電戰能力，以期更明確完成多領域與複雜電磁環境下的作戰任務，並確保電磁頻譜的絕對優勢。

陳育正教授的〈俄烏戰爭後的中共海軍電子戰轉型發展之研究〉一文，則剖析共軍海軍如何視俄烏戰爭為「無聲實驗場」，從

「莫斯科號」沉沒等戰例吸取俄軍教訓，並借鏡美軍先進戰術。此轉型思維已反映於其 2024 年軍改及複雜電磁環境演訓，劍指奪取「制電磁權」以遂行體系對抗。文章結論明確，並點出此發展對我國海空指管韌性構成重大挑戰，值得深思。

外稿學者 **Pak Tin** 則精確地就高度戰略性、足以癱瘓國家的致命威脅——電磁脈衝（EMP）議題為文；在其 *A Comparative Analysis of EMP Defensive Measures of the PRC, United States, and Taiwan* 一文中，為我們進行了系統性的三方戰力評估。文章明確指出，中國在高功率微波（HPM）武器領域處於全球領先地位，並正快速擴充其高空核爆電磁脈衝（HEMP）潛力；而美雖擁有更強大的武庫與更完善的軍規防護標準，但在攸關國家命脈的民用基礎設施防護上，卻因缺乏強制性法規而面臨困境。最令人警醒的是，相較之下，台灣無論在攻擊性或防禦性 EMP 能力上，都處於最弱勢的一方，民用設施的防護標準遠不足以應對軍事級攻擊，使國家整體處於高度脆弱的狀態。

最後，本院研究員 **詹祥威** 則以〈電磁砲的百年軌跡：技術、競賽與應用〉一文，窺探未來戰爭的可能樣貌。首先該文釐清電磁砲雖屬「定向能武器」，但其運作時產生的強烈脈衝電磁干擾（IEI），使其被納入電磁頻譜管理的範疇。文章回顧美、英、中、日等國的發展路徑，點出其雖具備超高初速、遠程打擊、低單發成本等顛覆性潛力，卻也始終面臨高耗能、砲管磨損與平台整合等三大技術瓶頸。該文對比美國計畫的暫停、中國的大膽推進，及日本憑藉其材料科學優勢在砲管耐用性上取得的突破，揭示不同國家在戰略權衡與技術路徑上的差異。電磁砲的發展，預示著一場足以改變海戰「成本交換比」的深刻革命，其成敗將根本性地重塑未來的海權格局。

本期七篇專文，從不同視角共同指向一個核心結論：電磁頻譜的攻防，已成為涵蓋技術研發、作戰概念、組織架構乃至國家戰略的總體對抗。解放軍「革命性」的軍事改革，使其在理論整合上展現出強大潛力；而美軍根植於數十年實戰的「演進式改良」，則在體系韌性與人員經驗上佔有優勢。

對於台灣而言，本特刊每一頁都足具示警。對手正傾盡全力試圖在未來可能的衝突中，率先奪取「制電磁頻譜權」以癱瘓我防禦體系。面對此一嚴峻挑戰，必須以「全社會防禦」思維，將電磁頻譜韌性建設，提升至國家安全的戰略高度，並強化關鍵基礎設施防護，到建立軍民一體的頻譜協調機制；從借鑒盟邦的先進作戰概念，到務實地投資不對稱防禦技術，每一步都至關重要。

我們深信，本特刊所匯集的洞見，能為所有關心國家安全與此議題之讀者，提供堅實的知識基礎。

複雜電磁環境下的頻譜管理與機動

杜貞儀

網路安全與決策推演研究所

壹、前言

所謂電磁環境（electromagnetic environment, EME），依照目前北約國家以及美軍的準則定義，指的是資訊環境（information environment）的電磁頻譜部分，包括所有以頻率和波長為特徵的電磁頻譜輻射範圍，橫跨軍事、自然電磁輻射現象以及商用、民用領域。電磁頻譜作戰環境（electromagnetic spectrum operation environment, EMOE），則是特指在影響作戰運用的各種電磁環境條件、狀況與影響因素的綜合體，包括功率、時間分配、頻率範圍等等。高度動態的電磁頻譜作戰環境，不僅包括既存的電磁環境背景輻射，以及能夠在電磁影響區域內輻射的友軍、中立、敵對及敵方電磁系統。對電磁頻譜作戰環境的掌握，能影響戰力發揮，也同時影響指揮官決策。¹

以美國為首的北約等國，自從二戰至冷戰期間，因應需求發展出各式基於射頻無線電波應用的各式指管通情監偵系統。由於電磁頻譜連結陸、海、空、太空、網路各作戰領域，使現行各級作戰的所有層面，均仰賴看不見的無線電波，並深受電磁頻譜可用程度所影響。然而，電磁頻譜受物理限制有固定範圍，代表頻譜資源是有限的。在無線通訊應用與商用需求快速擴展下，電磁頻譜已經逐漸由政府、軍事應用專有，逐漸演變成高度擁擠受限的環境，不僅與敵方競爭，商用用戶也同樣和政府及軍事應用競爭此有限的資源。

¹ U.S. Joint Chiefs of Staff, Joint Electromagnetic Spectrum Operations, Joint Publication 3-85 (Washington, DC: Joint Chiefs of Staff, 2020).

從頻譜專有專用、到動態分享機制（dynamic spectrum sharing）與機動的概念演進與發展，更凸顯軍事部隊在高度競爭電磁頻譜環境下維持行動自由的挑戰與可能機會。

為此，本文將從文獻與近期衝突案例，探討頻譜管理概念最新演進與發展，就政策與執行面，藉由軍民共通技術促進合作、加速創新，以提升在競爭激烈且密集的複雜電磁頻譜環境下行有效機動，維護己方行動空間並拒止敵方遂行作戰的能力，並且關注在地緣政治發展下，在國際標準制定層級的下一代通訊標準競逐，可能如何影響未來作戰。

貳、頻譜管理演進與發展

一、頻譜資源有限而運用需求無限

一般來說，電磁頻譜涵蓋範圍從無線電波、微波、紅外線到紫外線與 X 射線、伽瑪射線，電磁頻譜是連續的，但受限於材料物理特性，實際可用的電磁頻譜範圍資源卻很有限，多半應用集中在無線電波至微波，也就是 3Hz 到 30GHz 這個範圍。商業行動寬頻技術（Commercial mobile broadband）的發展，預期透過重新利用電磁頻譜來推動經濟成長，但同時在經濟發展的前景之餘，這對軍事行動自由（military freedom of action）以及機動，產生前所未有的限制。²

有限的頻譜資源運用，由國家層級進行統籌，並以發照的方式授權運用。在商用寬頻發展的經濟前景下，認為傳統上由軍事部隊獨家使用關鍵頻譜頻段的假設已不合時宜，亦提出這些裝備持續佔用寶貴頻率、卻缺乏相應的作戰價值的想法。³ 在此同時，民用設備在免執照頻段的密集使用，更創造出複雜的電磁環境。其中最典型

² “DoD Electromagnetic Spectrum Superiority Strategy 2020,” *Department of Defense*, October 2020, <https://shorturl.at/LQIIIG>.

³ *Ibid.*

的案例就是 2.4 GHz 工業、科學與醫療（Industry, Science and Medical, ISM）頻段的嚴重擁塞。在國際電信聯盟（ITU）無線電規則中，ISM 頻段的應用定義為「設計用於在本地產生和使用射頻能量的設備運作，用於工業、科學、醫療、家用或類似目的，但不包括電信應用」，在這些規則下開發的各種裝置包括無線電話、家庭安全系統、電子玩具、無人機、電腦區域網路和無線網路設備等，為全球最廣泛使用的頻段。⁴

即使 2.4 GHz ISM 頻段內的各項設備，也有嚴重互相干擾的問題。例如藍牙（bluetooth）技術使用跳頻展頻（FHSS）將 2.4 GHz ISM 頻段分成 79 個 1 MHz 通道，以偽隨機模式每秒在通道間跳躍 1,600 次，自適應跳頻（Adaptive Frequency Hopping）嘗試偵測現有的 WiFi 訊號並避開。⁵在全球範圍，2.4 GHz 頻段廣泛用於無人機控制且無需執照，但容易受到 WiFi 和藍牙干擾。這也使得無人機主要廠商，投注大量資源開發通訊協定與系統軟體，以改善飛行控制與傳輸效能，解決此嚴重無線電波干擾的問題。⁶

ISM 頻段運用產生的電磁特徵，也可能暴露出軍事行動，影響任務執行。例如，美軍曾在艾爾文堡（Fort Irwin）進行的演習中，透過偵測飛行員的 iPhone，暴露以每小時 120 英里的速度高速飛行的阿帕契直升機位置，這顯示商用裝置產生的電磁特徵，在戰場上的危險性。

對美國與北約等國家而言，在與對等競爭對手進行戰略競爭的狀況下，必須需要做出相當艱難的決定：既要透過淘汰傳統的既有

⁴ “Frequency Bands for Ten Most Popular IoT Protocols,” *Haltian*, October 11, 2024, <https://haltian.com/resources/frequency-bands-for-ten-most-popular-iot-protocols/>.

⁵ “2.4 GHz ISM Band: Avoiding Interference,” *EE Times*, August 3, 2022, <https://www.eetimes.com/avoiding-interference-in-the-2-4-ghz-ism-band/>.

⁶ *Ibid.*

用途來實現頻譜分配現代化，又要在充斥商業無線裝置的電磁環境中維持作戰效能，同時確保基本軍事能力不受損。⁷

二、近期衝突經驗與教訓

俄烏戰場上大量運用無人機，不僅反映出激烈的電磁頻譜爭奪，更催生了烏克蘭軍隊從被動防禦、主動攻擊，逐步發展至結合傳統發射源管制（Emission Control, EMCON）與戰術管制（Tactical Control, TACON）的全新作戰概念——「頻譜機動」（spectral maneuver）。這項概念轉變的背景，源於俄烏雙方在電磁頻譜領域展開的持續對抗。烏克蘭每月因俄軍的電子干擾損失約 10,000 架無人機，同時，俄軍在前線部署了大量戰術層級「壕溝級」電子戰系統，包括士兵可攜帶的背包式便攜系統，取代了易受 FPV 無人機攻擊的大型車載平台。在這種高強度電磁對抗環境中，烏軍被迫發展出更為精密的頻譜管理與機動能力。⁸

頻譜機動概念的第一項核心變革，是透過前線分散化部署的電戰系統，創造「干擾泡」（jamming bubbles）以化解敵方 FPV 無人機的威脅，同時精確控制干擾範圍，避免造成「友軍干擾」（fratricide）而影響烏軍自身的通訊或無人機運作。基輔電子戰公司 Kvertus 於 2024 年 2 月提出建立一道 1,500 公里長的偵測器與干擾器「電子牆」，用以偵測和對抗來襲的第一人稱視角（FPV）無人機

然而，單純的大功率干擾會造成嚴重的友軍干擾問題。烏克蘭開發的創新型電子戰系統如 Pokrova，採用技術手段取代衛星訊號並混淆敵方無人機的導航裝置，使其偏離航線並飛過目標或墜落而不造成損害，約 40% 的俄軍 Shahed 無人機因欺騙（spoofing）而「未

⁷ Aaron Pluto, “It’s Time for the US Military to Prioritize Spectrum Policy,” *The Defense Post*, October 8, 2024.

⁸ Kateryna Bondar, “Ukraine’s Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare,” *Center for Strategic and International Studies*, March 20, 2025, <https://www.csis.org/analysis/ukraines-future-vision-and-current-capabilities-waging-ai-enabled-autonomous-warfare>.

能到達目標」。

其次，烏軍電子戰已完全整合至其「偵測—指定—打擊」循環（detection-designation-strike cycle）之中，使電磁頻譜操作成為殺傷鏈（kill chain）的重要組成元素，而非獨立的支援功能。俄烏雙方的部隊常規性地使用車載和無人機攜帶的電子感測器，透過無線電傳輸偵測敵軍位置，並以砲兵或火箭進行攻擊。這種整合不僅體現在戰術層級。烏克蘭軍方越來越要求所有無人和偵察系統必須與態勢感知和火力校正平台整合，目標是即時建立共同作戰圖像（common operating picture）。為滿足這一需求，製造商必須確保其系統能夠無縫地將資料輸入共享的態勢感知和指揮控制環境。⁹

最後，烏軍作戰單位經訓練後，以「頻譜靜默」（spectral silence）模式執行任務，僅在經協調後的特定時間開啟發射源，來避免被偵測。頻譜靜默的實施需要嚴格的組織紀律和協調機制。烏軍旅級單位設有專門的電子戰單位，負責即時管理戰場上持續變化的電磁頻譜環境，並協調與同步無人機、打擊武器系統與通訊系統的頻譜使用，這些電戰單位的功能不僅是操作干擾設備，更重要的是扮演「頻譜交通管制員」的角色，確保己方的多個發射源能夠在時間和頻率兩個維度上協調運作，最大化作戰效能的同時最小化電磁特徵暴露。¹⁰

烏軍的戰場經驗，凸顯頻譜管理在電磁戰場管理（Electromagnetic Battle Management）的重要。不僅無人機本身消耗性的資源，其所使用的工作頻段，也應視作有限的資源。在傳統的頻譜管理思維中，頻譜被視為可重複使用的資源：只要時間和空間上適當隔離，相同頻率可以被不同用戶反覆使用。但在高強度電磁

⁹ Ibid.

¹⁰ Consortium for Defense Information, “The Transformation of Electronic Warfare in 2022-2025,” *New Geopolitics Research Network*, July 23, 2025, <https://www.newgeopolitics.org/2025/07/23/war-in-the-spectrum/>.

對抗環境中，頻率一旦被敵方識別和針對，其可用性就會急遽下降甚至完全喪失。如二戰期間和最近在烏克蘭的電磁頻譜競爭所示，電子戰技術在戰時的運作壽命往往很短暫，一方部署新的干擾器或誘餌後，另一方很快就會開發出對策或應變方法。¹¹

為能讓大量無人機及時運用並同步發揮戰力，了解頻譜特性及其運用原則，不能只是頻譜管理專業人員的責任，任何使用相關系統的作戰人員，都應對頻譜運用具備基本概念。這種「全員頻譜意識」（spectrum awareness for all）的要求，反映現代戰場的一個基本現實：幾乎每個作戰平台和士兵，都在使用某種形式的無線通信或感測器，因此每個人都既是頻譜的使用者，也是潛在的電磁干擾源和被偵測目標。

參、加速創新與地緣政治的新挑戰

一、軍民通用科技發展與頻譜運用

近年來，關鍵新興科技與創新已經由私部門而非政府實驗室所主導，尤其在商用領域因經濟效益催化，形成具規模經濟的生態系，更能支持新科技快速迭代發展。17項關鍵新興技術中有17項現在源自私部門而非國防實驗室，這一根本性轉變對國家如何實現和維持軍事技術優勢具有深遠影響。因此為維持科技優勢，與其繼續由政府獨立研發，各國國防部門更應著重於如何有效利用和整合民間商業技術創新成果。

這種轉變在電磁頻譜技術領域尤為明顯。商業 5G / 6G 通信、物聯網、人工智慧驅動的頻譜管理等技術的發展速度，遠超過傳統軍事採購週期。電子戰技術在戰時的運作壽命越來越短，如烏克蘭衝突所示，需要持續開發、測試和部署多樣化的電子戰效果，以維

¹¹ Bryan Clark, "The US Military Will Need More, Not Less, Access to Electromagnetic Spectrum," *Hudson Institute*, February 19, 2025, <https://www.hudson.org/defense-strategy/us-military-will-need-more-not-less-access-electromagnetic-spectrum-bryan-clark>.

持有效的對抗能力。

以美軍為例，為因應日益複雜的電磁作戰環境，美國國防資訊系統局（DISA）頻譜專案辦公室（Program Executive Office）與戰略司令部共同推動「聯合電磁戰場管理」（Electromagnetic Battle Management - Joint, EMBM-J）計畫。EMBM-J 以分階段方式逐步釋出能力，其初期版本「EMBM-J 態勢感知」（EMBM-J Situational Awareness）作為最小可行能力釋出（minimum viable capability release），即該工具的第一次迭代。這個基於雲端的平台符合「聯合全域指揮管制」（Combined Joint All Domain Command and Control, CJADC2）架構，將一系列電磁頻譜能力和功能整合到單一系統中，無縫收集並將資料整理成單一視覺化顯示介面。¹²

EMBM-J 的核心創新在於實施通用資料層（common data layer），使其能夠與各軍種專用的電磁頻譜系統互通，包括陸軍的「電磁戰規劃管理工具」（Electromagnetic Warfare Planning & Management Tool, EWPMT）、陸戰隊的「頻譜服務架構」（Spectrum Services Framework）以及海軍的「即時頻譜作戰」（Real Time Spectrum Operations, RTSO）系統。這種互通性解決了長期以來困擾聯合作戰的「煙囪式系統」（stovepipe systems）問題，使不同軍種的電磁頻譜作戰能夠在統一的作戰圖像下協調運作。

「聯合電磁戰場管理—決策支援」（Electromagnetic Battle Management - Joint Decision Support, EMBM-J DS）作為 EMBM-J 進階能力釋出，進一步整合 Palantir 專擅的人工智慧驅動決策支援功

¹² Defense Information Systems Agency, “DISA Releases New Electromagnetic Spectrum Operations Reference Architecture,” *news release*, 2023, https://www.disa.mil/en/NewsandEvents/2023/DISA_releases_new_electromagnetic_spectrum.

能，為指揮官提供即時的頻譜衝突預警、自動化的頻率分配建議，以及基於任務優先順序的動態頻譜管理方案。¹³

在北約部分，北約對於 AI 賦能頻譜管理的全面性方法，代表向智慧化、自動化和協作式頻譜作戰的典範轉移。透過整合雲原生技術、機器學習演算法和先進處理能力，使北約在頻譜規劃和去衝突化（deconfliction），實現前所未有的速度和效率，也為規劃人員、作業人員和監管機構提供了使用傳統頻譜管理方法無法實現的共享即時態勢感知和決策能力。¹⁴

北約的願景是在頻譜作戰中實現速度、靈活性、適應性和回應性。動態頻譜管理（Dynamic Spectrum Management, DSM）使頻譜的更有效利用和重複使用成為可能，以提高服務的容量和品質，特別是在軍事使用者之間以及軍民協調方面的共享。在北約創新加速機制 DIANA 於 2024 年 7 月啟動第二輪國防與安全挑戰，在能源與電力、資料與資訊安全、感測與監視等領域確定了五項新挑戰，其中即包括 AI 驅動的動態頻譜分配，用於自主頻率管理，實現無需人工干預的即時頻譜優化。

DIANA 與 10 億歐元的北約創新基金連結，為成功的 DIANA 參與者提供了從原型到生產的清晰路徑，解決傳統上研究與採購之間的「死亡之谷」（valley of death）問題。

二、頻譜運用與下一世代通訊標準競逐

展望未來，地緣政治頻譜衝突最激烈的區域，預計將集中在具備了下一代行動網路所需覆蓋範圍與容量的最佳平衡的微波中頻

¹³ Palantir Technologies, “Palantir to Deliver Electromagnetic Battle Management - Joint Decision Support (EMBM-J DS) Prototype to the Defense Information Systems Agency (DISA),” *news release*, 2024, <https://investors.palantir.com/news-details/2024/Palantir-to-Deliver-Electromagnetic-Battle-Management---Joint-Decision-Support-EMBM-J-DS-Prototype-to-the-Defense-Information-Systems-Agency-DISA/>.

