編輯報告

電子戰對於國防安全研究社群而言，是既熟悉又陌生的領域。雖然耳聞電子戰在戰場上的重要性，但相較於一般耳熟能詳、甚至一不小心就親身遭遇的網路戰，即使電波隨時存在於周遭空間，但電子戰的消息往往因不解其專業術語，讓一般人難以領會。

在實務上，電子戰屬於各軍核心機敏，即使軍事同盟要做到最基本的電磁頻譜相容避免相互干擾，也要小心翼翼而大費周章，其專業社群相對不大。電子戰及電磁頻譜戰場經營不僅跨越太空、陸、海、空及網路域，其攻擊防護與支援也不同於其他領域之攻防，讓相關討論難以擴及專業圈外，常見圈內熱烈辯論，但圈外難以置喙的反差情景。

面對中共解放軍高唱網電一體作戰、又遭逢俄烏戰爭電子戰激烈攻防，加上台灣軍民目睹我軍及烏俄雙方以電子反制無人機侵擾，對於電子戰研究的需求遽增。有鑑於此，國防安全研究院匯集跨所及院外研究能量，出版開院以來首期電子戰專題特刊，希望藉由專業但深入淺出的呈現方式，從頻譜管理、陸海空域運用、以及海軍在海上與陸上之部隊電子戰，讓國安社群讀者一窺電子戰圖像的同時，能先避開專業圈內的神祕隱晦與令人卻步的艱澀辯論。

本期需要預先提醒的有以下三點：首先，各篇採用通說，對於電子戰的界定及頻譜管理，均與常用定義一致。電子戰按一般定義，是將其分為三大類：電子保護、電子攻擊、電子支援。詳細定義在本期美國陸軍、海軍電子戰二篇中有所引介。

其次，本期各篇兼顧新趨勢與反映實務需求。藉由介紹美國陸軍、海軍電子戰以及頻譜管理，揭示電子戰在聯合多領域作戰／電磁頻譜作戰的角色。此外，運用聯合防空作戰、艦隊支隊電子戰以及岸置攻船部隊電子戰，除了適時呼應當前俄烏戰爭所揭示防空作

戰以及艦隊飛彈防禦、以陸制海的重要性，也藉呈現中共在電子戰之威脅，反映我方防務需求。

最後，本期作為電子戰專題系列之首，先著墨陸海空域及海軍部隊電子戰之運用，未來希望藉由各界指導與支持，能陸續推出關於俄烏戰爭實際應用案例、當面敵方之電子戰威脅、陸空部隊電子戰等專題。國防安全研究院研究團隊希望經由增益國安社群對於電子戰理論與實務的了解，能對我國常年保持緘默避免曝光、難以彰顯戰功的電子戰部隊，有更深層的理解與更積極務實的支持鼓勵。

頻譜管理與電子戰

曾怡碩

網路安全與決策推演研究所

壹、前言

在全球通訊走向 B5G/6G 將蜂巢無線通訊與衛星通訊融合的同時，[1]除了對頻寬需求持續增高，各式數位傳輸與終端裝置出現彼此干擾的狀況，滋生對生命、經濟與國家安全的風險。美國 5G 與航機高度表頻率干擾疑慮、[2]以及 2023 年台灣桃園機場 GPS 訊號遭覆蓋的案例，[3]都凸顯出頻譜管理的重要性。

另一方面，新型態戰爭的趨勢朝向多領域聯合作戰，指管通資情監偵構成共同作戰圖像的過程，離不開電磁頻譜的運用，網路戰與電子戰更愈來愈被視為電磁頻譜作戰。[4]根據 2020 年 5 月 22 日美軍參謀長聯合出版 3-85 號 *Joint Electromagnetic Spectrum Operations*

---

[1] 有關蜂巢式布置，「行動通訊基地台電磁波則是較高頻的射頻電磁波，穿透性較差、容易因建築物的結構阻擋而變弱，因為需要雙向傳遞，因此行動通訊系統採取「蜂巢式」建置來維持通訊品質。每一個通話地區依容量及環境的不同，被劃分為一塊塊小區域，每一個區域中都有一個基地台，負責收發訊號，整體看來就像蜂巢般緊密地串聯」，參閱：https://memf.ncc.gov.tw/files/site_node_content_file/429/%E5%85%92%E7%AB%A5%E7%89%88-%E5%B0%8F..pdf。B5G/6G 的應用頻段分別在 0.1~0.3 THz 與 0.1~10 THz 範圍內，此頻段稱為太赫茲（Terahertz）頻段，因太赫茲頻段在太空不存在吸收損耗的問題，具有傳輸速度快和傳輸距離遠的優勢，更能應用於衛星間通訊。參閱：張麗敏、蔡政禹、官祺恩、鄭志龍，〈B5G 材料發展〉，《材料世界網》節錄自《工業材料雜誌》418 期，2021 年 10 月 5 日，https://www.materialsnet.com.tw/DocView.aspx?id=47389。

[2] 〈美國示警 5G 訊號恐擾飛安，為什麼 NCC 表示台灣的頻譜不受影響？〉，《關鍵評論》，2022 年 1 月 20 日，https://www.thenewslens.com/article/161785。

[3] 〈桃園機場等空域遭 GPS 干擾 NCC：公務機關測試產生溢波所致〉，《自由時報》，2023 年 4 月 26 日，https://news.ltn.com.tw/news/life/breakingnews/4282607。另參閱：〈漢光演習首度桃機操演 7 月 26 日擬禁航 1 小時〉，《中央社》，2023 年 6 月 27 日，https://www.cna.com.tw/news/ahel/202306270182.aspx。

[4] 「電磁頻譜作戰是指使用電磁輻射能控制電磁作戰環境，保護己方人員、設施、設備或攻擊敵人，在電磁頻譜域有效完成任務的軍事行動。電磁頻譜作戰是基於電磁頻譜空間，實施電磁頻譜防禦和電磁頻譜攻擊，確保己方利用電磁頻譜的能力，同時阻止敵方有效利用電磁頻譜，實現戰場中『制電磁權』。電磁頻譜連接陸海空天各域協同作戰，電磁頻譜作戰與陸海空天等域作戰緊密結合，在平時即為典型無煙硝的對抗。」 引用自：〈電磁頻譜是什麼？看美國國防部電磁戰鬥管理的十大願景就知道了！〉，《電子技術設計》，2020 年 7 月 2 日，https://www.ednchina.com/news/5344.html。

（Joint Publication 3-85，以下稱為 JP 3-85），電子戰為電磁頻譜作戰的一環，而電磁頻譜作戰端賴有效的頻譜管理。[5]

有鑑於此，本篇著眼頻譜管理在電子戰中的重要性，依序介紹頻譜管理的重要性，分析頻譜管理的電子作戰軍事意義，最後檢視當代頻譜管理面臨之挑戰。

貳、頻譜管理

一、電磁頻譜特質

電磁波依頻率一般區分為無線電波、微波、紅外線、可見光、紫外線、X 射線和伽瑪射線等形式；而電磁頻譜就是電磁波按照頻率或波長分段排列所形成的結構譜系。作為無線通訊傳輸介質，電磁頻譜資源為人類共同擁有，國際共用、無疆無界，屬性上是自然資源，雖是大家共同使用的空間，但受限於技術，可使用空間有其侷限，一般以國際電信聯盟（International Telecommunication Union，ITU）規劃的可用電磁頻譜 10kHz-400GHz 為範圍。[6]

此外，在一定的時間、地域和頻域空間內，一旦特定頻率被使用，就不能在相同的技術模式下運用該頻率，造成頻譜資源在本質上即具稀缺性與排他性。再加上 B5G、物聯網、智慧自駕汽車、無人機、通訊衛星等新技術、新服務，造成頻譜需求急遽增加，進一步擴大頻譜資源的稀缺性。3GHz 以下應用早已趨於飽和，5G 使用 Sub 6GHz（應用頻率為 6G Hz 以下），讓 3GHz-10GHz 的頻譜競爭更趨激烈；隨著 B5G 從毫米波頻段（30-300 GHz）擴展到太赫茲頻段（100 GHz-30 THz），[7]讓 10GHz-60GHz 的頻譜之運用技術日趨成

[5] 黃彥銘，〈國軍「電磁頻譜戰」未來發展之缺析-以美軍為例〉，《陸軍通資半年刊》第 137 期，2022 年 4 月 1 日，頁 5。

[6] 〈電磁頻譜知識鏈接〉，《人民網-軍事頻道》，2015 年 7 月 8 日，http://military.people.com.cn/BIG5/n/2015/0708/c397387-27273025.html。

[7] 季平，〈你今天 5G 了嗎？2030 年後迎接 B5G/6G 時代〉，《CTIMES：零組件雜誌》378 期，2023 年 4 月 24 日，https://www.ctimes.com.tw/DispArt-tw.asp?O=HK74OA7EFF4ARASTDQ。

熟，搶佔優先使用權的趨勢也隨之愈加明顯。

約 90%以上的頻段都由多種無線電業務共用，當多種用頻裝備密集部署時，在一定的空間域、時間域和頻率域上，多種電磁信號同時存在並密集變化交錯，形成複雜電磁環境，容易導致用頻設備產生自擾、彼此互擾，也容易受到干擾。循此，避免用頻裝備彼此間干擾，可以規畫好空間域、時間域和頻率域這三域之一，並藉此達到頻譜共用。[8]此外，面對有限頻寬，利用不同的調變與多工技術，可讓相同頻寬的電磁波具有更高的資料傳輸率，達到更高的頻譜效率（spectrum efficiency）。[9]

二、頻譜管理原則

雖然電波無疆界，但由於無線電頻率在使用上具有排他性，為避免不同國家使用無線電頻率時相互干擾，世界各國制定頻譜管理政策時，均循國際電信聯盟所劃分區域與分配、指配頻段，在和諧共用原則下，以行政與技術手段，並與時俱進彈性因應使用環境與新興科技，甚至運用次級市場，以維護使用秩序及增進使用效率。[10]

按照我國 2020 年當時主管頻譜管理機關「國家通訊傳播委員會」之說明，頻譜管理工作主要包括：[11]「（一）頻率分配：頻率分配係指在特定條件下，將某一指定頻段，指配給一個或數個地面或太空無線電業務使用；（二）頻率指配：頻率指配係指在特定條件下，指定頻道給予某一電台的核准過程。（三）頻譜規劃：頻譜規劃是為了達成頻譜管理的目標，使頻率資源的運用能兼顧國家發展

[8] 〈電磁頻譜知識鏈接〉，《人民網-軍事頻道》。

[9] 曲建仲，〈5G 前瞻通訊原理與應用〉，《科學月刊》，2019 年 1 月 1 日，https://www.scimonth.com.tw/archives/227。

[10] "Developments in Spectrum Management for Communication Services," *OECD Digital Economy Papers*, No. 332, October 2022, pp. 30-47.

[11] 引用自：〈中華民國無線電頻率分配表〉，《國家通訊傳播委員會》，2020 年 2 月，https://naer.siim.org.tw/%E4%B8%AD%E8%8F%AF%E6%B0%91%E5%9C%8B%E7%84%A1%E7%B7%9A%E9%9B%BB%E9%A0%BB%E7%8E%87%E5%88%86%E9%85%8D%E8%A1%A8.pdf，頁 7。

與安全，滿足持續增加的頻率需求。（四）頻譜監測：頻譜監測係維護空中電波使用秩序所採行之措施。（五）頻率收費：藉『收費機制』反映有限資源之使用效率，貫徹『使用者付費』之理念，促使無線電頻率公平分配，頻率資源有效利用。」

國家管制層級以下，平時一般會區別軍用與民用頻段（如下圖示），戰時軍方可接管民用頻譜區段，軍民各單位之頻譜管理員則可以通過對於時間域、空間域與頻率域之區分，以規劃頻譜管理。例如：區分設備使用時段；裝置部署拉開間隔距離；制定用頻方案劃分、規劃、分配和指配頻率。[12]除了上述行政手段，頻譜管理在技術面須具備前瞻規劃思維，針對數位通訊傳播之新興科技載具、通訊手段、提升國安與數位韌性部署等技術，先行研析是否與現有裝置彼此之間頻率產生干擾，並預作規畫安排。例如：我國數位發展部在部署低軌與中軌通訊衛星之前，先行研析非同步衛星與 5G 行動通信使用頻段和諧共用與干擾排除機制。[13]

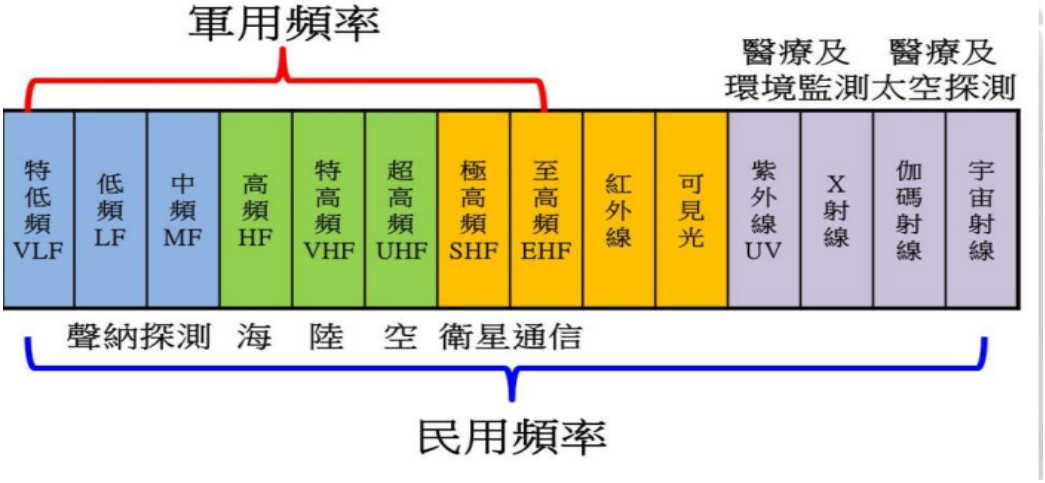

圖 1、頻率範圍示意圖

資料來源：黃彥銘，〈國軍「電磁頻譜戰」未來發展之缺析-以美軍為例〉，《陸軍通資半年刊》第 137 期，民國 111 年 4 月 1 日，頁 6。

[12] 〈電磁頻譜知識鏈接〉，《人民網-軍事頻道》。

[13] 參閱：〈5G/B5G 數位通傳資源前瞻整備研究計畫〉，《數位發展部資源管理司》，2023 年 3 月 22 日，https://www-api.moda.gov.tw/File/Get/moda/zh-tw/uktGes6T0fuwVSM。

