美國陸軍多領域作戰下的電子戰

舒孝煌

中共政軍與作戰概念研究所

壹、前言

冷戰結束後，美國在沙漠風暴、持久自由等軍事行動獲得壓倒性勝利，除軍事科技優勢外，新作戰概念如聯合作戰、精準打擊、聯合 C4ISR、有效的聯合火力（effective joint fires）等，都是其作戰成功不可或缺的要素。[1]近年來新發展的技術，例如人工智慧（AI）、極音速、機器學習（machine learning）、奈米技術及機器人等，隨著這些技術逐漸運用在軍事上，有可能再一次徹底改變戰場的作戰型態。[2]

美國正擔心其優勢受到挑戰。中共、俄羅斯、伊朗、北韓等「修正主義國家」，除藉「灰色地帶」手段威脅美國的盟友與夥伴外，並運用多重領域手段，包括海上、空中、陸上、太空、網路與電磁空間，設法擊敗對手，這樣可在低於武裝衝突的門檻下達到目標，並使美國的聯合作戰部隊失去作戰優勢，或派遣美軍介入的自由。

美國陸軍長期忽略電子戰發展，面對中共、俄羅斯的威脅，為保持作戰優勢，美國防部必須尋求革命性的、跨越式技術和能力，重獲電子戰優勢，以便與一系列對手競爭。

貳、中共及俄羅斯電子戰威脅

美國的競爭者在建設和現代化其地面部隊電子戰能力，都獲得長足進步，例如俄羅斯、北韓和中共等，其電戰能力將使美國陸軍

[1] Jeffrey M Reilly, “Multi-Domain Operations,” *Essay of Joint Air & Space Power Conference 2019*, October 8-10, 2019, https://www.japcc.org/multi-domain-operations/.

[2] US Army, “The U.S. Army in Multi-Domain Operations 2028”, *US Army*, December 6, 2018, https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf.

現有通訊裝備（包括所有語音和衛星通訊）退化、情況感知（包括所有 GPS 和即時功能）、所有指揮管制、火力偵測和測向雷達、無人機指揮鏈、以及許多其他運用電磁頻譜計畫的能力均受到影響。報告認為，美國陸軍正面對巨大的電子戰威脅。[3]

美國智庫蘭德公司（RAND）提莫西·邦德斯（Timothy Bonds）2017 年向眾議院作證指出，俄軍在現代防空網路、長程飛彈、網路空軍、電子戰能力，持續發展新系統或改良現有系統，美軍在電子戰上已輸掉與俄軍的競爭。[4]

一、中共及俄羅斯電子戰的挑戰

美國國防部 2022 年《2020 年中國軍事及安全發展報告》（*Military and Security Developments Involving the People's Republic of China 2022*，以下簡稱《中國軍力報告》）指出，解放軍認為電子戰是現代戰爭不可或缺的組成部分，並尋求運用網路戰及電子戰以保護自己的資訊網路，並阻止敵人使用電磁頻譜，從而在戰爭中獲得資訊優勢。

中共電子戰強調在整個衝突過程中壓制、降級、干擾或欺騙敵方電子設備，並在衝突開始時運用電子戰來警告並阻止對手的攻勢行動。其潛在的電子戰目標包括運用無線電、雷達、微波、紅外線或光學頻譜範圍內運作的敵方系統，以及敵方的資訊系統。解放軍電戰部隊經常在演習期間對多個通訊、雷達及全球衛星定位系統（GPS）進行干擾或反干擾操作，測試這些作戰單位對電戰武器、設備及程序的理解，並使作戰人員提高在複雜電磁環境中有效作戰的信心，同時也在演習中測試及驗證電子戰裝備。[5]

---

[3] "Short History of US Army Electronic Warfare," *SITREP*, Q1, 2016, https://www.leonardodrs.com/sitrep/q1-2016-the-invisible-fight/short-history-of-us-army-electronic-warfare/#_ftn1.

