第七章　網路電磁活動

杜貞儀*

壹、前言

網路電磁活動（Cyber Electronmagnetic Activity, CEMA）為同時在網路空間（cyberspace）與電磁頻譜環境（electromagnetic spectrum environment）占據、保持並利用己方優勢，同時阻止、降低對手與敵方使用同樣手段的能力，保護任務指管系統。[1] 在複雜電磁環境（complex electromagnetic environment）下，網路作戰（cyberspace operation）、電子作戰（electronic warfare）、電磁頻譜管理作戰（spectrum management operation）三者合流，已是趨勢。過去美軍在伊拉克與阿富汗作戰時，可完全掌握網路空間與電磁頻譜，擁有絕對優勢，但在今日面對能力相當競爭者（near-peer competitor）所展現之複合能力，美軍於網路與電磁頻譜空間自由運用之優勢，便逐漸受挑戰。網路電磁活動的基礎在於戰場網路現代化，整合既有指管通情系統，並應用資通訊科技進展強化能力，形成不對稱之作戰優勢，而最終將面對未來大國軍事競爭之作戰行動。

貳、科技演進與新型威脅

一、戰場網路現代化得力於軟體定義無線電

以網狀化的指管通情系統（C4ISR）建立戰場共同圖像，縮短決策時間，取得先機，已成為現代戰爭的核心，而其中「看得到，打得到」的關

* 杜貞儀，國防安全研究院網路安全與決策推演研究所博士後研究。

1 “Field Manual 3-38: Cyber Electronmagnetic Activity,” Department of the Army, February 12, 2014, https://armypubs.us.army.mil/doctrine/index.html; “Joint Publication 3-85: Joint Electromagnetic Spectrum Operation,” Joint Chief of Staff, May 22, 2020, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_85.pdf.

鍵鏈結就是數位化的無線通訊。隨著商用無線通訊技術的快速發展，逐步由類比轉為數位，傳統通訊設備基於硬體電路定義的規格與功能，也因軟體定義無線電（software-defined radio, SDR）所帶來的革新，而有重大變革。數位訊號處理器（Digital Signal Processor, DSP）及現場可程式化邏輯閘陣列（FPGA）等可程式化之數位訊號處理元件普及，更加速軟體定義無線電的實現。[2] 軟體定義無線電的特點是具備多重規格支援與擴充彈性，可輕易重新配置，由軟體程式控制其載波頻率、發射功率、傳輸格式、頻寬、接取方式及通訊協議。也就是說，單一收發系統只需由軟體修改，即可支援不同標準規格，傳送並接收不同頻寬與規格的訊號。[3]

在應用上，軟體定義無線電以更低成本實現跳頻、展頻、無線網狀網路（wireless mesh network）等功能，可提升抗干擾（anti-jamming）能力，以保密機制強化通訊安全，並依實際需求重新調整。[4] 過去 20 多年來，軍事裝備與系統廣泛採用軟體定義無線電技術，從根本改變無線電、雷達、GPS 系統與其他電磁系統的設計方式。以美軍為例，聯合戰術無線電系統（Joint Tactical Radio System, JTRS）計畫原先目標，即是建立能透過其軟體通訊架構（Software Communication Architecture, SCA）上傳即時新增使用頻率、模態（一般合稱為「波形」waveforms）的全軍通用單一軟體無線電系統。雖然後來 JTRS 計畫並未真正實現，但後續經大幅修正與部分項目取消後，有許多元素仍然可見於其他系統。如北約版的 LINK-16 數

2 “Software defined radios –overview and hardware (1),” *News from Rohde & Schwarz* (no. 182), 2004, https://cdn.rohde-schwarz.com/pws/dl_downloads/dl_common_library/dl_news_from_rs/182/n182_radiocomunit.pdf.

