國防譯粹

NATIONAL DEFENSE DIGEST

◆中華民國一一三年十一月 ◆第五十一卷第十一期 ◆國防部發行

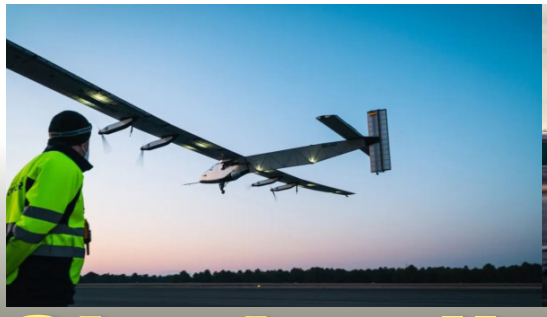
資訊作戰

- 正視影響力科學
- 美軍網路部隊如何應對長期衝突
- 美軍網路資安隱患
- 加速培養網路領導幹部

Enduring Shield 恆久盾牌防空系統

2021年9月24日，Leidos旗下的Dynetics公司與美陸軍簽署價值2億3,738萬美元合約，著手研發恆久盾牌防空系統，全案預劃交付16架發射架與60枚飛彈。本系統為陸基機動武器系統，具備巡弋飛彈與無人飛機反制能力，亦可防護關鍵民間與軍事基礎設施，彌補戰術短程防空系統與戰略武器系統空防間隙。未來，恆久盾牌防空系統亦可交由現行整體空中暨飛彈防禦戰鬥指揮系統(Integrated Air and Missile Defense Battle Command System, IBCS)遂行指管，接收哨兵雷達目標情資，納入陸軍既有整體防空體系。2023年12月22日，Dynetics成功交付第一批發射架。2024年，陸軍接續進行發射架性能測試，而第二批發射架也預於2025年交付。

(Source: Dynetics)



(Source: Skydweller Aero)

Skydweller

天巡者太陽能動力無人飛機

Skydweller Aero公司參考瑞士陽光動力2號(Solar Impulse 2)載人飛機構型，成功開發出天巡者(Skydweller)太陽能動力無人飛機。機身為極輕碳纖維材質，翼展236呎，機身重5,620磅，以太陽能為單一動力，可持續飛行長達一週以上，同時降低操作成本與環境衝擊，達到淨零碳排的永續目標。在作戰效益方面，該機可在現行機場執行起降，搭載800磅酬載進行中高度飛行，機載感測器得以近距離蒐集地面情資。此外，該機亦可執行空中巡邏、海上監視、查緝毒品走私及追蹤野生動物足跡等任務。2024年10月4日，該機在密西西比州史坦尼斯(Stennis)國家機場完成連續22.5小時的飛行測試。

Report
本刊所登載文章皆為譯文，內容不代表本部立場
國防譯粹月刊 NATIONAL DEFENSE DIGEST

資訊作戰是現代戰爭中最重要的元素之一，不僅可影響決策程序，操弄指揮與管制，擴大敵我資訊缺口，也可造成心理衝擊，誤導個人或團體認知資訊，以形塑未來作戰優勢。尤其現今社會發展，各項民生基礎設施或重要軍事機構運作皆已電子及網路化，雖然提供使用者較佳之便利性，亦會使之產生依賴性。因此應研擬資訊作戰適當防禦與反制措施，據以維護國家安全。

參考烏俄戰爭，網路戰部隊亦在資訊作戰中扮演重要角色，然網路戰部隊之兵力結構、組成人員及運用方式，仍有許多討論空間。除了正規網路戰部隊，後備與民間專才也應妥適納入考量，方能提升資訊作戰之攻擊與防禦力。縱然各國持續強化重要基礎設施資安防護，民眾及官兵等「個人」卻仍成為無可避免的資安漏洞，因為利用人性弱點及社交網路系統疏漏，已成為資訊作戰慣常手段之一。為使資訊作戰防禦成效最大化，不僅須著眼於關鍵設施資安防護，亦應完善資安教育及提升「個人」防護措施；另應將相關專業知識與技能納入軍事教育，從基層培育網路與資安專才，同時重新檢討網路管理及專才運用，方能減輕資訊作戰對國家安全造成之危害。

發 行 人：藍靜婷
總 編 輯：吳貞正
副總編輯：吳馥琰、孫弘鑫
主　　編：丁勇仁
副 主 編：黃坤銘、謝榕修
美術指導：張進龍
編輯人員：劉宗翰、黃依歆、林　敏
出 版 者：國防部政務辦公室
地　　址：臺北市中山區北安路409號
電　　話：(02)8509-9545
傳　　真：(02)8509-9547
Email：mndmhd@mail.mil.tw

網　　址：http://www.mnd.gov.tw/Mp/MPPeriodical.aspx?id=2
定　　價：非賣品
著作財產權人：中華民國國防部
創刊日期：中華民國63年1月
發行日期：中華民國113年11月
GPN：2006300041
ISSN：1560-1455

目 錄
CONTENTS

● 作者/Douglas J. Bryant ● 譯者/王建基 ● 審者/丁勇仁

正視影響力科學

Get Serious About the Science of Influence

取材/2024年6月美國海軍學會月刊(*Proceedings*, June/2024)

美國國家安全機關對其影響北京行為，以嚇阻或延遲與中共發生衝突之能力，下了重大賭注。此一賭注──可能是盲目的──有其風險，因為有力證據顯示，外來影響並無法動搖不支持之受眾。雖然影響與說服之科學存在於行銷與廣告領域，但目前還沒有人替國家安全發展出此類科學。

今天，各界並不清楚外國影響力活動是否有效、是否會產生反效果，或者根本不管用。這些問題或許在經過嚴肅之研究計畫後能加以解答。然而，迄今為止，美國在影響力方面並未投注心力，隨著流行心理學的興致隨意行事，希望能有成效，但幾乎從未驗證是否真正產生效果。對於事關重大問題，這樣的做法是不負責任的。

對真理之犀利言論而聞名的美國哲學家羅逖(Richard Rorty)曾說過：「照顧好自由，然後真理就會懂得照顧自己」。[1] 他的意思就是，只有自由，才能提供真理所需的一切保護。羅逖有許多頗具爭議性的觀點，但在今天尤為不受人所喜。諸多關於資訊戰之學術與政府工作，不僅

2020年8月，香港媒體大亨黎智英遭拘捕。在一次以國內為目標之資訊戰行動中，北京查禁黎智英的《蘋果日報》。
(Source: 達志/Reuters)

對錯誤訊息(Misinformation)與假訊息(Disinformation)、外國惡意影響、認知領域操弄或認知作戰的危險提出警告，也提倡媒體識讀(Media Literacy)教育，以加強美國人所謂的認知安全(Cognitive Security)。