[4] Maj. Morgan J. Spring-Glace, "Return of Ground-Based Electronic Warfare Platforms and Force Structure," *Military Review*, July-August, 2019, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/July-August-2019/Spring-Glace-Electronic-Warfare/.

[5] "Military and Security Developments Involving the People's Republic of China 2022," *US DoD*,

中共電子戰能力分布在戰略支援部隊，解放軍持續為其部隊實施現代化，並在陸、海、空、太空及網路作戰。由於資訊及快速決策對現代作戰至為重要，中國極重視解放軍在近距離及遠距離戰場指揮複雜聯合作戰能力，正在增強解放軍的聯合指揮及管制系統、聯合後勤、以及其 C4ISR 系統。

中共也可能開發專門針對情監偵系統的干擾設備，安裝在軍事偵察平台上，干擾美國偵察衛星運作以保護其地面資產，並開發針對衛星通訊的干擾系統。中共也在其文獻中提及對台灣實施兩棲入侵的不同概念，在聯合島嶼入侵戰役中，中共設想一系列對台行動，依賴電戰、後勤、空中及海上作戰支持，以奪佔全台。

二、俄烏戰爭的電子戰

俄羅斯也長期投入資源，發展各種規模和能力的陸基電子戰系統，包括機動式及固定式，有的系統可在遠距離干擾無線電和雷達。俄羅斯能夠在戰術、作戰和戰略層級上整合網路空間和電子戰能力。

在戰略和作戰層級上，俄羅斯共編組 5 個電子戰旅，在西部軍區編組兩個電子戰旅，這屬於俄羅斯地面部隊（RGF）。地面部隊作戰和戰略部隊試圖在各層級混淆和欺騙敵對部隊的軍事決策者，這藉由結合網路空間和資訊戰能力，同時也將防空能力整合為反介入／區域拒止戰略（Anti-Access/Area Denial，A2/AD）的一部分，保護作戰資產並避免進入衝突地區。俄軍在每個作戰旅中都設有電戰連，軍區下還設有電戰旅，[6]每個電戰旅均包括 4 個電戰營，可以完成作戰和戰略任務，或支持較小的地面部隊單位，例如師或更低階部隊。[7]機動旅有一個電戰連，一個無人機（UAS）連和一個情報

November 29, 2022, https://www.defense.gov/News/Releases/Release/Article/3230516/2022-report-on-military-and-security-developments-involving-the-peoples-republi/.

[6] "Army Boosts Electronic Warfare Numbers, Training, Role," *Breaking Defense*, August 7, 2018, https://breakingdefense.com/2018/08/army-boosts-electronic-warfare-numbers-training-role/.

[7] "Return of Ground-Based Electronic Warfare Platforms and Force Structure," *Military Review*, July-August, 2019, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-

支持排。

在電戰連中，有12個車載電戰平台和15個便攜式平台干擾器，每個車載干擾器都有不同的功能，可為旅長提供一系列通信、雷達和其他干擾功能。每個電戰連都可以通過電子方式定位目標；阻塞和破壞高頻、超高頻和超高頻通信；並干擾、破壞或欺騙 GPS，包括模仿 GPS 位置／定時，以及對無人機通用數據鏈路的其他干擾，這可能會危害或劫持大多數的無人機。它們可干擾地面、機載和海事雷達，干擾範圍達300公里。

2022 年俄對烏發動特別軍事行動後，俄、烏雙方均在戰場上運用電子戰，定位、干擾及阻斷對手的武器、無人機的操作及 GPS 訊號，以及對方的通訊。俄羅斯在烏克蘭戰場使用電戰干擾日益增加，但星鏈系統（Star Link）不易受干擾，因為破譯十分困難。[8]