3 〈選擇 ASIC、FPGA、DSP 設計無線電系統的準則〉，《CTIMES》，2002 年 8 月 5 日，https://www.ctimes.com.tw/DispArt/tw/FPGA/%25E5%258F%25AF%25E7%25B7%25A8%25E7%25A8%258B%25E8%2599%2595%25E7%2590%2586%25E5%2599%25A8/ASIC/%25E8%25BB%259F%25E9%25AB%2594%25E7%2584%25A1%25E7%25B7%259A%25E9%259B%25BB/DSP/0208051409BF.shtml；陳逸民，〈軟體定義無線電技術與平台架構〉，中華民國無線電協進會，2014 年 2 月 19 日，https://www.cra.org.tw/download/downloadd.aspx?11。

4 電磁頻譜管理與軟體定義無線電，另參饒廣衡，〈美國防部同意頻譜釋出與後續共享協議之意涵〉，《國防即時評析》，2020 年 8 月 27 日。

據鏈路 —— 多功能資訊分配系統（Multifunctional Information Distribution System, MIDS），其中的通訊組件：聯合戰術無線電（MIDS-JTRS）終端，即是相容於 JTRS SCA 的軟體定義無線電系統（圖 7-1）。隨著 JTRS 計畫改制為聯合戰術網路中心（Joint Tactical Networking Center, JTNC），JTNC 負責營運並維護全軍波形使用軟體（如 SCA）與相關文件的資訊儲存庫，並針對儲存庫資訊安全進行強化。[5]

軟體定義無線電的高度彈性，在 MIDS-JTRS 及其後續發展改良中展露無疑。MIDS-JTRS 為四通道無線電終端，涵蓋 LINK-16 數據鏈路、指管數位語音及戰術空中導航系統（Tactical Air Navigation System, TACAN，又稱太康）能力，並可新增其他協定，提供美國與盟邦在陸、海、空及聯合作戰下安全可靠的無線指管通信與數據鏈路環境。MID-JTRS 近期更新即是在既有的地空聯合作戰使用之士兵無線電波形（Soldier Radio Waveform, SRW）、寬頻網路波形（Wideband Networking Waveform, WNW）外，持續擴充以滿足未來聯合空戰網路 —— 戰術前緣（Joint Airborne Networking – Tactical Edge, JANT-Ed）需求。[6]

5 "JTNC Frequently Asked Questions," Joint Tactical Networking Center, https://www.jtnc.mil/About/JTNC-FAQ/.

6 Barry Rosenberg, "US, Allies Getting Larger Airborne Network With New JTRS Radios," *Breaking Defense*, July 18, 2019, https://breakingdefense.com/2019/07/us-allies-getting-larger-airborne-network-with-new-jtrs-radios/.