對上述各項主張持懷疑態度之研究，大多未被廣為宣傳。雖然各界一致認同俄羅斯、中共及其他國家在國內外受眾中散布假訊息，以掩蓋對自己不利之敘事。然而，針對外國受眾所進行的相關活動是否有效，卻是相當分歧。

各界對於旨在保護美國公民免受外國影響之干預措施(諸如媒體識讀與資訊識讀[Information Literacy]訓練等)，抱持類似的懷疑態度。針對影響力活動效果所做之科學研究，確實是個令人警醒的領域，相關學術論文包括〈建立在錯誤訊息上的錯誤訊息〉、〈避免回音室的回音室效應〉、〈回音室效應被誇大〉，以及〈為何那麼少人分享假新聞？這會損害他們的聲譽〉，以及對該領域本身之若干批判性研究：〈效能研究與效能之欠缺：軍事領域中戰略溝通之運用〉，以及〈對影響力作戰反制措施衝擊性研究之社會科學研究回顧〉。[2]

國際危機組織(International Crisis Group)的歐立克(Olga Oliker)在美國國會就俄羅斯對烏克蘭之影響力作證時，做出極佳的結論：「儘管我們可以確定俄羅斯在這方面投注了大量心力，但最重要的問題是：所投注之心力真的有效嗎？」[3]

美國諸多對手在攻勢「資訊戰」能力(這是個沒有公認定義之詞彙)做了大量投資。[4] 中共光是在外國資訊操弄這方面，

就估計投入數十億美元，而且每年都在增加。[5] 北京運用國有媒體並透過資助外國記者手段，形塑國際對中國大陸之報導。中共利用虛假之YouTube、推特(Twitter)及臉書(Facebook)帳號──此類帳號經常被發現並遭封鎖──製造關於新冠肺炎(Covid-19)、共軍在南海的活動、對維吾爾人禁錮之作為、俄羅斯入侵烏克蘭，以及其他與北京官方敘事不同調之一切議題的假訊息。已知的俄羅斯資訊戰作為，包括其於2016年美國大選期間，利用社群媒體離間美國民眾，並企圖破壞前蘇聯附庸國之顏色革命(Color Revolution)。中共與俄羅斯皆會逮捕、綁架、監禁、攻擊，甚至殺害那些提供不為其所好消息之人士，並使其行蹤不明。[6]

就本質言，資訊戰只是控制資訊取得作戰優勢。「資訊戰」與影響力相關分類一直存在著術語與概念混淆的現象，素來是錯誤與假訊息研究領域中的一個常見批評點。[7] 美國國防部經常更改其與資訊、影響力及相關概念之準則詞彙──不斷修改、刪除、添加，甚至重新使用若干術語。[8]

兩種資訊戰

廣義地說，資訊戰可分為兩類：指管操弄(Command and Control Manipulation)與心理影響。前者是旨在強化並防禦自身指管的同時，也破壞對手之指管──使敵無法獲得資訊，或饋送其錯誤或誤導性數據。此一做法通常是透過電子信跡管制為之──隱藏自身信跡、對其進行偽冒，以及發現、標定敵人信跡位置。這必須重複進行信跡偵測、干擾、反干擾、反反干擾，以及其他作為。網路工具亦可用於防禦、攻擊指管，甚至簡易如停電都可做為相關手段。重要的是，此類資訊戰主要用於戰術層級，不需要對目標之心理或認知有獨特見解。瞭解對手機構的現行決策程序；戰術、技術及程序(Tactics, Techniques and Procedures, TTPs)；以及擊殺鏈──這些過程發生在個人與單位之間，而不會存在於某個人腦中。

另一類資訊戰──心理影響──主要用於戰略、作戰或戰役層級，而且與指管操弄不同的是，該類型依賴對某些個人或團體(例如當地居民、軍事領導人等)之心理與認知資訊。這類資訊戰是當今極為流行的一種手段。

中共、俄羅斯、伊朗及北韓在國內外均進行資訊戰(包含對付自己人)。在這兩個面向，他們都宣傳有利於己之真相與謊言，並限制那些可能對他們造成傷害的內容。這是透過嚴格網路控制，以及對新聞與言論的限制加以達成。俄羅斯拘留《華爾街日報》(*Wall Street Journal*)記者格什科維奇

(Evan Gershkovich)，以及中共拘禁《蘋果日報》創辦人黎智英等，就是兩個例子。北京查禁《蘋果日報》，而該報是香港最後的獨立媒體之一。[9] 根據美國筆會(Pen America)2023年「寫作自由指數」(Freedom to Write Index)，除了記者之外，中共所囚禁之作家比任何其他國家還多。排名其後者為沙烏地阿拉伯、伊朗及越南(均位列第三)；以色列(包括其所占領土)；以及俄羅斯與白俄羅斯(同列第六)。

這些手段儘管成效不彰，國際間也是會加以使用。為影響國際敘事，威權國家轉而採取秘密影響、顛覆及破壞活動。除了社交媒體，還會利用國際法、金錢及政治來形塑敘事──正如他們運用這些方法塑造基於規則的國際秩序使己得利。

在競爭之中，通過社交媒體、國有媒體，以及接受金錢收買之外國媒體操弄新聞的做法大多無效。[10] 雖然此類作為之規模與數量極大，但是成效不彰。中共臉書活動的多數扈從者，實際上是中共擁有或購買之機器人。[11] 危言聳聽者警告，人工智慧生成之新聞與深偽技術很快將與真實新聞無從區分，民眾恐將易遭欺騙，或對自己所能辨別的事實產生懷疑──但同樣也有可能的是，消費者會變得更加懷疑所見所聞、更具辨別力。深偽偵測器(Deep Fake Detector)業已問世。美國之對手，對這些無效影響力之手段投注大量資金，因此吾人是否應將納稅人的錢花在對抗這些手段，確實值得深思。

研究結果

俄羅斯之影響力作戰，對於不信任俄羅斯的美國人或其他群體的態度而言，幾乎毫無影響。[12] 而中共之行動，有時顯得拙劣到可笑。史丹佛大學網路觀察站(Stanford University Internet Observatory)研究人員，在2020年這樣評價北京對新冠病毒疫情之假訊息行動：

> 網路上的帳號很少達到顯著影響力或參與度，而且這些帳號所推廣的諸多敘事，都被發現在過去曾被取締。相關帳號持續缺少人物誌發展相當明顯。從中共傾其所有作戰能力，企圖影響全球受眾對於國家重大事務看法這一角度來看，此一行動顯得特別有趣。尤其在新冠病毒疫情背景下，我們如今已發現一套完整之宣傳戰範圍，其中涵蓋了公開、可追溯的國家媒體，以及隱蔽真實身分的社群媒體