英國智庫「皇家三軍研究所」（Royal United Services Institute，RUSI）報告認為，俄羅斯電子戰能力，從開戰至今已發揮相當效果，對烏克蘭的無人機操作造成干擾，烏軍要結合火力、射程及精準來擊敗俄軍，部隊就要能建立從識別到回傳目標資訊的擊殺鏈（Kill Chain），這可由無人機提供，但會被俄軍電子戰阻礙，傳遞即時資訊也會被偵測。但若無法建立擊殺鏈，就會阻礙烏克蘭運用西方提供的先進武器。[9]

俄軍曾在敘利亞戰場運用手持和固定式干擾槍壓制無人機。俄烏戰前也曾要求各部隊接受反無人機訓練（c-UAS），並發展可偵測及標定其他無人機的新型雷達及無人機，例如最新的 Krasukha-S4

Archives/July-August-2019/Spring-Glace-Electronic-Warfare/.

[8] "How Electronic Warfare is Reshaping the War Between Russia and Ukraine," *The Record*, August 16, 2022, https://therecord.media/how-electronic-warfare-is-reshaping-the-war-between-russia-and-ukraine/.

[9] Greg Waldron, "Russia poses tough EW problem for Ukrainian UAVs: RUSI," *Flight Global*, July 13, 2022, https://www.flightglobal.com/military-uavs/russia-poses-tough-ew-problem-for-ukrainian-uavs-rusi/149311.article?utm_source=rss&utm_medium=Sendible&utm_campaign=RSS.

複合式電戰車，以及便攜式反無人機槍。[10]

參、美國陸軍電子戰發展現況

依美國國防部定義，電子戰是一種使用電磁能控制電磁頻譜（electromagnetic spectrum）並攻擊敵人的軍事行動，頻譜則指電磁波能量的範圍。電子戰也包括讓我方軍事指揮官藉通訊指揮部隊，並阻止敵方藉電磁頻譜進行通訊，因此電子戰也被認為是反介入／區域拒止（A2/AD）戰略的一環。

一、陸地電子戰

陸地電子戰是陸軍及海軍陸戰隊的一系列作戰程序，用以影響地面部隊作戰的電磁頻譜。電子戰指使用電磁頻譜以發現、監聽、干擾、欺騙敵方雷達、通訊、資料鏈、以及其他電子系統。相關作戰程序包括：簡易爆炸裝置反制系統（Counter Improvised Explosive Device，C-IED）、無人機反制系統（Counter Unmanned Aerial Systems，C-UAS）、以及通訊及雷達干擾系統等。[11]

電子戰分為三大類：

電子保護：採取行動保護我軍人員、設施、裝備，避免因敵方使用電子手段，使我方戰鬥能力減弱，這包括電磁頻譜管理、電磁強化、傳輸器管制等。

電子攻擊：使用電磁能來減少或阻止敵人電磁頻譜的使用，包括電磁干擾（如自我保護干擾裝置或是距外干擾）、定位、導航及即時拒止、電磁欺騙、直接能、反輻射飛彈、消耗性措施如熱焰彈、干擾絲等。

電子支援：尋找、識別、分類及標定屬於友好或敵方部隊的發

[10] Samuel Bendett, "Russia's real-world experience is driving counter-drone innovations," *Defense News*, May 24, 2021, https://www.defensenews.com/opinion/commentary/2021/05/23/russias-real-world-experience-is-driving-counter-drone-innovations/.

[11] "Ground Electronic Warfare: Background and Issues for Congress," *CRS Report*, September 17, 2019, https://www.everycrsreport.com/reports/R45919.html#_Toc19692667.