¹⁴ “Technology Strategy towards 2030,” *NATO Communications and Information Agency*, May 2025, https://www.ncia.nato.int/resources/site1/General/newsroom/publications/Public_NCIA_Technology%20Strategy_external_v6%20-%20digital.pdf.

段。其中一個關鍵案例是 4.0 - 8.0 GHz 的 C 頻段（對應北約的 G / H 頻段），目前以商業衛星通訊和專用的北約軍事應用為主。然而，中國對特定的 5G 新無線電（New Radio）頻段（如 n79：4,400 - 5,000 MHz）的積極研發和試驗承諾，直接與北約協調軍用頻段（4,800 - 4,990 MHz）產生重疊。這個頻譜區段，已有大量軍方的固定及行動通訊系統，包括必要的航空應用，而其軍事系統先前已因早期的商業頻譜釋出而被擠壓遷移至此。因此，在 2023 年的 ITU 世界無線電通信大會（World Radiocommunication Conference, WRC）上，已經對此明確表示反對，表示任何進一步推動將此區段識別為「國際行動通訊（International Mobile Telecommunications, IMT）」用途的政治壓力，都將北約盟國的軍事互操作性構成嚴重的威脅。¹⁵

同樣，Ku 頻段（12.0 - 18.0 GHz）也面臨著巨大的壓力，北約明確反對將 14.5 - 15.35 GHz 頻段識別為 IMT 用途，理由是其對協調盟軍的固定和移動系統至關重要。這種戰略的本質在於：透過推動全球 IMT 標準化，不僅能為其國內供應商建立壓倒性的規模經濟，同時也創造出監管和共存上的負擔，系統性地削弱北約進行聯合作戰的能力。中國積極將 6 GHz 頻段上部 700 MHz 開放用於特許行動用途，宣稱這是滿足 5G / 6G 增長需求的唯一大容量中頻帶資源，更凸顯了這種地緣政治上的積極承諾。¹⁶

這種頻譜侵佔的後果，將超越單純的技術共存挑戰，進一步實質限縮軍事行動並影響戰力。將大功率、高密度的商業網路引入先前受保護的聯邦頻段，會產生普遍存在的電磁「雜訊底線」（noise floor），降低低攔截率（LPI）雷達和安全通訊等敏感軍事資產所需

¹⁵ “Forging the 5G Future: Strategic Imperatives for the US and Its Allies,” *Atlantic Council*, March 13, 2025, <https://www.atlanticcouncil.org/in-depth-research-reports/report/forging-the-5g-future-strategic-imperatives-for-the-us-and-its-allies/>.

¹⁶ *Ibid*

的信號雜訊比。這樣強制性的系統置換，迫使軍事系統不得不向其妥協，通常是遷移至信號衰減更大、設備成本更高的頻率，進而犧牲了作戰距離、韌性和靈活性。

因此，引入認知無線電系統（cognitive radio），使相關軍事應用均具備快速識別、分類並適應意圖性干擾和非意圖性商業雜訊的能力，未來將確保軍隊在日益擁擠和持續爭奪的電磁環境中保持暢通無阻的進入權和有效機動能力的必要手段。這場關於頻譜的戰略競爭，實質上是一場定義未來戰爭和全球商業技術與監管架構的關鍵之戰。¹⁷

肆、結語

俄烏戰爭已無可辯駁地證明：電磁頻譜不再是支援軍事行動的配角，而是決定勝負的主角。從烏克蘭在戰爭初期快速損失無人機，到自主開發電戰系統並發展「頻譜機動」概念，再到北約 DIANA 與美軍 EMBM-J 系統對新興科技在電磁頻譜運用與決策支援層面的戰略投資，都顯示在複雜電磁環境下，頻譜管理與機動能力的提升是跨越技術、組織和地緣政治層面的轉型。掌握並妥善管理電磁頻譜，已成為現今與未來作戰的關鍵。

頻譜競爭已從單純技術問題演變為多層次戰略對抗，包括商業 5G / 6G、物聯網和 AI 驅動頻譜管理的快速發展下的技術軍備競賽，使電子戰技術的運作壽命縮短，各國必須持續建立技術「深度彈藥庫」以因應快速失效的電子戰手段。以及作戰概念革新，從美軍以 EMBM-J 整合陸軍、陸戰隊與海軍的頻譜系統，實現聯合作戰的統一電磁態勢感知，以及烏克蘭旅級電戰單位，在時間和頻率維度協調多發射源，實踐從靜態分配到動態機動、從集中控制到分散

¹⁷ Doc. CPG(25)016 ANNEX IV-07, “Draft CEPT Brief on WRC-27 Agenda Item 1.7,” *CEPT Electronic Communication Committee*, July 3, 2025, https://cept.org/documents/cpg/89977/cpg-25-016-annex-iv-07_draft-cept-brief-on-wrc-27-agenda-item-1_7-.

執行、從支援功能到核心能力的根本轉變。

無可避免的，在龐大商業利益下，推動下一代通訊標準制定，也隱藏有地緣政治競爭的企圖。中國積極推動 n79 頻段（4,400-5,000 MHz）運用，與北約軍用頻段（4,800-4,990 MHz）直接重疊；北約認為這將「系統性削弱聯合作戰能力」。這也顯示頻譜分配與下一代通訊標準的競逐，已不單純是技術共存問題，而是透過標準化與規模經濟重塑全球戰略格局的博弈。

為解決當前所在的技術、組織以及戰略困境，以加速創新架構橋接商業與軍事需求，並透過各國在標準制定國際組織合作，與中國由國家主導的舉國體制競爭。同時強化能力建設，藉由認知無線電、AI 驅動頻譜管理等投資，讓頻譜管理由被動反應轉為主動，以機器處理解決大量發射源同時運作的辨別與去衝突化難題，才能在擁擠的電磁頻譜環境保有遂行作戰的機動能力。

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。主要研究領域為：網路戰略、資訊作戰、科技評估。

Spectrum Management and Maneuver in Complex Electromagnetic Spectrum Environment

Chen-Yi Tu

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: Electromagnetic Spectrum Environment, Electromagnetic Spectrum Operations, Spectrum Management

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，讓敵電戰干擾效果打折扣或者難持續，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

美空軍電子戰整備對我制空作戰之啟示

高志榮

網路安全與決策推演研究所

壹、前言

電子戰的起源可以追溯到 20 世紀初，當時無線電技術的出現，使得探索軍事創新作法為提升戰略優勢的目標，更在第一次世界大戰期間，無線電通信的重要性變得顯而易見，其後，在兩次世界大戰期間，對干擾和截收策略的促進有了實質上的運作，¹並對信號參數獲得、保護及電磁信號管理的策進，開啟了新的思維。

第二次世界大戰期間，包括雷達干擾裝置和欺騙技術的創新開發，作戰時扭曲或誤導敵方感測器，使作戰戰術發生改變，並為現代電子戰系統奠定了基礎。電子戰的發展在敵人如隱身技術和電子攻擊規避等的對策快速發展下，使檢測和干擾運作變得複雜，應對這些挑戰需要持續創新和快速部署新系統。²電子戰未來趨勢勢必與人工智慧（Artificial Intelligence, AI）和網路能力深度融合，AI 所增強的演算法，將改進即時分析、威脅檢測和決策，從而提供戰略優勢。

美國空軍內部的電子戰已經取得了重大發展，最初是以側重基本的干擾和欺騙，現在則側重在檢測、破壞或欺騙對手雷達和通信的先進系統，這種演變是透過保護資產和阻止敵人的能力來提供任務優勢，從而提高整體作戰效率，³隨著技術的進步，電子戰的重要性不斷增長，使其成為現代空中戰略的重要組成部分。

¹ “Tracing the Historical Development of Electronic Warfare in Military Operations,” *Defense Strategists*, 9 August 2024, <https://defensestrategists.com/historical-development-of-electronic-warfare/>.

² “Tracing the Historical Development of Electronic Warfare in Military Operations.”

³ “Advancing Defense Capabilities through Air Force Electronic Warfare Strategies,” *The Operation Edge*, 7 July 2024, <https://theoperationedge.com/air-force-electronic-warfare/>.

本文將以美國空軍電子戰建軍整備、美電子戰飛機及裝備能力優勢、對我制空作戰啟示及影響與結語，析述如後。

貳、美國空軍電子戰建軍整備

美國空軍電子戰建軍，中隊是以任務型態來建制編成，其運用電磁頻譜攻擊敵人，或透過不讓敵人使用電磁頻譜方式，來阻礙其軍事行動，同時確保友軍使用電子裝備的自由，⁴綜整美國空軍電子戰中隊如表 3-1。

表 3-1、美國空軍電子戰中隊統計表

中隊	部署位置	機型 / 裝備系統	任務
第 16 航空隊第 55 電子作戰大隊第 41 電子戰鬥中隊	亞利桑那州圖森大衛斯-蒙森空軍基地	EC-130H (待換裝 EA-37B) 7 架	干擾壓制敵方防空系統、通信、雷達和指揮管制偽冒欺敵
第 16 航空隊第 55 電子作戰大隊第 42 電子戰鬥中隊	亞利桑那州圖森大衛斯-蒙森空軍基地	EC-130H (待換裝 EA-37B) 7 架	干擾壓制敵方防空系統、通信、雷達和指揮管制偽冒欺敵
第 16 航空隊第 55 電子作戰大隊第 43 電子戰鬥中隊	亞利桑那州圖森大衛斯-蒙森空軍基地	EA-37B 10 架	破壞敵方指揮和管制通信、雷達和導航系統，阻礙對手的協調，反制其指揮、管制、計算機、通信、網路、情報、監視和偵察目標 (Counter-C5ISR) 等任務
第 15 航空隊第 390 電子戰鬥中隊	華盛頓州惠德比島海軍航空基地。	EA-18G 20 架	全頻譜電子戰能夠針對所有已知的地對空威脅提供檢測和干擾壓制或實施反輻射飛彈攻擊
第 350 頻譜戰聯隊下轄第 350 頻譜戰大隊、第 850 頻譜戰大隊和第 950 頻譜戰大隊 (共 11 個中隊及 1 個專為 F-35 執行即時空中傳輸協作支援單位)	佛羅里達州埃格林空軍基地	不詳	負責為 70 個美國和外國電子戰系統提供電磁頻譜支援功能，有關空軍電磁頻譜的整合，並負責系統工程、測試、評估、戰術開發和維護，另於戰時緊急重新程式設計和傳輸電戰系統任務數據軟體及版本檔案至作戰飛機。

資料來源：統整自美國政府公開資訊。

⁴“55th Electronic Combat Group,” *Official United States Air Force Website*, October 21, 2021, <https://www.dm.af.mil/About-DM/Units/Mission-Partners/55th-Electronic-Combat-Group/>.

參、美電子戰飛機及裝備能力優勢

現今，美國空軍整體空中優勢作為規劃，是以包括空中、太空和網絡空間的人員、組織和能力之整合，整體運用來籌建，為國家提供全球監視和全球力量，以在捍衛美國及其全球利益時，提供精確的脅迫效果，現就其能力分述如後。

一、EC-130H 型電戰機

EC-130H Block 30 採用的是「羅盤呼叫（Compass Call）」系統，包括 AN/ALQ-173「閃爍式干擾機」、AN/ALQ-175 高波段干擾機及 AN/ALQ-198 低波段射頻干擾機等，亦可在每個機翼下攜帶兩個高功率定向「矛（特殊輻射源陣列，SPEAR）」莢艙，能同時對多個輻射源，實施精確度更高距離更遠的干擾。另 Block 35 上配備了新的工作站和任務計算機以及「戰術射頻截獲與對抗子系統（TRACS）」、增強的「射頻分發單元（RFD）」、「增強高頻子系統（EHBS）」。

根據美國空軍的官方介紹，「羅盤呼叫」具備拒止或擾亂作戰對手無線電通信系統及傳感器的能力，其作戰目標是敵防空系統、語音／數據通信鏈路、低頻預警和目標搜索防空雷達等。經過一系列升級改進後，還能與 RC-135V/W「鉚釘（Rivet）」飛機配合，⁵為武器系統提供實時精確的目標指示，其定位精度和處理速度也得到極大改善。

在 2015 年 9 月 15 日美國空軍協會舉辦的航空航天會議上，美國空軍負責網絡攻擊行動的第 24 航空隊司令伯克·威爾遜（BURKE Wilson）少將就針對 EC-130H 指出，「我們已經進行了一系列演示試驗，能夠從空中接觸網絡目標並對其進行操控。」威爾遜少將指

⁵ 兵工科技，〈具備神秘的網絡攻擊能力，美軍 EC-130H 電子戰飛機〉，《每日頭條》，2023 年 7 月 27 日 <https://kknews.cc/zh-tw/military/rk5a93o.html>。

出，這種在飛行中進行的無線攻擊能夠「觸及敵方網絡，而這些網絡在大多數情況下對傳統的攻擊方式是封閉的」。2019年8月13日，美國國會服務署（U.S. Congressional Service）在一份專題報告中指出：「EC-130H 也被用於通過射頻信號向無線設備發送計算機編碼。在這類行動中，即便敵方網絡是封閉的（沒有連接到網際網路），我方仍然能通過無線網路發射數據包」。⁶判此能力能干擾現行封閉自成一體的指揮系統，殊值持續關注其發展。

二、EA-37B 型電戰機

EA-37B 為基於灣流（Gulfstream）G550 商用公務機研改的美國空軍電戰機，提供更新的電子攻擊能力，它配備了現於 EC-130H Compass Call 電子攻擊機上的 Compass Call EW 系統集成，在確保飛行員和電戰操作員能在遠於防區外執行任務，除確保安全之外，亦提供高效率干擾能力。

其航空電子設備包括先進的駕駛艙、現代電子和通信套件、干擾設備、數據鏈、戰術無線電以及發射和接收天線，均全面數位化、軟體提升及 AI 運用，允許將來升級時無需對系統進行任何重大重新配置，並降低後勤維護成本，⁷未來將全面取代 EC-130H，並可在更遠的反介入 / 區域拒止防區外實施任務，為美國空軍提供更強的遠端干擾能力。

三、EA-18G 咆哮者電戰機

咆哮者是 F/A-18 系列飛機的改進型，保留原 F/A-18E/F 的所有多任務能力，可執行各種對敵防空制壓任務，咆哮者是一種機載集成最新的電子攻擊技術戰機，包括 ALQ-218 接收器、ALQ-99 戰術干擾莖艙、ALQ-227 通信對策套件、AN/ALQ-214 綜合防禦對策和

⁶ 兵工科技，〈具備神秘的網絡攻擊能力，美軍 EC-130H 電子戰飛機〉。

⁷ “EC-37B Compass Call Electronic Warfare Aircraft, US,” *Airforce Technology*, June 13, 2024, <https://www.airforce-technology.com/projects/ec-37b-compass-call/>.

聯合戰術終端-接收器 (JTT-R) 衛星通信，另加快測試中的 AN/ALQ-249 是下一代干擾莢艙，正在最後發展階段，將成為 ALQ-99 吊艙的接替裝備。⁸

咆哮者可由己方編組 3 機以上，針對敵方威脅，運用 ALQ-218 接收器，在防區外對敵雷達系統精確定位，作為電子戰攻擊計畫的確認，目前攜掛 ALQ-99 干擾莢艙，能針對 2-18 GHz 頻率範圍實施干擾，未來如完成裝配 AN/ALQ-249 莢艙後，其頻率涵蓋為 18GHz 以下，能發揮更精確的定向及更高輸出功率之干擾，其模組化設計，可確保能夠適應不斷變化的未來威脅升級所需，⁹另可運用其他飛機或衛星，傳輸即時截獲之電子參數給地面電子戰頻譜分析編鍵單位，用以更新制定反干擾策略，提供指揮部門決策參據。

四、第 350 頻譜作戰聯隊地面電戰裝備系統

美空軍第 350 頻譜作戰聯隊，可藉由運用 EC-130H、EA-37B、EA-18G、E-11A、RC-135 電子偵察機、預警機及各式空中戰機之偵蒐裝備，在軍事行動中偵蒐對手之各式雷達運作模式電子參數，並運用數據鏈路傳輸回聯隊，續由官兵導入人工智慧、機器學習參數識別及干擾模式編成等技術，完成電子戰支援任務，快速執行編建電子戰攻擊及防護之電子資料反應檔版本，於 3 小時內回傳給美空軍 70 餘種飛機及武器系統，並完成半數以上武器裝備載入，續逕行後續作戰。¹⁰另有關聯隊系統回傳空中飛機版本載入能力部分，數據頻寬仍顯不足，尚無法進行，此項能力仍須持續關注其發展。

肆、制空作戰中電子戰運用及啟示

⁸ “EA-18G Growler Airborne Electronic Attack Aircraft,” *AMERICA'S NAVY*, September 17, 2021, <https://www.navy.mil/Resources/Fact-Files/Display-FactFiles/Article/2166036/ea-18g-growler-airborne-electronic-attack-aircraft/>.

⁹ “F-18 Jamming Pod: Advanced Electronic Warfare Capabilities,” *Bolt Flight*, March 19, 2025, <https://boltflight.com/f-18-jamming-pod-advanced-electronic-warfare-capabilities/>.

¹⁰ 丘學陞，〈美空軍「迅捷渡鴉」演習 驗證電戰反制能力〉，《青年日報》，2025 年 6 月 11 日，<https://www.ydn.com.tw/news/newsInsidePage?chapterID=1683650>。

依美國空軍制空作戰教則，制空計畫應考慮所有軍種、聯合作戰部隊、跨機構及友盟國家的能力，以及國家所有可用以實現反空中目標的手段。在某些情況下，非軍事的國家權力手段可能是至關重要的，例如運用外交努力獲得友盟基地或空中飛越權等。

制空作戰旨在擾亂、削弱或摧毀敵方的防空能力，為了實現目標，可不必完全摧毀敵人多項能力，而是暫時削弱它，並將戰力資源挹注於關鍵目標。空中攻擊性作戰力量通常以戰力集中達成戰果的方式呈現，以系統性的觀察敵人確定其作戰重心和相關的關鍵脆弱點，通過基於效果的作戰方法（EBAO）規劃於行動中，將這些目標優先排序攻擊，根據對這些目標所達成的破壞效果，使其產生影響並在整個系統中引發次級連鎖效應，降低其作戰能力。¹¹

一、攻勢制空作戰電子戰規劃考量

在攻勢制空作戰（OCA）階段，其目標包括電力基礎設施、關鍵通信和指揮控制節點、網絡基礎設施、國家軍事領導層，以及敵方防空系統中的關鍵節點。在早期作戰階段，優先排序目標的數量可能超過所能執行的能力，適當的目標優先排序是確保力量掙節使用的關鍵。¹²依照上述目標思考分析，軍事武器裝備均有抗炸防護之備用電源，且多為自主封閉網路，故初始當面對我制空作戰影響至鉅的目標有防空飛彈、指揮中心、空軍基地、預警雷達、戰機及火箭軍，在考量執行目標任務、數量、所須打擊效能（遲滯、癱瘓或摧毀）及風險等評估後，規劃執行。

此外，在攻勢制空作戰任務中可運用之電子戰規劃，概可歸納如下：

（一）福州、漳州及空中預警機等指管中心，由 EC-130H 或 EA-37B

¹¹ “COUNTERAIR OPERATIONS,” *U.S. AIR FORCE*, June 15, 2023, https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-01/3-01-AFDP-COUNTERAIR.pdf.