虛假帳號。[13]

在停泊於東京灣之美國海軍密蘇里號(USS *Missouri*)戰鬥艦甲板上舉行受降典禮，就是「心理影響型」(Psychological-Influence-Style)資訊戰的最佳例子。(Source: Naval History and Heritage Command)

四年後，中共的假訊息機構幾無進展。2023年9月，美國國務院全球參與中心(Global Engagement Center)所提出之報告，詳細描述中共是如何擴大其行動範圍，透過資訊操弄、公開與秘密影響、收買記者與平臺、恫嚇，以及發展、使用、出口科技監控與審查技術等手段，控制全球資訊。[14] 然而，關於這些行動之影響，該報告僅警告，「人工智慧科技之最新發展，可能會使中共精確鎖定外國受眾，從而『可能影響』其有利之經濟與安全決策」。(『』強調部分係作者加註)。

在一個知名的無效影響力作戰案例中，俄羅斯行為者利用美國德州之一座清真寺開幕，在臉書上建立相互對立的群體，來招募抗議者與反抗議者。約有10名白人民族主義抗議者，與50至100名反抗議者到場，並隔著街道相互嘶吼。該起事件並無暴力行為。[15] 在另一起由俄羅斯臉書團體所發起的活動中，約有5,000至一萬名抗議者，於2016年11月川普(Donald Trump)當選後，從聯合廣場(Union Square)遊行至川普大廈(Trump Tower)。[16] 評估該起俄羅斯行動之影響力所要考量因素相當複雜，因為遊行是同年11月紐約市的第四次抗議川普活動，也是全美諸多抗議活動的其中一次。

有兩個據稱是假訊息造成有害影響之案例：分別是2021年1月6日對美國國會大廈的襲擊，以及對施打新冠肺炎疫苗產生猶豫的現象。前述例子至少在表面上看起來是合理的，儘管上述案例之證據與論點超出了本文範疇，但衍生出的問題顯示，影響力作戰可能奏效之決定條件，以及多個獨立變數的不同因果貢獻，是相當複雜的。例如，如果2020年總統大選的假訊

在假訊息的推波助瀾下，可能造成嚴重的衝突事件。圖為2021年1月6日，美國國會大廈前支持川普總統的群眾暴動場景。
(Source: 達志/Reuters)

息，確實造成了2021年1月6日攻擊事件，那麼這種影響有多大程度是來自國內假訊息(而不是來自國外假訊息)？同樣地，在評估新冠肺炎錯誤訊息與假訊息之影響時，當人們尋求與自己早已認同的觀點時，對大多數錯誤訊息會產生多大程度影響？

這些與假訊息及動態效應雙重攻擊之潛在後果全無關聯。即便假訊息之價值是短暫的，它在危機或衝突初期的混亂時刻，也可能帶來超乎預期之利益。今天，如果有段深偽影片聲稱，美國總統指出勒索惡意軟體攻擊已造成沿海電網損壞，而在被迅速揭穿之前，其所可能造成的傷害十分有限。但同樣的影片，在真正衝突爆發之際，與造成停電的網路攻擊同時發布，就可能造成極大困惑與混亂──甚至遲滯防禦性與軍事性反應。

雖然美國目前處於競爭之中且盡力設法避免衝突。美國《國家安全戰略》(*National Security Strategy*)這樣描述當今現況：「美國及我方之盟邦與夥伴國即便與中國及俄羅斯處於競爭之中，仍有機會形塑外部環境，從而影響其行為。」[17] 換句話說，《國家安全戰略》很大程度上是一種影響力戰略。因此，吾人應該思考的是，在國家安全領域之中，影響力在何種條件下能發揮作用、效用有多大。

當心理影響力可能奏效時

核嚇阻做為一種影響力戰略是否有效，是個開放式且具爭議性的問題。部分核嚇阻戰略可能有效，而其他可能無效。核嚇阻從未能阻止他國獲得核武。其實，它反而是促使各國追求核武，以嚇阻其敵國，而其中許多已擁有核武。有可能，但很難

證明，核武能夠在與其他擁核國之衝突中，阻止局勢升級超過某個門檻。這可能就是美國在保衛烏克蘭時沒有直接攻擊俄羅斯的一個原因；然而，這個假設只要失敗一次，對所有人來說就會失去效力。

新冠疫情期間，假訊息伴隨陰謀論如病毒般蔓延，致使人們對施打疫苗產生猶豫，進而危害公眾健康。(Source: Shutterstock)

外交關係和談判，可能是影響力作戰與活動之最典型例子。它們至少有時奏效，而且當其奏效時，就能夠產生若干具體且實在之成果，諸如和約與協議──這比大多數資訊戰之心理影響案例更具實效。軍事上的特例，可帶來具體的、心理影響形式的資訊戰結果，就是受降儀式──例如1945年9月2日，日本在東京灣的密蘇里號戰艦甲板上投降。除了澈底消滅外，戰爭──甚至像是第二次世界大戰這樣的戰爭──本質上也是一種影響力活動。

俄羅斯在克里米亞成功使用影響力活動，而該地有大量黑海艦隊官兵及退伍軍人傾向支持俄羅斯敘事──研究者普遍認為，在這類情況下，影響行動可能有效──這顯示出，美國若干特定亞群體可能會受到外國惡意影響的影響。例如，「俄羅斯是我們的朋友」這句口號，就在美國夏綠地(Charlottesville)的白人至上主義者遊行中響徹雲霄。[18] 但是，因為總是有少數美國公民與美軍官兵，可能傾向於相信對手的訊息，就算是錯誤與假訊息干預措施的媒體識讀教育，對他們來說不可能有好處。他們的問題在於價值觀──而不是在於防範惡意訊息。

國家安全的影響力科學

吾人目前對外國惡意心理影響類的資訊戰之理解(包括錯誤與假訊息)，並不足以證明媒體、決策者及民眾每天所表現出的執著與恐懼是合理的。這需要進行更多、更嚴謹的研究來檢驗這些影響及其影響規模。在將資源轉向諸如媒體與資訊

俄羅斯黑海艦隊停泊於克里米亞塞凡堡(Sevastopol)。俄羅斯運用影響力活動並結合退伍軍人支持，強化對當地的敘事掌控。

(Source: 達志/AP)