射源，並分辨其威脅、目標、計畫，以保護我軍部隊，或發展拒止敵方運用電磁頻譜的計畫。

這些手段可以相互支持，也可以獨立進行。電子支援系統可以評估友軍及敵軍的發射裝置，並發展保護計畫，維持我方對電子頻譜的運用，或發展電子攻擊計畫，拒止敵方運用，例如干擾敵方雷達或通訊等。

軍事能力愈先進，則電子戰便能發揮愈大效果。現代武器都要透過電磁頻譜來進行導引，將破壞力集中至預定的目標，另也依賴電磁頻譜來發現目標，並完成擊中目標前必要的資訊傳遞、追蹤等程序，這常被稱為「擊殺鏈」，因此電子戰的目的，也在於使用電磁頻譜來阻止這些武器攻擊目標；而發射電磁訊號的發射源，如雷達和通訊系統，本身也會成為被攻擊的目標。

電子戰可以影響所有軍事領域，包括陸地、海上、空中、太空，以及網路空間，每個軍種都有自己的電子戰能力與計畫。電子戰傳統上分為地表及空中兩類，由於每一類型都有其優缺點，因此需要多重功能才能提供所需要的效果，例如機載式電子戰系統，常被用於對廣區域通訊、雷達、以及其他指揮管制系統的攔截、解密及破壞。但這些功能受限於飛機本身的耐航能力，常無法提供適當的電戰效果；地表式的感測器及干擾器，通常裝置在地面，或是海面的船艦上，則受限於可用功率的限制，以及作戰區域的地形限制。

二、美國重新重視電磁頻譜優勢

美國國防部 2020 年 10 月 29 日提出《電磁頻譜優勢戰略》（*Electromagnetic Spectrum Superiority Strategy*），[12]揭示 5 大目標：

[12] "Electromagnetic Spectrum Superiority Strategy," *US DoD*, October 29, 2020, https://media.defense.gov/2020/Oct/29/2002525927/-1/-1/0/ELECTROMAGNETIC_SPECTRUM_SUPERIORITY_STRATEGY.PDF.

1、開發卓越的電磁頻譜功能。

2、演變為敏捷且完全整合的電磁頻譜基礎架構。

3、在電磁頻譜中尋求全面的部隊準備。

4、建立持久的合作夥伴關係，以獲取電磁頻譜優勢。

5、建立有效的電磁頻譜治理。

這顯示美國國防部對電磁頻譜的看法，已從作戰指揮和一般管理用途，轉變為成為電磁頻譜作戰（EMSO）。美國陸軍將應用「電子戰計劃和管理工具」（EW planning and management tool，EWPMT）管理電子戰場，可以提供指揮官有關電磁戰場的可視圖，並協調多項裝備，發起電子攻擊活動。在部隊編制方面，美國陸軍打算在旅至作戰司令部各階段都引入「網路／電磁活動」（Cyber/Electromagnetic Activity，CEMA）活動，整合網路及電磁戰任務，並建立新電戰排、在軍級單位建立電戰連、並在多領域特遣隊成立新分支。CEMA 要整合網路及電子戰，以運用網路進行電子攻擊行動。

肆、美國陸軍需重獲電子戰優勢

美軍面臨的電子威脅逐漸升高，俄、中都在發展電子戰能力，美國電子戰能力絕大部分都編配在空軍和海軍，陸軍在面對更具電磁優勢的俄羅斯或中國等同等級對手挑戰時，已無法繼續依靠友軍提供電子支援。

一、美國陸軍尋求重獲電子戰優勢

傳統上美國陸軍並不重視電子戰。在反恐戰爭時，恐怖分子廣泛運用以遙控等方式引爆的簡易爆炸裝置（Improvised Explosive Devices，IED）攻擊美軍部隊，使得地面部隊也要以簡易的干擾裝置反制。陸軍逐漸意識到在地面領域，發射器和接收器在複雜地形上，加上景觀持續變化，因此需要陸軍自己的專家團隊，熟悉如何

經營電子戰，瞭解戰場地形以及部署陸軍部隊。[13]

冷戰結束後，陸軍每個師都還有電子戰和情報作戰（CEWI）部隊，本可在作戰期間為其下屬旅級部隊提供電戰支持，卻在專注於反恐戰爭時，淘汰掉某些電子戰裝備及單位，結果陸軍只好依賴海空軍提供包括電子攻擊在內的多種能力，僅保留了訊號情報能力，不過其本質上是防禦性的。[14]