¹² *Ibid.*

型機，對其指管空中各型戰機，實施語音及數據通信鏈路干擾，降低其空軍對我攻擊任務機指揮管制的攔截能力。

(二) 對敵當面影響最鉅之預警搜索雷達及防空飛彈系統主接戰雷達，由 EA-18G、EC-130H 或 EA-37B 型機，執行電子干擾或欺騙，產生雷達盲區，並造成其反干擾處置負荷，以利我任務機執行攻擊任務（反輻射飛彈攻擊或其他目標打擊行動）。

(三) 任務執行時，各型電戰機能實時精確對目標確認及定位，為攻擊戰機提供武器系統指示，發揮攻擊效能。

(四) EC-130H 或 EA-37B 型機，能夠從空中對敵指管系統封閉網路或資訊設備，進行發送計算機編碼數據包，操控其設備，擾亂其指揮體系，以利我方執行任務。

二、守勢制空作戰電子戰規劃考量

在守勢制空作戰（DCA）階段，空軍及防空飛彈能力，不足以防護所有區域內的部隊，DCA 規劃通常須優先考慮哪些資產和能力需要防護。為了確保可用的 DCA 能集中在最需要的地方，聯合部隊指揮官（JFC）應建立一份關鍵資產清單（CAL）和被防護資產清單（DAL）。¹³國軍防護主戰裝備及設施為優先，另有關行政院公布的關鍵資產 310 處，行政院政務委員蒞臨本院（國防安全研究院）針對社會韌性演習報告時，亦律定國家能源、醫療及通訊等三面向為優先防護重點。空中作戰指揮官（AADC）針對 CAL，分配可用的空中防空能力來防護所需的優先資產，並因應作戰進程不斷評估 CAL，調整 DCA 工作重點，以確保能分配和集中防空戰力，在所必要防護的目標。

此外，在守勢制空作戰任務中可運用之電子戰規劃，概可歸納

¹³ Ibid.

如下：

- (一) 福州、漳州及空中預警機等指管中心，由 EC-130H 或 EA-37B 型機，對其指管空中各型戰機，實施語音及數據通信鏈路干擾，降低其空軍對我攻擊時，指管掩護攻擊機群的能力，增強我方攔截效能。
- (二) EA-18G 可對敵攻擊機雷達實施干擾，使其對我地面目標鎖定攻擊增加困難。
- (三) EC-130H 或 EA-37B 型機，能夠從空中對敵指管系統封閉網路或資訊設備，發送編碼數據包操控其設備，擾亂其指揮體系，以利我方任務執行。

五、結語

近年來，美國空軍對電子戰強化進行深入研究，尤其在增強多領域的電磁頻譜管控，2023 年 12 月 11 至 14 日，作者赴美華盛頓參加「2023 年國際電子戰協會」60 周年年會心得從陸地、空中、太空和海上的系統互通性，使電子戰適用於所望的戰場區域。美空軍在整合電子戰裝備、物聯網路能力、人工智慧、機器學習、大數據資料蒐整運算及雲端或機房的資料庫建立等，已取得快速進展，未來，國軍當效法美國在電子戰領域成果，積極建軍備戰，研提政策建議如下，

一、籌建電戰裝備能力

我國僅 C-130HE 天干機及 GLQ-9 無線電干擾車執行電子戰攻擊任務，應提出籌購美國空軍 EA-18G、EC-130H 或 EA-37B 型電戰機，或考量美國 2023 年部署之地面輕型機動干擾裝備，能對敵衛星及空中通訊（含數據鏈路）、定位及合成孔徑雷達（SAR）偵照實施干擾，增強制空作戰能力。

二、訂定電戰支援協議

美空軍近年來持續強化在印太地區的部署及電子偵察行動，目的就是一旦發生軍事衝突時，美軍能在制電磁權上將持續保持優勢，尤其，其 EC-130H、EA-37B、E-11A 及 RC-135 電子偵察機等的遠程域外偵蒐能力，除可即時將情資轉換語言傳輸給我國外，又可結合美空軍地面作業的第 350 頻譜作戰聯隊，快速執行各式電子戰反制版本更新載入執行作戰，爰此，與美空軍簽署上述協同作法，實有其必要。

三、強化電戰情資交換。

我國在 F-16 ALQ-184 電戰莢艙及 ALR-56M 雷達預警器，電子戰任務資料檔，均由美軍依合約時限提供，然現代作戰進程節奏快速，該時限已不符所需，應在後續的 F-16V 電戰裝備籌建及鏈路系統（提升 Link-16 或 Link-22）更新上，希協定能依 3 小時內完成作業時限規範，除提升台美電戰參數共享之外，亦可強化跨國聯合作戰能力。

本文作者高志榮為國防大學戰爭學院畢業，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委任助理研究員。主要研究領域為：戰爭指導、野戰戰略、空戰戰略、聯合作戰、電子戰。

Implications of U.S. Air Force Electronic Warfare Readiness for Our Air Superiority Operations

Chih-Jung Kao

Division of Cyber Security and Decision-Making Simulation

Abstract

This article analyses the U.S. Air Force's advanced electronic warfare (EW) capabilities and provides key insights for Taiwan's air superiority operations. It traces the evolution of USAF EW from basic jamming to sophisticated systems integrated with AI and cyber functions. Core assets include the EC-130H, its successor EA-37B, and the EA-18G Growler, which execute offensive and defensive counter-air missions by disrupting enemy command and control, communications, and radar.

The 350th Spectrum Warfare Wing provides critical ground support, rapidly reprogramming mission data for over 70 aircraft systems. The author argues that achieving air dominance hinges on targeting an adversary's key technological vulnerabilities. Consequently, the article recommends that Taiwan procure advanced EW platforms, establish formal EW support agreements with the U.S., and enhance intelligence sharing to ensure timely mission data updates for its F-16 fleet.

Keywords: Electronic warfare, electronic warfare attack, electronic warfare support, and air superiority operations

美國陸軍電子戰發展現況

舒孝煌

中共政軍與作戰概念研究所

壹、前言

川普政府正推動部隊轉型，將嚇阻中國視為戰略重心，其國防資源將向印太地區傾斜，其中陸軍將進行結構重組，在大國競爭的戰略架構下，參考俄烏戰爭的經驗及教訓，推動多領域作戰概念，並且讓陸軍能具備全領域作戰能力，反制中國的反介入／區域拒止能力。為此，美國陸軍進行結構轉型，持續發展多領域作戰能力，並建立多領域實驗部隊，如今此一組織變化向下發展至旅以下的基層部隊，以便建立快速多領域作戰能力。由於組織調整，美國陸軍仍持續發展其電戰能力中，以便支持基層部隊的戰鬥反應能力，以及涵蓋更大作戰範圍的作戰能力。

貳、電戰是美國陸軍結構轉型核心能力

川普政府的國防部長赫格塞斯正在推動陸軍的深度結構式轉型。2025年4月30日的一份備忘錄中，他指示陸軍部長，調整部隊組織及裝備採購方式。新政府雖將本土防衛列為首要任務，但也將嚇阻中國視為戰略重心，這將使資源重心向印太地區傾斜，而會犧牲其他戰區。

陸軍的重大調整是縮編或關閉功能重覆的司令部，並合併各級司令部，以整合動能、非動能、太空與無人系統作戰能力；減少並重組載人攻擊直升機部隊；以蜂群無人機增強戰力；逐步淘汰「過時」部隊，如部分裝甲與航空單位，但具體名單未公開；建立新型

旅戰鬥隊與無人化部隊。

另外，有多項目標設定要在 2026 或 2027 年前完成，例如達成「電磁與低空制空領域取得優勢」。陸軍參謀長蘭迪喬治（Gen. Randy George）表示，陸軍的問題不是缺乏創新，而是速度不夠快。2024 年起陸軍推動「接觸中轉型」（Transforming in Contact），旨在加快採購及部隊設計流程，讓部隊在演訓及部署中直接試驗新興能力，例如 2025 年 1 月，第 10 山地師第 3 旅的接觸中轉型驗收演習，無人機使用數量創下新高。過去一年已有三個旅轉型為機動或輕型旅戰鬥隊，下一階段將聚焦裝甲師及多領域特遣隊（MDTF）。¹

目前電子戰已獲得美國陸軍更多的關注。²陸軍參謀長在最近一次簡報中提到，電磁作戰是核心能力之一。負責電磁作戰的陸軍能力經理勒斯利·戈爾曼上校（Col. Leslie Gorman）今年 5 月在喬治亞州舉行的「AFCEA 科技網路大會」（TechNet）發表演說時說，電戰是一項跨領域的功能，陸軍每天都在各項作戰功能中積極觀察到其存在。其他官員也指出，陸軍正愈來愈重視電磁作戰在現代衝突中的重要性。

在經歷長達 20 年的全球反恐戰爭後，陸軍需要調整重心，其中一項即為陸軍轉型倡議（Army Transformation Initiative）。過去的電戰體系是依照全球反恐與反叛亂戰爭所設計，但那與未來將面對的大規模戰鬥行動不相容。冷戰後，陸軍曾大幅裁編其許多庫存裝備，近年來才展開多年努力以重振並再投資先進的電子戰能力。對

¹ “Hegseth Orders Sweeping Changes to Army Structure,” *Defensescoop*, May 1, 2025, <https://defensescoop.com/2025/05/01/hegseth-orders-sweeping-changes-army-structure-transformation/>.

² “Electronic Warfare Receiving More Senior Level Attention within the Army,” *Defensescoop*, August 21, 2025, <https://defensescoop.com/2025/08/21/electronic-warfare-army-senior-level-attention/>.

手在此期間則早已認識到頻譜的重要性，並發展出新能力、技術與準則。

2014 年俄羅斯入侵烏克蘭，對陸軍來說是一記警鐘。陸軍從中觀察到俄軍戰術。自那時起，陸軍開始投資相關能力，並把電戰領域提升到更高層級——包含干擾技術與友軍訊號管理（signature management），因為若發射訊號被發現，很可能在數分鐘內遭到攻擊。

作為電戰投資的一部分，陸軍於 3 月發布了一份機密的電戰戰略，該戰略由陸軍戰略行動管理辦公室主任關少將（Maj. Gen. Jake Kwon）擬定，而此這項戰略的一部分是基於參謀長蘭迪喬治將軍對頻譜重要性的認知。這分機密戰略為部隊提供方向。戰略中提出五大路線，主要在於建立並制度化的電戰體系、檢視多領域作戰，並確保持續進行現代化與轉型工作。陸軍正在制定實施計畫。此一戰略也與國防部 2025 年指令及陸軍轉型倡議相互配合。陸軍尚成立電戰委員會（electronic warfare board of directors），由負責作戰、計畫與訓練（G-3/5/7）的副參謀長層級將官領導。該委員會協助監督執行前述戰略，並能在戰場來自部隊的議題提出時，於五角大廈高層提供指導。該委員會可確保陸軍高層充分注意這些議題，並把戰場經驗或陸軍想推動的方向納入參謀長與國防部長指引，將共同方向推送到基層部隊，並為解決基層提出的電戰相關問題提供整體方向，協助驅動投資與能力優序。

陸軍近年來的另一項重大投資是新兵力編組。軍軍已開始建立新的電戰連與排，最近亦開始大幅增加這些兵力規模。由於認知在戰術最前緣需要更多能力，陸軍最近決定將機動旅（mobile BCT）電戰排的人數翻倍。這與陸軍整體結構調整有關，陸軍近期決定建

立機動化旅戰鬥隊（mobile brigade combat teams），使作戰單位在戰場上更輕巧、更具機動性。當陸軍從史崔克（Stryker）、裝甲與步兵部隊轉向這種機動概念時，需要更多電戰馬力（EW horsepower），未來幾年內，還會把機動旅的電戰排人數加倍。

參、陸軍編組排級多領域作戰單位

2017 年美國陸軍提出多領域作戰概念時，時任陸軍參謀長的麥克·米利（Mark Milley）要求檢視陸軍在電子戰方面的短缺，其最終目標是要將電戰變成從各角度打擊敵人的關鍵環節之一。美國陸軍在 1991 年之後幾乎完全放棄電子戰發展，但在 2014 年俄首次入侵烏克蘭時，陸軍重新認識到電子戰能力的高度威脅。電子戰及網路戰略有不同，2017 年 4 月時啟動的電子戰檢視，和網路檢視是分開的，網路檢視著於簡化及強化陸軍各種系統，並抵抗網路及電子攻擊，而電子戰檢視則側重更主動的措施，包括偵測、欺騙及擾亂敵方無線電及雷達。這兩項檢視都觸及網路戰（Cyber Warfare），在軍用無線網路上，網路與電子戰是不可分割的，電戰檢視的目的就在研究網路、電戰及情報整合的缺口。另外，美國陸軍重建電戰的能力主要放在旅級單位，在阿富汗或伊拉克的反恐戰爭中，旅級單位較能獨立作戰，然後在與大國如俄羅斯進行高強度作戰時，則需要更高層級的司令部如師或軍團，在更廣區域及更緊湊的時間軸上作戰。³

美國陸軍仍在持續發展多領域作戰概念。2019 年美國陸軍 3-19 教範，已將電子攻擊視為是一種火力，該教範 1-18 指出，多領域火

³ “Invisible Artillery: Army Wants Electronic Warfare at All Levels,” *Breaking Defense*, August 21, 2017, <https://breakingdefense.com/2017/08/invisible-artillery-army-wants-electronic-warfare-at-all-levels/>.

力多領域火力（Multi-domain fires）是指來自兩個或多個作戰領域的火力效果，集中對同一目標發動攻擊。多領域火力可以產生「協同效應」，其總合效果超過各領域單獨行動時效果的總和。當地面火力與其他領域的效果融合時，能對敵方造成多重困境，使其難以有效應對。例如，指揮官可以同時發動進攻性網路作戰（offensive cyberspace operations）以攻擊敵方防空網路，並使用地對地火力摧毀敵方防空雷達，同時利用空對地火力打擊敵方防空指揮與控制節點。這些整合後的協同效果能降低友軍作戰飛機的風險。⁴

2025年春季，美國陸軍進行一次多領域效應排（Multi-domain effects platoon, MDEP）新興能力的演練。在此次演練中，一支隱藏在叢林中的電戰小隊發現疑似敵方頻率，另一架配備相同偵測裝置的無人機也偵測到同一訊號，兩個平台對發射源進行定位後，電腦計算敵方可能位置，排長在整合的電戰顯示器上看到發射位置，並派遣無人機前往確認，在發現敵方的車輛及天線群後，排長下令發射滯空攻擊武器（Lottering Munition）攻擊目標，同時對敵方頻率進行干擾，並迅速撤離。⁵

MDEP 是一個新編成的作戰單位，旨在把多領域效應帶入旅級戰鬥，使透過電磁頻譜、網路與物理領域之跨領域能力融合，迅速偵測並摧毀威脅。在陸軍準則強調「所有行動皆為多領域行動」的時代，MDEP 為旅級指揮官提供了一種實際方法，讓指揮官能掌握過去要在更高層級才能調度的戰力，這也是陸軍將多領域作戰

⁴ “Army Doctrine Publication (ADP) 3-19,” *US Army*, July 2019, <https://rdl.train.army.mil/catalog-aws/view/ADP3-19-Audiobook/index.html>.

⁵ “The Multi-Domain Effects Platoon: A Brigade-Level Solution for Multidomain Operations,” *US Army*, September 3, 2025, https://www.army.mil/article/288009/the_multi_domain_effects_platoon_a_brigade_level_solution_for_multidomain_operations.

(MDO) 直接下放到更基層單位的努力。

透過干擾敵方通訊，MDEP 可對電磁頻譜實際提供壓制火力。在戰區層級，多領域任務部隊 (multi-domain task force, MDTF) 將遠程火力與網 / 電結合，MDEP 則結合電戰及無人系統，以實現「融合」(convergence)。相較於火砲的煙幕或敵防空網壓制 (SEAD) 任務，該行動使敵方無法干擾突破部隊。此舉符合將攻勢網路與電子戰效應納入火力戰鬥功能，以「剝奪、降級、擾亂與摧毀」敵方能力，作為聯合兵種作戰一部分的準則。

《野戰手冊》3-12 (Field Manual 3-12) 指出：「電戰專業人員在電磁頻譜中專業人員在電磁頻譜 (EMS) 中對敵方網路、系統與武器實施各種效果，如攻擊或干擾行動。這些行動可降低敵方戰鬥力、保護友軍，並提升友軍與武器的致命性。」⁶在這次演訓的案例中，MDEP 運用干擾器，證明僅將電戰侷限於被動蒐集情資的思維，並不利於支援機動單位與多領域作戰。旅級單位必須依據準則與戰術情勢，動態且甚至攻勢性運用這些能力。

MDEP 的組成概念起源於一項認知：旅級在近距離與深度作戰時，缺乏一個有機的手段，以跨領域感知與打擊。組織上，MDEP 編為多功能偵察連 (Multi-Functional Reconnaissance Company, MFRC) 內的一個排，與獵殺排 (hunter-killer platoons, HKP) 並列運作。不同於傳統的騎兵中隊或軍事情報連，MFRC 是一個獨立於旅本部下的連，直接向旅戰鬥隊 (brigade combat team, BCT) 指揮官回報。這種指揮關係使旅級單位能在不需經過多層協調的情況下

⁶ “FM 3-12 Cyberspace and Electronic Warfare Operations,” *US Army*, September 11, 2017, https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN45009-FM_3-12-000-WEB-1.pdf?fbclid=IwY2xjawNsnLVleHRuA2FlbQIxMABicmlkETF1dHI2MzVqQUVKTVpZdVBNAR6gYTHzoXK4HIAgHIOEnC-Ibdm9s4QWROPESaZnl0UEAh2zwO-Xh0o6O5CXWg_aem_qRhqyTznEevB7UZuis9swA.

使用 MDEP 的戰力，將多領域工具直接置於旅指揮官的即時運用之下。

兩個獵殺排提供傳統偵察與小型無人機能力，而 MDEP 則補足技術型感測器與長程精確打擊的能力。這些排共同為旅指揮官形成一個分層且多功能的偵察資產：獵殺排負責發現並限制敵方，而 MDEP 則能透過動能或非動能火力去發現、定位或收尾目標。事實上，置於 MFRC 內的 MDEP 為旅提供了一個微型的多領域特遣隊（MDTF），在戰術層級下整合非動能與動能效應於單一指揮官之下，雖然規模遠小於 MDTF。值得注意的是，儘管 MDEP 在聚合與整合原則上類似 MDTF，但它並不複製 MDTF 的戰區級射程或戰略影響力，而是提供一個縮減版、以旅為中心的能力，與多領域作戰原則一致，但不完全相同。

MDEP 的組成，也將無人機與電戰結合。過去電戰小組與戰術無人機通常平行存在，分屬不同單位，也被其狹義的職責所限制。電戰人員僅負責訊號蒐集，而非機動支援資產，無人機也僅負責其監偵任務，雙方都未整合在旅的機動火力構想中。指揮官傾向將電子戰視為戰略或戰區層級的工具，將無人機視為情報參謀的附屬，而非對近距離作戰有直接貢獻的要素。這種各自為政的做法導致錯失良機，且機動部隊領袖常對兩者的效能抱持懷疑。

在演訓中，機動營常常忽視可用的干擾能力，或是需用者因通訊落差與等級劃分問題而未使用無人機拍攝的影像。再者，多年來在準則上也缺乏對電子攻擊如何在戰術層級上進行攻勢運用的明確指引，這使作戰人員產生謹慎心態，使得干擾器很少被啟用，生怕違規或造成非預期的電磁干擾。⁷

⁷ “The Multi-Domain Effects Platoon: A Brigade-Level Solution for Multidomain Operations,” Ibid.