參、頻譜管理與電子戰

一、頻譜管理與電子戰之關聯

電磁作戰不論是電子攻擊、防護與支援，均需具暢通安全的指管通信系統，並確保其不會相互干擾，同時也避免受到敵方干擾的影響，而這都有賴於有效的頻譜管理，對有限的電磁頻譜資源的劃分、分配、指配和控制。[14]現代戰場上客觀既有及敵我各式電磁信號充斥於一定的作戰時間與空間，客觀上就使戰場呈現複雜電磁環境。若是敵方電磁干擾壓制而我方抗干擾差，或者是我方裝置電磁相容性差、電磁頻譜分配和管控不力而造成嚴重自相干擾，將讓戰場電磁環境愈形複雜。[15]

凡是電子戰強國均重視從源頭設計就建置電子和資訊化武器裝備的電磁相容性與抗干擾能力，從元件到武器載台均須具備防電磁脈衝輻射能力和電磁相容性。此外，美、俄等主要電子戰強國先後頒布了一系列頻譜管理法規，藉由不斷更新修正，建立權威電磁頻譜管理體系，更強化了對電磁頻譜的有效分配管控，讓電磁頻譜管理成為多領域先進戰鬥管理中電磁戰鬥管理的一環。[16]電磁戰鬥管理是多領域電磁頻譜作戰一環，其與電磁頻譜管理彼此不同但相關，電磁頻譜管理藉由調配戰場電磁頻譜資源，並協同電子戰、信號情報等部門，共同支援電磁戰鬥管理。[17]

二、頻譜管理與電子戰技術

相對於海、空與太空作戰領域，地面部隊面對電磁環境相對複

---

[14] Appendix A Electromagnetic Spectrum Management of "Joint Electromagnetic Spectrum Operations," *US Joint Chief of Staff*, May 22, 2022. 另可參閱：諍聞軍事，〈只有高效的電子頻譜管理，才能有電子對抗作戰的勝利〉，《每日頭條-軍事》，2017 年 4 月 16 日，https://kknews.cc/military/4q4yvmv.html#google_vignette。

[15] 〈電磁頻譜知識鏈接〉，《人民網-軍事頻道》。

[16] 陳勇、張余、柳永祥，〈電磁頻譜戰發展剖析與思考〉，《指揮與控制學報》第 4 卷第 4 期， 2018 年 12 月，頁 319−324。

[17] 郭蘭圖，〈從電磁頻譜管理到電磁戰鬥管理：演進與展望〉，《CIE 智庫》，2022 年 12 月 10 日，https://www.cie.org.cn/list_42/11110.html。

雜。有鑑於此，以下將引用2023年更新的美國陸軍技術刊物（Army Technical Publications，ATP）3-12.3《電磁戰技術》（*ATP 3-12.3 Electromagnetic Warfare Techniques*）中的準則，具體呈現頻譜管理在電子戰中的角色。

（一）頻譜管理員與電子戰指揮官

1.頻譜管理員：頻譜管理員對電磁頻譜資源進行管理，以保證己方電磁頻譜的使用。頻譜管理員的職責包括：「（1）領導、制定電子戰行動，並且通過評估電子攻擊對己方設備的影響，制定電子防護措施。（2）與上級和下級單位進行協調，以減輕電子攻擊對己方的影響。（3）與同級、下級和上級組織合作，確定電磁輻射單元，並將其列入聯合限用頻率清單。（4）將電子攻擊的效果與情報進行整合，增加情報資訊。（5）編寫電子戰相關文檔，對電磁干擾展開調查，為聯合頻譜干擾解決方案提供支援。（6）參與網路電磁作戰工作組，解決電磁頻譜需求中的矛盾，並為電子戰作戰行動的規劃和執行中提供建議和協助」。[18]

2.電子戰指揮官：戰鬥進行中電磁頻譜資源的效果瞬息變化，電子戰指揮官須注意更新電磁波的變動，在執行電子戰時考量：「（1）敵軍的電子作戰命令；（2）信號作戰指令；（3）聯合限制頻率清單；（4）電磁干擾預測與回報」。[19]

（二）電子戰準備—避免電磁頻譜衝突

避免頻譜衝突是電磁頻譜管理的一部分，避免頻譜衝突就是協調戰爭和通信中頻譜使用與情報功能的系統化管理過程。要避免電

[18] "ATP 3-12.3 Electromagnetic Warfare Techniques," *Headquarters, Department of the Army*, January 30, 2023 (Updates of ATP 3-12.3 July 16, 2019), https://irp.fas.org/doddir/army/atp3-12-3.pdf.

[19] Appendix A Electromagnetic Spectrum Management of "Joint Electromagnetic Spectrum Operations," *US Joint Chief of Staff*; "ATP 3-12.3 Electromagnetic Warfare Techniques," *Headquarters, Department of the Army*.

磁頻譜使用衝突，需要瞭解任務需求。電子戰指揮官要考慮：「裝備的作用距離、定位精度和對友軍頻率以及受限頻譜依賴程度，並交付建議信號操作條例和聯合限制頻率清單。信號操作條例包括呼叫符號、呼叫語音、頻率分配、符號，並將其分配給友軍。針對信號操作條例和聯合限制頻率清單的避免衝突措施，電子戰指揮官需要考慮以下事項：頻譜的用途；波形特性；定位和使用時間」。[20]

（三）電子攻擊、支援與防護之電磁頻譜規畫

鑒於敵軍須利用電磁頻譜下達指令與進行情監偵暨導航，我方可趁機藉由輻射源威脅定位進行態勢感知以及目標瞄準：電子支援可以借助測向定位威脅輻射源，一旦定位，指揮官便可以對目標實施致命火力打擊，也可以請求電子攻擊以達到預期效果。至於「電子防護，網路電子戰指揮官和通信部門需要考慮以下內容：電磁加固、電磁隱蔽、輻射控制、電磁頻譜管理、戰時預備模式、電磁相容。其中，電磁頻譜管理通過操作、工程和管理程式來計畫、協調和管理電磁頻譜的使用。電磁頻譜管理會影響部隊進行電子防護的能力。頻譜管理員準備並維護一個友軍頻率清單，並與情報部門聯繫交換取得威脅頻率清單。瞭解電磁頻譜資源的目的及其特性後，頻譜管理者可以在準備操作或執行電子防護任務時，協助網路電子戰指揮官瞭解操作區域中友軍發射機的類型和數量，以避免操作時產生電磁干擾」。[21]

肆、結語：頻譜管理面臨的挑戰與機會

未來的戰場電磁環境愈形複雜多變，頻譜管理的難度、所要求的即時決策支援愈發形成挑戰。首先是因應多領域聯合作戰，要求作戰頻譜規劃能同時應用於作戰、通信、情報、電子對抗等，及時

[20] "ATP 3-12.3 Electromagnetic Warfare Techniques," *Headquarters, Department of the Army*.

[21] Appendix A Electromagnetic Spectrum Management of "Joint Electromagnetic Spectrum Operations," *US Joint Chief of Staff*; "ATP 3-12.3 Electromagnetic Warfare Techniques," *Headquarters, Department of the Army*.

主動地發現與調整潛在頻率衝突和干擾。其次，未來頻譜規劃系統將朝向動態作戰頻譜規劃，貫穿聯合作戰全程，強調頻譜輔助作戰決策，藉頻譜分析提供戰場頻譜決策支援資訊。[22]雖然迄今尚無任何國家足以將電磁頻譜單獨列為作戰領域以遂行電磁頻譜作戰，未來可望藉由運用雲端運算與人工智慧於認知頻譜管理、[23]戰場頻譜決策支援，藉由人工智慧或機器學習輔助之監測頻譜、動態感知與品質量算，即時掌握通訊連結是否遭削弱，[24]並適時發展部署補強體系，讓電磁戰鬥管理規劃系統功能更為強大。[25]

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、網電作戰、認知作戰、中國數位監控。

[22] 郭蘭圖，〈從電磁頻譜管理到電磁戰鬥管理：演進與展望〉。

[23] Marcin Frąckiewicz, “The Future of Spectrum Management: Cognitive Radio Networks,” *TS2Space*, July 15, 2023, https://ts2.space/en/the-future-of-spectrum-management-cognitive-radio-networks/.

[24] Tim Fountain, “Space EW: a Practical Approach,” *Rohde & Schwartz Webinar*, July 14, 2023.

[25] “Air Force Doctrine Publication (AFDP) 3-51 Electromagnetic Warfare and Electromagnetic Spectrum Operations,” *Curtis E. Lemay Center for Doctrine Development and Education*, July 30, 2019, https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-51/3-51-AFDP-EW-EMSO.pdf.

Spectrum Management and Electronic Operations

Yisuo Tzeng

Division of Cybersecurity and Decision-making Simulation

Abstract

Electronic operations, whether electronic attack, protection or support, require secure and clear command, control and communication systems that depend on effective spectrum management to prevent mutual interference as well as adversarial jamming. Spectrum managers manage electromagnetic spectrum resources to ensure their availability.

On the battlefield, commanders of electronic operations must focus on the dynamics of changing electromagnetic waves and electromagnetic spectrum resources, taking into account adversarial electronic combat order, signal operations directives, joint list of limiting frequency, as well as prediction and reporting of electromagnetic interference. Adversarial radiation sources can be located through such electronic support measures as situational awareness and target acquisition; once located, commanders issue lethal strike orders through electronic attack and kinetic means. In terms of electronic protection, electro-cyber combat commanders and communications units must take into account electromagnetic hardening, electronic masking, radiation control, electromagnetic spectrum management, combat-ready module, as well as electromagnetic compatibility.

To prepare for multi-domain joint operations in the future, complex and real-time decision-making support requiring spectrum management represents a growing challenge. With the support and application of cloud computing and artificial intelligence in cognitive spectrum management,

spectrum planning apparatus can move towards significantly more powerful dynamic battle spectrum management.

Keywords: Spectrum Management, Electronic Operations, Battle Spectrum Management

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

美國海軍電子作戰的現況與展望

翟文中

國防戰略與資源研究所

壹、前言

海軍承平時期的例行巡弋或是戰爭時期的接敵交火，都是在範圍廣大的洋面執行。就指管通信與搜尋敵艦言，必須仰賴各式通電裝備與偵測系統方能有以致之。隨著海軍作戰範圍不斷擴大，載台間的協調整合日趨密切，指揮通信需求因此大幅增加。在這種情況下，海軍對電磁頻譜的運用進入了一個嶄新的境界。倘若能對敵方發送的電子信號加以截收或破密，即可瞭解敵人意圖提早採取因應作為。此外，尚可透過實體摧毀或軟體中和等方式，對敵方的電子控制系統（electronic control system）進行攻擊，使其喪失功能無法有效支援海軍作戰。另一方面，我們亦須保護己方的電子裝備與系統，防止敵方對我進行軟硬殺等各式電子攻擊。海軍引進無線電進行通信開始，電子作戰進行了百餘年，其重要性隨著電子科技發展與日俱進。在可預見未來，通信網路與人工智慧等新興科技運用於電子作戰領域，將使電子作戰的型式與手段更趨多元。因此，無論採攻勢性或防禦性作為，若能將電子作戰與指揮管制或軍事行動予以結合，可對戰局的最終結果產生決定性影響。由於美國海軍在電子作戰領域擁有優越的地位，本文希望透過對其電子作戰的運用歷史、當前作為與未來走向等不同面向說明，使讀者對海軍電子作戰的整體輪廓能有更為清晰的認識。

貳、電子作戰的分類與運用

一、電子作戰的分類

長期以來，電子作戰依其運用方式歸為四種不同類別，即電子

反制（Electric Counter Measures，ECM）、電子支援（Electric Support Measures，ESM）、電子反反制（Electric Counter-Counter Measures，ECCM）與電子發射管制（Electric Emission Control，EMCON）。[1]除前揭區劃方法外，亦有將電子作戰分為「戰略性與戰術性」以及「攻擊性與防禦性」等不同區劃標準。當前，隨著電子科技的進步與作戰方式的擴大，美軍對電子戰的範疇亦做了些許的修改，在美國防部 2012 年 2 月發佈的《聯合作戰出版物 3-13.1 電子作戰》（*Joint Publication 3-13.1 Electronic Warfare*）中，將電子作戰定義為「運用電磁能與導能（directed energy）控制電磁頻譜（electromagnetic spectrum，EMS）或攻擊敵人的軍事行動」，其包括了三個部分：電子攻擊（electronic attack，EA）、電子防護（electronic protection，EP）與電子作戰支援（electronic warfare support，ES）。[2]在下文中，將對此三者的定義與運用範疇進行扼要地說明。

（一）電子攻擊

運用電磁能、導能或反輻射武器，對人員、設施或裝備進行攻擊，用以降低、抵消或摧毀敵人的戰鬥能力，其被視為一種對敵攻擊形式。電子攻擊包括主動電子攻擊與被動電子攻擊兩大類，前者係以電子攻擊系統或武器在電磁譜頻釋放射量；後者指運用非輻射／再輻射手段，例如施放金屬箔片（干擾絲）。

（二）電子防護

電子防護指採取行動用以保護人員、設施或裝備不受友軍、中

[1] 電子發射管制經常為人忽略，實施起來卻是相對比較容易。無線電靜止（radio silence）係最顯著的例子。1941 年，日本海軍運用無線電靜止規避了美軍對其進行的偵監，而能成功地發起對美國珍珠港海空基地的奇襲行動。

[2] The Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02 (Washington, D.C.: Department of Defense, April 2001), pp.177-178; and Joint Chiefs of Staff, *Electronic Warfare*, Joint Publication 3-13.1 (Washington, D.C.: Department of Defense, February 2012), p.viii.