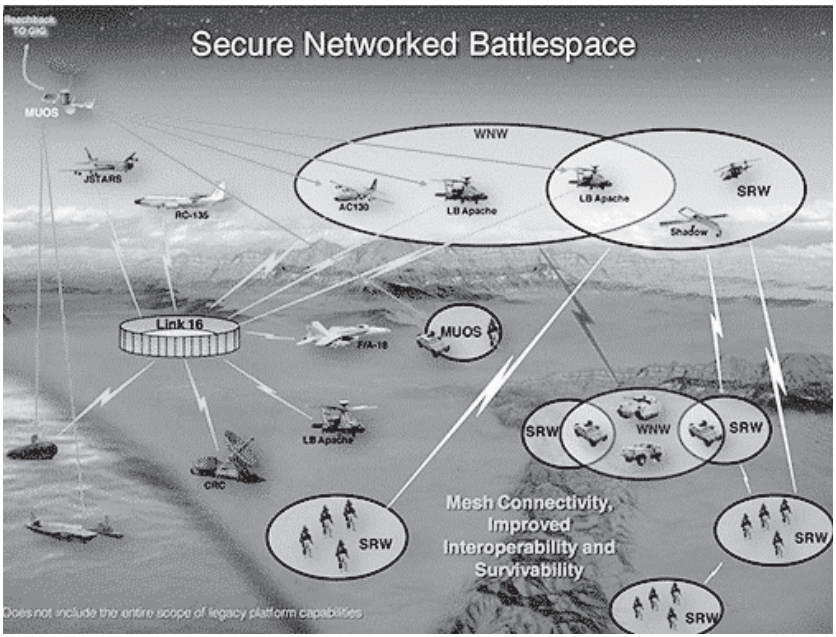

圖 7-1　由 MIDS-JTRS 構成之安全網狀化戰場環境示意圖

資料來源：S.S. Kamal and John T. Armantrout, "The U.S. Military's Joint Tactical Radio System," *CHIPS*, January-March 2013, https://www.doncio.navy.mil/Chips/ArticleDetails.aspx?ID=4344.

二、從「舒特」系統到網路電磁活動

然而，軟體定義無線電的強大能力，亦帶來新的潛在威脅。在軟體定義無線電變革以前，無線電、雷達或其他電子系統的主要威脅來自干擾（jamming，即「軟殺」soft-kill）或動能武器（即「硬殺」hard-kill）攻擊，但採用軟體定義無線電、提高彈性後，這些系統將必須仰賴資料鏈接受軟體更新，此即形成新的潛在弱點。也就是說，惡意程式透過此管道，直接植入系統，即可產生各種影響，包括使系統生成假資料、系統關機，甚至以超頻（overclocking）等方式對系統中的微處理器造成不可逆的物理損害。

藉由電磁頻譜進行網路攻擊時，惡意程式將會以無線電波或微波訊號傳遞至受害系統的接受端，並由受害系統將訊號轉換回數位形式的軟

體。在此網路與電磁空間合流的情形下，電戰系統若以非動能方式（non-kinetic）對敵方電子系統進行攻擊，就可能有直接干擾與網路攻擊兩種類型，就像一把槍有兩種不同的子彈，可擇一攻擊，此即網路電磁活動（CEMA）的核心概念所在。但目前攻擊以外的其他作戰模式，如目標標定（targeting）、網路防禦（cyber defense）與電子防護（electronic protection）如何進一步整合，仍是持續發展中的構想。[7]

雖然當時 CEMA 的概念並未完全成形，但早在 2007 年時，美空軍「舒特」（Suter）空載電戰攻擊系統，就已經推測於以色列空軍進入敘利亞摧毀核能設施的行動中，藉由戰機展現類似的攻擊能力。敘利亞防空系統遭以軍戰機攻擊後，並未發現任何異常，且雷達顯示幕上也未顯示以軍戰機，使以軍在攻擊行動中如入無人之境。當時以網路匿蹤（cyber stealth）稱之，但此即為 CEMA 在戰場上的實際應用。[8]

參、大國競爭之作戰行動下的網路電磁活動

一、中共「網電一體戰」與「戰場網電制權」

共軍對於網路電磁活動的詮釋，即「網電一體戰」概念。戴清民少將於 2002 年出版之《網電一體戰引論》，認為「網電一體戰」為「綜合運用多種手段實施體系破擊的軍事對抗行動，由信號層次的能量壓制、網絡層次的協議攻擊、信息層次的信息欺騙等行動組成」，並以美軍協助以色列之「舒特」系統欺騙敘利亞防空系統作說明，認為此即「網電一體戰」之典型範例，網路戰受實體線路範圍的限制已逐漸打破，將其概念逐步延伸至無線電及其所在之複雜電磁環境。

7　John Knowles, “Cyber-EW Synergies,” *Journal of Electronic Defense*, February 2020.

8　Col. Matthew Willis & Lt. Col. Panagiotis Stathopoulus, “Cyber-Electronic Domain: The Necessity of Integrating the Electronmagnetic Spectrum’s Disciplines Under a Single Domain of Operations,” NATO Joint Air Power Competence Centre, September 9, 2020, https://www.japcc.org/cyber-electromagnetic-domain/.