MDEP 概念已示範多領域作戰不僅可由專職的戰區軍級單位執行，旅級部隊的作戰員也能勝任。它將電戰與無人機的能量，與步槍、機槍與火砲合併運用，以新穎方式將火力投射至敵方。其教訓是：在現代戰場上取得優勢，需要在最低可行的層級實現整合。

「多領域作戰是所有作戰形式快速且連續式的整合。MDEP 在旅級層面回應這一指令。它是機動旅為贏得下一次衝突所需的敏捷、致命且高度賦能編成的經過驗證且可擴展的模型。透過接受並進一步發展 MDEP，陸軍能加速多領域效應向戰術等級戰鬥的整合，確保旅戰鬥隊在每一作戰領域始終領先對手一步。

肆、美國陸軍的多領域特遣隊

印太地區的廣大海域，加上中國日益增強的反介入／區域拒止（A2 / AD）能力，成為美國的挑戰。除新科技及作戰概念外，美國需要一種新型軍事單位。多領域任務部隊（Multi-Domain Task Forces, MDTFs）正是應對此嚴厲挑戰而提出的新範式。這份深入分析檢視將使這些實驗性編成能在廣闊距離與多重領域同時投射力量的九項關鍵系統。

2016 年，時任太平洋司令部（USPACOM，2017 年更名印太司令部，INDOPACOM）司令的哈里·哈里斯（Admiral Harry Harris）上將，在 2016 年 10 月於美國陸軍協會（AUSA）年會透過視訊發言時指出，「當前與未來的安全環境，將要求所有軍種在非傳統域發揮影響力，」哈里斯說「這意味著陸軍必須能夠擊沉艦艇、癱瘓衛星、擊落飛彈，乃至駭入或干擾敵方指揮控制能力。」這對一支多年來主要在對抗非國家武裝集團的部隊而言，是頗具挑戰性的任務。哈里斯進一步談到「路徑依賴」（path dependency）的概念，

說明過去所作的決定如何約束或影響現在與未來的選擇與結果。美軍必須打破既有的路徑依賴，而且要迅速行動。⁸

當時哈里斯挑戰在場的陸軍人員：「在我離開太平洋司令部前，我希望看到陸軍地面部隊在聯合作戰環境中進行演習，在聯合與結合部隊於其他領域運作的複雜環境下，能同時擊沉一艘艦艇、擊落一枚飛彈與發射該飛彈的飛機……」令人意外的是，陸軍在相當程度上達成他所提出的許多目標。哈里斯於 2018 年 5 月離任，由菲利普·戴維森上將（Adm Philip Davidson）接任。

此時陸軍已成立多領域任務部隊試點計畫（MDTF Pilot Program，MDTF-PP），以第 17 野戰砲兵旅為基礎，將情報、資訊、網路、電磁作戰與太空（I2CEWS）能力整合進既有的火力指揮架構中。在 2018 年 8 月的環太平洋演習（RIMPAC）期間，陸軍曾以 M1075 卡車發射的海軍打擊飛彈（Naval Strike Missile）擊沉一艘艦艇，顯示出其新的長程打擊能力。當時，一個地面愛國者資訊協調中心提供對實驗單位的防空支援。透過 Link 16，MDTF-PP 與數個不同的防空感測器連接，可對飛機及其發射的模擬飛彈進行攔截與打擊。

目前尚不清楚 MDTF 是否完全同時完成所有這些任務，但該次環太平洋演習的成功，促使陸軍在 2019 年 10 月結束 MDTF-PP 試點後，即已有建立另外三個 MDTF 的計畫，以汲取試點經驗與教訓。印太司令部在新聞稿中說：美國印太司令部把陸軍的多領域作戰努力視為其在該地區發展聯合戰鬥概念的基礎概念。」隨後，陸軍 MDTF 應運而生，且開始著手裝備化與實體化。如今 MDTF 開始展

⁸ “Capability profile: The US Army’s Multi-Domain Task Forces,” *European Security & Defence*, October 7, 2025, <https://euro-sd.com/2025/10/articles/armament/46971/capability-profile-the-us-armys-multi-domain-task-forces/>.

現實力；例如在 2025 年「護身軍刀」（Talisman Sabre）演習中再次進行擊沉演習（SINKEX）；但這次是以「中程能力發射器（Mid-Range Capability Launcher，即堤豐系統）發射的標準 6 型飛彈（SM-6），並由陸戰隊提供支援。演習中也展示了長程極超音速武器發射器。儘管外界多聚焦於 MDTF 所部署的飛彈，實際上支持其作戰能力的有九項關鍵能力，而其中首要者即為偵察。

美國陸軍多領域效應營（Multi-Domain Effects Battalion，MDEB）內包含發射與操作高空氣球的分隊。MDEB 的角色是提供目標情報與非動能的攻防能力。它們藉由在戰場上創造作戰窗口，支援 MDTF 的動能要素。這可能包括「導航作戰」（NAVWAR），例如針對對手的衛星導航系統進行攻擊或干擾。

MDEB 涵蓋五項非動能能力：

- 一、情報（Intelligence）：蒐集與分析資訊。
- 二、資訊（Information）：塑造資訊環境以影響敵我雙方。
- 三、網路（Cyber）：網域內的攻防作業。
- 四、電子戰（EW）：利用電磁頻譜攻擊或防護資產。
- 五、太空（Space）：使用並能拒止敵方使用太空資產。

在 2024 年 10 月由第 3 多領域任務部隊（3rd MDTF）所屬之多領域效應營（MDEB）舉行的先鋒 24（Vanguard 24）演習中，該營的某些任務面向被揭示。美軍解釋說，該單位著重於「整合網路、電子戰、延伸距離感測與資料傳輸。訓練區與小隊間的距離模擬需在印太司令部作戰時所需面對的距離。

MDTF 的小隊能夠有效定位感興趣的訊號、彙整感測器資料，回傳到位於華丘卡堡（Fort Huachuca）的 MDEB 戰術指揮所，然後把資料整合進包括陸軍情報資料平台（Army Intelligence Data

Platform，AIDP）在內的任務指揮系統，並將資料傳送回位於夏威夷的戰鬥團級全領域作戰中心（All Domain Operations Center）。該單位致力於定位感興趣的訊號；鑒於 MDTF 在反介入 / 區域拒止（A2 / AD）中所扮演的分解（disintegrating）角色，這意味著他們可能會聚焦於為某些火力任務定位雷達。AIDP 目前基於帕蘭泰爾技術公司（Palantir）的多種工具，將來自多元來源的資料彙整並融合為單一畫面，為使用者提供資料模式與關鍵要素，該平台可供來自美軍各軍種的情報人員存取。

MDEB 的情報與偵察並非 MDTF 唯一仰賴的來源。2025 年 1 月與日本舉行的利劍（Keen Sword）演習示範虛擬化神盾武器系統能為第 3 MDTF 提供火力協調支援的能力。VAWS 被用來在多個平台之間提供數位射控協調，其中包含先進野戰火砲戰術資料系統（Advanced Field Artillery Tactical Data System），因而免除了命令的人工傳遞。該演習展示 MDTF 能與盟國如日本自衛隊，以及海軍部隊協同，進行並執行模擬的長程打擊。

MDEB 內有三個系統，包括 K1000 超長程無人飛行載具，擔任持續情監偵任務，高空氣球系統，提供長時間存在且具韌性的持續情監偵平台，補足飛機及衛星等平台；以及戰術情報目標接入節點（Tactical Intelligence Targeting Access Node，TITAN），TITAN 是一個行動式地面站，包括衛星通訊鏈路及其他裝備，用以支援 MDTF 指揮官在目標選擇與接戰時的決策；它是各類情報匯流的通道。

另外 MDTF 的組成部分包括暗鷹長程極超音速武器、堤豐中程能力發射系統、M142 高機動性多管火箭發射系統（HIMARS）及精準打擊飛彈（PrSM）。非動能打擊則包括整合火力防護能量武器—

高功率微波（Integrated Fires Protection Capability High-Powered Microwave，IFPC-HPM），用以保護固定基礎設施與發射點，運用高功率微波免受無人機群（UAV swarm）攻擊；反無人機系統包括固定／低慢小型無人機整合擊敗系統（Fixed Site-Low, slow, small unmanned aerial system Integrated Defeat System，FS-LIDS），是一種模組化系統，設計整合多種感測模組來追蹤並攔截至 Group 3 等級的無人機，包括較大型的偵察機（如俄製 Orlan-10）以及小型商用無人機。除動能攔截外，還整合電戰系統，干擾及削弱無人機控制鏈路。

美國陸軍在極短時間回應哈里斯上將的挑戰，建立一種新型的長距離作戰能力。MDTF 現在能在延伸射程上對解放軍海軍（PLAN）艦艇及其他重要目標構成威脅；MDTF 有可能前進部署到日本、菲律賓或韓國，這一場景將成為中國在發動區域衝突中必須考量的因素。某些系統仍處於研發階段；例如極超音速武器與情報蒐集／理解功能。但整體而言，MDTF 試驗計畫看來頗具成效。關鍵之一在於中國 A2 / AD 能力所提出的明確挑戰，使得美國陸軍相較於其他軍種而言，擁有開發協助削弱該威脅的獨特能力。

伍、美國陸軍尋求新電戰能力

陸軍正在設計一種新的通用電子戰能力，以便能在任何平臺上迅速更新裝備。模組化任務酬載艙（Modular Mission Payload）是一種標準化套件概念，可整合到各類平臺，允許幾乎任何電子戰（EW）能力被載入與替換。推動這種通用啟用能力的部分原因，源自軍方準備裁撤若干系統。在 4 月公布的持續轉型（continuous transformation）計畫下，陸軍逐步淘汰悍馬（Humvee）與聯合輕型

戰術車（JLTV），並將停止採購灰鷹（Gray Eagle）型無人機等裝備。鑑於陸軍尚未確定未來哪些平臺會取代這些系統，電子戰體系需尋求發展與平臺無關的電戰系統，以便能與陸軍未來選用平臺整合。⁹

情報、電子戰與感測器專案執行辦公室下，電戰與網路專案經理史考特·沙弗上校（Col. Scott Shaffer）很清楚陸軍正在進行轉型，但無法明確知道會走向何方，這能鼓勵更多創新與創意，而非只為某一種單一平臺如車輛或飛機量身打造。」理想情況下，此酬載艙會像軌道系統一樣通用，擁有相同底座，並能視任務需求整合所需的無線電或放大器等元件。目前陸軍先從小型酬載艙（payload）著手，若未來需要擴展，亦能為未來平臺提供更遠的射程與更強的能力。其中一個原因是希望把電子戰能力裝上更小型的無人機；另外則是某些開放架構系統對於小型平臺來說，體積或功率需求可能過大。

藉由模組化電戰系統，陸軍在尋求更輕量的底盤，有時候是雙用途的 EW 感測器；目前軟體定義無線電（SDR）已能做很多事，陸軍在思考如何透過軟體修改這些感測器與效應器，來獲得可在多種作戰平臺上整合的模組化能力。

陸軍已放棄以灰鷹無人機作為空中電子戰（MFEW）的主要平臺，官員現在正研究如何把感測器與效應器安裝到更小的 Group 1 與 Group 2 無人機，甚至是在前線作戰的自主戰鬥車輛上。陸軍已決定以漸進方式遞送能力，隨著時間演進以滿足整體空載電磁攻擊需求，陸軍將優先採用商用現貨與政府現貨方案，以便在 2026 會計年

⁹ “One Electronic Warfare Payload to Rule Them All?” *Defensescoop*, August 21, 2025, <https://defensescoop.com/2025/08/21/army-electronic-warfare-modular-mission-payload-vision/>.

度初，迅速向在接觸轉型（Transforming in Contact）單位進行測試與回饋交付能力。

採用標準化電子戰配置後，所有東西都可以封裝在單一酬載艙內。模組化概念仍處於原型階段，但符合陸軍更廣泛的趨勢——儘量採用商用現貨裝備（COTS）。陸軍已從從頭建立電戰能力開發轉向，改為採用更多 COTS，可在未來實驗時有更多選擇，並能檢視不同的空中及地面電戰平台：空中、地面，一旦有標準套件，只要供應商遵循該架構，就能無縫地插入其功能。

陸軍正逐步放棄專用的電戰車輛來執行干擾或偵測任務，不再推進旅級地面層系統（Terrestrial Layer System-Brigade Combat Team, TLS-BCT），該系統原先設想為安裝於史崔克甲車上的車載整合訊號情報（SIGINT）與電子攻擊系統。現在陸軍則將改用模組化轉接套件（Modular Adapter Kit）把 Manpack（背負式）系統安裝到車輛上。

再者，採用模組化載艙的話，幾乎任何載具都能成為電子戰系統。陸軍已經超越那種使用專用電子戰車、在戰場上橫衝直撞、天線像豪豬般豎起來的時代。陸軍想要的是更任務導向的模組化載艙，因為認知到電磁作戰是貫穿所有作戰功能的一項關鍵推手。

雖然陸軍放棄了旅級版的 TLS，但仍在檢視為師級設計、具更長程電子戰能力的 Echelons Above Brigade（EAB）系統家族。陸軍希望該家族包含訊號情報（SIGINT）版本、電戰版本與延伸射程版本，但現在著眼於讓該平台比最初構想更具模組化，以便能在不同車輛間交換設置。

陸軍在加州沙漠舉行的「聚合計畫」（Project Convergence）實驗中，測試了各式發展中的電戰能量與概念。作為陸軍與其他軍種

測試新概念的場域，聚合計畫頂點 5（Project Convergence Capstone 5）被陸軍網路司令部發言人稱為「關鍵試驗台」，用來檢驗正在發展中的電子戰能力。於該實驗中，陸軍不僅著重在受限環境下快速產生與部署效應，也力求簡化目標識別流程、研發對敵方能力的對策，並以滿足大規模戰鬥所需速度的方式，跨多套電子戰系統交付這些對策。

現代電子戰是一場持續的貓捉老鼠遊戲：敵我雙方一方面設法干擾或剝奪對方對頻譜的使用，也試圖根據電子發射定位對方部隊，為自身爭取機動自由。陸軍與其他軍種正為未來在更遠距離與面對更先進對手的大規模戰鬥行動做準備，這與以往區域性、對抗技術較落後敵手的反恐作戰不同。

陸軍與其對應單位致力恢復冷戰後曾裁撤的電戰能量。陸軍十多年間持續努力重振電戰能力，雖然仍經歷波折。陸軍目前正優先部署一套新的電戰架構，以支援在戰時速度下快速蒐集、傳遞與重編程頻譜信號。

美陸軍網路司令部（ARCYBER）在聚合計畫下，與多個合作與下屬單位如：陸軍網路科技創新中心實驗室（Army Cyber Technology Innovation Center Lab）；執行戰術地面網路作戰（多以射頻效應為主）、電子戰與資訊作戰的第 11 網路營；陸軍網路卓越中心；陸軍重編程分析小組（Army Reprogramming Analysis Team）；電子戰與網路專案經理（Project Manager Electronic Warfare and Cyber）；網路與太空專案經理（Project Manager Cyber and Space）；陸軍網路研究所（Army Cyber Institute）；C5ISR 中心之研究與技術整合主任組；以及全領域感測跨功能小組（All-Domain Sensing Cross-Functional Team）。

此次實驗主要聚焦於電磁支援活動（electromagnetic support activities），例如感測環境以偵測與攔截訊號，並特別在於精進資料流、流程與電子戰系統的標準。實驗旨在透過接收器改良來提升電磁支援的特徵化能力。

部隊使用陸地層人攜式（Terrestrial Layer System Manpack，TLS Manpack），數十年來首種正式提供給徒步士兵的電子攻擊能力，可在機動中進行定向尋址並具有有限度干擾，以及商用系統和改良的商用軟體定義無線電（SDR）。

雖然主要焦點為電磁支援，但聚合計畫也力求精進支持其他電戰領域的流程與標準：電子攻擊，主要透過干擾，以及為防範干擾而進行的電子防護。

模組化任務酬載艙與反應式電戰重編程生態系統（responsive EW reprogramming ecosystem）是實驗與持續建構電戰能力的核心。這些模組化酬載艙代表從平台導向轉向載台導向的能力概念——效應可跨多種平臺部署，操作人員幾乎不需進行整合作業。

藉由提升電磁頻譜系統的回應速度，及採用模組化系統，陸軍期望在大規模作戰所需的速度與規模下，迅速產生並交付，顯著提升在動態環境中主導電磁頻譜與達成作戰目標的能力。

網路司令部亦試圖展示從中央資源庫（central repository）到前線單位的端到端電子戰效應開發與部署流程，採用一套共通框架與多套電戰系統介面，交付定向電子火力。陸軍還進一步測試其「射頻資料試點（Radio Frequency Data Pilot）」，以釐清在戰場上快速重編程系統所需的條件。

射頻資料試點（RF Data Pilot）團隊成功示範快速偵測戰場上電子戰目標、將資料分享至 Army Warfighting Mission Area System，並

將資訊傳至快速效應生成企業（Rapid Effects Generation Enterprise）。該企業可在數日內開發出一項新模組化技術，並將其載入多套電子戰系統，使其能自動標示並分類先前的不明異常訊號，賦予這些系統新的能力。

當發現一個不在已知信號庫中的訊號時，過去可能需要數月時間來處理、分類並開發對策。美軍如今追求一個可在數小時內完成該作業的重編程體系，某些情況下更期望能在戰鬥情況下即時完成，而非把訊號回送到遠端的靜態地點處理。

RF Data Pilot 計畫提供寶貴的洞見與資料，進一步鞏固朝向非動能效應發展的方向。實驗所展示的整合速度與技術生成能力，是陸軍在電磁頻譜中構建更佳態勢感知能力的一項重要里程碑。¹⁰

陸、結語

美國陸軍在 2017 年起啟動多領域作戰概念發展，一方面是因應印太地區挑戰，建立全領域作戰能力，應付中國 A2 / AD 能力挑戰，使包括陸軍在內的所有部隊，都有能力執行多樣化任務，另一方面則認識電磁頻譜的重要，將電戰能力視為作戰能力的一部分，可與部隊的火砲等火力結合，成為部隊指揮官的選項，因此美國陸軍須加速電戰能力發展。

美國陸軍認為，要嚇阻對手，美軍必須快速創新，而美軍並非沒有創新，而是速度不夠快。美國陸軍藉實驗進行新作戰能力及新編組的實驗，以便快速建立多領域作戰能量。目前美國陸軍的轉型仍在推動中，調整組織編裝，裁汰重覆或過時單位，並汰換老舊裝

¹⁰ “Army Evaluates Several Evolving Electronic Warfare Concepts at Project Convergence,” *Defensescoop*, April 15, 2025, <https://defensescoop.com/2025/04/15/army-project-convergence-electronic-warfare-concepts/>.

備，同時繼續推動部隊向多領域作戰轉型，不僅在旅以上的師或軍團級單位，執行戰略等級的遠距離、廣範圍任務，且向基層單位發展，加快戰術層級的作戰反應速度及能力。

本文作者舒孝煌為淡江大學國際事務與戰略研究所博士，現為財團法人國防安全研究院中共政軍與作戰概念研究所副研究員。主要研究領域為：美國國防政策、軍事科技、先進作戰概念、現代戰略問題、中共軍事發展。

Current Status of Electronic Warfare Development in the U.S. Army

Hsiao-Huang Shu

Division of Chinese Politics, Military and Warfighting Concept

Abstract

The Trump administration is pushing force transformation that places deterring China at the center of its strategy, shifting defense resources toward the Indo-Pacific. As part of this, the Army is undergoing structural reorganization to develop whole-of-domain combat capabilities and counter China's anti-access/area-denial (A2/AD) posture, drawing on lessons from the Russia-Ukraine war to advance the concept of Multi-Domain Operations (MDO).