立方或敵人運用電磁頻譜以降低、抵消或摧毀友軍戰鬥能力的任何效應影響。雖然，防禦性電子攻擊與電子防護都是用來保護人員、設施、能力與裝備，然而前者係使敵人無法運用電磁頻譜標定、導引與觸發武器對我發起致命性攻擊，後者則是對電子攻擊或電磁干擾（electromagnetic interference，EMI）效應進行防護。

（三）電子作戰支援

作戰指揮官採取或在其直接控制下的行動，對蓄意或無意發射的電磁能進行搜尋、攔截、確認與定位，用以降低對辨識、標定、計畫與執行未來行動形成的威脅。就此而論，電子作戰支援為指揮官執行作戰任務備便所需的電磁環境（electromagnetic environment，EME）。此外，電子作戰支援數據可以產生信號情報（signal intelligent，SIGINT），做為電子標定或是實體攻擊用途。[3]

二、電子作戰的運用實例

在近代歷次軍事衝突中，參戰各方都不同程度地運用電子作戰做為防禦或攻擊的手段，掌握電子作戰優勢的一方經常可以取得令人驚羨的戰果。1967 年 10 月，以色列驅逐艦「艾拉特號」（Eilat）在第三次以阿戰爭期間，為埃及海軍配備冥河飛彈的飛彈快艇重創沉沒。歷經此次重大戰損，以色列痛定思痛針對冥河飛彈進行了各項研究，發展出因應此型飛彈的電子作戰準則和反制技術。1973 年 10 月的第四次以阿戰爭期間，以色列海軍運用干擾絲與電子干擾器等不同型式電子作戰手段，成功地反制了敵方運用冥河飛彈對其海軍艦船發起了攻擊。整個戰爭期間，埃及與敘利亞共發射了 52 枚冥河飛彈無一擊中以色列艦船。[4]另一著名例子係 1982 年 6 月的貝卡山谷（Bekaa Valley）之役，以色列成功地運用電子作戰諸般手段，同

[3] Joint Chiefs of Staff, *Electronic Warfare*, pp. I-4-6.

[4] Christian H. Heller, "The Impact of Insignificance: Naval Developments from the Yom Kippur War," *Center for International Maritime Security*, February 19, 2019, https://cimsec.org/the-impact-of-insignificance-naval-developments-from-the-yom-kippur-war/.

時配合空軍戰機運用，在傷亡極小情況下，將敘利亞部署在貝卡山谷的防空飛彈陣地悉數摧毀。

其後，在波灣戰爭（Gulf War）、科索沃戰爭（Kosovo War）與納卡（Nagorno-Karabakh）衝突中，電子作戰均扮演著重要角色，成為現代衝突與戰爭中影響軍事行動成敗的關鍵性因素。隨著各項嶄新作戰思維不斷引進軍事作戰領域，電子作戰運用範圍亦相應做了大幅地擴張，當前資訊作戰（information warfare，IW）、網界空間作戰（cyberspace warfare）與認知作戰（cognitive warfare）等作戰型式，均可看到電子作戰的身影與重要作用。例如，在網界空間作戰中，電子作戰可藉激勵網絡感測器（stimulating networked sensors）、排拒無線網路（denying wireless networks）或其他各類行動，用以設定形塑對己方有利的網界環境。即令處於防禦態勢，電子系統仍可對無線存取點（wireless access points）的攻擊進行偵測並挫敗敵方攻擊行動。[5]2014 年俄烏戰爭期間，俄羅斯曾滲透至烏克蘭的電訊系統，運用拒絕服務（denial of service）與操控社群媒體，對烏克蘭的 C4ISR 重要節點進行針對性的網界與電磁譜頻作戰。[6]未來，電子作戰在各領域的運用將更加廣泛，海軍作戰領域自然不會例外。

參、美國海軍電子作戰的歷史與現況

電子戰的戰術、科技與裝備發展，係與電磁能輻射的偵測、運用與干擾等因素息息相關。1900 年代初期，當無線電被引進海軍通信領域後，揭開了海軍電子作戰的序幕。當時，電子作戰關切的重點係如何干擾與利用敵人的通信，同時發展測向（direction-finding）裝備，用以標定敵人的無線電發射機。安裝在驅逐艦的測向儀，被證明能有效地標定敵方潛艦位置。兩次世界大戰期間，海

[5] Joint Chiefs of Staff, *Electronic Warfare*, pp. I-15 - 16.
[6] Department of the Army, *Cyberspace Operations and Electromagnetic Warfare*, FM 3-12 (Washington, D.C.: Headquarters, Department of Army, 2021), p. 2-2.

軍電子裝備的發展則在提升無線電接收機與發射機的性能，電子戰科技相較戰時不曾出現太大改變。1922 年，科學家發現了雷達工作原理，海軍電子作戰遂邁入了另一嶄新領域。其後，電子裝備的發展主要用於對機艦進行確認（identification）與鑑別（recognition）、干擾敵人的雷達與通信系統、中斷敵人電子控制系統以及反制敵方運用電子戰術對我方裝備與人員進行干擾。高頻通信與測向裝備的引進，提升了電戰裝備的準確度（precision）和精密度（accuracy）。二次世界大戰期間，各項電子作戰戰術被廣泛地運用於實戰中，例如英國運用信標（欺敵）系統混淆德軍以及美軍運用噪音干擾器（noise jammers）與鋁箔片（Aluminum foil）干擾德軍雷達用以保護美軍軍機安全。[7]

冷戰初期，美國海軍為了執行對蘇聯的戰略打擊任務，其戰機必須具備穿透蘇聯防空系統的能力。由於戰機機體過小加上對重量特別地敏感，美國海軍遂捨棄了重量較重的噪音干擾器採用較輕的欺敵干擾器（deception jammers）。此外，美國海軍發展了內建與外掛式干擾絲與火焰彈（chaff and flare dispensers），用以對其艦船提供防護。越戰期間，由於蘇聯防空飛彈問世，美國海軍電子作戰的發展聚焦於歸向暨預警接收器（radar homing and warning receivers，RHAW）以及雷達干擾器的研發。此時，嶄新的電子作戰概念、裝備與武器被引進戰場，包括了反輻射飛彈（anti-radiation missiles，ARM）、遠距離干擾、紅外線預警接收器與干擾器（IR warning receivers and IR jammers），這些先進裝備使得電子作戰的遂行更加地複雜與多元化。[8]至此，海軍電子作戰涵蓋的範圍日益擴展，包括了雷達、通信、水聲、光電以及遙控、遙測和導航等領域，雷達電

[7] Naval Electronic Systems Command, *Electronic Warfare,* NAVELEX Program Information Series (Washington, D.C.: Naval Electronic Systems Command), p. 3, https://www.navy-radio.com/manuals/navelex-ew-brochure.pdf.
[8] Ibid., pp. 5-8.

子戰最重要，這是因為現代海戰主要係以飛彈進行接戰。[9]

冷戰結束，蘇聯對美國的軍事威脅不再，這並未為美國軍方帶來任何「和平紅利」，主因係電子作戰面對的環境更加地複雜，這是電子、通信與網路科技快速發展與三者間近乎無縫接合導致的必然結果。面對電子作戰環境遽變，為了掌握電子作戰優勢，美國海軍軍令部長格林納（Jonathan Greenert）上將遂提出了「電磁機動戰」（electromagnetic maneuver warfare，EMW）的嶄新作戰概念。2014 年 3 月，其向參議院撥款委員會下設國防小組委員會（Subcommittee on Defense Senate Committee on Appropriations）報告時指出，「電磁機動戰」係指美軍能在電磁頻譜空間自由地進行機動，同時阻止敵人如此地做。[10]雖然，美國海軍未進一步地說明「電磁機動戰」的內涵與如何實踐，由格林納上將的談話中不難推知，此作戰概念意味著要最大限度地運用電磁譜頻和際界空間來進行電子作戰的攻擊與防禦。為能有效地發起「電磁機動戰」，必須對作戰全域的電子作戰裝備與戰術進行協調和集成，電子裝備的更新和作戰技術的創新就成為美國海軍建立電子作戰能力的重要考量。[11]

肆、美國海軍電子作戰的走向與發展

隨著電子作戰技術與裝備的不斷演進，美國海軍目前面臨的電子作戰威脅來自各個不同面向，計有寬頻帶（wider frequency bands）、低功率信號、頻率分集（frequency diversity）、複雜的發射器與電磁能力／電磁干擾等等。面對這些日益嚴苛挑戰，美國海軍近年開始對機艦的電子裝備進行性能提升，同時發展嶄新的電子

[9] 〈海軍雷達電子戰〉，《快懂百科》，https://www.baike.com/wikiid/4039975500895959261?view_id=1vhbser85aww00。

[10] "Statement of Admiral Jonathan Greenert U.S. Navy Chief of Naval Operations before the Subcommittee on Defense Senate Committee on Appropriations on FY 2015 Department of the Navy Posture," *Subcommittee on Defense Senate Committee on Appropriation*, March 26, 2014, https://www.appropriations.senate.gov/imo/media/doc/hearings/Adm%20Greenert.pdf.

[11] 〈美國海軍電子戰發展綜速〉，《搜狐》，2019 年 1 月 25 日，https://www.sohu.com/a/291523484_465915。

作戰概念與架構，雙管齊下用以強化電子作戰能力。在下文中，將對相關發展進行扼要說明。

一、E-2D 艦載預警機 AN/ALQ-217 電子支援設備的性能升級

AN/ALQ-217 為無源感測器系統，能夠進行自動掃瞄，透過搜索、攔截和定位等方式，提供 E-2D 大區域的環境覺知資訊。[12]2020 年 1 月，美國海軍授予洛克希德馬丁公司（Lockheed Martin）金額 4,300 萬美元合約，用於對該系統的戰鬥識別（combat identification，CID）網路以及天線與整流／回饋單元（active front ends，AFEs）進行性能提升，藉此 E-2D 預警機可與航艦其他不同型式艦載機實現多點地理定位，並對具高威脅性的先進雷達進行偵測。[13]

二、水面艦船電子作戰改善計畫（Surface Electronic Warfare Improvement Program, SEWIP）

此計畫係分為四階段的批次（block）性能改良，用以提升艦載 AN/SLQ-32 電子作戰系統性能，[14]使其具有更佳的電子監視與攻擊能力。[15]目前，已進行的前三階段批次改良，依序對 AN/SLQ-32 電子作戰系統的電子作戰能力（攻船飛彈防禦、反制標定與反制監視）、電子支援能力（天線、接收器改良與建立開放式戰鬥系統界

---

[12]〈美軍未來電子戰能力建設淺析〉，《安全內參》，2020 年 11 月 2 日，https://www.secrss.com/articles/26679。

[13] "U.S. Navy Awards Lockheed Martin $ 43 Million Contract Modification For E-2D AN/ALQ-217 Electronic Support Measures Upgrade," *Lockheed Martin*, January 14, 2020, https://news.lockheedmartin.com/us-navy-awards-lockheed-martin-43-million-contract-modification-e-2d-an-alq-217-electronic-support-measures-upgrade; "AN/ALQ-217 Electronic Support Measures: Unparallel Support for the Warfighter," *Lockheed Martin*, https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/electronic-warfare/AN-ALQ-217-brochure.pdf.

[14] AN/SLQ-32 電子作戰系統於 1970 年代末期為美國海軍採用，主要功能係提供早期偵測、信號分析、威脅預警與反制攻船飛彈攻擊。此系統具有完整的電子作戰能力，可以透過操控台進行人工管理與操作，或是由艦載戰鬥管理系統進行半自動或全自動操作。

[15] Sally Cole, "U.S. Navy's electronic warfare modernization effort centers on COTS," *Military Embedded Systems*, September 3, 2015, https://militaryembedded.com/radar-ew/sigint/u-modernization-effort-centers-cots.