為與歐美慣用之「網路空間」（cyberspace）進行區隔，並由作戰層面出發，比較其定義上之異同，共軍空軍所屬之指參與研究單位的楊帆等人，以音譯之「賽博空間」（cyberspace），與共軍「網電一體戰」的場域「網絡電磁空間」（簡稱網電空間）進行比較與分析。該文認為，「網電空間」一詞較具共軍特色，並強調四點：第一，「網電空間」可反映其平台和手段是基礎設施，包括有線與無線手段；第二，「網電空間」實現自身功能之載體為信號與信息；第三，效果上，「網電空間」為融合物理、實體與認知三個領域的融合域；第四，其特殊目的是控制實體行為，也就是控制人的行為以及含有預置邏輯的各種人造設備的行為，主要指晶片上的控制程序、軟體或匣道等。

該文更進一步指出，美軍所謂的「賽博空間」不包括認知層面，因此人不屬於「賽博空間」的範疇，是「賽博空間」與「網電空間」最主要的區別，也認為在「賽博空間」概念中，「賽博域」（cyber domain）及認知域（cognitive domain）存在一明顯邊界，兩者間聯繫是基於紐帶作用的外顯功能，而非如「網電空間」的內在本質。在概念延伸上，「網電空間」將影響認知域、社會域以及最終影響決策判斷。[9]

從「網電空間」概念延伸，共軍認為未來作戰中，「戰場網電制權」行動將會是雙方鬥爭焦點，故應聚焦於此，並強調「網電空間」的心理、認知層面，表示「奪取戰場網電制權，就是要著眼影響或破擊敵心理認知體系，基於網電空間隱蔽性好、滲透性強的特性，遵循『力由心使』的作戰規律，充分挖掘網電施計用謀空間，想方設法麻痹敵神經、擊垮敵心理，造成敵情報失實、判斷失誤、決策失當。」此外，也認為網電作戰與火力打擊融合後，可有效結合兩者優勢，發揮「軟硬一體、效能倍增」的作戰機制，實現「斷首制盲、毀骨傷身」的有機結合，而達到加速推進作戰進程的作用。[10] 此構想與俄羅斯軍方近年在敘利亞、烏克蘭戰爭中將電

9 楊帆、郭慶豐、陳湘葯、王宏，〈網絡電磁空間與賽博空間的區別分析〉，《國防》，2017 年第 2 期，頁 54-57。

10 劉國軍、余志鋒、周延安，〈如何有效奪取戰場網電制權〉，《解放軍報》，2020 年 8 月 4 日，http://www.81.cn/jfjbmap/content/2020-08/04/content_267666.htm。

戰結合砲兵火力打擊的作戰方式吻合，顯示共軍不僅密切觀察俄羅斯軍方相關發展，將其納入作戰構想並應用於未來大國競爭下的作戰行動中。

自共軍軍改後，戰略支援部隊的網絡系統部整合過去總參三部（技術偵查部）、四部（電子對抗與雷達部）的攻勢網路作戰與電戰能量，進行「網電一體戰」的具體落實。在 2019 年 10 月 1 日的中共「建政」七十周年閱兵中，戰略支援部隊與陸軍電子對抗旅分別抽組成 4 支信息作戰方隊接受檢閱，展示裝備亦有差異，顯示戰略支援部隊和各軍種原先資訊作戰部隊在任務上應有所區隔。戰略支援部隊強調其具「破擊節點、癱瘓體系、初擊致勝」的能力，應為透過針對關鍵節點與指管系統進行打擊，並且表示其在網電空間外，在提供戰場環境資訊如水文、地形等，亦扮演關鍵角色，以形成戰略面之資訊優勢。陸軍電子對抗旅則稱其為「偵擾一體、網電一體、軟硬一體、空地一體」，重點明顯為「戰場網電制權」，並在實戰上與砲兵結合。[11]