識讀之類未經證實的概念之前，應先確定中共與俄羅斯的投資及行動是否構成真正威脅。目前，有更多、更確切之證據，支持美國政策制定者應鼓勵俄羅斯與中共增加在無效影響行動上之投資，這樣他們就會有更少資源可用於武器彈藥之觀點。當然，這方面可用投資、時間及經驗加以改變。更令人擔憂的是，心理與動能攻擊結合後可能對美國本土所造成難以預測的影響；然而，這些想定卻鮮少受到注意。

電子戰與網路戰、情報蒐集及反情報，在現代衝突中不僅具有優勢，而且確有其必要。世上或許沒有對照研究可證明其效果，但是依賴上述作為之軍隊，卻知道雷達、干擾機、反干擾機故障及網路防禦不足，會有甚麼後果。

對於錯誤與假訊息行動抱持懷疑態度之研究，未曾顯示這些行動不具任何效果。相反地，此類研究卻顯示相關行動是否有效，或者在何種條件下有效，仍為未知之數。若欲回答這些問題，需要既能檢測效果、又能衡量影響規模之嚴謹對照研究。美國《國家安全戰略》與《國防戰略》(*National Defense Strategy*)指出，美國將利用外國影響力，形塑伊朗、北韓、俄羅斯及中共政府之行為。「影響力」與「認知管理」這兩個流行語，在當今的華府隨處可聞，但國安機關卻還未能展現出對於外國影響力之科學理解，也無意願加以發展。

迄今，為數不多的研究結果顯示，對外國受眾施加心理影響力之效果有限，且成效主要取決於受眾對傳遞者與訊息的既有態度。例如，烏克蘭固然是爭取到了國際的援助與支持，但援助該國者僅限於本來就支持烏克蘭的國家──或至少是反對俄羅斯的國家。

威權政府之國內運作則完全是另一回事。對於生活在中共「防火長城」之內、身處於無所不在監控下的人們來說，中共不僅控制他們所能接觸之資訊，也控制了他們所能散播的資訊。儘管北京主導全球資訊之企圖努力未能得逞，但黨國體制在國內的控制卻異常有效，這著實令人不安。中共國安部部長袁亦鯤(原名袁鵬)是這樣說的：「是真相是謊言已不重要，重要的是誰掌握話語權。」[19] 這或許對於20世紀專制政權下的歷史學家而言並不意外。然而，這表示在開放社會中，維護自由──使話語權民主化──是抵抗外國操弄的最佳防禦手段。羅逖所提「照顧好自由，然後真理就會懂得照顧自己」的意思，換句話說就是「如果人們能無懼地表達自身信念，那麼……他們為自己辯護與追求真理的任務就會合而為一」。[20] 如果美國意欲透過影響力作戰，來形塑俄羅斯與中共之行為，並避免戰爭，就必須認真看待影響力科學，並建立一套嚴謹的研究計畫，並將此一科學應用於國家安全領域。事關重大，任何低於此一標準之做法均將無法承擔後果。

作者簡介

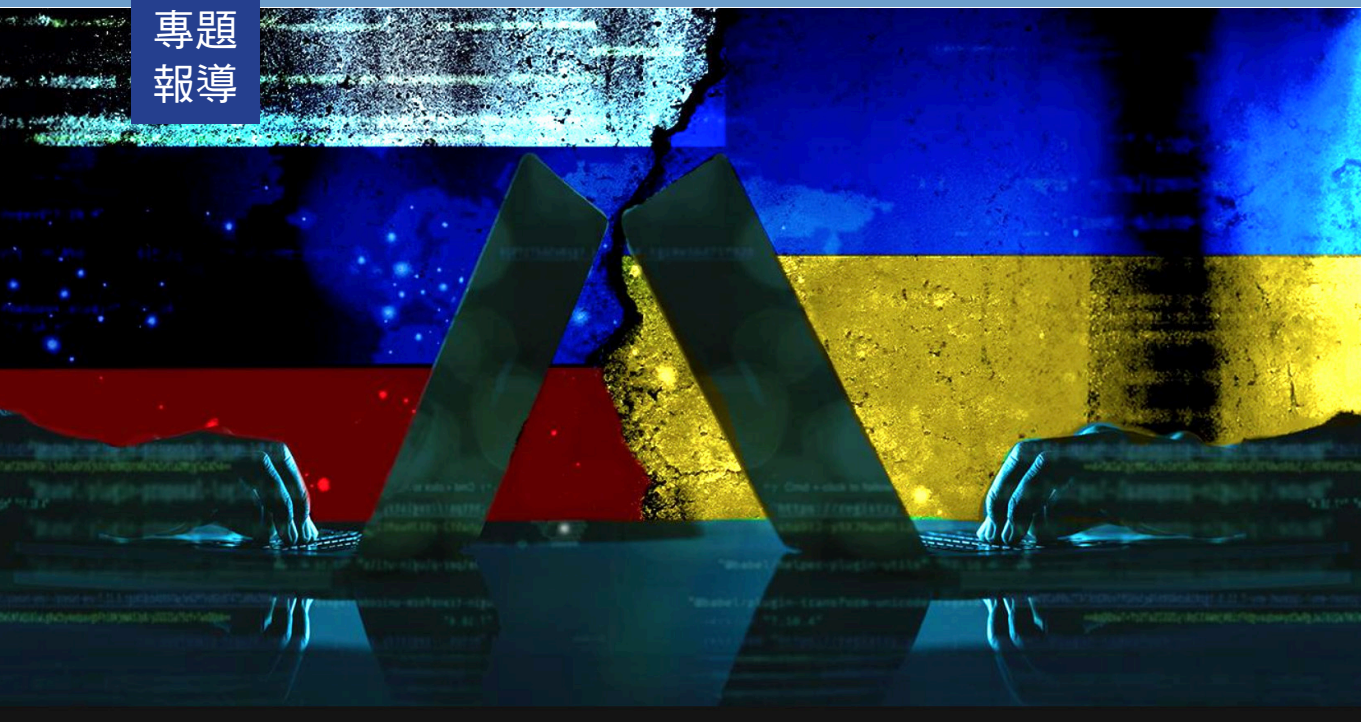
Douglas J. Bryant係社會暨行為科學家，美陸戰隊副司令(主管資訊)之資訊戰效能專家，喬治城大學兼任助理教授，具有心理科學碩士、分子暨神經行為生物學—心理學博士學位。2010年至2014年間，曾擔任美陸軍情報官乙職。

註釋

1. Robert B. Brandom, ed., *Rorty and His Critics* (Malden, MA: Wiley-Blackwell Publishers, 2000), 347.
2. Sacha Altay et al., "Misinformation on Misinformation: Conceptual and Methodological Challenges," *Social Media and Society* 9, no. 1 (January 2023); Andrew Guess et al., "Avoiding the Echo Chamber about Echo Chambers," Knight Foundation 2, no. 1 (2018): 1–25; Elizabeth Dubois et al., "The Echo Chamber Is Overstated: The Moderating Effect of Political Interest and Diverse Media," *Information, Communication & Society* 21, no. 5 (2018): 729–45; Sacha Altay et al., "Why Do So Few People Share Fake News? It Hurts Their Reputation," *New Media & Society* 24, no. 6 (2022): 1303–24; Claes Wallenius and Sofia Nilsson, "A Lack of Effect Studies and of Effects: The Use of Strategic Communication in the Military Domain," *International Journal of Strategic Communication* 13, no. 5 (2019): 404–17; and Laura Courchesne, Julia Ilhardt, and Jacob N. Shapiro, "Review of Social Science Research on the Impact of Countermeasures against Influence Operations," *Harvard Kennedy School Misinformation Review* 2, no. 5 (September 2021).