To that end, the U.S. Army has been transforming its force structure and continuously developing MDO capabilities, including standing up multi-domain experimental units. That organizational change is now being pushed down to units below the brigade level so as to build rapidly responsive, multi-domain tactical capability. As part of the restructuring, the Army is continuing to develop its electronic-warfare capabilities to support lower-echelon units' combat responsiveness and extend operational reach. By experimenting with new operational capabilities and new force formations, the Army is rapidly building multi-domain combat power. The transformation is ongoing: beyond reorganizing formations and retiring legacy equipment, the Army is pressing units at and above the brigade level to adopt MDO concepts while also extending them to lower echelons to accelerate tactical-level responsiveness and capability.

Keywords: Electronic Warfare, Multi-Domain Operations,

Electromagnetic Spectrum

俄烏戰爭後的中共海軍電子戰轉型發展之研究

陳育正

國防大學中共軍事事務研究所

壹、前言

近年來，伴隨地緣政治緊張局勢的升高，資訊與電磁權的爭奪日益成為現代戰爭的核心要素。另一方面，由於中共海軍的發展趨勢，逐漸朝向更遠海域活動，關注中共在海軍的電子戰發展，也有其必要性。根據中共軍事學者研究指出，俄烏戰爭爆發後，美國為首的西方國家軍事體系與俄羅斯軍方戰場上展開的激烈對抗，不僅重新定義未來作戰的關鍵因素是取得電磁頻譜空間優勢，也為共軍提供觀察與學習現代聯合作戰的「無聲實驗場」。¹一方面學習美國與北約國家如何協助烏克蘭提高電磁頻譜能力，同時也歸納俄羅斯軍隊在應對電磁作戰方面的缺點。²共軍並非僅被動觀察，而是積極蒐集俄軍在複合戰（hybrid warfare）、網路與電磁空間系統對抗的經驗，藉此調整自身能力。³其中，對於海上電子戰的學習尤為明顯。

事實上，中共從 2024 年 4 月增加信息支援部隊等調整軍事組織

¹ Howard Wang and Brett Zakheim, "China's Lessons from the Russia-Ukraine War," *RAND*, May 22, 2025, pp. 1-3, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA3100/RRA3141-4/RAND_RRA3141-4.pdf; 許登榮，邵正途，翁呈祥，張路，〈美軍電磁頻譜作戰發展分析與啟示〉，《國防科技》，2023 年 6 月第 3 期，頁 139；〈烏克蘭成西方"電子戰試驗場"〉，《中國青年報》，2022 年 9 月 1 日，https://m.cyol.com/gb/articles/2022-09/01/content_490jOuWZP.html。

² 武坦然、易楷翔、皇甫冬琦、鄭皓，〈俄烏沖突中北約電磁頻譜作戰介入與俄軍教訓〉，《航天電子對抗》，2022 年第 3 期，頁 1-4。

³ Howard Wang and Brett Zakheim, "China's Lessons from the Russia-Ukraine War," pp. 28-29.

結構，就是對「資訊化作戰」與「智慧化聯合作戰」的重新認識重視。⁴此外，預計於2025年9月舉行的八十週年閱兵將集中展示共軍在定向能武器、電子干擾裝置、無人海空平台等新型作戰能力之進展，其實戰導向與頻譜主導思維已日漸顯著。⁵

整體來說，共軍正關注如何透過電子壓制，進而削弱敵方艦隊的感測、指揮與武器鏈接能力，以奪取「制資訊權」、「制電磁權」，從而掌握軍事衝突時優勢。⁶因此，本研究透過探討中共從俄烏戰爭中與美國有關電磁頻譜運用情況，分析共軍觀察與實踐情況，並進一步研析其對中國未來海上作戰模式、裝備建設與戰法調整的意涵。

貳、中共從俄烏戰爭吸取海上電子戰經驗

俄烏戰爭無疑是一場結合資訊化與電子化手段的現代戰爭，為各國軍事戰略界提供可貴的觀察樣本。對於中共而言，這場衝突暴露出電子戰在高強度衝突中的真實應用場景與其背後的技術瓶頸，同時也凸顯電磁頻譜控制對於未來海上聯合作戰的重要性。從俄羅斯戰艦「莫斯科號」被擊沉、重要軍港——塞瓦斯托波爾港（Sevastopol）——遇襲，到烏克蘭無人艇精準打擊俄羅斯海軍艦艇等戰例可見，電子戰在現代戰場的地位早已不亞於火力打擊與裝備性能，甚至成為「戰場主動權」的關鍵因子。⁷

⁴ 〈號令如山！建立一支強大的現代化資訊支援部隊〉，《中國軍網》，2024年12月5日，>tsysb_207739/qjxsd/yw_207743/16356400.html。

⁵ Liu Xuanzun and Liang Rui, "Land, Sea, Air-based Strategic Weapons, Hypersonic Weapons to Debut at V-Day Military Parade: Official," *Global Times*, August 20, 2025, <https://www.globaltimes.cn/page/202508/1341288.shtml>.

⁶ 談何易、雷根生、逮杰編著，《現代電磁戰》（北京：國防大學出版社，2016年），頁1-4。

⁷ 謝興、蔡玄、梁武、陳虎、游卓，〈俄烏海戰對我國海軍建設的啟示〉，《數字海洋與水下攻

尤其烏克蘭一方面運用 TB-2 無人機干擾俄羅斯艦艇雷達探測，並且結合「海王星」飛彈實施突擊，成功擊沉「莫斯科」號，即為成功的「電子結合火力」聯合打擊的成功代表案例。⁸這意味著小國亦可透過分散式、低成本、高效能的非對稱裝備，對抗傳統重型艦隊，也反映未來海上作戰勢必整合電磁頻譜與電子戰以取得優勢。

首先，俄羅斯海軍「莫斯科號」遭到烏克蘭反艦飛彈攻擊而沉沒，為電磁頻譜防護與裝備現代化兩大領域，帶來深刻的教訓。俄羅斯「莫斯科號」巡洋艦於 2022 年 3 月遭到烏克蘭導彈擊沉，這過程反映出俄軍在電子戰防護與訊號遮蔽上具有明顯弱點。來自中共軍方與軍工產業的研究指出，該船之所以遭到烏克蘭飛彈擊沉的其中一原因是俄羅斯軍方電子戰存在的弱點，根據相關報導，該艦並未啟動完整的電磁隱蔽、干擾措施，導致無法進行有效反映。⁹另外，也有分析認為莫斯科號的防空飛彈與雷達系統過於老舊，在反制烏克蘭先進反艦飛彈方面處於劣勢。¹⁰這起事件讓中共軍事觀察家深刻認識到，即便「莫斯科號」的沉沒不僅暴露俄軍電子戰防護能力的不足，同時反映其艦載雷達與防空系統的老舊，雙重因素導致在實戰中的致命缺陷，即便配備防空火力，若電磁生存鏈薄弱，仍難逃精準打擊。

其次，塞瓦斯托波爾港遭到烏克蘭軍隊襲擊是電子戰與非對稱手段的融合。烏克蘭軍隊 2022 年 10 月 29 日首次以「空、海」協同

防》，2023 年 12 月第 6 期，頁 713-718。

⁸ 〈從俄烏衝突看未來空戰的演變趨勢〉，《新華網》，2025 年 2 月 12 日，<https://big5.news.cn/gate/big5/www.xinhuanet.com/milpro/20250212/ecdaf82353354328a6581cdd41df8b3a/c.html>

⁹ 謝興、蔡玄、梁武、陳虎、游卓，〈俄烏海戰對我國海軍建設的啟示〉，頁 717。

¹⁰ Nick Childs, "The Moskva Incident and Its Wider Implications," *IJSS*, April 29, 2022, <https://www.ijss.org/online-analysis/military-balance/2022/04/the-moskva-incident-and-its-wider-implications/>.

的無人機，搭配無人艇編組突襲俄羅斯黑海艦隊母港塞瓦斯托波爾港。烏克蘭曾發動「海空突襲」，以無人機與無人艇的「蜂群」戰術同時攻擊俄軍基地，意在混淆與癱瘓其防禦系統。接著，在俄軍被迫應對這些小目標、電磁頻譜資源被佔用時，烏軍便發射隱身性能優越的「風暴之影」或「海王星」等巡航飛彈，對停泊在港口的高價值目標實施精準打擊。其中半潛式高速無人艇依託低雷達截面與衛星通訊超視距導控，於夜間與海況遮蔽下貼近目標實施定點爆炸，造成俄羅斯多艘軍艦受損。¹¹

此外，隨著戰爭的持續進行，俄羅斯 A-50 空中預警機數量有所減少，對於塞瓦斯托波爾港港口周邊空中監視能力與預警效率被大幅降低，¹²使得烏克蘭持續利用無人艇、無人機和反艦飛彈對俄黑海艦隊的巡邏艦艇，以及基地發動突襲，凸顯俄國電子防護能力與岸基反無人化能力的結構性弱點，面對這種新型態的戰術，讓俄羅斯海軍處於被動態勢。

參、從強敵身上學習：應對美國電磁頻譜作戰

中共學界與軍方透過觀察美國與俄羅斯的電磁頻譜作戰模式，逐步確立有關共軍作戰能力認識。尤其多篇共軍文獻與軍工企業研究報告反覆強調，未來取得「制空權、制海權」的前提是必須奪取「制電磁權」。如《信息化作戰研究》中即指出，現代戰場將由電子戰與網電攻擊所主導，瓦解敵人作戰體系的結構與物質技術基礎

¹¹ 董科軍，〈俄烏衝突中無人艇作戰及啟示〉，《遠望智庫》，2024 年 1 月 2 日，<https://reurl.cc/NN1mbq>。

¹² 〈烏克蘭為什麼頻襲俄羅斯登陸艦〉，《新華網》，2024 年 3 月 26 日，http://www.news.cn/mil/2024-03/26/c_1212345597.htm。

是首要任務。¹³學習俄羅斯的戰場經驗非常重要，學習美國的軍事發展亦同樣關鍵，尤其美國擁有強大海軍與豐富的作戰經驗，「以敵為師」成為中共海軍提升能力的一種思維。¹⁴

先進武器載台能建立作戰初期優勢。美國海軍 EA-18G「咆哮者」電戰機已成為一體化作戰的重要武器平台。美國海軍的 EA-18G「咆哮者」電戰機，早在 2016 年就已經具備「無源」定位打擊能力。美國海軍 2022 年開始，持續將「咆哮者」電戰機部署至德國與地中海地區，支援北約執行空中巡邏任務，並且涵蓋俄烏戰場在其作戰半徑之內，進行空中電子壓制與情報監控。¹⁵另外，美軍派出包括 E-8C、P-8A、RC-135W、RQ-4 等多款情監偵機種，於波蘭、羅馬尼亞、立陶宛等地周邊地區進行密集地空中偵察活動，蒐集電子輻射源定位與追蹤俄軍部隊動態，對烏克蘭提供高精度戰場情報。¹⁶

除了主要的電子作戰平台之外，共軍研究還主張美軍持續創新電磁頻譜作戰戰術。例如，利用無人機蜂群戰術進入作戰區域，達到破壞敵人防空系統、干擾通訊聯絡，這是美軍強調利用低成本、小型無人電子戰平台，所進行電磁欺敵與偽裝作業，以彌補傳統大型平台不易抵近、風險高昂的限制。¹⁷甚至，美軍亦積極測試「有人

¹³ 軍事科學院作戰理論和條令研究部，《信息化作戰研究》（北京：軍事科學出版社，2009 年），頁 24。

¹⁴ Ryan D. Martinson and Conor Kennedy, “Using the Enemy to Train the Troops—Beijing’s New Approach to Prepare its Navy for War,” *China Brief*, March 25, 2022, <https://jamestown.org/program/using-the-enemy-to-train-the-troops-beijings-new-approach-to-prepare-its-navy-for-war/>.

¹⁵ 於曉華，郭濤，〈美軍電磁頻譜作戰裝備及其作戰應用分析〉，《航太電子對抗》，2023 年第 3 期，頁 44-49。

¹⁶ 武坦然、易楷翔、皇甫冬琦、鄭皓，〈俄烏沖突中北約電磁頻譜作戰介入與俄軍教訓〉，頁 1-2。

¹⁷ 周瑞岩、陳行勇，〈基於美軍電磁頻譜戰的應對策略研究〉，《艦船電子工程》，2024 年第 5 期，頁 12；田佳禾、孫繼澤，〈關於電磁頻譜作戰與電磁規則的思考〉，《艦船電子對抗》，第 48 卷第 2 期，2025 年 4 月，頁 4-5。

機—無人機」協同戰術，例如「咆哮者」電戰機已與 Dash-X 無人機進行聯合任務，利用以分布式平台擴大電子戰縱深的新式戰術作為。¹⁸特別是在幾次聯合演習當中可以看到這類「有人機—無人機」協同戰術運作，目標就是為了在有關信號偵察、電磁干擾和壓制、反輻射攻擊等方面取得優勢。¹⁹

從若觀察中共海軍演訓，近年來已經在北部與南部戰區執行多項提升電磁頻譜作戰的操演，訓練項目涵蓋反潛作戰、艦機協同、雷達抗干擾、電子欺敵等重點內容，一定程度反映共軍對抗美國的電磁作戰能力。例如中共海軍與海軍航空兵聚焦「複雜電磁環境作戰能力」。中共北部戰區海軍航空兵多次組織涵蓋反潛作戰、複雜電磁環境下進行偵蒐、攻擊等課目。訓練中強調使用聲納浮標、建立水下監聽網，以及運用飛行數據與影像等資料，就是模擬在受到敵人干擾情況下，能持續進行反潛任務，同時具備打擊敵人能力。²⁰

另外，中共海軍還演練其艦艇編隊遭遇「敵軍」電磁干擾、無人艇突襲之應變訓練，以及努力在港區及岸置系統，建立制度法規，作為強化硬體電磁防護基礎。²¹這些線索意味著中共海軍提升電子戰準備時，不僅結合目前最新俄烏戰場的發展趨勢，而且涵蓋岸

¹⁸ 吳航、吳克剛、楊旭，〈美軍電子戰無人機發展態勢〉，《國防科技工業》，2023 年第 2 期，37-39。

¹⁹ 〈美軍推進電磁頻譜力量建設〉，《人民網》，2022 年 8 月 1 日，<http://military.people.com.cn/BIG5/n1/2022/0812/c1011-32501247.html>。

²⁰ 〈北部戰區海軍航空兵某部進行複雜電磁環境下搜攻潛訓練〉，《解放軍報》，2025 年 7 月 21 日，<http://www.xinhuanet.com/milpro/20250721/7bea03389c874ca5b26c761fb6665e43/c.html>；〈攜手淬煉勝戰鐵翼！海軍航空兵某部協同訓練展鋒芒〉，《新華網》，2025 年 8 月 25 日，<https://big5.news.cn/gate/big5/www.xinhuanet.com/milpro/20250825/0e387a390ef1473eadde92030ab61334/c.html>。

²¹ 〈海軍某大隊：艦機協同出擊淬煉打贏硬功〉，《中國國防部》，2025 年 8 月 10 日，<http://www.mod.gov.cn/gfbw/wzll/hj/16401766.html>；王亮、童忠誠，〈海軍后方倉庫戰時面臨的電磁威脅及應對措施〉，《艦船電子工程》第 3 期，2023 年，頁 198-201。

基系統礎設施與演訓項目的能力。

值得注意的是，在某護衛艦支隊訓練中，還出現海空聯合反制電子戰，涵蓋海區封鎖、反潛、防空反導等項目，²²可能意味著中共海軍訓練平台朝向「跨域相互操作性」方向發展，甚至是驗證局部海域的封鎖時，亦需優先取得電磁優勢。這些發展不能排除中共海軍在操演課程當中，預想包含「台灣海峽」等不同的作戰場域。此舉符合習近平所強調「全面推進軍事訓練轉型升級」、「加快實現訓練與實戰一體化」的目標。²³

中共部分研究認為未來海上防衛不再僅限於火力與艦載防空系統的布局，更取決於是否擁有一套分層、模組化、可快速部署的電子對抗體系，用來應對快速變化的電磁頻譜壓制與反制行動。筆者認為近期一篇研究論文點出共軍海上電戰發展的一種想像，該研究者來自中共海軍工程大學、海軍指揮學院，以及海軍 91715 部隊所共同撰寫，提出共軍艦載電戰機與無人機協同的理論架構，這項主張既是回應平時面臨敵人「偵察威懾」的作法，亦是爭奪電磁權的一種手段。²⁴然而，現實的問題是，中共在「偵察威懾」的經驗累積與電戰系統，可能並未達到美軍同等水準，因而無法過於樂觀看待；即便如此，仍實際反映共軍在一定程度上的努力。

肆、結語

綜合俄烏戰爭經驗與中共近年的體制與訓練動向可見，未來海

²² 〈犁波踏浪礪精兵 海軍某護衛艦支隊艦艇編隊訓練〉，《央視網》，2025 年 6 月 24 日，<http://big5.cctv.com/gate/big5/military.cctv.com/2025/06/24/ARTIb1xIhbsUxCWdQ9LC8yF250624.shtml>。

²³ 〈2022 年 1 月國防部例行記者會文字實錄〉，《中國國防部》，2022 年 1 月 27 日，<http://www.mod.gov.cn/gfbw/xwfy/lxjzhzt/2022njzh/2022n1y/4903774.html>。

²⁴ 熊鵬、嚴必虎、程志鋒、程智琦，〈艦載電子戰飛機與無人機協同作戰視圖研究〉，《火力與指揮控制》，第 8 期，2024 年 8 月，頁 115-118。

上聯合作戰的勝負，關鍵在於先奪「制電磁權」、繼而穩固「制資訊權」，再以多域協同方法轉化為成可持續的火力與機動優勢。

共軍持續努力借鏡俄羅斯軍隊在俄烏戰場的經驗，修正自身有關電磁頻譜，以及反無人化系統等能力不足，使得軍方研究人員提出組織調整、複雜電磁環境演訓與「艦載機、無人系統」協同構想等方式，試圖彌補聯合作戰能力的短板，朝向「體系對抗」的目標前進。透過上述討論說明，中共認為目前與美軍電磁頻譜作戰能力相比，仍然在偵察威懾、分布式協同，以及反制干擾等層面，確實還有改進空間。

綜合而言，中共海軍正積極擴展其電子戰能力，以因應未來高強度戰場對持久通信與精準打擊的需求。這種發展趨勢必定影響我國周邊海域的軍事對峙環境，尤其在共軍執行聯合封鎖演練、戰備警巡等行動時，對我國海軍與空軍的指管通信系統，形成更大的壓力與干擾。因此，我國必須強化電子防護能力，並且建立韌性通聯架構，以因應中共未來更複合型態的軍事威脅。

本文作者陳育正為中興大學國際政治研究所博士，現為國防大學政戰學院中共軍事事務研究所副教授。主要研究領域為：戰略研究、中共政治作戰、中共海權、中共灰色地帶行動。

The Transformation of the People's Liberation Army Navy's Electronic Warfare in the Wake of the Russo-Ukrainian War

Yu-Cheng Chen

Graduate Institute of China Military Affairs Studies

Abstract

This article examines the transformation of the People's Liberation Army Navy's (PLAN) electronic warfare (EW) capabilities, drawing significant lessons from the Russo-Ukrainian War. The conflict has served as a "silent laboratory", highlighting the criticality of electromagnetic dominance for modern maritime operations. Key events, such as the sinking of the Moskva and successful Ukrainian asymmetric attacks using drones and missiles, have exposed the vulnerabilities of inadequate EW protection and outdated systems.