從冷戰結束到建立以「旅級戰鬥隊」（BCT）為中心的陸軍部隊，已經淘汰一些能力，最顯著的即是電子戰，特別是電子攻擊能力，建立模組化陸軍，使得陸軍只好依賴海空軍提供包括電子攻擊在內的多種能力。[15]

陸軍重建電子戰計畫集中在作戰旅，忽略師和軍等更高層級的部隊。在反恐作戰時，恐怖分子只以小團體進行作戰，每個陸軍旅都可以在指定區域獨立行動。但在與像俄羅斯這樣的國家進行快速、高強度的戰爭中，旅級單位很容易被壓制，師和軍等更高層級的司令部必須在更緊迫的時間範圍內，指導更大範圍的作戰。

陸軍多年前已開始恢復地面電子戰能力，例如向旅級戰鬥隊提供電子戰人員，及提供電子攻擊能力和加強電子支援能力，例如車載式、人攜式、直升機載裝備、或是無人機載系統。[16]其他還包括加強網路空間電磁活動人員，讓電子戰與軍、師和旅級戰鬥隊同步。

二、美國陸軍電子戰發展新方向

目前美軍主要陸上電子戰系統，包括簡易爆炸裝置反制系統、

[13] "Short History of US Army Electronic Warfare," *SITREP*.
[14] Maj. Morgan J. Spring-Glace, "Return of Ground-Based Electronic Warfare Platforms and Force Structure".
[15] Maj. Morgan J. Spring-Glace, "Return of Ground-Based Electronic Warfare Platforms and Force Structure".
[16] "Electronic warfare prototypes improve operational understanding against near-peer threats," US Army, May 11, 2018, https://www.army.mil/article/205064/electronic_warfare_prototypes_improve_operational_understanding_against_near_peer_threats.

無人機反制系統、通訊及雷達干擾系統等三類。[17]

要重獲電子戰優勢，就要管理電磁頻譜的運用。要有效管理電子戰——電磁頻譜中的衝突，取決於信號、數據和關鍵決策的複雜混合。為管理電子攻擊和電子支援能力，陸軍使用 EWPMT，通常安裝在天線和無線電收發器之間。EWPMT 允許操作員透過一個名為「掠食爪」（Raven Claw）的計算機程序來中和並利用敵方信號。

EWPMT 旨在獲取散射訊號，加以分析並提出攻擊建議，它從戰場上各感測器獲得數據，綜合到一個清晰的地圖中，顯示訊號通過及被干擾的位置，並模擬潛在對策的效果，以便指揮官可就對付敵人做出明智決定，這將使操作者能夠管理整個電磁頻譜，可以協調多個電子戰資產之間的電子攻擊活動。它可以識別和協調整個作戰過程，從定向、電子攻擊到特定訊號等，功能十分多樣化。雷神公司已在 2019 年獲得合約，為陸軍擴張中的電子戰部隊完成 EWPMT 指揮管制軟體。[18]

美國陸軍正在發展新的電戰系統，包括空載型（air-launched effects，ALE）及地面型（ground-launched effects，GLE）。[19]地面型是以史崔克 8X8 裝甲車或戰術車輛改裝成「地面層系統」（Terrestrial Layer System，TLS），進行整合式電子戰、訊號情報和網路平台的實驗。2021 年 1 月開始提供給部隊進行實地測試。

無人機也是理想的電子戰平台，若配備適當電子訊號情報系統，可偵測敵方電子訊號，若大氣條件適當，無線電訊號可傳導到極遠距離，裝置高靈敏度的偵測系統，在空中便可偵測到遠距離的電磁訊號。無人機也可作為電戰平台，洛馬正發展供 MQ-9 無人機

[17] "Ground Electronic Warfare: Background and Issues for Congress," *CRS Report*.