3. Olga Oliker, “Russian Influence and Unconventional Warfare Operations in the ‘Grey Zone’: Lessons from Ukraine,” Statement before the Senate Armed Services Committee Subcommittee on Emerging Threats and Capabilities (2017).
4. Sarah White, “The Organizational Determinants of Military Doctrine: A History of Army Information Operations,” *Texas National Security Review* 6, no. 1 (Winter 2022/2023): 51–78; and Mark Pomerleau, “Out: ‘Information Warfare.’ In: ‘Information Advantage,’” C4ISRnet, 29 September 2020.
5. U.S. State Department Global Engagement Center, “How the People’s Republic of China Seeks to Reshape the Global Information Environment,” 28 September 2023.
6. Kaela Malig, “How Russia’s Press Freedom Deteriorated over the Decades Since Putin Came to Power,” *PBS Frontline*, 26 September 2023; and Reporters Without Borders, “China,” September 2023.
7. Tim Hwang, “Deconstructing the Disinformation War,” MediaWell, Social Science Research Council (June 2020).
8. White, “The Organizational Determinants of Military Doctrine.”
9. Austin Ramzy and Tiffany May, “Hong Kong Arrests Jimmy Lai, Media Mogul, Under National Security Law,” *The New York Times*, 9 August 2020.
10. Zuri Linetsky, “China Can’t Catch a Break in Asian Public Opinion,” *Foreign Policy*, 28 June 2023.
11. Carly Miller et al., “Sockpuppets Spin COVID Yarns: An Analysis of PRC-attributed June 2020 Twitter Takedown,” Stanford University Freeman Spogli Institute for International Studies (June 2020).
12. Oliker, “Russian Influence and Unconventional Warfare Operations.”
13. Miller et al., “Sockpuppets Spin COVID Yarns.”
14. U.S. State Department Global Engagement Center, “How the People’s Republic of China Seeks to Reshape.”
15. Christopher A. Bail et al., “Assessing the Russian Internet Research Agency’s Impact on the Political Attitudes of American Twitter Users in Late 2017,” *Proceedings of the National Academies of Sciences of the United States of America* 117, no. 1 (September 2019): 243–50.
16. Ali Breland, “Thousands Attend Protest Organized by Russians on Facebook,” *The Hill*, 31 October 2017.
17. Joseph R. Biden, *National Security Strategy of the United States of America* (Washington, DC: The White House, October 2022).
18. David Neiwert, “Explaining ‘You Will Not Replace Us,’ ‘Blood and Soil,’ ‘Russia Is Our Friend,’ and Other Catchphrases from Torch-Bearing Marchers in Charlottesville,” Southern Poverty Law Center, October 2017.
19. Matt Pottinger and Mike Gallagher, “No Substitute for Victory,” *Foreign Affairs* 103, no. 3 (May/June 2024).
20. Brandom, *Rorty and His Critics*, 347.

回目錄→



● 作者/Jason Vogt, Kendrick Kuo, and Dan Grobarcik ● 譯者/洪琬婷 ● 審者/丁勇仁

美軍網路部隊如何應對長期衝突

Preparing the U.S. Cyber Force for Extended Conflict

取材/2024年6月美國海軍學會月刊(*Proceedings*, June/2024)

在未來戰爭中，網路戰是不可或缺的一環。網路戰在其能否扮演舉足輕重角色與其作戰效益未可知的情況下，仍然是輿論激烈爭辯的焦點所在。在過去十年內，美軍網路戰部隊雖已參與無數作戰行動，但尚未對抗科技先進對手，以通過高科技衝突的考驗。這導致美軍聯參缺乏足夠資訊，無法因應多變的網路衝突以完善美軍兵力結構規劃。

烏俄戰爭顯現了與網路戰部隊有關的兵力結構決策必須有所取捨。其作戰節奏轉瞬便超越了網路攻擊的速度；與此同時，這又弱化了訓練精良的網路戰部隊達成戰果的能力。因此，維持此類型網路戰所需資源可能較戰爭初始時期所預判的更多。消耗戰與人海戰術，這些與烏克蘭戰場相關的術語，現在也可能延伸進網路領域當中了。

在衝突的早期階段，俄羅斯為奪取其軍事目標，以精銳網路戰部隊支援作戰部隊執行高強度網路戰。但是，作戰進程消耗了其為數不多的網路滲透資源，網路戰速度也隨之減緩；戰況膠著，俄羅斯能力也逐漸受限。

在入侵初期，俄羅斯癱瘓了烏克蘭數萬名用戶的網路寬頻，並在衝突第一週內發動逾22次網路攻擊。然而數月後，隨著地面戰事陷入膠著，俄軍網路戰部隊持續應付親烏駭客團體的數千次網路攻擊，疲態盡現。（Source: Shutterstock）

相較之下，烏克蘭的網路戰能力在早期階段相對較薄弱，隨著時間進展，大批的志願團體逐漸凝聚力量支持烏克蘭。近期從烏俄戰爭獲致的初步經驗教訓顯示，兵力結構能否平衡可能是網路戰部隊在作戰初期以後保持關鍵能力或漸趨邊緣化之關鍵所在。

烏克蘭網路戰的淬鍊

整體看來，烏俄戰爭下由兩種網路戰模式相互競爭，即俄羅斯精銳部隊與烏克蘭的志願團體。俄羅斯傳統軍事模式為運用菁英所組成的部隊，這些人具備高度專業能力，負責高強度作戰行動，主要隸屬於政府機構，如俄羅斯軍事情報局(GRU)、聯邦安全局(FSB)，以及對外情報局(SVR)。[1]