Consequently, the PLAN is accelerating its development, learning from both Russian failures and advanced U.S. capabilities, such as the EA-18G Growler and manned-unmanned teaming tactics. This has prompted recent military reforms, including the 2024 creation of the Information Support Force, and intensified naval exercises focused on anti-jamming and cross-domain interoperability in complex electromagnetic environments. While acknowledging gaps with U.S. capabilities, the PLAN's evolving EW posture significantly heightens the threat to regional stability.

Keywords: Strong enemy, Combat-Oriented, Maritime Electronic Warfare, Electromagnetic Dominance, Distributed Coordination

A Comparative Analysis of EMP Defensive Measures of the PRC, United States, and Taiwan

Pak, Tin¹

Rainier Institute for Foreign Affairs

The electromagnetic spectrum is emerging as a critical domain of warfare, where attacks using electromagnetic pulses (EMP) aim to jam, disable, or destroy electronics. As reliance on electronics grows in military forces globally, EMP threats pose exponentially significant risks to critical infrastructures.

In response, the United States, the People's Republic of China (PRC), and Taiwan are not only advancing their EMP weapon capabilities but are also investing heavily in hardening measures to protect vital networks and infrastructure from these threats.

This article first analyzes the EMP weapon capabilities of these countries. It then examines the defensive measures they have taken to mitigate vulnerabilities and improve resilience in the face of potential EMP attacks.

1. PRC:

The PRC fields two main types of EMP weapons: high-power microwave (HPM) devices and high-altitude EMPs (HEMPs). The PRC leads globally in HPM development, holding 90% of HPM-related patents,

¹ President & Co-founder of Rainier Institute for Foreign Affairs.

with its technology exponentially improving in strength and precision.² HPMs are devices that emit rays of high-frequency EMPs at a narrow target. Notably, the PRC unveiled its FK-4000 land-based HPM system at the 2024 Zhuhai Airshow, and some other HPM designs are reportedly compact enough to be equipped onto missiles, raising concerns about integration with their growing arsenal of hypersonic missile systems.

Additionally, the People's Liberation Army's (PLA) HEMP arsenal is growing rapidly. HEMPs can generate pulses over wide areas, inducing destructive electrical charges across critical systems. With 600 nuclear warheads today, the PRC plans to have 1,000 by 2035 delivered by systems like the DF-26—each warhead representing a potential HEMP.³

These weapons reflect the PLA's informatized warfare doctrine, targeting technological nodes to paralyze adversary forces. When paired with its active defense doctrine, which increasingly embraces preemptive strikes, EMP weapons serve as a modern "Assassin's Mace" type weapon.⁴ A few well-placed HEMPs over Taiwan, combined with precision HPM strikes, could achieve strategic surprise and cripple that nation's electronic infrastructure.

As the PRC develops its EMP arsenal, it has also taken steps to protect its own infrastructure from potential EMP attacks.

The PRC's State Administration for Market Regulation enforces EMP

² Tin Pak and Yu-cheng Chen, "Weaponizing the Electromagnetic Spectrum: The PRC's High-Powered Microwave Warfare Ambitions," *China Brief* 25, No. 9, May 9, 2025, *The Jamestown Foundation*, <https://jamestown.org/program/weaponizing-the-electromagnetic-spectrum-the-prcs-high-powered-microwave-warfare-ambitions/>.

³ Hans M. Kristensen, Matt Korda, Eliana Johns, and Mackenzie Knight, "Chinese Nuclear Weapons, 2025," *Bulletin of the Atomic Scientists* 81, No. 2, March 12, 2025, pp. 135-60, <https://doi.org/10.1080/00963402.2025.2467011>.

⁴ Tin Pak and Chen Yu-cheng, "China Has Found Its Assassin's Mace," *Taipei Times* (Taipei), May 6, 2025, *sec Editorial & Opinion*, <https://www.taipetimes.com/News/editorials/archives/2025/05/06/2003836382>.

hardening standards for commercial electronics, which aim to ensure a level of protection against EMP disturbances. However, unlike their IEC counterparts, they stop short of specifying exact shielding attenuation levels or frequency requirements within their open source regulations. That said, the PRC's GB/T 17626.3 regulation sets out the required frequencies needed for electromagnetic immunity testing, and these appear consistent with most international practices.⁵

On the military side, the PLA is actively exploring strengthening its EMP defense research and development, as reflected in a variety of reports published by PLA-affiliated institutions. For example, the Laboratory on Electromagnetic Effects and Electro-optical Engineering at the Army Engineering University in Nanjing conducts research into defensive EMP measures, including protection for naval vessels against electromagnetic disturbances.⁶ A 2023 paper from the PRC's National University of Defense Technology, presented at the 11th China Conference on Command and Control, focused on electromagnetic mobile defense tactics.⁷

Additional studies published in the Journal of China Academy of Electronics Science focus on examining the effects of EMPs on critical electronic systems. The China Luoyang Electronic Equipment Test Center

⁵ GB/T 17626.3-2023, Electromagnetic Compatibility — Testing and Measurement Techniques — Part 3: Radiated, Radio-Frequency, Electromagnetic Field Immunity Test, issued December 28, 2023, implemented July 1, 2024, by the Standardization Administration of China and State Administration for Market Regulation.

⁶ Gaofei, Pei, Chen Hailin, and Gao Cheng. "Lightning Protection Evaluation Technology of Surface Ship Based on Leader Progression Model," *强激光与粒子束* 30, No. 1, 2018, p. 013202-1.

⁷ LIN Dong-Xu and WANG Jin-Song, "Analysis on Electromagnetic Maneuver Defense Tactics," *College of Electronic Engineering, National University of Defense Technology*, October 24, 2023, document no. ZHKZ202310001133.

conducted research on the probability of detection for radars that are being electromagnetically jammed.⁸ Another paper from the PRC’s National University of Defense Technology simulated the effects of electromagnetic disturbances on air defense platforms.⁹

This emphasis on EMP hardening among the PRC’s leading military technology institutions reflects growing recognition of the electromagnetic domain’s strategic importance for future conflicts.

Regarding exact standards of EMP protection for military facilities, the PLA adheres to the “中华人民共和国国家军用标准” (National Military Standards of the PRC). This regulatory framework includes provisions for EMP defense. For instance, GJB 8848-2016 sets out electromagnetic environmental effects test methods for systems and equipment as provided in its commercial standards.¹⁰ However, documents detailing exact EMP protection thresholds remain restricted.

2. United States:

The United States’ research and development of EMP weaponry is

⁸ Zhang Zhengchao, Xu Peiwei, Li Wenchen, and Li Hong, “Research on Detected Probability of Radar Network under Complex Electromagnetism Jamming,” *Science & Technology Review (Keji Pinglun)*, National Key Laboratory of Complex Electromagnetic Environment Effects on Electronic Information Systems and China Luoyang Electronic Equipment Test Center, 2023, <https://kjpl.cbpt.cnki.net/WKD/WebPublication/paperDigest.aspx?paperID=58f6d254-4028-47ea-a154-fc6447537984>.

⁹ Dai Huanyao, Li Lin, Cui Jianling, Qiao Huidong, and Zhao Jing, “Analysis and Simulation of Air Defense Weapon System Complicated Electromagnetic Environment Effect,” National Key Laboratory of Complex Electronic Environmental Effects on Electronic Information Systems and School of Electronic Science and Engineering, *National University of Defense Technology*, 2023, CNKI, <https://kjpl.cbpt.cnki.net/WKD/WebPublication/paperDigest.aspx?paperID=aa40951b-0888-436a-aa2c-e257f0f3f80e>.

¹⁰ Equipment Development Department of the Central Military Commission, 系统电磁环境效应试验方法 [System Electromagnetic Environmental Effects Test Methods], GJB 8848–2016 (Beijing: *Equipment Development Department*, 2016), <http://detech.net.cn/uploads/soft/20200402/1585798138.pdf>.

significantly more advanced than that of the PRC. The United States has not only developed missile-borne EMP weapons, but also possesses a nuclear arsenal approximately three times larger than the PRC's, totaling around 3,700 nuclear warheads—each of which is a potential HEMP weapon.¹¹ Coupled with its flexible nuclear use policy and a wide range of yields and delivery mechanisms, the United States maintains a diversified and highly capable HEMP arsenal.

The United States is also actively developing advanced non-nuclear EMP systems. In 2016, the Office of Naval Research Science & Technology and the Air Force Research Laboratory launched the High Power Joint Electromagnetic Non-Kinetic Strike (HiJENKS) project.¹² Designated as the successor to the Air Force's Counter-electronics High Power Microwave Missile Project (CHAMP), HiJENKS aims to produce a missile-borne HPM weapon intended to disable or destroy electronic systems as it flies above its targets. Although many details about the HiJENKS weapon remain classified, the Air Force reported that it successfully conducted battlefield tests in 2022. Its predecessor, CHAMP, integrated the Air Force Research Laboratory's HPM payload with Boeing's AGM-86 Conventional Air-Launched Cruise Missile. In a 2012 test, it was able to disable seven separate electronic targets in a single mission.¹³

¹¹ Hans M. Kristensen, Matt Korda, Eliana Johns, and Mackenzie Knight, "United States Nuclear Weapons, 2025," *Bulletin of the Atomic Scientists* 81, No. 1, January 2025, pp. 53-79, <https://thebulletin.org/premium/2025-01/united-states-nuclear-weapons-2025/>.

¹² High Power Joint Electromagnetic Non-Kinetic Strike (HiJENKS), AD 1195640, *Defense Technical Information Center*, March 9, 2023, <https://apps.dtic.mil/sti/trecms/pdf/AD1195640.pdf>.

¹³ Robert Johnson, "Boeing Now Has a Missile That Destroys Only Electronics and Leaves All Else Intact," *Business Insider*, October 25, 2012, <https://www.businessinsider.com/boeings-counter-electronics-high-power-microwave-advanced-missile-project-2012-10?0=defense>.

Beyond missile-borne HPM systems, the United States is also investing heavily in land-based HPM weapons to counter unmanned aerial drones. In 2019, the Air Force Research Laboratory began development of the Tactical High-power Operational Responder (THOR), a land-based HPM weapon designed primarily for anti-drone operations.¹⁴ Additionally, beginning in 2023, the U.S. Army started to procure land-based Leonidas HPM systems to defend its installations from drones.¹⁵

In terms of defense measures, the United States has been the most publicly proactive among the three nations on this front.

Within the military, the U.S. Department of Defense adheres to its regulation MIL-STD-188-125-1 when hardening its critical infrastructures and systems.¹⁶ It states that hardened facilities must be able to withstand an EMP with an intensity of 80 decibels at a one gigahertz frequency. The extent of hardening across military facilities is classified. It is likely confined to strategically critical facilities.

The Trump Administration's 2019 Executive Order on Coordinating National Resilience to Electromagnetic Pulses marked the first time EMP protections were directly addressed at the national level.¹⁷ The order directed the Department of Homeland Security (DHS) to coordinate

¹⁴ Air Force Research Laboratory, "TACTICAL HIGH POWER OPERATIONAL RESPONDER (THOR)," *Air Force Research Laboratory*, accessed June 26, 2025, <https://afresearchlab.com/technology/thor>.

¹⁵ Epirus, Inc., "U.S. Army Awards Epirus \$66.1 M Contract for Leonidas™ Directed Energy System," press release, *Los Angeles, CA*, January 23, 2023, Epirus Inc., <https://www.epirusinc.com/press-releases/u-s-army-awards-epirus-66-1m-contract-for-leonidas-tm-directed-energy-system/>.

¹⁶ DEPARTMENT OF DEFENSE, MIL-STD-188-125-1: High-Altitude Electromagnetic Pulse (HEMP) Protection for Fixed Facilities, *U.S. Military Standard*, July 17, 1998, public release, <https://www.volta.it/wp-content/uploads/2017/09/MIL-STD-188-125-1.pdf>.

¹⁷ Donald J. Trump, Executive Order 13865: Coordinating National Resilience to Electromagnetic Pulses, March 26 2019, published in Federal Register 84 FR 12041 (March 29 2019), *Trump White House Archives*, <https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-coordinating-national-resilience-electromagnetic-pulses/>.

national EMP defense, review protection standards, and develop an integrated, cross-sector plan to address identified gaps. However, the order framed private-sector participation as collaborative rather than mandatory. DHS is directed to only share its analyses on EMP threats to private utilities and other agencies, and as appropriate, provide “incentives” to private-sector partners to address these vulnerabilities.

The executive order lacks a strong legal imperative granting agencies the authority to enforce EMP protections. A similar weakness characterized the Department of Energy’s 2017 Electromagnetic Pulse Resilience Action Plan, which did not specify EMP protection levels that utilities must meet, unlike those provided in the military standard.¹⁸ Instead, it remained consultative, focused on sharing best practices and promoting mitigation strategies rather than setting requirements.

Since the implementation of the 2019 executive order, the energy utilities represented by the North American Electric Reliability Corporation (NERC) formed an Electromagnetic Pulse Task Force in accordance with the executive order. The outcome of this initiative was its Strategic Recommendations report.¹⁹ In line with the presumably voluntary and collaborative nature of the executive order, the recommendations they delivered are just that, recommendations for which no promise of implementation is made.

At the state level, several governments have attempted to strengthen

¹⁸ U.S. Department of Energy, “Electromagnetic Pulse Resilience Action Plan,” January 10, 2017, *U.S. DOE*, <https://www.energy.gov/sites/prod/files/2017/01/f34/DOE%20EMP%20Resilience%20Action%20Plan%20January%202017.pdf>.

¹⁹ EMP Task Force, EMP Task Force: Strategic Recommendations Report, draft, North American Electric Reliability Corporation, August 30, 2019, *NERC*, https://www.nerc.com/pa/Stand/EMP%20Task%20Force%20Posting%20DL/EMP_Task_Force_Strategic_Recommendations_Report_08302019.pdf.

EMP protections for critical infrastructure, with limited success. In 2013, Maine passed An Act To Secure the Safety of Electrical Power Transmission Lines, directing its Public Utilities Commission to examine grid vulnerabilities to geomagnetic and electromagnetic interference and issue recommendations for utilities to address these threats.²⁰ However, the law stopped short of granting the government authority to compel utilities to implement these recommendations. Two subsequent bills that attempted to establish such authority were vetoed and died in the legislature.

Another example is Virginia. In 2015, Virginia amended its legal code to require the Department of Emergency Management to plan for disasters caused by EMP incidents.²¹ Yet, as of a 2019 Virginia Joint Commission on Technology and Science report, EMP considerations had not been incorporated into the department's annual assessments.²² Moreover, this measure focuses on response rather than prevention.

Other states, including Texas and South Carolina, drafted bills to assess the EMP resilience of their electric grids and propose protective measures. All these bills failed to become law.

3. Taiwan:

Taiwan's investment in EMP weapons is the weakest among the three nations explored in this article. Beyond their procurement of

²⁰ Resolve, Directing the Public Utilities Commission To Examine Measures To Mitigate the Effects of Geomagnetic Disturbances and Electromagnetic Pulse on the State's Transmission System (Resolve Chapter 45, L.D. 131, 126th Legislature of Maine), August 6, 2013, <https://www.ourenergypolicy.org/wp-content/uploads/2013/08/Maine-126-HP-106-item-3.pdf>.

²¹ Virginia General Assembly, Joint Subcommittee to Study State Preparedness for an Electromagnetic Pulse (EMP) or Geomagnetic Disturbance (GMD) Event, State Electromagnetic Pulse (EMP) and Geomagnetic Disturbance (GMD) Preparedness Assessment (Report SD5), published 2019, *Richmond, VA: Virginia General Assembly*, <https://rga.lis.virginia.gov/Published/2019/SD5/PDF>.

²² Virginia General Assembly, State Electromagnetic Pulse (EMP) and Geomagnetic Disturbance (GMD) Preparedness Assessment (Report SD).

electromagnetic hand-held jamming guns aimed at disabling aerial drones, they do not have any EMP weapons.

Similarly, Taiwan's efforts at defending against EMPs are also the weakest, leaving the nation acutely vulnerable. A large-scale EMP attack, whether through targeted HPM strikes on critical nodes or broad-based HEMP attacks, could trigger cascading failures across both Taiwan's military and civil society.

EMP attacks can swiftly disable military command and control systems, paralyzing defensive operations. Key assets such as Taiwan's Patriot and Tien Kung surface-to-air missile batteries, which rely on vulnerable electronic sensors and radar, would be at significant risk. While many of Taiwan's critical military installations are hardened to withstand HEMP-grade attacks following U.S. military standards, these protections remain susceptible to higher-frequency HPM attacks, which can operate at frequencies many times greater than those of HEMPs.²³

The civilian sector faces even greater dangers. Essential services, including telecommunications, water treatment, transportation—and most importantly, its energy grid—depend on electronics that are highly vulnerable to EMPs. Taiwan's Bureau of Standards, Metrology and Inspection enforces International Electrotechnical Commission (IEC) EMP hardening standards for commercial infrastructure.²⁴ However, these standards are designed primarily to address naturally occurring EMP events, such as lightning strikes or solar storms, and fall short of protecting

²³ Tin Pak and Yu-cheng Chen, "Could Taiwan Survive an EMP Attack by China?" *The Diplomat*, May 7, 2025, <https://thediplomat.com/2025/05/could-taiwan-survive-an-emp-attack-by-china/>.

²⁴ U.S. Department of Commerce, International Trade Administration, "Taiwan – Standards for Trade," *International Trade Administration Country Commercial Guide*, last updated January 10, 2024, <https://www.trade.gov/country-commercial-guides/taiwan-standards-trade>.

against the more high-intensity pulses generated by HEMPs or HPMs.

Unlike the United States, Taiwan has not enacted a single piece of legislation focused on strengthening civilian EMP defenses. Nevertheless, there are encouraging signs that Taiwan is beginning to recognize and address this critical vulnerability. Under President Lai Ching-te's whole-of-society defense resilience strategy, asymmetric threats like EMPs have gained greater prominence.²⁵ This initiative seeks to enhance civil-military cooperation and build a more integrated defense posture.

Moreover, Taiwan's military is also showing increasing awareness of electromagnetic threats, as evidenced by its acquisition and integration of hand-held anti-drone electromagnetic rifles into its forces.²⁶ As more electromagnetic weapons are integrated into its operations, the military's understanding of its own vulnerabilities to similar weapons wielded by its adversaries will likely sharpen, potentially driving further policy action on this front.

Yet, time is a critical factor. Failure to act swiftly could leave Taiwan greatly exposed. A 2019 South Carolina legislative proposal to harden that state's energy grid estimated it would take a decade to fully implement protective measures.²⁷ Taiwan may not have that long; some experts suggest that the People's Liberation Army could be ready for an attack as early as 2027, or perhaps by 2035. Therefore, the window to take action is narrowing, and Taiwan's resilience will depend on how quickly its

²⁵ Office of the President, Republic of China (Taiwan), "Whole-of-Society Defense Resilience Committee," accessed June 26, 2025, *Policy Vision page*, <https://english.president.gov.tw/Page/670>.

²⁶ Kelvin Chen, "Taiwan Completes Anti-Drone Gun Deployment," *Taiwan News*, February 19, 2024, <https://www.taiwannews.com.tw/news/5098108>.