[18] "Visualizing The Invisible Battle: Raytheon's EWPMT," *Breaking Defense*, October 3, 2019, https://breakingdefense.com/2019/10/managing-the-invisible-battle-raytheons-ewpmt/.

[19] Colin Demarest, "Jam, spoof and spy: US Army looks to energize electronic warfare," *C4ISRNET*, October 10, 2022, https://www.c4isrnet.com/electronic-warfare/2022/10/09/jam-spoof-and-spy-us-army-looks-to-energize-electronic-warfare/.

使用的電戰莢艙，稱為「多功能電子戰–空中–大型」（Multi-Function Electronic Warfare-Air-Large，MFEW），再透過 EWPMT 與地面層系統結合，已在 2021 年開始進行評估。[20]美國陸軍也持續發展直升機電戰能力，但將會與陸軍進行中的「未來垂直舉升」系統（Future Vertical Lift，FVL）結合。[21]電戰系統則成為未來垂直舉升系統或無人機的酬載。

這些系統都將演變成大型及小型系統家族，依通用硬體及軟體標準建置，彼此能共享資料，並建立多樣化的數位武器資料庫，可偵測敵人傳輸、破解敵方密碼、標定敵方部隊位置並加以打擊、並透過干擾及駭客手法破壞其網路，而最高境界是敵方甚至無法偵測到被欺騙。[22]

伍、未來多領域作戰的發展趨勢

多領域作戰是美國陸軍發起的新作戰概念，在美國陸軍的多領域作戰（Multi Domain Operation，MDO）概念下，陸、海、空、太空、網路及電磁五大領域，均是作戰領域一部分，網路及電子戰將成為指揮官麾下的「火力」，指揮官可以決定使用火砲或電子戰，將目標摧毀。

一、多領域作戰概念下的網路及電子戰

美國陸軍正進行「多領域戰鬥」（Multi-Domain Battle）的驗證。「多領域」泛指海上、空中、陸上、太空以及網路 5 個領域。多領域作戰的中心思想是快速且持續整合所有領域的作戰，以嚇阻並挫敗對手，如果嚇阻失敗，聯合部隊將穿透並瓦解敵人的 A2/AD 能力，挫敗敵人的系統、序列及目標，並實現我方的戰略目標。

---

[20] "Army Electronic Warfare: Big Tests In '21," *Breaking Defense*, August 12, 2020, https://breakingdefense.com/2020/08/army-electronic-warfare-big-tests-in-21/.

[21] "US Army seeks new airborne tech to detect, defeat radar systems," *C4ISRNET*, August 14, 2020, https://www.c4isrnet.com/battlefield-tech/2020/08/14/us-army-seeks-new-airborne-tech-to-detect-defeat-radar-systems/.

[22] "Army Electronic Warfare: Big Tests In '21," *Breaking Defense*.

多領域作戰是美國陸軍發起的新作戰概念，已在進行多領域特遣隊的驗證。多領域作戰也需要「聯合全領域指揮管制」（Joint All-Domain Command and Control，JADC2）支持，將每個感測器連接到每個射手，以及每個指揮管制節點，運用 AI 技術協助，在情監偵能力及決策速度上將比過去更快。

美國陸軍正在進行的多領域特遣隊，已在印太區域部署第三多領域特遣隊，這是戰區特定單位，其組成包括網路、電子戰、情報、遠程火力等長程精確作戰效果，可在空中、陸地、水域、太空及網路領域使用致命及非致命能力。[23]多領域部隊除具極強機動性及分散部署能力，有極佳生存力，容易在隧道、叢林、山脈等特殊地形地物中隱藏，儲存足夠彈藥及其他武器，攔截敵方彈道飛彈、擊落敵機、擊沉敵艦，為海上及空中力量提供火力掩護的保護傘，相當於美國版的 A2/AD。除「物理」的火力外，特遣隊創建的「情報、資訊、網路、電子戰和太空」營（Intelligence, Information, Cyber, Electronic Warfare, & Space，I2CEWS），可匯集來自衛星、無人機、偵察機等的外部資訊，並在網路及電磁頻譜空間發動戰爭，入侵並干擾敵人擊殺鏈的網路與感測器，這不僅需要被動收集情報，還要主動測試敵方系統，運用電子傳輸及物理機動，「刺激」敵方雷達、干擾器、網路防禦活動，並藉刻意揭示某些活動、隱藏其他活動來嚇阻對手。[24]