烏克蘭的情況則相反，烏軍缺乏一支完整訓練的網路戰部隊，並把有限資源集中在整體防禦能力上。自俄羅斯入侵以來，烏克蘭持續培養民間志願者組成大規模網軍，以對俄羅斯實施反擊。這兩種網路戰模式不是涇渭分明，而是各自具備不同的優缺點。隨著戰事推移，這些優缺點逐漸顯現。

在烏俄戰爭爆發前一年，俄軍網路戰部隊大肆增加對烏克蘭和北約會員國的網路釣魚攻擊，重點置於入侵烏克蘭政府機構、國防軍事及關鍵基礎設施的資訊網路。[2] 入侵烏克蘭前夕，俄軍實施大規模網路攻擊，在烏克蘭數百個系統植入惡意程式，並對美國衛訊公司(Viasat)展開阻斷服務(Denial-of-Service, DoS)攻擊，影響了數以千計的歐洲與烏克蘭寬頻用戶。[3] 俄羅斯在發起戰事首週之內便對烏克蘭發動逾22次網路攻擊；此外，在戰事爆發後四個月內，俄軍使用惡意程式攻擊的次數遠較過去八年總和高出許多。[4] 然而，俄軍網路攻擊在

戰爭爆發後兩個月內迅速減少，次數降低到每週僅一至兩次。第五個月後，大型資安服務公司便發現網路攻擊行動頻次變少。[5]

烏俄戰爭中，IT軍團可透過癱瘓網站與入侵電廠，導致大規模停電。圖為烏克蘭赫梅利尼茨基(Khmelnytskyi)核電廠。
(Source: 達志/Reuters)

俄軍網路攻擊減少有幾個可能原因。自2014年以來，烏克蘭自抵禦俄軍網路攻擊積累了大量經驗。此外，西方政府與科技公司的支持強化了烏克蘭的網路防護能力，也減緩了俄羅斯的作戰節奏。戰爭期間，美軍網路司令部(U.S. Cyber Command)發動了「前進追捕行動」(Hunt-forward Operations)，此一攻勢網路作戰或許是協助烏克蘭保護重要網路的關鍵所在。一些大型科技公司(如微軟、Google或美國資安公司麥迪安[Mandiant])也在相當程度上為烏克蘭政府機構和民間網路提供防護。[6] 另外，隨著俄羅斯消耗了其原有的網路滲透資源，作戰部隊節奏便超越了網路戰部隊的腳步。[7]

俄軍精銳網路戰部隊在入侵烏克蘭初期的激烈戰事中可謂準備充分，但隨著戰事膠著且無法奪取烏克蘭首都後，其效益便不再顯著。假使俄軍當時順利突破烏軍防線，觀察家可能會把網路戰之戰果與入侵行動相結合，並視為俄羅斯戰勝的關鍵因素。但實際上俄羅斯的閃電戰卻演變成壕溝戰與陣地保衛戰，網路戰部隊也隨著顯露疲態，難以在烏軍強化後的網域上有所突破。後來，烏俄戰爭持續迄今，其網路作戰規模愈趨簡化且零散。

在俄羅斯網路作戰攻勢轉弱後，親烏志願者組成的網軍增加了攻勢網路行動，迫使俄軍必須應付數千起中斷式(Disruptive)網路攻擊。親烏志願者包括一部分支持烏克蘭的國際駭客團體，例如由國家資助的烏克蘭IT軍團(IT Army of Ukraine)，其在Telegram即時通訊軟體平臺上一度擁有30萬名關注者。[8] 他

們與其他駭客組織活動主要為發起分散式阻斷服務(Distributed Denial-of-Service, DDoS)攻擊，以癱瘓俄羅斯網站，其中包括莫斯科證券交易所和幾家知名銀行。據稱，烏克蘭IT軍團甚至入侵了列寧格勒州(Leningrad Oblast)的一處電廠，導致該州發生大規模停電事件。[9]

儘管上述網路攻擊的影響大多可在政府機構不介入的情況下自行解除，但因此攻擊規模之龐大和眾多國際志願者的參與，仍然讓俄羅斯政府感到頭大，必須權衡究竟應投入多少資源以抵禦親烏駭客組織的攻擊。雖然上述行動無法定調烏俄戰爭勝敗，但仍顯現烏克蘭積極抵抗決心，同時點出俄羅斯民眾無法免於戰爭負面影響的事實。

綜觀歷史，俄羅斯長期依賴駭客團體和無國界駭客組織來推動其任務。2007年針對愛沙尼亞的大規模網路攻擊，以及2008年喬俄戰爭(Russo-Georgian War)中網路攻擊行動顯示，這些團體是俄羅斯網路作戰固定班底；不過，他們在現在的烏俄戰爭中效果似乎有限。[10] 舉例而言，在德國政府宣布提供戰車予烏克蘭之後，與俄羅斯軍事情報局有關的駭客組織XakNet癱瘓了數個德國網站。此外，親俄駭客組織Killnet也針對烏克蘭的盟邦發起一連串的阻斷服務與侵入洩密行動。[11]

目前，儘管私人部門人才的影響力難以量化顯現，烏俄雙方仍高度依賴相關人才。隨著戰爭衝突持續，國內人才庫可能逐漸萎縮，導致網路作戰難以持續。2022年俄羅斯入侵烏克蘭之時，數萬名IT專業人員離開俄羅斯。[12] 人才流失嚴重促使俄羅斯立法免除IT專才的所得稅直至2024年底。[13] 烏克蘭狀況則好得多，其IT產業表現出極高韌性，屬於衝突第一年內為數不多的成長產業之一。[14] 不過，對於前線作戰新兵的需求，可能會阻礙烏克蘭進一步發展其網路戰能力。對IT人才的長期需求，凸顯出網路戰領域同樣也在乎兵力集中的軍事原則。

美軍網路司令部兵力結構啟示

烏俄雙方網路戰成效顯著與否仍然是現行討論話題之一。不過，烏俄戰爭的確是史上首次出現大規模網路作戰的重大衝突，為美國未來可能面臨的挑戰提供了寶貴經驗啟示。美軍聯參必須考量大規模作戰行動所需之網路資源，包括強化部隊網路攻擊能力選項，同時也要防禦針對美國本土的相應威脅。

烏俄戰爭經驗明顯指出，僅依賴精銳網路部隊是不夠的，美軍應考慮

發揮後備人員專長，並在傳統兵力結構之外，凝聚網路戰志願團體的力量。

美軍網路司令部隸屬於美國國防部的功能型作戰司令部，負責聯合網路作戰行動，其成立於2010年，目標在2027年具備約7,000名現役與後備役人員，組成共計147個小隊的網路任務部隊(Cyber Mission Force, CMF)。網路司令部下轄數個指揮部，於各自責任區或任務目的下領導這些部隊，任務目的包括支援美軍作戰行動或保護美國利益不受惡意網路攻擊侵犯等。

