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