面）與電子攻擊能力進行提升。計畫進行的批次四階段改良，計畫賦予此系統更先進的光學與紅外線監視對抗能力。[16]

三、發展「針對整合感測器的多元素信跡網路化模擬」（Netted Emulation of Multi-Element Signature Against Integrated Sensors, NEMESIS；簡稱「復仇女神」）計畫[17]

就美國海軍電子作戰言，「復仇女神」計畫係最具潛力與影響最深遠的一項計畫，其將海軍各式載台的電子作戰酬載與網路通信科技整合，透過聲學與電磁學手段將虛擬的機艦等目標，投射至敵人艦船與潛艦等載台的感測器，用以干擾敵人達成欺敵目的。[18]「復仇女神」系統具有通信、欺敵與電子干擾等功能，打破了過去電子作戰各自為戰的方式，將過去欺敵干擾的個別或局部效應擴及至對敵人艦隊與感測器網路的全面攻擊。[19]換言之，此系統使海軍電子作戰的運用由傳統的「系統」擴大到「體系」面向，可視為「網電一體」作戰概念的落實。

除前揭進行中的各項計畫外，美國海軍目前亦積極引進「認知型」與「智能型」電子作戰系統，例如為保護 F-18 戰機進行的「自適應雷達反制」（adaptive radar countermeasures，ARC）[20]軟體開發

---

[16] "Surface Electronic Warfare Improvement Program, *U.S. Navy Office of Information*, September 20, 2021, https://www.navy.mil/Resources/Fact-Files/Display-FactFiles/Article/2167559/surface-electronic-warfare-improvement-program-sewip/.

[17] 這個計畫雖未出現在海軍年度預算清單項目中，然而其提出與執行已有相當時間，例如國防工業協會（National Defense Industrial Association, NDIA）舉辦的第 15 屆年度科技與工程技術會議，即將此計畫列入破壞性海軍科技（Disruptive Naval Technologies）進行簡報說明，參見 Bob Smith, Director of Disruptive Technologies, "Disruptive Naval Technologies," in NDIA 15th Annual Science and Engineering Technology Conference, College Park, Maryland, April 9, 2014, https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/02/NavyDisruptiveNavalTechnologies.pdf.

[18] "The U.S. Navy completes the "UxS IBP 21" exercise at the San Diego Naval Base in California," *MINNEWS*, https://min.news/en/military/6bb333fe02c47dd7ac85ca5cfd09ea98.html.

[19] Brett Tingley, "The Navy's Secretive And Revolutionary Program To Project False Fleets From Drone Swarms," *THE DRIVE*, November 7, 2019, https://www.thedrive.com/the-war-zone/29505/the-navys-secretive-nemesis-electronic-warfare-capability-will-change-naval-combat-forever.

[20] John Keller, "Leidos to develop electronic warfare (EW) adaptive radar countermeasures software to protect F/A-18 aircraft," *Military + Aerospace Electronics*, August 28, 2020, https://www.militaryaerospace.com/computers/article/14182542/electronic-warfare-ew-adaptive-radar-countermeasures-fa18.

與提升EA-18G電子攻擊機電戰與攻擊能力發展的「自適應電子作戰行為學習」（Behavioral Learning for Adaptive Electronic Warfare，BLADE）無線電通信系統[21]以及「反應式電子攻擊措施」（Reactive Electronic Attack Measures，REAM）[22]篋艙。種種跡象均顯示著，美國海軍現正透過機器學習與人工智慧演算法發展認知電子作戰（Cognitive Electronic Warfare）能力，[23]這將加快電子作戰的節奏與縮短電子反制的回應時間，賦予海軍電子作戰一個嶄新面貌。

伍、結語

總體而論，電子作戰的演進就是一部電子裝備發展史，美國海軍利用並引進新興科技用以強化整體電子作戰能力，其發展呈現在「認知電子作戰」與「網電一體作戰」兩個面向。就認知電子作戰言，當前通信科技、機器學習與人工智慧演算法的能力不斷地提升，賦予電子裝備反制威脅的自我學習與自主回應能力，能在複雜的電磁環境中快速地對敵人的電子信號進行偵測與分類，且能以自主干擾的模式在極短時間內完成反制。就「網電一體」而言，透過硬體與軟體的整合，電子作戰的主體將由過去的個別裝備擴大至未來的整個網路，配備先進軟體的裝備不僅可獨立作業，更成為軟體

[21] 此系統由國防部國防先進研究計畫署（Defense Advanced Research Projects Agency, DARPA）負責，相關細節參閱：Charlotte Adams, “Cognitive Electronic Warfare: Radio Frequency Spectrum Meets Machine Learning,” *Avionics*, https://interactive.aviationtoday.com/avionicsmagazine/august-september-2018/cognitive-electronic-warfare-radio-frequency-spectrum-meets-machine-learning/; “Behavioral Learning for Adaptive Electronic Warfare (BLADE),” *Defense Advanced Research Projects Agency*, https://www.darpa.mil/program/behavioral-learning-for-adaptive-electronic-warfare; Mark Pomerleau, “AFRL seeks cognitive electronic warfare research,” Jul 12, 2016, *C4ISRNET*, https://www.c4isrnet.com/c2-comms/2016/07/11/afrl-seeks-cognitive-electronic-warfare-research/.

[22] Gerard Frawley, “Upgrading Electronic Attack Capabilities on the Growler,” *Defense.info*, July 10, 2019, https://defense.info/defense-systems/upgrading-electronic-attack-capabilities-on-the-growler/.

[23] 認知電子作戰的最基本概念，係指能對敵人不同目的使用的電子信號進行偵測與分類，其後在機器學習與人工智慧演算法協助下，能進一步發展自主反制與反反制措施。參見：Joseph Trevithick, and Tyler Rogoway, “Cognitive Electronic Warfare Could Revolutionize How America Wages War With Radio Waves,” *THE WARZONE*, July 7, 2020, https://www.thedrive.com/the-war-zone/34606/cognitive-electronic-warfare-could-revolutionize-how-america-wages-war-with-radio-waves; and “Cognitive electronic warfare,” *Australian Government Department of Defence Science and Technology*, https://www.dst.defence.gov.au/sites/default/files/publications/documents/DSC%202035%20CogEW%20Fact%20Sheet%20PRO.pdf.

系統網路的一個節點，系統性能將隨著網路節點增加不斷拓展，可望在節點間實現資訊共享，若加上偽信號與欺敵作為的運用，這種「集成」電子作戰將賦予海軍電子作戰嶄新面貌，使得美國海軍成為未來電子作戰的「改變遊戲規則者」（game changers）。透過這些軟硬體領域的創新，美國海軍可自由地運用電磁頻譜同時並剝奪對手使用此空間的能力，從而成為電子作戰的支配者與優勝者。

本文作者翟文中為淡江大學國際事務與戰略研究所碩士，現為財團法人國防安全研究院國防戰略與資源研究所助理研究員。主要研究領域為：中國軍力、海軍作戰與海軍科技。

US Navy Electronic Warfare: Current Development and Future Perspectives

Wen-Chung, Chai

Division of Defense Strategy and Resources

Abstract

Electronic warfare refers to the use of electromagnetic energy to exploit, deceive, or attack enemy forces and equipment. Electronic warfare aims to disrupt, disable or neutralize enemy radar systems, command and control nodes, and intelligence, surveillance and reconnaissance capabilities through various electronic measures and means. Strictly speaking, the origins of electronic warfare can be traced to World War I when direction-finding equipment was employed. During World War II, electronic warfare made notable progress, with new techniques introduced to the naval warfare domain, including radar jamming, noise jammers, and aluminum foil, etc. In the Cold War era, as the US Navy stood up to the Soviet military threat, more sophisticated equipment appeared and was deployed, such as deception jammers, chaff and flare dispersers, radar homing and warning receivers, anti-radiation missiles, and IR warning receivers and IR jammers. In the foreseeable future, as naval operations face a contested electronic environment, the US Navy will focus on cyberspace operations. Through artificial intelligence and machine learning assistance, US Navy electronic warfare capabilities will reshape and transform traditional electronic warfare into a new concept and domain, that is "Cognitive Electronic Warfare." Consequently, the US Navy will be better able to respond to emerging threats and gain the advantage in electronic competition.

Keywords: US Navy, Naval Electronic Warfare, Cognitive Electronic Warfare, Netted Emulation of Multi-Element Signature Against Integrated Sensors（NEMESIS）

聯合防空作戰之電子戰支援研究

高志榮、詹祥威

網路安全與決策推演研究所

壹、前言

隨戰爭型態改變，軍事事務不斷深入革新，以及科技發展支持下武器裝備日新月異，「聯合作戰」（joint operation）已成為戰爭理論及作戰思想共同發展趨勢；本世紀最具代表性的幾次戰爭中，無論是波灣戰爭與科索沃戰爭，以及後續美國出兵阿富汗與伊拉克等皆可看出，以美軍為首之盟軍的行動模式，係在開戰之初以飛彈、空中武力載台為主，對敵實施遠距精準打擊，摧毀敵軍防空火網，以期能有效支援地面部隊後續作戰。而在地面部隊勃發後，空中部隊仍持續支援與協調機動，基本此種作為即是「聯合作戰」之概念與運作，其中多軍、兵、種的「聯合防空作戰」為作戰防衛保存並發揮後續戰力之積極作為，實為至關重要。

現當前中國並未面臨外在軍事安全威脅，但共軍仍不斷增加軍備支出，不僅持續提升其彈道飛彈、空軍載台與陸海空綜合精準打擊能力，更藉由越界挑釁與環台繞行等方式襲擾我及周邊鄰國，對區域防空安全形成重大威脅。針對台灣，未來台澎防衛作戰，面對的場景極有可能是中共「多批次、多層次；不同方向，同一時間」的不對稱「空襲與反空襲」戰場景況，我軍如要確保用兵的行動自由，聯合防空戰力的發揮是部隊戰力保存及發揮之憑藉。

電子戰是 20 世紀通信電子科技運用於戰爭手段中衍生出之產物，隨著電子科技發展，電子戰也由戰爭中輔助的配角，演變成必要且不可或缺的要角；1991 年波灣戰爭聯軍能在短時間內擊潰伊拉克，除精良武器、先進指管系統及快速後勤外，電子戰所發揮的戰力是令人刮目相看，可說是「大軍未動、電戰先行」的典範。細數

通信電子，其基本可提供電子偵測、通訊、導航、指揮管制、防空預警、目標尋獲、飛彈導引、火力控制等軍事技術，手段涵蓋整個作戰期程，因此掌握電子戰優勢即能掌握主動，制敵機先。

貳、聯合防空之定義與詮釋

《國軍聯合作戰要綱》草案中，將「聯合作戰」定義為「凡兩個（含）以上軍種單位，不論其階層或指揮關係如何，在統一機構指揮管制下執行共同任務，達成同一作戰目的所遂行之作戰，謂之聯合作戰」。而按美軍的相關解釋，「聯合作戰」係指在不建立一個新的「聯合部隊」（Joint Force）前提下，聯合部隊以及以特定指揮關係受僱的軍種部隊之間，所共同執行的軍事行動。而所謂「聯合部隊」則是由在單一聯合部隊指揮官領導下作戰的兩個、或多個軍事部門分隊所組成的部隊。[1]

綜整上述二者之意涵，基本可知所謂「聯合作戰」即是由單一指揮架構下，不同單位間的協同聯合行動；而依此概念，所謂「聯合防空」自是以「防空」為任務核心，由不同軍、兵種單位之間的協同、聯繫以及共同應處作為，藉以發揮各單位防空軍兵力與武器系統，達成統合性作為，以確保整體空中安全，並進一步達成我方空中與後續相關兵力運用之指管通勤與運動順暢。

而整體防空作戰的概念，除「聯合防空」外尚有作戰區為主的「野戰防空」。例如，我國當前整體「聯合防空」由空軍作戰指揮部（JAOC）主責，下轄不同區域作戰管制中心（ROCC）、雷達中隊與雷達分隊等；但若有「防空作戰」的實際需求時，則由空作部協調指揮其他軍、兵、種如海軍防空艦艇，或陸基地對空之載台等，進入戰術位置並完成整體防空接戰的準備。而所謂「野戰防空」大多以陸軍為核心，以陸軍各戰區、軍團等單位針對作戰地為

[1] The US DoD, *Joint Operations 3-0: Joint Operations* (Joint Chief of Staff, 2018), p. ix.