從烏俄戰爭汲取的經驗顯示，美軍網路戰部隊應將更多網路防護任務轉移給後備單位，以擴編現役部隊規模，並且同時建立一個新架構可整合志願團體支援能量。 (Source: U.S. Cyber Command)

美軍網路司令部主要藉其現役部隊人員強化攻勢網路作戰能力，培養一位高度專業網路作戰人才約需一至三年，每人所需訓練預算為22萬至55萬美元不等。[15] 有鑑於訓練成本高昂，如強化後備部隊的攻勢網路作戰能力會顯得不切實際，因為後備預算與部隊可受訓的時間都十分有限。因此，美國國防部雖然目前能力足以執行穩定狀態下的任務，但要擴編部隊以因應長期衝突將會困難重重。

將美國網路戰部隊與烏俄兩國相比，其結構更近似於俄羅斯軍事情報局和聯邦安全局所採取的精銳部隊路線。這表示在衝突初期，美軍大致可執行幾次有效的攻勢網路作戰，但隨著對手受到攻擊並強化其網路防禦之後，網路部隊可能會難以跟上作戰節奏。再者，美軍要針對強大對手採取持續攻勢網路作戰將遭遇許多困難，在防禦對本土次數漸增的攻擊方面也可能讓美軍決策者感到捉襟見肘，因他們必須把有限的網路戰資源用在刀口上。

為應對此一需求，美國國防部應採取下列措施：一、擴編美軍網路司令部現役攻勢網路作戰部隊規模，將多數防護性任務交由後備部隊負責；二、正式賦予國民兵防護美國本土關鍵基

軍網路司令部之網路任務部隊成員參加訓練與戰備演習。

(Source: U.S. Cyber Command)

礎設施之責；三、提前規劃並建構基礎設施，以在情況緊急時讓志願者網路團體加入作戰行列。

如能深化後備部隊網路戰防護實力，將可讓美軍網路司令部現役部隊不受限制，進而提供較強攻擊力量。目前，約有半數的網路任務部隊分配到網路戰防護任務，旨在保護國防部龐大的軍事網路，即美國國防部資訊網路(DoDIN)。[16] 然而，在衝突發生時如能迅速動員後備與各軍種人員來防護軍網，網路任務部隊就能更專注於高成本與耗時的網路攻擊行動。

後備部隊包括美陸軍國民兵、美空軍國民兵及各軍種後備役人員，目前已組成33個網路防護小組及3個國家任務小組，每個單位約有1,300至1,500人。[17] 他們在網路事件應變與支援作戰部隊的網路防護任務中累積了許多寶貴經驗。2022至2023年間，美陸軍後備網路防護旅參加了歐洲和太平洋地區舉行之大型演習，並於2023年5月支援戰區素有盛名的陸軍第3多領域特遣部隊(3rd Multi-Domain Task Force)網路防護任務。[18]

美國國防部應可考量賦予國民兵網路戰的關鍵基礎設施防護任務優先地位，讓國民兵針對此一任務目的推動相應訓練、裝備及編制，以支持州和聯邦政府需求。在州政府授權下，國民兵執行網路相關任務，經常應對網路突發事件，並接受動員支持多項網路任務，例如在美國選舉期間監測網路狀態。2019年，國民兵人員有效應對了在五個州發生的勒索軟體攻擊，在2020年針對15個州計33次網路事件實施應變。[19] 在特定情況下，國民兵人員可以同時在州與聯邦政府的雙重動員身分下服役，如此做法將可讓國民兵單位在應對廣泛目標攻擊時更具彈

性。[20]

最後，美國國防部應制定相應政策以動員民間有意願的網路人才。組織動員與協調志願團體可以有不同的方式，但首先應設立專責辦公室，例如國防部網路政策副助理部長辦公室，以研究相應政策並找出法律面可能的障礙。志願團體應與何種軍方層級相互整合，此事尚待討論；例如，烏克蘭IT軍團貌似有核心領導層級可以對軍事與情報機構直接聯繫，並且透過Telegram這類即時通訊軟體平臺協調出一場草根性的公開運動。其他待探索的議題包括民間公司在協調過程中可以發揮何種作用，以及網路公司高層與專家在軍事決策過程的參與程度等。這些議題並不容易處理，但可透過先期討論和提前規劃來做為整體解決方案的一部分。

美國國防部網路戰部隊編成時間未逾十年，此事也讓聯參在討論決策時缺乏可供參考的歷史數據。然而，從烏俄戰爭所汲取經驗顯示，在長期衝突中維持攻勢網路作戰屬於艱鉅的任務，國防部應考量採取可增進網路攻擊能力之選項。

有鑑於相應的時間和成本，當前要擴編後備部隊中具備網路攻擊能力之單位數量實屬困難，但後備部隊具有支援更多網路防護任務能力，從而讓現役部隊更能專注於推動攻勢網路作戰。重新調整各部隊任務分配，將有助於軍事單位對於國家安全貢獻程度的最大化，並有助於降低美軍網路精銳部隊在長期衝突中過度損耗能力的風險。

作者簡介

Jason Vogt自美陸軍退役後曾於美國國防情報局任職，現為美海軍戰院戰略作業研究部門助理教授，其專長為網路戰與兵棋推演。

註釋

1. Andrew S. Bowen, *Russian Cyber Units* (Washington, DC: Congressional Research Service, 2022).
2. Shane Huntley, *Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape*, Google Threat Analysis Group, 16 February 2023, 10–12.
3. Huntley, *Fog of War*, 14.
4. Microsoft Digital Security Unit, *An Overview of Russia's Cyberattack Activity in Ukraine*, Special Report: Ukraine, 27 April 2022, 4.
5. Huntley, *Fog of War*, 15.
6. GEN Paul Nakasone, USA, Posture Statement of General Paul M. Nakasone Commander, United States

Cyber Command Before the 117th Congress Senate Committee on Armed Services April 5, 2022, United States Cyber Command, 5 April 2022; and Microsoft Digital Security Unit, *An Overview of Russia's Cyberattack*, 4.

