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）