中心所進行的防空任務，例如中科院研發自製的陸基天劍二型與 40 快砲組成的野戰防空，即是作為戰區防空任務的主要裝備。即便現今整體科技與裝備的發展下，雷達偵蒐與武器打擊的範圍皆更為廣闊，但就野戰防空的威脅性質、裝備層次或防禦範圍仍然不及於聯合防空之裝備內容。

參、聯合防空作戰之威脅態樣

如同上述，隨科技、裝備日新月異，全球的聯合防空作戰威脅越趨增加，本段將以中國為例，以戰略層次至戰術層次做案例的示意分析。

從戰略面而言，衛星作為戰略性的武器是中國在 80 年代後大力發展的重點項目之一；中國發展北斗系列衛星已有多時，1986 年 3 月的「國家高技術研究發展計劃」中提出大力發展「航天」與「信息（資訊）」技術，開啟了中國資訊、電機與電腦工程的現代化的起始；隨後在 1989 年由陳芳允院士帶領，藉由兩顆衛星提供的定位展開「北斗」衛星的相關計畫，並且到 2010 年完成了第二顆衛星的發射與運行。[2]當前的北斗已進化至第三代，其第二代、第二號系統是一個包含 16 顆衛星的全球衛星導航系統，分別為六顆靜止軌道衛星、六顆傾斜地球同步軌道衛星、四顆中地球軌道衛星，2012 年 11 月，第二代北斗系統開始在亞太地區為用戶提供區域定位服務。

第三代的北斗三號系統，則由三種不同軌道的衛星組成，包括 24 顆地球中圓軌道衛星（覆蓋全球），三顆傾斜地球同步軌道衛星（覆蓋亞太大部分地區）和三顆地球靜止軌道衛星（覆蓋中國）。北斗三號於 2018 年提前開放了北斗系統的全球定位功能，其全功能的完整開通則於 2020 年 7 月 31 日完成。2014 年 12 月，央視公開探討的節目中，評論員則透露北斗軍用訊號基本已可達成全球覆蓋，

[2] 〈20 年磨一劍——北斗導航系統的發展歷程〉，《中國數字科技館》，2021 年 3 月 30 日，https://bit.ly/44quaB4。

並且可讓解放軍的多彈頭洲際飛彈接收訊號，依照各種跡象研判，此種所謂「覆蓋」應或是機動式覆蓋，並非全面性的持續覆蓋。而根據上述發展歷程揭露其目標，北斗衛星導航系統的「三步走發展規劃」，其中在 2004 年要實現「區域有源定位」、2012 年要實現「區域無源定位」，至 2020 年則要達成「全球無源定位」的目標。[3]亦即，2014 年所謂的「全球覆蓋」係指衛星的有限時限性覆蓋已達成全球性，但在區域上可提供「區域無源定位」。

2021 年 7 月 21 日「北京航天宏圖信息技術股份有限公司」（中國遙感衛星與北斗導航衛星應用服務商之一）公告委託「銀河航天」於 2022 年 3 月 5 日發射的「遙感」衛星應具備「合成孔徑雷達」（Synthetic Aperture Radar，SAR）的技術。SAR 衛星內建的「微波成像」（microwave imaging）雷達可穿透雲層，不受日夜與天候影響，產生地面高解析度影像，更可全天候偵測地面、地形與地貌，監測海面船隻、路面車輛、自然資源、環境、工程等活動，可預知中共將其視為軍事上，除上述北斗導航衛星外的情監偵等目的之重要工具。

當前中共亦自有建構具規模的「合成孔徑雷達偵察衛星群（Synthetic-Aperture Radar Satellite）」「高分」（GaoFen）系列。根據美智庫 2049 計畫主持人 Mark Stoke 等人的報告分析，中國在 2013 年後至少發射了八枚高分衛星，而此些衛星除合成孔徑外尚配有高光譜傳感器（hyperspectral sensors）；[4] 所謂「合成孔徑」如前所述，係一「主動」收集數據，傳感器產生自己的能量，然後記錄與地球相互作用後反射回來的能量之技術，[5]而「高光譜傳感器」則係一收集和處理電磁頻譜資訊，以獲得圖像中每個像素的頻譜技

[3] 〈20 年磨一劍——北斗導航系統的發展歷程〉,《中國數字科技館》。

[4] Mark Stokes, et. el., "China's Space and Counterspace Capabilities and Activities," *Project 2049 Institute & Pointe Bello*, March 30, 2020, p. 29, https://www.uscc.gov/sites/default/files/2020-05/China_Space_and_Counterspace_Activities.pdf.

[5] Kelsey Herndon, et. el., "What is Synthetic Aperture Radar?," *Earth Data Discovery*, https://bit.ly/3NOBmQQ.

術；基本可以處理光譜中大部分人類難以肉視的，從很長的無線電波、微波、紅外輻射、可見光、紫外線和 X 射線，到很短的伽瑪射線；[6]因此，中國透過結合上述二者而將高分 SAR 衛星運用在軍事用途並無可議。至於通訊與科研部份，則有 70 年代發展的「東方紅」低軌同步衛星。1970 年代晚期發展的軍用「遙感」偵察衛星尚有「尖兵」系列，其亦結合合成孔徑與光學傳感。

圖 1、圖-154 偵察機

資料來源：〈飛抵東海防空識別區？中國空軍偵察機遠海訓練或藏玄機〉，人民網，2017 年 12 月 06 日，https://bit.ly/3KkD8Zh。

說明：圖-154 偵察機（英語：Tu-154 Electronic Intelligence Aircraft）是中國人民解放軍空軍在蘇聯售予的圖-154 客機 M 型（英語：Tu-154M Airliner）的基礎上研製的電子戰偵察機，正式代號為圖-154MD。

中共於 2015 年 12 月 31 日編成戰略支援部隊，其中原為總參電子部（總參四部）負責之電子對抗，也改由戰略支援部隊負責，除衛星外中國亦長時發展其空中情監偵與電子戰的能力；盤點共軍空中具電子戰能力的單元，大致有殲-16D、電轟 6（轟 6G 攜掛電戰莢艙）、電運 8（可掛載「長生一號」RPV）、電運 9、圖-154 等。

上述提及，由蘇聯客機 TU-154 改造而成的解放軍空軍圖-154MD（圖 1）為其當前較為主力的電偵機，從其外觀上分析，比

[6] "What is Hyperspectral Imaging: a Comprehensive Guide," *Specim*, https://bit.ly/3NNQUUV.

照為改造的原型機加裝了多個雷達罩、天線和電子戰設備，裝備了一部合成孔徑雷達系統，該系統與美國空軍 E-8「聯合星」聯合監視及目標攻擊雷達系統相似。合成孔徑雷達系統妥善運用在高空偵察上，能夠明顯的提升中國空軍作戰飛機在一場「進攻性空中戰役」中的作戰效率，亦可能對戰術彈道飛彈提供訊號使彈頭導向目標。

殲-16D 則為當前中共大力發展之電子戰攻擊飛機，基本構型係以俄國 SU-27 重型戰機開發的殲-16 為基礎，除機身塗有複合雷達吸收的塗料層外，尚配有主動電子掃描陣列雷達（AESA），並且可搭載 YJ-91 反輻射飛彈等；據信當前搭載最新的電戰莢艙，其電戰干擾功率已從 30~40 KW 大幅上升至與美軍當前的 EA-18G 所使用的 ALQ-99 電戰莢艙的 100 KW 相近，但由於殲-16D 並未公開相關數據且也未有實戰經驗，此數據之可信度遠不及實戰經驗豐富的 EA-18G，但基本已經可以判斷中共意識到並且從過去美國或聯軍的幾次重大戰爭學取經驗。中共當前既有的空戰電戰設備整理如表 1。

綜上，基本對整體聯合防空而言，包含衛星、空中以及地面的威脅為主要來源；而整體聯合防空的作戰構想，係以戰機、電戰、預警及防空飛彈（反飛彈及反飛機）等執行規範區域之整體防空，在遠程預警及多層攔截下，以防空飛彈先期攔截高、中空來犯之敵機，再以戰機實施防空作戰，對低空（2,000 呎～500 呎高度之空域）及超低空（500 呎高度以下之空域）敵機以小型輕便攜行防空飛彈執行攻擊，進行全縱深防空，確保空域之安全。

表 1、共軍既有空戰電戰設備盤點

共軍既有空戰電戰設備盤點		
戰略性		戰術性
衛星	遠程	戰機
北斗	轟 6	殲 16
高分	運 8	
尖兵	運 9	
東方紅	圖 154	

資料來源：作者依各方資料統整。

肆、電戰支援定義、詮釋與運用

電子作戰支援（Electronic Warfare Support，ES）其範圍擴及整體軍事行動所需要的各種相關電子作戰情報之參數，如頻率、脈波來復頻、雷達模式……等，並且依此對威脅來源進行分析辨識、定位，以供武器載台電戰版本編建威脅的參數、產生威脅符號顯示及干擾模式。

近代戰爭中最著名的電子作戰案例，莫過於聯軍對伊拉克執行的沙漠風暴。在開戰初期，美國空軍以 EF-111 烏鴉（Raven）電戰機作為壓制，搭配 F-117 以及 F-15E 針對伊拉克的雷達與機場進行低空突穿精準轟炸任務。在任務進行中，EF-111 為上述的轟炸任務偵蒐安全的飛行航道、在敵方防區外壓制敵方的地面防空設備，並且根據任務的需求對敵方的雷達等偵蒐設備進行干擾壓制，甚至可以投放實火彈藥攻擊偵蒐系統等。[7]藉由摧毀伊拉克防空的雷達與地對空反制武力，盟軍的空襲有效摧毀伊拉克的反擊能力，為後續地面大規模部隊的挺進排除了危險與障礙。除 EF-111 外，美軍尚有以 C-130 改裝的 EC-130H 羅盤呼叫（Compass Call），該機具有長時高空盤旋的能力，因此可在戰場執行長時任務；並且有效的干擾敵方指管通訊的相關訊號，使得伊拉克地面部隊難以呼叫轟炸或對空反制的相關能力。[8]

以當代美國空軍的電子戰相關設備盤點，上述的 EF-111 以及 EC-130H 皆已逐漸汰換，取而代之的是 RC-135W Rivet Joint、EA-18G 咆嘯者（Growler），以及正在開發中的 EC-37B 3 款。RC-135W Rivet Joint 此類飛機主要任務乃是蒐集雷達參數、監聽無線電頻率及通話內容及運用相位陣列雷達及合成孔徑雷達標定目標，並

[7] Directed by Eliot A. Cohen, "Gulf War Air Power Survey Volume IV Weapons, Tactics, and Training and Space Operations," *Library of Congress*, pp. 94-96.
[8] Directed by Eliot A. Cohen, "Gulf War Air Power Survey Volume IV Weapons, Tactics, and Training and Space Operations," pp. 96-97.

偵照成像，是電子作戰支援當中重要的裝備之一。EA-18G 則是由波音的 F-18 機身，由格魯曼軍火商（Northrop Grumman）製作電子戰莢艙 ALG-99 的攻擊式電戰機。

咆嘯者的主要任務基本是在行動開始前或早期階段，針對敵方發動電子攻擊（EA）和壓制敵方防空系統（SEAD）；Block 1 型號可搭載 3 個電子莢艙，分別為 AN/ALQ-99 高輻射功率干擾發射器、AN/ALQ-218（V）2 數字雷達預警接收器，以及 AN/ALQ-227 通信對抗系統；Block 2 型號則有「被動探測模式和主動雷達抑制功能」的 APG-79 多模式雷達、AN/ALQ-218（V）2 數字雷達預警接收器等。APG-79 為先進戰術有源電子掃描陣列（AESA）雷達，可以提供空對空和空對地能力，其本身具有探測、瞄準、跟踪和保護等功能。AN/ALQ-218（V）2 數字雷達預警接收器主要為「被動對抗系統」，其功用係「提供威脅檢測、識別和定位等」。[9]

EC-37B 則係美國空軍用以取代 EC-130H 的次世代戰術干擾平台，主要機身以灣流 G550 為基礎，除具備前述 EC-130H 既有的相關能力外，並且可能搭載最新具機器學習能力的「憤怒小貓」ALQ-167（Angry Kitten）電戰莢艙，可供執行「反指揮、控制、電腦、通訊、網路、情報、監視和偵察目標（Counter-C5ISRT）」之相關任務。[10]但由於該型號仍在試飛階段，其實際的作戰能力與相關數據，須待日後觀察方才日漸明朗。

伍、聯合防空下的電子作戰支援

如前述，電子作戰貫穿整體作戰全程，包含前、中、後且持續循環，綜合前述分析，基本可依照以下程序理解。在**作戰前階段**，以電子作戰相關支援任務為主，平時已例行偵蒐之相關資訊，需在

[9] "EA-18G Growler Electronic Attack Aircraft, US," *Naval Technology*, April 12, 2022, https://bit.ly/44FYlV6.

[10] Stefano D'urso, "A Closer Look At The EC-37B Compass Call, U.S. Air Force's Future Tactical Electronic Attack Platform," *The Aviationist*, June 1, 2023, https://bit.ly/3JWRw9K.