I2CEWS 分遣隊為營級單位，由四個連構成，包括情報、資訊戰、網路及電子戰、太空與訊號，可即時發現目標、進行精確火力支援，支持砲兵、空中及飛彈防禦等任務。這些資產原屬於一個軍或戰區司令部級別的單位，但將其全部集中到一個單位則是前所未

[23] "Third Multi-Domain Task Force will be at full operating capacity by May," *Inside Defense*, March 7, 2023, https://insidedefense.com/insider/third-multi-domain-task-force-will-be-full-operating-capacity-may.

[24] "Army's Multi-Domain Unit 'A Game-Changer' In Future War," *Breaking Defense*, April 1, 2019, https://breakingdefense.com/2019/04/armys-multi-domain-unit-a-game-changer-in-future-war/.

見，而 I2CEWS 也將成為多領域特遣隊的一個重要組成部分。[25]

二、網路與電磁活動的結合

在多領域作戰環境下，「網路／電磁活動」（CEMA）是新興概念，致力於解決網路空間作戰、電子戰和電磁頻譜管理作戰的整合和同步問題。

2018 年決定行動輪替（Decisive Action Rotation）演習中，美國陸軍網路司令部及其 780 軍事情報旅（網路），第一資訊作戰司令部和陸軍網路保護旅（Cyber Protection Brigade，CPB）的網路戰士進行支持第三旅級戰鬥隊、第一裝甲師的訓練和戰備，作為網路保護旅正在進行的網路／電磁活動的一部分，或「CEMA 支持軍及以下部隊」（CSCB）程序。[26]

2018 年 1 月，美國陸軍發布《2025-2040 年美國陸軍網路空間和電子戰行動概念》（*U.S. Army Concept for Cyberspace and Electronic Warfare Operations: 2025-2040*），[27]指出要擊敗擁有先進能力的未來敵人，陸軍是聯合部隊的一部分，在多個領域進行同時和依序的行動。在多領域戰鬥中，未來的陸軍將在所有爭議空間作戰並獲勝，並創造優勢窗口，抓住聯合部隊的行動自由，保留主動權並加以利用。

陸軍未來要在網路空間和電磁頻譜中作戰，並完全整合網路、電子戰和電磁頻譜戰，作為聯合作戰的一部分，應對未來作戰環境挑戰。這些行動為指揮官提供在多個領域內同步行動的能力，並為指揮官量身定製各種物理、虛擬，以及致命和非致命能力，以增強

---

[25] "Hack, Jam, Sense & Shoot: Army Creates 1st Multi-Domain Unit," *Breaking Defense*, January 24, 2019, https://breakingdefense.com/2019/01/hack-jam-sense-shoot-army-creates-1st-multi-domain-unit/.

[26] "Cyberspace-Electromagnetic Activities program builds maneuver unit readiness," *U.S. Army Cyber Command*, June 20, 2018, https://www.army.mil/article/207321/cyberspace_electromagnetic_activities_program_builds_maneuver_unit_readiness.

[27] "U.S. Army Concept for Cyberspace and Electronic Warfare Operations: 2025-2040," *US DoD*, January, 2018, https://www.hsdl.org/?abstract&did=807334.