二、美軍如何面對反介入／區域拒止挑戰

面對能力相當競爭者的威脅，美軍逐步瞭解在於網路與電磁頻譜空間自由運用之優勢已受到嚴重挑戰，未來作戰情境下，無可免地面臨「擁擠又爭奪不斷」（congested and contested）的複雜電磁環境狀態，以及「受限、受損、間歇性及延遲」（denial, degraded, intermittent and latent, DDIL）的不穩定連線環境。美國防部於 1997 年提出的網路中心戰（Network-Centric Warfare）概念，讓網路成為作戰平台，因應節奏更快且不斷演化的威脅。不過，美軍發展網路中心戰概念時，是以取得全頻譜優勢（full spectrum dominance）為前提，資訊環境不會受到任何限制，但未來的威脅，掌握相對資訊優勢（information superiority），已成為作戰之關鍵。即使對於美軍而言，掌握網路與電磁頻譜空間，亦屬不易，需跨軍

11 以上均參自《解放軍報》，2019 年 10 月 2 日，http://www.81.cn/jfjbmap/content/2019-10/02/node_2.htm。

種，甚至跨部會的整合，但整體來看，美軍各軍種的做法，是持續爭取資源，在各自依據其作戰任務需求進行建軍規劃。

以美國陸軍為例，在「大西洋決心」（Operation Atlantic Resolve）作戰支援烏克蘭的經驗，催化並加速陸軍內部對於網路、資訊、電子作戰的整合，首次制定《野戰教則：網路電磁活動》（*Field Manual 3-38: Cyber Electronmagnetic Activity*），並進行一系列之組織調整。[12] 佛加提中將（Lt. Gen. Stephen G. Fogarty）2018 年接任美陸軍網路指揮部（Army Cyber Command, ARCYBER）之指揮官後，由於 2016 年俄羅斯干預美國總統大選影響，配合美陸軍提出的多領域作戰概念（multi-domain operations），並以為期 10 年的轉型戰略，目標在多領域作戰預計於全軍落實的 2028 年，將 ARCYBER 徹底轉型為資訊戰指揮部（Information Warfare Command）。[13]

由於電戰極度仰賴訊號情報（signal intelligence, SIGNIT）提供相關參數，因此 ARCYBER 的第一階段轉型，即將其總部由維吉尼亞州原址移至喬治亞州戈登堡（Fort Gordon, Georgia），可就近與美國家安全局（National Security Agency, NSA）負責訊號情報的喬治亞密碼中心（Georgia Cryptologic Center）合作。在實戰單位部分，則是首建網路電磁活動專門部隊 —— 網路作戰第 915 營（915th Cyberwarfare Battalion）。此營將關注攻勢作為，未來也將擁有海外遠征部署能力。

此一系列之 ARCYBER 組織調整，表示美軍不僅在為全面大國競爭之大規模作戰行動（large-scale combat operation, LSCO）做準備，未來對於網路司令部（USCYBERCOM）之網路任務部隊（Cyber Mission Force）及網路指揮部新成立之聯兵旅級以下資訊作戰專門單位（目前即網路作戰

12 Lt. Col. Matthew J. Sheiffer, “U.S. Army Information Operations and Cyber-Electromagnetic Activities,” *Military Review*, March 19, 2018, :https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2018-OLE/Mar/Army-Info-Ops/.

13 以下見杜貞儀，〈從資訊戰到資訊優勢：美陸軍網路指揮部作戰概念演進〉，《國防安全雙周報》，第 14 期，2020 年 10 月 23 日，另參 Mark Pomerleau, “Out: ‘information warfare.’ In: ‘information advantage’, ” *C4ISRNET*, September 29, 2020, https://www.c4isrnet.com/information-warfare/2020/09/29/out-information-warfare-in-information-advantage/.