此階段進行行前確認，包含「地面電子偵蒐測站」所蒐整之敵方電子參數、航空器所掛載之偵蒐設備（如 E-2K、幻象戰機攜掛 ASTAC 莢艙…等），以及海軍船艦之偵蒐設備（如 AN/SLQ 電戰裝備）等方式，實施偵蒐並交叉比對與定位，對戰場應知之各種威脅，如敵方作戰系統及載台電子參數蒐整，並將蒐整的電子參數（如各裝備之頻率、脈波來複頻、波長…等）完成我方武器系統、載台電戰版本威脅符號，以及干擾模式等的資料編整與建置。例如，作戰前針對共軍S-300防空飛彈之雷達電子訊號參數進行截收、辨識、確認以及針對其佈署位置進行標定；上述之參數蒐整與編建，亦能用於平時電戰防護之加強與電戰攻擊任務的訓練。

在作戰過程中，由於已進入對敵交戰狀態，因敵作戰行動之需求，我方相關設備可蒐到敵方平時較難蒐整之參數，而上述戰前所蒐整之資料，亦可於作戰中進行交叉比對，完整我方電子參數數據庫與正確性；而更新後的參數版本亦可用於作戰過程中的對敵作戰戰術行動。**在作戰後**，我方設備、裝備勢必有所損傷，此時我方以尚可運用之陸、海、空兵力，調整佈署後共同實施電磁偵蒐及偵照，並定位敵方武器系統位置、參數，以便後續將既有資料庫參數與我方武器系統、載台版本比對、修調以重複運用至後續戰場，以利各軍兵種聯合作戰或協同作戰，如此持續循環運作。

以當前我作戰環境為例，平時我針對S-300與各殲擊機及水面作戰艦雷達電子訊號參數蒐整，並建置於我方戰機與相關設備之電子參數資料庫中。進入接戰狀態後，戰機可以既有編建之電戰系統版本，運用自身電戰裝備實施防護干擾，空中部隊亦可與指揮中心彼此提供威脅告警、交叉比對，以確保整體部隊安全，並將我方作戰效能發揮極致。

陸、結語

電子戰無法單獨運用其能力達成軍事作戰目標，然於現代戰場中各項武器裝備，均以電磁或光電作為發揮戰力之介質，於作戰初期破壞後，除有利於後續作戰行動外，並可降低作戰時之戰損，此模式已成為全球軍事方面努力之方向與重點。

就聯合防空作戰而言，電子戰支援之電磁資訊掌握，為支持作戰輔佐情報之重要一環，也為電子戰攻擊及防護之重要支撐依據，俄烏戰爭中可看出，情報之獲得及後續之軍事行動作法極為重要，無論是他國的情資提供，或是無人載具監視等，在在都需運用電磁波傳遞來達成，可見這運用電磁頻譜的電子戰，在現今作戰中何等重要。

中共已從波灣及俄烏戰爭中吸取經驗，並持續積極發展電子戰，期能儘速追上歐美水準；故掌握敵情務實全般了解，整體規劃研究評估，並落實精進，期能於未來衝突中能掌握或瞭解電子情資所衍生之作戰規劃作為，精進作戰效能。

本文作者高志榮為國防大學戰爭學院 98 年班，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、聯合作戰、電子戰。

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研究所政策分析員。主要研究領域為：地緣戰略、台日海洋安全、區域安全、日本網路安全政策。

Electronic Warfare Support in the Context of Joint Air-Defense Operations

Chih-Jung, Kao and Siong-Ui, Tsiam

Division of Cyber Security and Decision-Making Simulation

Abstract

The Gulf War of 1991 in which the US and its allies were the main protagonists, has become a paradigm for modern warfare, further validating the vital importance of "air supremacy" in overall ground operations. Air supremacy is also a critical prerequisite for dominating the battlefield. Integrating air assets, such as fighter jets, drones, missiles, and air defense systems, is the focal point in the fight for air supremacy. Consequently, joint air defense has become a crucial defensive measure emphasized by various countries in joint military operations today.

Electronic Warfare (EW) has become a decisive factor in the fight for modern air supremacy. The side with the advantage in EW will win the battlefield initiative, seize the initiative from the enemy, and be likely to achieve victory. Currently, EW can be roughly divided into electronic protection, electronic attack, and electronic warfare support.

Electronic Warfare Support (EWS) measures can be further divided into pre-battle, in-battle, and post-battle electronic warfare attack and electronic warfare protection. This study includes parameter collection required for various operations, development of EW versions for different platforms and equipment, and provision of standard information for threat localization and battlefield management. The aim is to enhance the armed forces' overall combat capabilities through EW capabilities.

The study discusses the role, principles, and application of EWS in the context of "joint air defense operations." It aims to provide a thoughtful

approach in response to increasing military threats and the rapid development of electronic equipment. Taking the EW developments of the leading country, the US, as an example, including aspects such as electromagnetic spectrum, electronic equipment characteristics, development and application status, and operational trends, encourages EWS measure oriented reflection and planning within the framework of joint military operations.

Keywords: Electronic Warfare, Air Supremacy, Joint Air-Defense Operations

海軍艦隊支隊級作戰電子戰計畫作為與戰術運用概念

常漢青

台灣戰略研究學會秘書長

壹、前言

海軍水面艦作戰的基本上單位通常分為特遣分隊（task element，TE；單艦）、特遣區隊（task unit，TU；3 艘軍艦）、特遣支隊（task group，TG；4-10 艘或至少包含兩個區隊以上）、航空母艦特遣支隊（含航空母艦的支隊）及特遣部隊（task force，TF；包含 2-5 支隊）、艦隊（包含若干特遣部隊）。就現代海戰需求而言，支隊層級的海軍作戰編組已成為海軍作戰的基本單位。這也如同陸軍的聯兵營，陸上作戰的基本單位的概念原則相同。

然就電子戰而言，任何軍種或聯合作戰在電子戰中所涵蓋的戰略、戰術及技術部分，基本上脫離不了電子支援措施（ESM）、電子反制措施（ECM）及電子防護或反制措施（EPM 或 ECCM）三個面向，然這三個面向必須根植於電磁頻譜的運用與管理。所以，在作戰計畫中有關電子戰任務計畫的擬定、運用與修訂，都必須在艦隊出港遂行任務前，對所有納編任務艦艇之電磁裝備執行性能與效能檢查與分析。

因此，本論文目的係以海軍艦隊支隊級作戰任務為假設，從艦隊支隊級作戰各類型作戰威脅分析、電磁裝備性能、電子戰裝備技術能力及電子戰威脅場景想定分析等要項，做為電子戰任務計畫作為與戰術運用概念為研究目標之途徑，並對海軍艦隊支隊級作戰有關電子戰作業部分提供建議。

貳、支隊電子戰計畫作為要項

海軍作戰的海軍特遣任務支隊的名稱中所謂「特遣」（task），就海軍專業用語而言，所指的可能是「攻擊」（attack）、「護航」（escort）、「封鎖」（blockade）等，因不同任務需求納編達成任所需的專業艦艇。例如海軍「攻擊」任務支隊（attack task group）的艦隊編組，若是採取攻勢防禦作為，通常納編具有遠程打擊能力的艦艇為主；反之採取守勢的近岸防禦作為時，通常艦隊編組以小型飛彈艦艇為主，再納編1-2艘中型作戰艦擔任任務指揮艦。故海軍攻擊任務支隊的主要作戰目標，通常是敵人的水面艦艇（作戰艦、登陸艦或高價值商（貨）船）。

而海軍「護航」任務支隊（escort task group）的艦隊編組，其任務通常為負責兩棲登陸艦艇或高價值的商、貨船航行期間的護航任務，確保這些受令被護航的船隻，從出港到抵達目的地的海上航行全程，免遭受敵人空中、水下及水面的攻擊，或將損失減至最低以使被護航的船隻能順利抵達目的地，順利完成其任務。就現代海戰而言，海軍「護航」任務支隊作戰的主要威脅來自於空中的戰機與飛彈與水下的潛艦，其次才是水面作戰艦艇。故海軍「護航」任務支隊納編的艦艇原則上須具備區域防空、反潛，抑或兩者兼具作戰能力的作戰艦，而反水面作戰所需的反艦飛彈裝置通常是中、大型水面艦的基本配備。

面對中共當前對我國可能的軍事威脅，就台灣四面環海的地理位置，以及缺乏能源與國防所需資源，以及中共海、空軍軍事能力已超越第一島鏈的現實情況下，中共對台採取海、空封鎖的軍事行動無可避免的將是海軍優先考量的問題。因此，從台灣安全的優先選項的考量上，編組海軍護航任務支隊將是確保台灣海上交通運輸線安全的重要憑藉。

就海軍護航任務支隊指揮架構編組而言，支隊指揮官進駐旗艦擔任戰術指揮官（Officer in Tactical Command，OTC），並指定具有區域防空作戰能力的作戰艦艦長擔任支隊防空作戰指揮官（anti-air warfare commander，AAWC），並兼任特遣部隊內支隊的防空作戰協調官（anti-air warfare coordinator，AAWC），具有中遠程反潛監偵能力（配備拖曳式聲納）的作戰艦艇擔任反潛作戰指揮官（anti-submarine warfare commander，ASWC），具有遠程反艦飛彈的作戰艦艦長擔任反水面作戰指揮官（anti-surface warfare commander，ASUW），[1]以及配備有較佳電子監偵裝備的作戰艦艦長擔任電子戰協調官（electronic warfare coordinator，Group EWC）。

支隊電子戰協調官之所以不是指揮官的主要因素在於，電子戰操作的核心要件在於調和支隊情資獲得的需求與隱密之間取得平衡。過多或長期間開啟搜索雷達監偵與建立海、空情資，不僅會暴露支隊的行蹤，亦可能發生戰場電子參數資料外洩的情況。例如，海軍護航任務支隊在無法獲得外部（作戰中心、岸置雷達站或友軍）提供支隊作戰半徑 200 海浬半徑範圍內的海、空情資時，支隊即必須運用所屬作戰艦的中、遠程搜索雷達執行空中與水面目標偵搜，以提供支隊早期預警需求。此時，可能發生防空作戰指揮官提出開啟遠程搜索雷達，以獲取防空作戰早期預警的需求。然對反水面作戰指揮官而言，則希望遠程搜索雷達盡可能有限度地開啟，以避免過早暴露支隊位置，影響反水面作戰遂行。

因此，支隊電子戰協調官在支隊出港遂行海上護航任務前，必須完成下列工作事項：

一、統計支隊所有艦艇電磁輻射裝備，如搜索雷達、射控雷達、紅外線裝備、雷射裝備、無線電通信裝備等。

二、依據支隊所有電磁輻射裝備特性，建立支隊電磁頻譜。

[1] 美國及北約所定義的「反水面作戰」即中華民國海軍所稱的「水面作戰」。

三、由於作戰艦電磁輻射裝備具備同質性（同一批裝備），故為避免電磁輻射裝備在運用時，發生相互干擾的情況，須明確電磁輻射裝備頻率使用計畫，並要求支隊各艦確依頻率使用計畫所規定，設定各艦電磁輻射裝備運用頻率。例如，1 號作戰艦遠程搜索雷達使用 1 號頻率，在執行電子反反制操作時使用 2 號功能；2 號作戰艦遠程搜索雷達使用 3 號頻率，在執行電子反反制操作時使用 5 號功能。

四、建立電磁波發射政策（ENCOM Policy），依據任務所處地作戰環境律定電磁波發射政策。例如航經不友善區域的島礁地區，遭受飛彈快艇威脅的等級較高時，支隊中、近程搜索雷達即須增加開啟時間，提高小型目標偵獲率。

五、建立電磁波發射管制計畫（ENCOM Plan），依據作戰需求將支隊電磁波發射管制作為預劃成 5 個等級。

六、依據上級頒發的電子參數情資，建立威脅信號參考資料表，並將相關電子參數設定在各艦電子戰裝備資料庫之中，以提高反飛彈作為的成功率。

七、對威脅支隊任務達成之目標載台，建立目標訊號參考資料表，以增加早期預警能力。

八、律定電子支援措施任務。電子監偵當值艦除監偵不明電子訊號外，亦需擔負監察支隊各艦是否依據戰術指揮官所發布的電磁波發射管制計畫，確實使用與管理電磁波發射裝備。

九、建立搜索雷達發射時間計劃表。律定搜索雷達採取不規則、間斷性的電磁波發射執行海、空目標搜索之目的，在提高支隊海、空情資獲得需求的情況下，亦可達到隱密與擾亂敵人艦隊對我支隊的有效掌握。

十、律定干擾器任務與使用原則，以及律定各艦運用干擾絲與誘標

的權責。

上述要項為支隊電子戰協調官於遂行任務前，必須完成的基本工作。並於支隊在海上執行任務期間，電子戰協調官仍必須依當時戰場電磁環境狀況，適時調整計畫內容，以支援支隊遂行任務需求。

參、支隊電子戰戰術運用概念

海軍護航任務支隊在執行高價值單位時，會依據計畫航線所經過的地理環境不同，支隊所面臨的防空、反潛與反水面作戰優先順序，也會有所不同。例如在禁航區外的國際航道航行期間，護航的船團所面臨的最優先的威脅就是潛艦。因為當兩方國家進入交戰狀態時，依據《戰爭法》與《聯合國海洋法公約》，在不影響第三國的海洋權益下，對於敵方艦船採取軍事攻擊行動是合適的。然在公海實施潛艦封鎖其難度亦非常高，即使是核子動力潛艦亦有其困難性。主要因素在於現代艦船的經濟速率最高可達 17 節的速率，即使高價值船團的經濟速率為 15 節，不管是傳統或核子動力潛艦，在就攻擊位置時都將面臨採取高速戰術運動時，潛艦俥葉與輔機系統噪音的過大而暴露行蹤，反而提供護航任務支隊反潛作戰早期預警情資，進而採取反潛制壓與指導船團採取遠離潛艦威脅區與反制措施（如採取之航等作為）。

對於海軍護航任務支隊而言，反潛作戰相對於防空與反水面作戰的威脅等級，它是一個緩慢且長時的作戰行動。另就水面以上的威脅而言，自二戰以來空中威脅始終高於水面威脅。換言之，海軍護航任務支隊最優先考慮的作戰型態就是防空作戰，尤其是沒有航空支隊可提供空中掩護的狀況下，防空作戰對於護航任務支隊將是一個嚴峻的挑戰。因此，支隊電子戰運用對防空作戰將扮演關鍵的角色。下面將從空中威脅型態與支隊電子戰戰術運用作為兩個面

向，分析支隊電子戰戰術運用概念。

一、空中威脅型態

由於空射攻船飛彈的發展，艦隊防空作戰已看不到飛機臨空作戰的戰場景象，而是面對空中戰機在超視距外即已採取攻船飛彈發射攻擊。1982 年發生「英阿福克蘭群島戰爭」可說是現代化海戰的典範，尤其是英國雪菲爾號驅逐艦，被阿根廷由本土起飛攜帶飛魚飛彈的兩架法製超級軍旗戰機所擊沉，已被視為海軍防空作戰的經典案例。

從英國雪菲爾號驅逐艦被阿根廷超級軍旗機所發射的飛魚飛彈所擊沉的過程中，可以獲得以下經驗教訓：

（一）阿根廷空軍對英國海軍艦隊的攻擊計畫中，並未明確針對英國兩棲登陸艦或運輸艦等後勤艦艇，而是隨機的目標。主要因素在於阿根廷無法有效掌握英國海軍艦隊的情資，對於英國所宣布的禁航區內的海上目標，基本上都應是英國的海軍艦船。