²⁷ South Carolina Revenue and Fiscal Affairs Office, Statement of Estimated Fiscal Impact: H. 4954, introduced January 25, 2024, analyzed March 21, 2024, *Columbia, SC*, https://www.scstatehouse.gov/sess125_2023-2024/fiscalimpactstatements/H4954%202024-01-25%20introduced.pdf.

government can begin implementing nationwide EMP security measures aimed at defending against higher-intensity EMP attacks.

4. Conclusion:

With the increasingly digitization and electronification of warfare, EMP weapons will be critical for any future conflict involving these three nations. Regarding their offensive capabilities, the United States and the PRC have advanced EMP arsenals, and Taiwan is beginning to invest in these systems. However, defenses against EMPs are lagging behind. Most discussions of EMPs in policy circles focus mainly on their battlefield applications, particularly in terms of their anti-drone capabilities. On the other hand, threats towards critical civilian infrastructures by HPM-borne missiles or HEMPs receive less attention due to their novelty and a pervasive normalcy bias surrounding the non-use of nuclear warheads.

A Comparative Analysis of EMP Defensive Measures of the PRC, United States, and Taiwan

Tin, Pak

Rainier Institute for Foreign Affairs

Abstract

The electromagnetic spectrum is a key warfare domain, with electromagnetic pulses (EMP) threatening electronic systems amid growing military digitization. The U.S., PRC, and Taiwan advance offensive EMP capabilities while hardening defenses, though gaps persist. This article analyzes their arsenals and resilience strategies.

The PRC excels in high-power microwaves (HPM), unveiling systems like FK-4000, and expands high-altitude EMPs (HEMPs) via a nuclear arsenal projected to 1,000 warheads by 2035. Defenses include commercial standards like GB/T 17626.3 and military research on EMP protections.

The U.S. leads with 3,700 nuclear warheads for HEMP and non-nuclear projects like HiJENKS and THOR. Military hardening follows MIL-STD-188-125-1, but civilian efforts via 2019 Executive Order remain voluntary and limited.

Taiwan lags, with only anti-drone jammers offensively and U.S.-standard military hardening vulnerable to HPMs; civilian IEC standards are inadequate. Conclusion: Offenses outpace defenses, underscoring biases against civilian threats.

Keywords: Electromagnetic Pulse (EMP), Defensive Measures, Geopolitical Comparison

電磁砲的百年軌跡：技術、競賽與應用

詹祥威

網路安全與決策推演研究所

壹、前言

「電磁砲 (Electromagnetic Railgun)」嚴格而言，並非「電磁頻譜作戰」中一環，其原理乃藉電流與磁場產生「物理推力」，進而在不依靠火藥前提下將彈藥以高速擊向目標，如雷射、微波一般，軍事領域將之歸納為「定向能武器 (Directed Energy Weapons)」；然而，由於其在運作時會產生瞬間高頻雜訊與「脈衝電磁干擾 (Impulse Electromagnetic Interference, IEI)」，這些訊號可能分佈在射頻 (Radio Frequency, RF) 範圍，也可能延伸至微波波段，在實際作戰環境中，電磁砲因其為發射源 (emitter) 特性，須視為電磁頻譜作戰環境 (electromagnetic spectrum operation environment, EMOE) 的一部分進行管制，才能確保其他依賴射頻運作的系統不受其運作干擾。謂此，美國與北約軍事概念定義中，電磁頻譜作戰 (Electromagnetic Spectrum Operations, EMSO) 不僅包含干擾、網電作戰，電磁砲之類的定向能武器亦涵蓋在其定義之內。¹

「電磁砲」並非一新興概念，其技術與構想可追溯至 20 世紀初，其以電磁力加速金屬彈體，具備超高速、無火藥、貫穿力強等特性；隨電源儲能與材料科技進步，美國等國自 2000 年起積極投入實驗與研發，以期打造射程更遠、精度更高、作戰成本更低的次世代武器系統。然，儘管具一定技術潛力，但同時也面臨諸多挑戰，

¹ “Electromagnetic Spectrum Operations,” *Air Force Doctrine Publication 3-85*, December 14, 2023, <https://shorturl.at/F4Rh6>, pp. 1-6.

包含能源需求大、砲管磨耗快、作戰平台整合困難等，導致多國研發計畫進展遲緩或暫緩。本文針對電磁砲的發展與近況進行綜整，探討其在電磁頻譜作戰中的持續影響力。

貳、歷史發展與原理

法國發明家安德烈·福雄—維爾普萊（André Louis Octave Fauchon-Villepleé）被認為是該概念的提出者，其在一戰期間提出「電砲（electric cannon）」的概念，希望可以將火炮的距離在電磁協助下，延伸射程使其超越德軍的「威廉皇帝砲（Kaiser-Wilhelm-Geschütz）」；1917年其在「都鐸蓄電池公司（Société anonyme des accumulateurs Tudor）」協助下，創造了一小型工作模型並於1922年獲得美國專利號。² 根據其申請的專利圖可理解，該模型係以電流通過兩條平行匯流排，在磁場中產生推力從而將具備翼片的彈丸沿匯流排射出。

法國軍備部研發總監為此於1918年7月25日委託維爾普萊開發一款30毫米至50毫米的電磁砲，然而該發明因第一次世界大戰中止而提前告終，最終此概念並未被落實。³ 這種武器概念十分單純，加上射擊距離長、超音速，以及高精準度等特性，使得其具備成為正式武器的潛力，雖概念簡單但由於技術、材料的高度限制，使得此概念長期未能被具體實踐化。

² A. L. O. Fauchon-Villepleé, "Electric Gun or Apparatus For Propelling Projectiles," *US Patent*, Patented March 1, 1921, <https://shorturl.at/tXpRW>.

³ Peter Suci, "Railguns: The Game Changer Weapon America's Military Can't Build," *The National Interest*, June 1, 2024, <https://shorturl.at/huusq>.

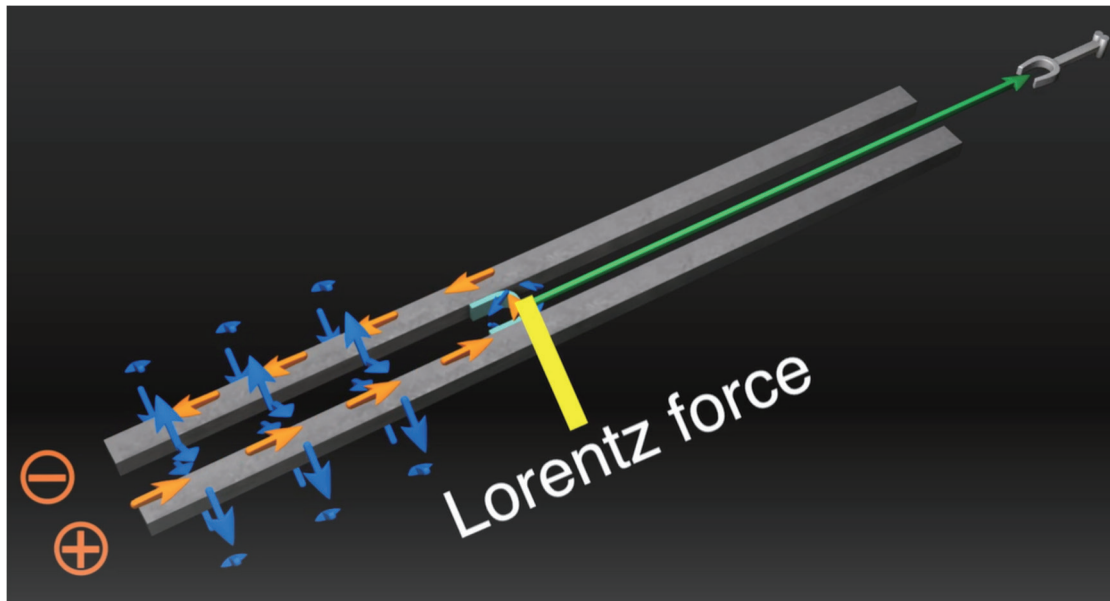


圖 7-1、電磁砲運作原理

圖片來源：截自 News Direct, “US Navy Railgun: How It Works,” *YouTube*, <https://www.youtube.com/watch?v=PQNHsS-BNs4>。

電磁砲的基本運作與運用，被稱為電磁推進（electromagnetic propulsion），其牽涉到「電子加速（Electron Acceleration）」、「電子聚焦（Electron Focusing）」，以及「電子偏轉（Electron Deflection）」三個原理。「電子加速」指在設備中施加高電壓，使電子從陰極被加速射出，此電壓所產生的電場對電子施加作用力而使其加速移動；而「聚焦」則指藉由線圈或其他導電元件產生的磁場可聚焦電子束，使電子會聚成一條細長的光束；在過程中移動電子會產生彎曲，導引至光束中心。「電子偏轉」，則是指磁場偏轉電子束，電子移動過程中所受的勞倫茲力，可改變其運動方向，將其導向不同目標點。當中運動牽涉到「勞倫茲力（Lorentz Force）」和「安培定律（Ampere's Law）」，簡言之就是一條為正極、一條為負極的兩條平行導電軌道，藉巨大電流從一條軌道流向電樞，再沿另一條軌道返回時，會在軌道之間產生一個強大的磁場，其方向

垂直於電流流動方向，而這種電流與磁場的相互作用產生勞侖茲力，從而以極高的速度推動電樞和彈丸沿軌道加速。⁴

與傳統火炮相比，電磁軌道砲確實具有多項顯著優勢，包含：

- 超高初速：在各項試驗中的電磁軌道砲，砲口初速可達 2,000 至 3,500 公尺 / 秒（即 5 馬赫至 7.5 馬赫以上），遠超傳統火藥推進火炮的約 1,219 公尺 / 秒的限制，這種超高初速可轉化為超高動能。
- 延伸射程：超高初速使得砲彈射程大幅增加，理論上潛在射程可達 200-250 海里（約 360-450 公里），超過現有海軍艦艇的艦砲，並且速度亦有相當水準；例如，200 海里的射程僅需約 6 分鐘即可覆蓋，而戰斧巡弋飛彈約需 8 分鐘。
- 純動能彈藥：巨大的撞擊動能意味彈丸無需裝載炸藥彈頭，簡化設計並降低操作人員的安全風險，理論上這種「撞擊殺傷（hit-to-kill）」能力足以摧毀大多數目標。
- 降低單發成本：無需推進燃料與複雜的爆炸彈頭，電磁軌道砲彈丸的成本顯著降低，估計每發僅需 1,000 至 10,000 美元，遠低於一枚數百萬美元的飛彈，例如一枚戰斧飛彈造價約 200 萬美元。⁵
- 增加彈藥儲備：由於無需前述的燃料與爆炸彈頭，整體砲彈體積縮小，在相同艦載空間內，可儲存的軌道砲彈丸數量可達傳統火炮的兩到三倍。

⁴ Peter Graneau, "Application of Ampere's Force Law to Railgun Accelerators," *AIP Publishing LLC*, June 22, 1982, <https://shorturl.at/97VDv>.

⁵ Roman Pryhodko, "United States Has Agreed to Sell the Latest Version of Tomahawk Missiles to the Netherlands," *Militarnyi*, April 26, 2025, <https://shorturl.at/1BQ8e>.

- 提高安全性：缺乏揮發性推進劑和爆炸彈頭，消除傳統彈藥處理和運輸相關的重大安全風險，即便彈藥電動搬運系統失效，人員搬運彈藥困難與危險性亦大幅降低。
- 難以攔截：一旦發射，電磁軌道砲彈丸的極高速度使其幾乎不可能被現有防禦系統摧毀或攔截。

然，要能順利以電磁進行砲彈的發射，其主要技術限制在於高耗能、熱管理以及耐久性等。當前研究普遍認為，要將數公斤重的彈丸加速到數倍音速，瞬間所需的電力會達到數十萬到數百萬焦耳，峰值功率可能高達數十兆瓦（megawatts）甚至百兆瓦，亦即數毫秒間的每一個發射動作，將「一次性釋放」一般家庭數日乃至數月的總用電量。而如前所述，在瞬間產生巨大電流的同時，除需要強大電力支持外，勢必面臨高衝擊 IEI、高熱，以及砲身、砲管所需承受的耐久性等問題；因此，「高耗能」、「超高溫」，以及「耐用性」一直是電磁軌道砲發展的三大技術阻礙。

參、各國發展現況與特徵

一、美國

1995 年在美國德州奧斯丁大學提出了當代先進電磁砲研究，並成功驗證電磁砲技術在軍事層次的應用可行性，在發射效率、結構設計與系統整合方面取得突破性進展。⁶該研究以 82% 石墨纖維與 18% 玻璃纖維組成「纖維複合纏繞外殼」，以及「AD-96 氧化鋁陶瓷」，嘗試克服「超高溫」及「耐用性」的問題，而使外殼足以提供軸向剛性並承受預載應力，既有強度又有必要之韌性，同時確保

⁶ Yun, H.D., Price, J.H., “Electromagnetic and Structural Analyses of Electric Gun and Integrated Launch Package Systems,” *Center for Electromechanics*, The University of Texas at Austin, January 1995, <https://shorturl.at/2PFLW>.

「陶瓷側壁」在放電過程中保持壓縮狀態，避免過多的瞬間位移影響發射的穩定。

在此研究下，基本達成了 0.2 秒快速發射率、每秒 1,850 公尺的射擊初速，以及「理論上」以 185 克彈藥在 1,500 公尺擊穿 73 毫米裝甲，以及 3,000 公尺擊穿 37 毫米裝甲的打擊效能。儘管此研究提供具體且看似可被解答的分析與解決方案，但實際測試電磁砲發射瞬間溫度可達數千度、殘留熱應力會衝擊金屬軌道，影響持續運作效力，同時其冷卻系統體積過度龐大，影響平台與系統的整合及有效運用。

根據後續美軍持續研究與測試，前述各種挑戰使電磁砲在平均使用 12 至 24 次發射後，就必須強迫更換砲管，而相對傳統火炮的數值為 600 次；⁷因此雖每次發射的成本遠低於傳統火炮，但在前述數值難達有效率的軍事作戰部署要求，且前述的各項管理問題無解下，美國在 2021 年最終取消了該研發的進行。總計美國在此 15 年的專案研發中，投入至少 11 億美元。⁸然，雖計畫以停止研發告終，但仍留下 2,500 m/s 初速的成績，以及可反覆充、放電的模組化電源與能量管理的「能量儲存與脈衝電源模組（Pulse Power Module, PPM）」技術。

二、英國

英國投入「電磁砲」的研發時間約在冷戰期間，英國皇家軍備研究與開發局（Royal Armament Research and Development

⁷ Bryan Lynn, "US Navy Cancels Development of High-Tech Railgun Weapon," *VOA*, July 7, 2021, <https://shorturl.at/Bf32V>.

⁸ "Navy Lasers, Railgun, and Gun-Launched Guided Projectile: Background and Issues for Congress," *Congressional Research Service*, April 1, 2022, <https://shorturl.at/aHOQN>.

Establishment, RARDE) 在蘇格蘭柯庫布里 / 鄧德倫南靶場建立「電磁發射設施 (Electromagnetic Launch Facility)」以藉由大型實體發射器驗證高初速彈體的可行性。⁹當時的整體運作模式，係由 RARDE 主導基礎科學技術與原理研究，國內產業進行後續可行性分析與子系統研製。

該設計原理，是將需要快速切換高電流脈衝電路的「高電流脈衝的主開關」與「砲膛尾端 (breach)」設計成一個平行軌式的「開關軌道」，在充電時由開關軌短路主軌；發射瞬間，開關軌上的滑動電樞跨越絕緣缺口，在開關軌上拉弧並抬升弧電壓，把電流快速「換流」進入主發射軌與砲彈電樞，達成極快速的大電流注入。¹⁰在該研究計畫最終達成的結果，是該方案可提供 12 百萬焦耳

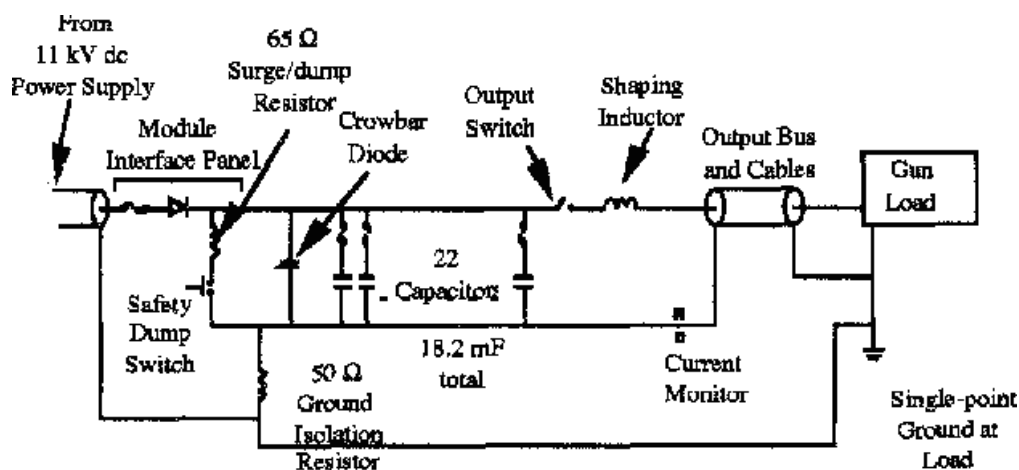


Figure 4. Simplified pulsed power circuit.

圖 7-2、英國 RARDE 設計之電磁砲運作原理

圖片來源：H. G. Hammon et al., “The Kirkcudbright Electromagnetic Launch Facility,” in *IEEE Transactions on Magnetics*, Vol. 29, No. 1, January 1993, pp. 975-979,

⁹ H. G. Hammon et al., “The Kirkcudbright Electromagnetic Launch Facility,” in *IEEE Transactions on Magnetics*, Vol. 29, No. 1, pp. 975-979, Jan. 1993.

¹⁰ David W. Scherbarth, et. Al., “Rotary Switch For Multiple Shot Electromagnetic Launchers,” *United States Patent* No. 4,841,833, June 27, 1989, <https://shorturl.at/kaulE>.

(MJ) 的槍口能量；射擊速度在 2.0 至 3.5 每秒 / 公里間；重複射擊率高達「每日 10 發」，兩次射擊之間的時間不超過 30 分鐘。

實際上，後續英國 RARDE 停止該系統的持續研發，而美英聯合軍火商 BAE 則將此系統於 2006 年投入美國海軍水面作戰中心合約中，甚至成功開發出 32 兆焦耳的原型機並於 2012 年交付海軍，當時美國海軍實驗室公開測試該系統影片仍留存在網路；¹¹而前述美國海軍所進行的研發雛形，便是 BAE 交付、由英國 RARDE 啟動研發產生的該方案。同時期美國海軍除採用 BAE 系統外，另有通用原子 (General Atomics) 與雷神公司 (Raytheon Co.)，最終英美分別因技術與能源問題難以克服而停止該研發計畫。

三、中國

中國始終是開發電磁砲最活躍的國家之一，冷戰後 2010 至 2011 年就已首次公開其電磁砲研發，而藉由美國的研發經驗，中國從研發初期就聚焦於電力系統的開發。中國工程院院士、海軍工程大學教授馬偉明在 2007 年由國家支持下建立「艦艇綜合電力技術國防科技重點實驗室」，¹²專門解決船艦電力系統問題，以克服普遍電磁砲的船艦電力瓶頸；亦即馬偉明領導的團隊不僅從電磁砲技術開發本身著手，更同時嘗試克服加大與穩定船艦供電系統的挑戰。

也因為此種雙管齊下的研發路徑，使得中國相較其他國家更早將電磁砲安裝於艦上測試；2018 年在社交平台 X (推特, twitter) 就揭露了 072II 型登陸艦 936 海洋山安裝了電磁軌道砲，然實際卻從未有射擊畫面揭露；而從露出的照片比例判斷，滿載 4,000 餘噸，長

¹¹ Airboyd, "Office of Naval Research Electromagnetic Railgun Program Commissioning Test of BAE Built Railgun at NSWC Dahlgren," *YouTube*, October 31, 2012, <https://bit.ly/45IFJ9e>.