第 915 營），其任務應會進一步區隔。網路司令部直接指揮網路任務部隊，將專注於戰略層面的任務，而新成立之資訊作戰單位，則負責各戰區之戰術任務。在佛加提中將提出的 ARCYBER 轉型規劃中，第二階段更預計將目前隸屬於特戰司令部（Special Operation Command）的心理作戰（Psychological Operation, PSYOP）與公共關係人員，也同樣納編入陸軍所屬資訊作戰單位中，由此形成全頻譜（full-spectrum）的完整資訊戰力。[14]

美陸軍首個戰術層級資訊作戰部隊 —— 網路作戰第 915 營，2020 年 10 月初進行 2019 年編組後首次的訓練演習，檢驗其作戰概念，改善其戰術、戰技與戰法。至於訓練的內容規劃與背景想定，仍處於發展階段，亦可預期和其他美陸軍資訊作戰相關單位，包括先前成立，以網路防禦為主要任務的多領域特遣隊（Multi-Domain Task Force）營級分遣隊（Intelligence, Information, Cyber, Electronic Warfare and Space detachment, I2CEWS）在內，同樣面臨編裝不足，甚至有編無裝的問題。[15] 以網路任務部隊的經驗來看，美陸軍網路作戰第 915 營至少須 1～2 年才能取得相關專長簽證，表示擁有全作戰能力（Full Operational Capability）而正式成軍。

在提升自身能力外，美軍將過去僅與少數五眼聯盟成員合作的電戰領域，拓展其合作關係至日本。作為同樣面對中共與俄羅斯威脅的美國盟邦，日本過去 10 年來積極籌建機動車載電子作戰系統，整合電子支援與攻擊兩項任務系統於一體。離島防衛作戰中，電子戰部隊將與水陸機動團進行聯合作戰，除提升南西諸島（即琉球群島）的離島防衛能力，也能與美國共同於第一島鏈反擊敵方之「反介入／區域拒止」企圖。從 2019 年美陸軍與陸自年度聯合演訓「東方之盾 19」（Orient Shield 19）的報導中觀察，不僅提及美陸軍「多領域特遣隊」（Multi-Domain Task Force）參

14 Stephen G. Fogarty & Bran N. Sparling, "Enabling the Army in an Era of Information Warfare," *The Cyber Defense Review*, Vol. 2 Num. 2, 2020.

15 Mark Pomerleau, "US Army conducts first-of-its-kind exercise for tactical information warfare unit," *C4ISRNET*, October 12, 2020, https://www.c4isrnet.com/show-reporter/ausa/2020/10/12/us-army-conducts-first-of-its-kind-exercise-for-tactical-information-warfare-unit/.

與，並將電戰列為該次演訓重點，美陸軍以網路防禦為主要目的之「網路閃電」（Cyber Blitz）演訓，更是首次與「東方之盾 19」同時舉行，提供網路電磁活動的實證場域。[16] 美陸軍資訊作戰部隊雖未正式成軍，但顯已直接參與不同規模之區域性演習，直接驗證概念，並從中擷取經驗，以期完成美陸軍 2028 年落實多領域作戰之目標。

肆、小結

資通訊技術的快速進展，包括數位訊號處理元件以及軟體定義無線電的出現，不僅推動無線電、雷達、GPS 系統與其他電磁系統設計上的革新，也因此產生藉由電磁頻譜進行網路攻擊的新威脅形式。此攻擊方式，擴大電磁相關系統的威脅來源，也顯示網路與電戰的逐步合流，形成網路電磁活動。尤其在未來大國競爭之作戰情境，網路電磁環境等「看不見」的爭奪，將會貫串作戰全程，過去完全掌握網路空間與電磁頻譜的絕對優勢，將越來越難達成，而相對優勢即能制敵機先，此資訊造成的不對稱作戰優勢，即是關鍵。從美陸軍轉型案例可知，情報合作是網路電磁活動的基礎，而與盟邦的交流才能實際驗證概念並累積經驗。台灣位於第一島鏈的關鍵位置，在複雜電磁環境的「反介入／區域拒止」中，應持續尋求與印太區域理念相近盟友的合作，並且思考所能扮演之角色。

16 杜貞儀，〈日本陸上自衛隊新電戰部隊於多領域作戰之啟發〉，《國防即時評析》，2020 年 8 月 27 日。