（二）阿根廷海軍也配備有與英國相同的對空搜索雷達，阿根廷瞭解英國驅逐艦對空搜索雷達的偵測死角，並在地球曲線天然限制的掩護下，採超低空（約 30 公尺高度）飛行接近英國船團。

（三）當英國雪菲爾號驅逐艦的對空搜索雷達在 50 海浬，發現不明目標並於第二次掃描搜索後消失，雪菲爾號雷達操作手將此部雷達迴跡誤判雷達雜訊，不予理會且未報告。就阿根廷戰機而言，此時是運用雷達預警器功能，經由爬升戰機飛行高度以測試英國對空搜索雷達的偵蒐死角，並於截收英國對空雷達預警信號時，即下降飛行高度持續向英國艦隊接近。

（四）當阿根廷戰機預判英國船團準備進入其飛魚飛彈最大射程範圍時，即爬升至飛彈發射高度（約 150 公尺），開啟戰機搜索／射控雷達實施海上目標搜索與標定。此時英國海軍艦隊方確認不明空中目標接近，立即發布艦隊防空一級備戰的命令。

（五）阿根廷兩架戰機於完成兩次雷達目標搜索及目標標定後，即對雪菲爾號各發射一枚飛魚飛彈。與此同時英國雪菲爾號驅逐艦電戰系統，對於截收的阿根廷的超級軍旗機搜索／射控雷達信號識別為友軍。

（六）當阿根廷的飛魚飛彈接近雪菲爾號驅逐艦 5 海里範圍時，飛魚飛彈主動尋標器即開啟，進入搜索、導引、歸向攻擊程序。而此時英國雪菲爾號驅逐艦的電戰系統亦將法製飛魚飛彈尋標器信號視為友軍，因而電戰系統對於持續高速接近的飛魚飛彈不採取電子式電子反制措施，以及發射機械式電子反制措施的誘標與干擾彈，使得阿根廷發射的飛魚飛彈成功的擊中英國雪菲爾號驅逐艦，進而導致軍艦沉沒。[2]

依據上述經驗教訓可以瞭解，英國雪菲爾號驅逐艦被擊沉，大部分的因素在於人為因素，一部分在於未做好電磁波頻譜管理（electromagnetic spectrum management，EMSM），以及電磁波發射管制計畫。此案例凸顯海軍護航任務支隊電子戰戰術運用對支隊防空作戰的成敗具有決定性的影響作用。

二、支隊電子戰戰術運用

海軍特遣任務支隊於海上航行期間，除了航行範圍距離敵人沿岸 100 海浬以內，可能遭受敵人岸置攻船飛彈攻擊，以及在兩棲登

[2] 軍艦在反飛彈防禦作為期間，電子反制措施對於飛彈尋標器干擾係由系統自動控制，並配合干擾誘標的使用，實施系統性反飛彈作為。主要因素在於攻船飛彈從尋標器開啟到擊中目標的飛行時間僅 10 餘秒鐘。

陸區沿岸，可能遭受敵空中戰機由內陸低空接近實施臨空炸射外，支隊水面以上的威脅主要仍是以遭受空中戰機發射的攻船飛彈為優先考量因素。

因此，敵戰機對我支隊採取空中攻船飛彈攻擊的作為，首先必須先掌握我支隊位置情報。而此情報可透過間諜衛星的偵照或遠程空中偵察機（含遠程無人偵察機）獲得，由於時間差與座標轉換等的誤差過大因素，無法做為導引攻船飛彈攻擊的參數資料設定之用，即勉強使用其命中率非常低是可以預判的，除非另有戰略或戰術運用需求，而不在於強調飛彈的命中率。

當敵方獲得海軍護航任務支隊與船團的初始位置情報後，即會派遣空中預警機與電子偵察機，對海軍護航任務支隊及船團實施進一步的位置定位。此期間敵方空中預警機、電偵機與地面站台或海軍特遣任務支隊之間的情報傳遞，通常使用的通信頻段為 SHF、UHF 及 HF 三種，實施語音或數據資料的指揮管制與情報傳遞。而在資料鏈路系統部分，則使用電子戰的 C 波段（通信波段為 UHF）頻率。因此，對海軍護航任務支隊而言，SHF、UHF 及 HF 通信頻段的信號截收，成為支隊防空作戰獲取早期預警的重要手段之一。

海軍護航任務支隊在評估當前海域以空中威脅為優先考量時，支隊電磁波發射管制措施應做調整，也就是支隊適度開放搜索雷達的發射管制措施，以期增加支隊空中監偵能力，有效提高早期預警能力。換言之，此時對於威脅的評估應該是空中威脅情資的獲得優先於支隊與船團的隱密作為。

當海軍護航支隊發現友軍電磁波信號以外的 I 波段信號時，支隊防空作戰指揮官應將此電子訊號視同敵方攻船飛彈來襲的威脅，發布支隊防空一級備戰，開放各艦實施干擾誘標與干擾彈的發射權。同時將近迫武器擺置全自動模式，並要求各艦間距不得低於 5 海浬（因近迫武器系統最大射程一般在 10,000 碼），以避免發生誤擊狀

況。

若海軍護航任務支隊獲得岸置空中兵力支援，遂行海空聯合防空作戰時，支隊必須明確規劃戰機交戰區、區域防空飛彈交戰扇區、空中安全走廊及空中安全區，其主要目的在於避免誤擊空中的友軍。

肆、結語

依據上述海軍支隊級作戰電子戰作為需求，可以瞭解到電磁波頻譜的規劃與運用是一切電子戰的基礎，不僅限於海軍，陸、空軍同樣面臨一樣的問題。支隊層級電子戰戰術的運用除了人為作業必須嚴密外，裝備的性能亦是影響支隊電子戰成敗的核心因素。不可否認大部分國家的海軍艦隊電子戰裝備基本上屬於防禦性的電子戰裝備，裝備操作頻率範圍通常在 D 波段到 J 波段之間。無法獲得早期預警所需的 A 到 C 波段，以及 K 波段所需的通信系統監偵頻段，特別是對一支無法獲得友軍空中預警機與戰機支援的海軍護航任務支隊來說，更將面臨非常嚴峻的挑戰。因此，海軍電子戰裝備應朝向通信頻段接收與干擾方向發展，以提升支隊層級電子戰支援各類型作戰的效能。

本文作者常漢青為淡江大學國際事務與戰略研究所博士，現為社團法人台灣戰略研究學會秘書長。主要研究領域為：國際關係、印太區域安全、美中台關係、戰略理論研究、海權、國家安全戰略、海洋安全戰略、國防戰略、軍事戰略、兵棋推演、中共軍事研究。

Electronic Warfare Program and Tactical Application Concept of Naval Fleet Group Level Operation

Han-Ching, Chang

Secretary General

Taiwan Strategic Research Institute

Abstract

In recent years, with the development of missile weapon systems, surface combat ships over the 2,000-ton frigate level have the capability to conduct cross-sea long-distance strikes. As a result, the naval task group has become the basic combat unit of the Navy, just as the Army Joint Battalion has become the basic combat unit of land operations. The word "task" in the naval term naval task group, may refer to "attack", "escort", "blockade", etc., based on different mission requirements of the task.

In terms of the formation of a task combat group, the main purpose of appointing the captain of a sub-component group as the electronic warfare coordination officer is to reconcile the group's intelligence acquisition needs with secrecy. Excessive or prolonged radar surveillance and the collection of naval and air intelligence may not only expose the location of the group but may also lead to the leakage of electronic parameter data on the battlefield. Therefore, the group electronic warfare coordinator plays a key coordinating role in the operations of the task group. Through spectrum management, the formulation of electromagnetic emission control policies and the formulation of electromagnetic emission control plans, the ability of a naval task combat group to effectively operate covertly and obtain early warning intelligence is ensured.

Keywords: Naval Task Combat Group, Electromagnetic Spectrum Management, EMCOM police, EMCOM plan

岸置攻船飛彈部隊電子防護作為之探析

江炘杓

國防戰略與資源研究所

壹、前言

一般而言，岸置攻船飛彈部隊（Coastal Anti-Ship Missiles Force，CASMF）的對海打擊能力頗具威嚇力，惟其電子戰（electronic warfare，EW）及防空作戰能力可能非常有限，大多僅及於目標搜索；若裝備本身具備一定程度抗干擾能力，還可以遂行基本的部隊電子戰，不過電子支援（electronic support，ES）、電子反制（electronic countermeasures，ECM）和電子反反制（electronic counter-countermeasures，ECCM）措施往往都必須依賴電子戰部隊提供支援與保障。

建立岸置攻船飛彈部隊的電子防護（electronic protection，EP）能力主要有四個途徑：第一，飛彈部隊應全面機動化，首先確保自身無被摧毀之虞，始能立於不敗之地；第二，飛彈部隊的搜索雷達應具備抗干擾能力，不被遮沒和干擾，始能精準掌握目標；第三，飛彈部隊需要友軍（防空飛彈部隊和電子戰部隊）掩護，始能發揮殲敵效果；第四，攻船飛彈應具較強的抗干擾能力，始能於巡弋（cruising）和歸向（homing）階段準確尋獲目標並有效攻擊。

岸置攻船飛彈部隊必須具備電子防護能力，首先確保自身安全，於作戰初期不被敵電子攻擊（electronic attack，EA）壓制，始有機會發揮「以陸制海」的作戰效益。因此本文以岸置攻船飛彈部隊的電子防護能力為析論焦點。首先說明飛彈部隊相關電子戰基本作法，接著分析機載（空中）電子攻擊能力對飛彈部隊可能構成的威脅，並指出現階段飛彈部隊電子防護能力的不足，最後探討強化飛彈部隊電子防護能力的具體對策。

貳、岸置飛彈部隊相關電子戰基本作法

電子戰裝備（EW Equipment）具有偵測、分析、定位、干擾、反制與反反制電磁波（electromagnetic waves，EM Waves）信號的能力，它由電子支援、電子攻擊和電子防護組成。理論上，一個軍團級的部隊應該建置基本的電子防護能力，但因各國軍隊資源配置不同，具備執行電子戰的條件與能力並不相同。有的擁有專屬的電子戰部隊，有的只能採取部隊電子戰，更多的連基本的電子防護條件都相當欠缺，因此只能依賴友軍的支援協助。

一、電子支援

電子支援是根據上級指揮官的作戰指導與命令，執行偵測、攔截、識別、追蹤電磁波來源，識別電磁環境（electromagnetic environment，EME）威脅，搜集包括電子情報（electronic intelligence，ELINT）、通信情報（communication intelligence，COMINT）等信號情報（signal intelligence，SIGINT）在內的電子戰資訊，[1]為攻船飛彈部隊提供可靠的電磁波資訊，提供部隊採取電子防護措施，或在具備反制的條件與能力下，對敵電子攻擊採取反制手段，確保攻船飛彈部隊通信、雷達及飛彈系統正常操作。

二、電子攻擊

敵電子戰部隊對岸置攻船飛彈部隊採取電子攻擊的目的是為了削弱、消除或摧毀飛彈部隊的作戰能力。[2]其手段包括干擾通信和雷達信號、採取電子欺騙（偽冒）以及使用雷射和無線電射頻（radio frequency，RF）武器組合的反制措施，[3]足以干擾飛彈部隊的指揮管制（command and control，C2）系統，使其失去目標獲得（target

[1] Purabi Sharma, Kandarpa K. Sarma, and Nikos E. Mastorakis, “Artificial Intelligence Aided Electronic Warfare Systems- Recent Trends and Evolving Applications,” *IEEE Access*, Vol. 8, 2020, p. 224762.

[2] “Electronic Warfare (EW) Operations,” *The Lightning Press*, https://www.thelightningpress.com/electronic-warfare-ew-operations/.

[3] “Electronic Warfare: Bring the Storm,” *BAE Systems*, https://www.baesystems.com/en/productfamily/electronic-warfare.

acquisition）和目標攻擊（targeted attack）能力。有些不被視為「電子攻擊」的手段，包括人為破壞在內，對飛彈部隊同樣具有毀傷作用。因此，對於飛彈部隊的威脅考量，不應局限於電子攻擊。

三、電子防護

岸置攻船飛彈部隊的電子防護涉及為了保護人員、設施及裝備不受電磁波頻譜（electromagnetic spectrum，EMS）的任何影響而採取的行動，[4]包括調變雷達的脈波來復率（pulse repetition frequency，PRF）或提高無線電的頻率捷變（frequency agility，FA），將衰減、抵消或破壞飛彈部隊作戰能力的不利影響降到最低。攻船飛彈部隊可採無線電反制和干擾絲以及在光電／紅外線（electro-optical/infrared，EO/IR）遂行反制，[5]保護人員、設施和設備。有效的電子防護作為可確保飛彈部隊作戰能力不至於下降、失效或遭到破壞。

參、電子攻擊對岸置飛彈部隊的威脅

電子攻擊可區分為軟殺和硬殺（soft-kill and hard-kill，SK/HK）。電子干擾屬軟殺範疇，它可以針對岸置攻船飛彈部隊的搜索雷達、通信系統和飛彈進行反制，使其失去正常的工作能力。光電等導能武器與高速反輻射飛彈（high-speed anti-radiation missile，HARM）則打擊電磁波輻射源，包括雷達站、機動雷達車（簡稱「機雷車」）、機動飛彈車（簡稱「機彈車」）、無線電台及干擾機（jammer），它是一種實體摧毀（physical destruction）的硬殺手段。[6]

除了導能武器、反輻射飛彈和人力破壞之外，機載電子戰系統

---

[4] Chairman of the Chiefs of Staff, *Electronic Warfare, JP 3-13.1* (Washington D.C.: Joint Doctrine Publications Office, February 8, 2012), pp. viii, I-5, I-6 and GL-8.