¹² 〈中國建立艦艇綜合電力技術國防科技重點實驗室〉，新浪軍事，2007 年 4 月 29 日，<https://shorturl.at/XXvsV>。

120 公尺、寬 15.3 公尺的 072II 艦，電磁砲砲身就可能長達 10 餘公尺，以比例而言其體積超過其他國家之測試品，更甚者相較於日美 40mm 砲彈，中國砲彈僅 25mm 而砲身卻更大，且疑似另外搭載貨櫃提供必要動力或發電裝置。¹³

為克服前述三大技術門檻中的「高耗能」，馬偉明的中國團隊從船艦發電系統著手，推出了有別於歐美使用數百年的「中壓交流 (MVAC)」系統，而採用「中壓直流綜合電力系統 (Medium Voltage DC Distribution Systems, MVDC)」，差異在於 MVDC 可提供更高的能源效率，且電力損耗通常較低，較能完整、有效的運用轉換船艦產生的有限電力，以及更好的整合船艦各種電力負載。而中國高效的「軍民融合體制」也為其有效推進軍事技術研發提供良



圖 7-3、中國艦載電磁砲

圖片來源：Dafeng Cao, on *X.com*, January 31, 2018, <https://tinyurl.com/23uje7us>。

¹³ Jeffrey Lin, P.W. Singer, “Looks Like China Just Installed a Railgun on a Warship, Beating the U.S. Navy To The Punch,” *Popular Science*, July 6, 2021, <https://shorturl.at/Xu0hw>.

好前提，「十五」、「十一五」的電力系統的基礎理論體系，為其船艦發電提供一定的研發基礎。¹⁴

除電力系統外，中國嘗試在克服三大門檻中的「超高溫」及「耐用性」的問題，使用液態金屬塗層減低砲管磨損，並開發「磁化電漿砲（Magnetized Plasma Cannon）」以「磁化電漿」技術改進發射機制，使其更適合移動平台應用；「磁化電漿砲」主要運用在電磁軌道砲的「砲管內壁」和「發射系統」，砲管內壁塗裝毫米厚的「磁化電漿保護層」覆蓋，保護層可減少彈丸與砲管間的摩擦和徑向力，並有效提供熱絕緣以解決傳統電磁軌道砲的軌道燒蝕問題。

當前中國藉新興科技協助，在測試裝置上大規模安裝人工智慧 AI 感測器，藉此蒐集大量數據以期改善既有裝置的不足；2024 年中國官媒「南華早報」公開揭露「電磁砲以 5 馬赫速度將砲彈發射至 15,000 公尺之平流層」，但由於上升過程旋轉太快而出現明顯偏航；¹⁵此外，該報稍早更強調在「實際測試」下，該系統可「快速發射大量子彈而不受損」，暗示著該系統已克服三大門檻中的「耐用性」。¹⁶雖始終沒有任何公開測試影片釋出，若根據事後的揭露資訊為真，即便 5 馬赫的出速低於美國的 7 馬赫，但能克服快速、大量、且無損害的發射仍是相當的重要進展。

可以肯定的是，在研發電磁砲同時啟動的電力系統研發，確實

¹⁴ 馬偉明，〈中國實現中壓直流綜合電力系統 世界首家〉，《人民網》，2014 年 11 月 14 日，<https://shorturl.at/zMBxO>。

¹⁵ Stephen Chen, “China’s Rail Gun Sends Smart Bomb into Stratosphere at Hypersonic Speed, then Something Goes Wrong,” *SCMP*, May 14, 2024, <https://shorturl.at/Mty4G>.

¹⁶ Stephen Chen, “2 Years After US Killed the Rail Gun, China Brings Weapon Back to Life with Technological Leap,” *SCMP*, December 9, 2023, <https://shorturl.at/UETyw>.

使得中國在電磁系統運用上取得相當進展，最終該技術也據傳被運用在最新「福建號」航空母艦的電磁彈射系統中。¹⁷

四、日本

相較於美國初期發展的定位乃是「進攻型」，日本自始便將電磁軌道砲發展定位在「防衛用途」；為有效因應西部方面的超音速導彈威脅，在 1990 年就由防衛裝備廳啟動小型電磁砲的基礎研究；2016 年正式啟動的研發汲取美國研發的教訓，在初期研發階段的經費投入，在 2016 年至 2019 年 3 年間的研發總投入約為 3 億美元，相較美國初期投入資金為 5 億美元相比，日本的經費要顯得更為謹慎。¹⁸

由防衛省防衛裝備廳（ATLA, Acquisition, Technology & Logistics Agency）陸上系統研究中心（GSRC, Ground Systems Research Center）主責的研發，在 2021 年成功試作 40mm 中型電磁軌道砲原型機，目標設定為將 320 克的彈丸以 2,297 公尺/秒（約 6.6 馬赫）的初速發射，雖該原型設計僅能進行單發射擊，但其目標是建立高出速與飛行過程中「彈丸穩定」的基礎關鍵技術，而此二者對後續的延續性開發與實質作戰至關重要。¹⁹

相較於中國的原型測試機長 10 餘公尺，日本的防衛裝備廳原型測試機口徑 40mm，全長約 6 公尺、總重約 8 噸，另外搭載三個外掛集成電源提供與管理。從 2016 年啟動的計畫，到 2022 年為止的 7 年間，日本投入總共約 650 萬美元，達成了「彈丸出速每秒 2,000 公尺

¹⁷ 馮小川、陳志輝，〈中國第三航母福建艦下水 新電磁彈射技術挑戰美國〉，《亞洲周刊》，2022 年第 26 期，2022 年 6 月 27 日，<https://shorturl.at/UE9Jz>。

¹⁸ “Japan’s New Railgun Naval Weapon,” *Australian Naval Institute*, July 6, 2025, <https://shorturl.at/58DxI>.

¹⁹ 內田泰，〈電磁砲で世界初の洋上射撃、防空網突破の極超音速兵器迎撃狙う〉，《日経クロステック》，2023 年 11 月 2 日，<https://shorturl.at/7tyNy>。

以上、砲身壽命 120 發以上」的單發型測試。

此原型機測試主要目的，在於先以小口徑原型機蒐集大量數據，藉此構想與驗證中口徑技術可行性並將成本效率化，同時藉此基礎技術透過國際技術交流與共同研究以期降低風險。2024 年度至 2028 年度，防衛裝備廳預計持續以原型機進行內部測試，主要著重在三大目標：最佳化放電模式和電路設計以達到技術節能與能源部件小型化、開發電磁砲彈專用裝填技術與確立射擊程序實現高速射擊目標，以及克服發射造成的熱力效應與砲彈彈體的改進達成高超音速飛行的穩定性和末端速度確保。²⁰

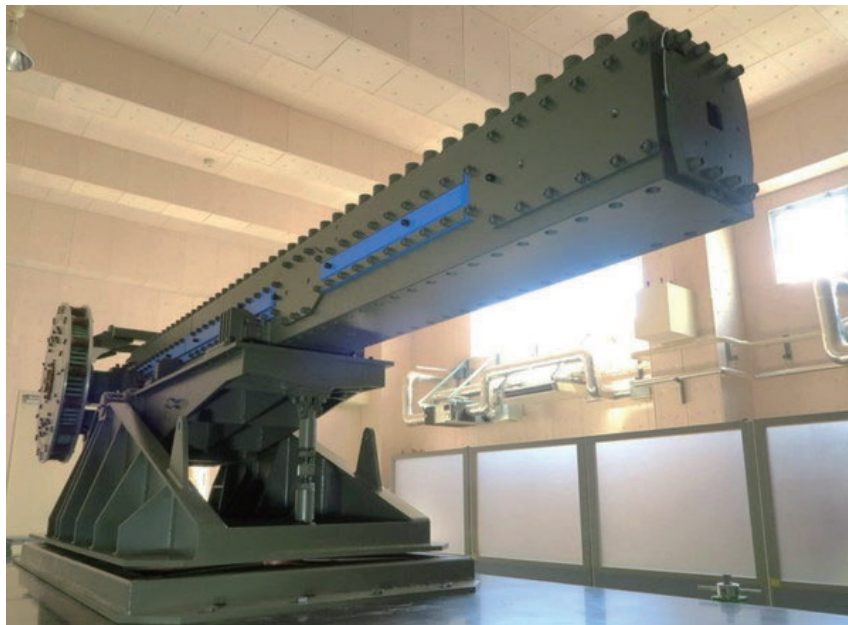


圖 7-4、防衛裝備廳於 2021 年成功試作的 40mm 中型電磁軌道砲
原型機

圖片來源：內田 泰，〈電磁砲で世界初の洋上射撃、防空網突破の極超音速兵器迎撃狙う〉，《日経クロステック》，2023 年 11 月 02 日，<https://shorturl.at/7tyNy>。

值得注意的是日本汲取他國開發的教訓，在研究開發的同時與

²⁰ 防衛裝備庁技術戦略部技術計画官，〈将来レールガンの研究〉，《令和 3 年度 政策評価書（事前の事業評価）》，2021 年 8 月，<https://shorturl.at/qwKFO>。

各國簽訂合作協議，交換各國研發的專長項目以減少誤區。2023 年防衛裝備廳派遣研究員與工程師赴美國海軍研究機構，以實質技術交流吸取美國既有研發經驗與教訓；2024 年，日本與法國、德國簽署《電磁砲技術合作實施指南》，建立三邊技術交流與專家互訪、定期召開技術會議，以及在研發、測試與評估領域展開協同合作的跨國合作機制。²¹

日本在其精密製造和材料科學等領域具有深厚基礎與獨特優勢，此點在開發電磁砲過程佔有相當決定性影響；如前述當前電磁砲三大門檻，日本產業技術綜合研究所就成功開展關於「化學沉積表面塗層」技術的研發；該技術主要是將「固態粒子」噴附薄膜上使其固化，藉此減少高溫加工可能造成的耗能與材料異劣，藉由將塗層材料如陶瓷研磨，或以其他工法製成微米乃至奈米級粉末，再以氣溶膠技術高速加熱噴附於欲加工之表面，形成極致薄膜陶瓷塗層。²²前述砲彈發射過程會產生高熱，並對砲身金屬形成熱應力累積，藉此陶瓷或其他材料的薄膜塗層技術，將可有效阻絕與避免此現象。

2023 年，日本產業技術綜合研究所成功進行首次海上試射，²³ 2025 年，ATLA 將電磁砲安裝於海上自衛隊測試艦飛鳥號（ASE-6102），雖為文時尚未進行擊發測試，但整體預計針對艦載化與航行間穩定性等項目蒐集數據作為後續研發的基礎。日本多次明確表示，電磁砲的運用在於綜合防空與超高音速飛彈攔截，以及作為海

²¹ Inder Singh Bisht, “Japan Signs Railgun Cooperation Agreement with France, Germany,” *The Defense Post*, June 4, 2024, <https://shorturl.at/6VsIB>.

²² 山田貴壽等，〈二次元ナノデバイス材料研究チーム〉，《ナノカーボンデバイス研究センター》，<https://shorturl.at/VF818>。

²³ “ATLA has Accomplished Ship-Board Firing Test of Railgun First Time in the World with the Cooperation of the JMSDF,” *X*, October 17, 2023, <https://tinyurl.com/2f7ytdmp>.

基、陸基反艦的制海打擊，並且尋求進一步將電磁砲與「13DDX」次世代驅逐艦進行整合，因此 2025 年的上艦測試可解讀為日本當前正逐步實踐其計畫的預期目標。

對於電磁砲的三大阻礙，「高耗能」、「超高溫」，以及「耐用性」的致命傷，日本藉由其深厚基礎研究顯然逐步克服，不僅實際部署在艦上進行進一步海上測試，更在實驗室達成連續 120 發而砲身為有明顯損害的階段性目標。下一步重點將是如何克服在艦載電力系統管理以及電磁砲的高耗能最佳化間取得平衡，乃至於最終如何將其與艦載作戰系統、指揮鏈路系統進一步整合。

肆、優劣與戰場態勢分析

除前述電磁砲開發的技術門檻與各國進展外，電磁砲此概念自身若能成功部署，其整體優劣勢為何，何以各國相繼投入資源進行開發？

前述提及，電磁砲的原理乃藉電磁驅動不帶火藥的砲彈進行高速動能打擊，由於砲彈不含任何火藥或引爆裝置，其破壞力來自發射時所賦予的「巨大動能」，其效果可想像等同一節火車以 160 公里時速穿過一面牆，憑藉彈體自身與 6 馬赫以上的動能，砲彈能輕易穿透既有金屬材料的船隻或建築物進而對目標物造成毀滅性打擊。即便缺乏傳統飛彈的後續爆炸破壞，但藉由動能打擊所造成的刺穿亦能使載具永久失效而失去作戰能力。

此種「動能殺傷」的作戰模式為既有戰場帶來兩大核心優勢，第一是「作戰安全」，由於艦艇不再需要儲存大量易燃易爆的彈藥，極大地降低了因戰損乃至於搬運意外而造成的各種風險，從而提高艦船與人員的安全與生存機率；其次也由於彈丸的體積相較傳

統彈藥更小、更輕，因此將對後勤需求大幅簡化。固態金屬彈丸不僅生產與運輸成本低廉且易於儲存，此將極大簡化後勤供應鏈乃至船艦儲存空間，進而使多餘空間可做更多彈性配置。也由於固態金屬彈丸的生產，無論體積或價格相較於既有飛彈都更低，因此可預期船艦可以裝載更多的彈藥儲備，面對潛在的敵方「飽和攻擊」便有更多的攔截成本，改變整體船艦防空作戰的態勢。

而在整體海戰方面，過去藉由昂貴的戰斧等飛彈方能達成的「短時超距」打擊型態，如今在 6 馬赫動能的電磁砲中，以相對極低成本即可完成；此外，由於彈丸體積小且相較飛彈沒有明顯熱源特徵，難以被攔截雷達探測並反制，搭配著高速特性極高的提升了有效打擊機率。而在防守端方面，由於直線高速與動能等特性，可搭配既有飛彈防禦、方陣快砲等形成了船艦的三層防空交錯網絡，依據戰場發展態勢與敵方來襲的種類進行最適防守選項。近年，隨高超音速武器崛起與定向能武器加速發展，電磁砲的角色逐漸轉變，從獨立武器系統轉為技術平台與模組應用的研發介面，未來亦可能與電磁脈衝武器、反飛彈系統等整合，持續在電磁頻譜作戰中發揮影響力。

此外，由於前述各國針對電磁砲各有其專長，美國、日本、法國、德國的合作亦形成了戰略武器為核心的合作模式，恰好再次強化了「印太民主國家」與「專制威權國家」為核心的地緣戰略對抗態勢，亦由於電磁砲的研發耗時冗長且需長期資金投入，因此中國的威權主義與軍民融合體制為其提供相當優勢，但前述民主國家的合作亦可平衡此種優劣對比。

伍、代結語

電磁砲的發展歷程，從一個世紀前的概念萌芽，到如今成為一種先進的武器系統，充滿了技術挑戰與戰略權衡。其核心優勢在於超高初速、遠程動能打擊、低單發成本和高安全性，此種優勢使其在理論上具備顛覆既有海戰的潛力。然而，其發展始終受到三大核心工程阻礙：巨大瞬間耗能、砲管在極端高溫和機械應力下的快速磨損與耐用，及將龐大系統整合到有限平台上的複雜性。

這些挑戰形塑了各國不同的發展路徑。美國在投入巨額資金並取得顯著技術成就後，因持續的技術障礙、財政限制及戰略重心轉向高超音速飛彈和定向能武器的研發而暫停其計畫。意味即便技術領先的國家，也必須在研發投入與實際部署可行性之間做出務實選擇。相對，日本與中國則持續推動各自計畫；日本採取小心務實的策略，以其深厚的金屬加工與材料研發功力，專注於高耗能與耐用性等關鍵問題，並已成功在 120 發連續射擊後，砲管耐用性上取得重大突破，後續更將此計畫作為高超音速飛彈威脅的防禦手段。

而相對中國則以大膽、炫目的技術引人注意，包括聲稱以先進人工技術 AI 輔助進行砲管管理，乃至於以「液態金屬」與其他冷卻技術解決熱應力等門檻，而儘管其測試彈丸口徑較小，實際擊發的測試也未可見，因此能否成功將研發轉至作戰部署仍待長期觀察。

而按電磁砲的運作原理，涉及「電子加速」、「電子聚焦」，以及「電子偏轉」三個原理，實際投入作戰時是否在擊發、運作同時產生大電流脈衝乃至強烈電弧，而對於既有設備造成「物理損傷」、「電磁設備干擾」，乃至於瞬間超高電流與高壓對周邊人員、設備可能造成的安全風險等，都是進一步投入戰鬥部署前，除了砲身自身技術外必須研究與克服的基礎課題。

電磁砲並非簡單的技術競賽，而是對基礎科學、加工技術乃至

工程整合的極限性挑戰。儘管其作為一低成本、高射速的動能武器，在防空、反艦乃至對地支援等具有獨特優勢，但其廣泛部署仍有賴於前述科學與技術的根本性突破。若能克服這些障礙，電磁砲將有望成為未來多層次防禦體系中的重要組成部分，與高超音速飛彈和定向能量武器形成互補。即便最終電磁砲以失敗告終，研發過程中的前述基礎科學、加工技術乃至工程整合得到的成果，亦可作為整體人類器物文明進展的新基礎。

本文作者詹祥威為淡江大學國際事務與戰略研究所博士，現為財團法人國防安全研究院網路安全與決策推演所助理研究員，主要研究領域為海洋安全、地緣戰略、電子戰與兵棋推演。

The Centenary Trajectory of Electromagnetic Railguns: Technology, Competition, and Applications

Siông-Ui, Tsiam

Division of Cybersecurity & Wargaming Simulation

Abstract

Electromagnetic railgun technology represents a significant military shift, using the Lorentz force to launch projectiles at hypersonic velocities exceeding Mach 5. This approach eliminates the need for explosives, leading to cheaper ammunition and deeper magazines, which overcome the imbalanced 'cost exchange ratio' of modern naval defence. However, the technology is plagued by immense power demands, rapid barrel wear, and guidance issues for projectiles at extreme speeds.

Once a pioneer, the United States discontinued its large-scale programme in 2021 after failing to resolve issues with barrel durability and power supply integration. In contrast, Japan has become a frontrunner, with its Agency overcoming the critical barrel wear problem with a new material, achieving a barrel life from its prototype. This success underpins Japan's strategic focus on using railguns for hypersonic defence. Concurrently, China is aggressively pursuing its path, leveraging its expertise in integrated shipboard power systems.

While the technology is still nascent, these diverging international efforts highlight its disruptive potential. The ability to field a high-volume, low-cost kinetic weapon is poised to fundamentally reshape naval strategy and combat economics.

Keywords: Electronic Spectrum Operations, Direct Energy Weapons, Railgun