執行聯合作戰的機動部隊戰鬥力。[28]

三、未來電子戰技術

未來電子戰將是精確電子戰，不再是用大功率將對手無線電蓋台，這樣也很容易曝露我方位置。未來電子戰與網路、訊號情報、結合人工智慧（artificial intelligence，AI），即使進行干擾，仍能竊聽敵方通訊，並運用精心設計的欺騙訊號，下載到對方接收系統，並更巧妙地進行干擾，這種技術可以擾亂對方無人機控制鏈、欺騙對方導航訊號，使其精確導引武器失效，或是欺騙雷達，但仍維持對敵監聽。

先進的電子戰相關技術發展，包括軟體定義無線電、精確電子戰、AI 在電子戰中運用、電子戰與網路戰結合，以及認知電子戰等。

認知電子戰技術偏重軟體及演算法，以便自適應雷達對抗、發展多功能認知干擾系統，電子戰系統能在戰場上自我學習，對抗敵方通訊系統，使部隊能在最小自我干擾情況下實施干擾，同時為友軍留下精確的通訊空隙。

陸、結論

美國國防部意識到在電子戰領域已落後中共及俄羅斯，因此要擴大對電子戰能力的投資，2020 年的《電磁頻譜優勢戰略》，認為未來複雜電磁環境下獲取優勢，美國國防部勢需採取新方法，發展革命性、跨越式的技術。

在未來電子戰場，美國陸軍將應用 EMPMT 管理電子戰場，在部隊編制方面，美國陸軍打算在旅至作戰司令部各階段都引入 CEMA 活動，整合網路及電磁戰任務。

---

[28] "Electronic warfare on the ground," *Military Aerospace*, February 1, 2019, https://www.militaryaerospace.com/home/article/16709607/electronic-warfare-on-the-ground.

多領域作戰概念下，陸、海、空、太空、網路及電磁五大領域，均是作戰領域一部分，都是指揮官可運用的「火力」，指揮官可以決定使用火砲或電子戰，將目標摧毀。多領域作戰是美國陸軍發起的新作戰概念，現已在進行多領域特遣隊的驗證。另外，新的電子戰技術將是精確電子戰，結合網路、訊號情報、AI 技術結合，結合電磁頻譜的多領域作戰，將大幅改變未來戰爭型貌。

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。

Electronic Warfare in the U.S. Army's Multi-Domain Operations

Hsiao-Huang, Shu

Division of Chinese Politics, Military and Warfighting Concepts

Abstract

After the Cold War ended, the United States achieved overwhelming victories in various military operations. In addition to relying on military technological advantages, it also used innovative warfare concepts such as joint operations, precision strike, joint C4ISR, and effective joint fire. However, in recent years, new technologies have gradually been applied in the military, which may, once again, change the combat pattern. The United States is worried that its military advantage will be challenged. Potential U.S. adversaries seek to employ multi-domain means, including sea, air, land, space, cyber, and Electromagnetic Spectrum, to defeat their enemies or deprive U.S. joint forces of operational superiority and freedom of intervention in other parts of the globe.

The U.S. Army has long neglected the development of electronic warfare. In the face of threats from China and Russia, in order to maintain its operational advantages, the Pentagon must seek revolutionary, step-across technologies and capabilities to gain advantage in the complex electromagnetic environment of the future, develop agile and integrated electromagnetic spectrum infrastructure, establish effective electromagnetic spectrum control, etc., and ensure that all personnel receive education and training on the electromagnetic spectrum concept. In addition, the United States also needs to develop AI and other technologies to assist electronic warfare reactive attacks.

On the future electronic battlefield, the U.S. Army will apply new

technologies to manage the electronic battlefield and provide commanders with a visual view. Under the multi-domain operation concept framework, the five major combat domains of land, sea, air, space, cyber and electromagnetic will be integrated, strengthening the combat effectiveness of joint operations to meet the challenges of the future combat environment.

Keywords: Electronic Warfare, Multi-Domain Operations, Electromagnetic Spectrum