[5] Massimo Annulli, "Defensive Electronic Attack," *Emsopedia*, https://www.emsopedia.org/entries/defensive-electronic-attack/.

[6] Maxwell Goldstein, "Electronic Warfare 101: Understanding the Basics and Applications," *Grey Dynamics*, April 6, 2023, https://greydynamics.com/electronic-warfare-101-understanding-the-basics-and-applications/.

（airborne EW system）是岸置攻船飛彈部隊的最大威脅，它可對截收的電磁波信號與其資料庫進行比對，鑑別威脅信號的特徵，然後自動採取一套預設的電子干擾手段。特別是加入人工智慧（artificial intelligence，AI）的應用後，機載電子戰系統可以即時判斷目標輻射源的弱點，找出最有效的干擾方法。[7]因此必須體悟不論是電子干擾或實體殺傷手段，都會給岸置攻船飛彈部隊帶來莫大的威脅。

電子攻擊主要係通過拒止、衰減、干擾、欺騙和摧毀等手段防止或減少敵人對電磁波頻譜的使用，以達到進攻或防禦的目的。[8]不論是進攻性或防禦性電子攻擊，電子反制和電磁欺騙措施都是主要的手段；電磁欺騙措施區分為操縱性電子欺騙（manipulative electronic deception，MED）、模擬性電子欺騙（simulative electronic deception，SED）以及模仿性電子欺騙（imitative electronic deception，IED）三種模式。[9]因此，岸置攻船飛彈部隊必須深入理解可能遭受的威脅態樣，才能據以採取合適的因應對策。可能的電子攻擊模式臚列如下：[10]

- 干擾雷達或指揮管制系統。
- 以反輻射飛彈攻擊防空系統。
- 以電子欺騙手段迷惑情報監偵系統。
- 採用自推式、縴引式或固定式誘標。
- 使用消耗性保護或強制保護的誘標干擾系統（火焰彈或主動誘標）。
- 運用導能武器或紅外線干擾系統。

---

[7] John Keller, “Air Force eyes artificial intelligence (AI) and machine learning for cognitive electronic warfare (EW),” *Military + Aerospace Electronics*, September 14, 2021, https://www.militaryaerospace. com/computers/article/14210232/artificial-intelligence-ai-machine-learning-electronic-warfare-ew.

[8] Electromagnetic Warfare Divisions, *Electromagnetic Warfare and Electromagnetic Spectrum Operations, AFDP 3-51* (Montgomery, AL: Curtis E. Lemay Center, July 30, 2019), p. 20.

[9] *Operational Terms and Graphics, FM 1-02; MCRP 5-12A* (Washington DC: Headquarters Department of the Army, September 21, 2004), p. 1-68.

[10] Army Publishing Directorate, *Electronic Warfare Techniques, ATP 3-12.3* (Pentagon, Arlington, Virginia: Headquarter, Department of Army, July 2019), p. 6-1.

上述電子攻擊的模式既有軟殺手段，也有硬殺作為。就軟殺手段而言，最為平常的手段就是電磁干擾，主要方式是刻意使電磁波輻射、再輻射或電磁波反射，防止或減少敵人有效利用電磁頻譜，並降低（degrading）其性能或癱瘓（neutralizing）敵人的戰鬥力。電磁干擾的技術模式至少有六種，雖然是技術性的能力，電磁干擾所帶來的威脅，仍應引起岸置攻船飛彈部隊的足夠重視。有關電磁干擾的技術資訊如表 1：

表 1、電磁波干擾的技術模式、方法與目的

模　　式	方　　法	目　　的
旁立式干擾（standoff jamming，又稱「遠距離干擾」）	藉由破壞或降低在EMS運作的威脅命令和控制系統以及偵測器來支援操作。旁立式干擾是在一個固定和受保護的位置進行。需要大功率和大天線，干擾才能深入到敵方行動的區域；也需要有關威脅頻率和接收器位置的精確情報。	提供部隊行動最大程度的保護，使其免受威脅；為部隊行動創造有利的機會。
伴隨式干擾（escort jamming）	屬防禦性電子戰，伴隨式干擾不需要大型天線和高發射功率，但需要對方相關頻率的精確情報。	可以支援友軍，保護機動部隊免於受到射頻武器系統的攻擊。
點頻干擾（spot jamming）	干擾一個特定的頻率，它是EA干擾最小的形式，不會干擾非目標頻率。需要特定的電子威脅特徵，才能成功計畫和執行點頻干擾，其發射功率較高。	保護自身免於對方射頻武器搜索、追蹤與鎖定。
掃頻干擾（sweep jamming）	電子威脅的特徵是一個頻率範圍，而非特定頻率時，可採掃頻干擾；以預定速率掃描已知的頻率範圍，干擾EMS的指定頻段，需要較高的發射功率。	保護自身或支援友軍免於對方射頻武器搜索、追蹤與鎖定。
抑制干擾（barrage jamming，又稱「阻塞干擾」）	若對手合併跳頻，在單一傳輸過程的不同時間使用兩個或兩個以上頻率，可採抑制或掃頻干擾技術。抑制干擾是同時干擾EMS指定頻段內的所有頻率。對每個抑制頻率的功率要求較少，因為功率已擴展到整個目標頻率範圍。與掃頻干擾或頻	可以一次抑制多個頻率。

	點干擾技術相比，抑制干擾通常要求EW的設備更接近目標的接收機。	
跟蹤干擾（follower jamming）	可在系統檢測到威脅時自動瞄準接收機，屬無源干擾，直到發射機發射信號。跟蹤干擾可使用點頻、抑制和掃頻干擾技術。EW人員須編製電子威脅特徵，確定威脅者使用的頻率，並確保適當的設備配置，以干擾指定的頻率。跟蹤干擾也會干擾威脅者的跳頻接收機，由於設備並不總是處於發射狀態，跟蹤干擾技術允許干擾機針對目標採取最大程度干擾，並將威脅感知及定位能力降至最低。	可攻擊特定頻率。

資料來源：Army Publishing Directorate, *Electronic Warfare Techniques, ATP 3-12.3*, pp. 6-8～6-10.

肆、岸置飛彈部隊需要加強防護能力

岸置攻船飛彈部隊可以藉由提高機動性能；採取防禦性電子攻擊措施；加強裝備的物理安全、通信安全和系統技術能力；提升飛彈抗干擾能力；以及藉助於友軍提供保護傘等五個方面來強化岸置攻船飛彈部隊的整體防護能力。

一、提高部隊機動性能

岸置攻船飛彈部隊全面機動化是提高安全防護和確保持續戰力的根本。機雷車和機彈車通過靈活的機動性，有利提高部隊存活力，從而對目標形成「存在就是威脅」的嚇阻作用。但發揮「以陸制海」目的的前提是擁有良好的電子防護能力，因此必須加強搜索雷達及通信系統的抗干擾和自動跳頻能力，為其確保完整的目標獲得與指揮管制能力，方能有效遂行目標打擊任務。

二、採取防禦性電子攻擊措施

電子攻擊是一種為了減少敵人對電磁波頻譜的有效利用而採取

的行動。[11]此一目的，敵我皆然。因此，岸置攻船飛彈部隊若能具備相當程度的防禦性電子攻擊能力，將更容易發揮打擊效力，並有機會立於不敗之地。岸置攻船飛彈部隊指揮官做好電子防護責無旁貸，應該積極推動部隊實施電子防護訓練，減少電子防護漏洞，提高部隊官兵的電子防護能力。

三、鞏固電子防護三大支柱

電子防護是用來對抗電子戰威脅的技術、設備和行動的總和，它不是部隊保護或自我保護。[12]而是依賴電磁頻譜系統，利用電磁能或物理特性讓自己免於受到敵人電子戰直接、間接或環境的影響，從而使岸置攻船飛彈部隊的雷達和通信系統無礙運作，維持指揮管制順暢。為了保證電子防護的效果，岸置攻船飛彈部隊應強化電子防護三大支柱——物理安全、通信安全、系統技術——的規劃能力。

所謂物理安全指的就是實體安全，包括以武力摧毀干擾源、提高部隊機動性、做好掩蔽和隱蔽作為等；通信安全是維繫指揮與管制能力的根本關鍵，應該強化通信裝備的抗干擾能力，包括運用跳頻技術和使用數位加密通信等；提高系統技術能力的作法有頻率捷變、電磁頻譜管理（electromagnetic spectrum management，EMSM）、電磁波發射管制（emission control，EMCON）、電磁屏蔽（electromagnetic shielding）以及漏洞評估（vulnerability assessment）等。

四、提升飛彈抗干擾能力

攻船飛彈發射後，於巡弋和歸向階段往往會遭到敵對目標採取反制措施，若不具備良好的抗干擾能力，可能導致無效攻擊。可見

[11] *Electronic Warfare Fundamentals* (North Virginia: Nellis AFB, November 2000), p. A-15.
[12] "Electronic Warfare," *Microwaves 101*, https://www.microwaves101.com/encyclopedias/electronic-warfare.

攻船飛彈的抗干擾能力與攻擊的效果密切相關。現代化的飛彈彈頭應該考慮採用多模式尋標器（multi-mode seeker），以強化抗干擾能力，進而提高對目標的毀傷能力；儘管因此不可避免會增加飛彈的生產成本，[13]但卻能夠大幅提高飛彈對水面目標的擊殺效益，其成本效益比（Benefit-Cost Ratio，BCR）甚高，非常值得投資。

五、藉助友軍提供安全防護

由於岸置攻船飛彈部隊本身缺乏足夠的防空能力和電子戰能力，必須藉由友軍部隊提供支援和防護。岸置攻船飛彈部隊的位置應該選擇於防空飛彈（陸基和海基）的保護傘之下，以降低來自空中——戰鬥機、無人機以及電子攻擊——的威脅。此外，岸置攻船飛彈部隊於戰時應獲得編配電子戰分隊以及執行電子戰所需配備，根據可能的電子威脅，為機雷車和機彈車提供可靠的電子戰防護。

伍、結語

分散式殺傷（distributed kill）的概念使美軍有利於其所選定的時間和地點實現制海（sea control）的目標，[14]而所謂「分散式殺傷」的兵力部署，其實就是海軍飛彈快艇（fast attack craft, guided missile，FACG）戰術所經常強調的「分散配置」（distributed deployments）和「分進合擊」（splitting attacks），此既能夠機動以提高自身的安全，也能夠協同攻擊目標（敵艦）的理念，也很適用於岸置機動攻船飛彈部隊。

由於機雷車是目獲的重要憑藉，機彈車則是攻擊的重要手段，指揮車是遂行指揮管制的神經中樞。因此，確保這些車組之間的通信聯繫與安全，是發揮岸置攻船飛彈部隊作戰效益的根本條件。為了發揮「以陸制海」的作用，提高岸置攻船飛彈部隊的安全性變得

[13] Global Data Thematic Intelligence, “Electronic warfare: technology trends,” *Army Technology*, January 6, 2022, https://www.army-technology.com/comment/electronic-warfare-technology-trends/.
[14] T.S. Rowden, *Surface Force Strategy: Return to Sea Control* (Pearl Harbor, HI: Naval Surface Forces, U.S. Pacific Fleet), p. 9.

非常重要，除了維持岸置攻船飛彈部隊的機動性之外，提高其電子防護能力以及得到友軍海、空部隊於機雷車和機彈車 10 浬／18.5 公里半徑範圍內的防空保護，亦須得到更高的重視。電子戰分隊與機雷車和機彈車於承平時期即應針對岸置攻船飛彈部隊和電子戰分隊的個別不足與需求，積極籌補，加強演練，戰時方能夠密切協同，配合無間，共同打贏濱海防衛作戰。

本文作者江炘杓為淡江大學國際事務與戰略研究所博士候選人，現為財團法人國防安全研究院國防戰略與資源研究所助理研究員。主要研究領域為：國際海洋法、武裝衝突法、戰略文化、戰略與政策、新型態作戰、中共軍事。

Analysis of the Electronic Protection Capability of the Coastal Anti-Ship Missile Force

Hsin-Biao, Jiang

Division of Defense Strategy and Resources

Abstract

The lack of an effective electronic protection capability of the Coastal Anti-Ship Missile Force (CASMF) may affect its strike power due to signal jamming by the enemy. Therefore, as a sharp tool for coastal attack, electronic protection capability should be given more importance. CASMF should first understand the basic electronic warfare protection practices related to the characteristics of the force, be fully cognizant of the threat posed by electronic attacks on missile forces so as to understand the inadequacies of its own protection capabilities, and then look for ways to strengthen electronic protection capabilities. Possible measures include improving mobility and utilizing hit-and-run tactics to ensure strike power and increase survivability; improving the electronic protection capability of the force by fully utilizing the capabilities of its own equipment and through friendly support and cover; strengthening physical security, communication security and system technology planning capability to provide electronic protection; improving the anti-jamming capability of missiles to increase the effectiveness of missile attacks. It also provides soft and hard kill security protection through sea-based and land-based air defense forces.

Keywords: Coastal Anti-Ship Missiles Force (CASMF), Electronic Protection, Electronic Attack