7. Andy Greenberg "Russia's New Cyberwarfare in Ukraine Is Fast, Dirty, and Relentless," *Wired*, 18 November 2022.
8. Aiden Render-Katolik, "The IT Army of Ukraine," CSIS.org, 15 August 2023.
9. Render-Katolik, "The IT Army of Ukraine."
10. Sarah P. White, *Understanding Cyberwarfare: Lessons from the Russia-Georgia War*, Modern Warfare Institute, 20 March 2018.
11. Alexander Ratz and Andreas Rinke, "Russian 'Hacktivists' Briefly Knock German Websites Offline," Reuters, 25 January 2023.
12. Cade Metz and Adam Satariano, "Russian Tech Industry Faces 'Brain Drain' as Workers Flee," *The New York Times*, 13 April 2022.
13. Liudas Dapkus, "As Russia Sees Tech Brain Drain, Other Nations Hope to Gain," Associated Press, 31 March 2022.
14. USAID, "With USAID Support, Ukraine's Tech Sector Thrives Despite Russia's Full-Scale War," 5 May 2023.
15. Mark Pomerleau, "GAO: CyberCom and Services Not on Same Page Tracking Personnel," *DefenseScoop*, 21 December 2022.
16. U.S. Department of Defense, *Quadrennial Defense Review* (2014), 41. 亦請參閱 Nakasone, Posture Statement Before the 117th Congress, 2.
17. 絕大部分軍種都擁有網路戰後備人員以支援網路防護小隊(Cyber Protection Team, CPT)架構以外的任務，這代表著執行網路戰人員的總數超過了網路戰單位編制人數。美陸軍後備部隊共有10個網路防護小組，分別隸屬於5個網路防護中心；美陸軍國民兵則有11個網路防護小組，由來自33個州的國民兵人員組成；美空軍國民兵下轄12個網路防護小組和3個網路國家任務小組，分布於11個州之內運作。請參閱 Jeffrey L. Caton, *Examining the Roles of Army Reserve Component Forces in Military Cyberspace Operations* (Carlisle, PA: U.S. Army War College Press, 2019), 7–11; and National Guard Bureau, National Guard Cyber Defense Team.
18. U.S. Army Reserve Cyber Protection Brigade, "Army Reserve Cyber Protection Brigade Contributes to Successful Northern Edge Exercise," U.S. Army, 30 May 2023.
19. Joseph Lengyel, "2021 National Guard Bureau Posture Statement" (2021); and Daniel Hokanson, "2022 National Guard Bureau Posture Statement" (2022).
20. U.S. National Guard, Dual Status Command Fact Sheet.

回目錄→

● 作者/W. Stone Holden ● 譯者/趙炳強 ● 審者/丁勇仁

美軍網路資安隱患

The Soft Cyber Underbelly of the U.S. Military

取材/2024年6月美國海軍學會月刊(*Proceedings*, June/2024)

美配備自動武器的武裝分子乘著滑翔傘從天而降；恐怖分子騎著機車穿越防線空隙蜂擁而入；平民被屠殺、從家中被拖出來當作人質；這些觸目驚心的畫面，在全球社群網路上直播放送。連保護數百萬以色列人的防禦系統，也遭致火箭彈轟炸威脅。[1]

更不為人知的是，駭客逐步破壞以色列安全組織的預警能力，並利用民用安全應用程式來安裝惡意軟體；除此之外，他們更透過以色列人個人裝置進行長年的偵察活動。2023年10月7日，哈瑪斯對以色列發起攻擊，在許多層面上都非常值得注意，其中一項便是哈瑪斯在事件發生前、中、後對資訊環境的整合運用。[2]

哈瑪斯的攻擊，顯露出在資訊環境中各種不對稱與非傳統的網路威脅，這些威脅都是確保美軍安全所必須加以應對的。雖然直到最近為止，非國家行為者一般都不被認為具備這種網路能力，但隨著取得更好的工具和技能，這些行為者便能以更高效率對先進部隊產生影響。此外，在網路

使用手機的美海軍新兵。美國國防部必須加強官兵資安教育，以保護他們遠離社交工程和惡意軟體所帶來的作戰風險。
(Source: USN/Stuart Posada)

空間未受保護的軍隊人員，這些整合攻擊也顯示出對其不良影響。這些跡象表明，對身處全球執行作戰任務的美陸戰隊員及美海軍官兵來說，網路攻擊都是真實且日益增長的威脅。

鑑於2023年秋季美國國防部及美海軍部發布的資訊戰相關戰略，這一點值得深入檢驗。[3] 這些文件說明美國對資訊環境的重視，也描述了在該領域作戰和致勝所需的工具。2023年《美國情報社群年度威脅評估》(*Annual Threat Assessment of the U.S. Intelligence Community*)強調主要戰略競爭者所帶來日益增長的網路威脅。儘管致力應對國家能力的戰略是合理的，但近期在以色列及加薩發生的事件，提醒我們必須透過不對稱和跨國行為者的角度(如恐怖組織)來更深入地審視相關戰略。

威脅識別是重要的第一步驟，但要改善美國部隊的網路韌性，則必須採取更具體的行動。這些步驟應包括加強網路安全訓練，擴大美國國防部核准工具的普及性，以便官兵能安全地存取和使用這些工具來保護自己，以及擴大使用防毒軟體。由於美陸戰隊官兵和美海軍官兵幾乎人手一機隨時連網；因此，他們也為敵方的網路作戰創造了直接的出入路徑。若疏於防範這些裝置和連線所帶來的漏洞，將讓軍事系統面臨風險。

網路釣魚和破解

哈瑪斯在攻擊中運用了網路能力來輔助空中及地面行動。在哈瑪斯發動第一波火箭襲擊後約12分鐘，網路安全公司便偵測到分散式阻斷服務(DDoS)攻擊，其目的在於癱瘓以色列對平

民提供火箭警報的網站。[4]

在襲擊當日，駭客控制電子廣告看板傳播恐嚇訊息，並對以色列境內手機發送大量威脅性文字簡訊。[5] 在隨後的幾天裡，其他團體也開始攻擊與衝突有關的網站和服務。部分網路攻擊利用應用程式中的程式碼漏洞發送虛假的火箭警報、攔截請求及暴露伺服器。應用程式的假冒版本讓駭客能搜集使用者的敏感數據。[6] 巴勒斯坦幽靈(Ghosts of Palestine)是親巴勒斯坦駭客組織，聲稱他們攻擊了包括以色列外交部和本古里安國際機場(Ben Gurion Airport)在內的以色列機構。[7]

巴勒斯坦幽靈駭客組織與哈瑪斯的關係尚未完全明朗，但部分觀察家認為該組織可能與哈瑪斯有關聯，透過網路作戰共同竊取以色列國防機密。(Source: Shutterstock)

雖然我們仍不清楚在相關攻擊的背後，這些駭客組織有多少是由哈瑪斯直接控制——畢竟這也有可能只是激進駭客主動參與大型衝突——但這種協調程度至少暗示雙方有密切的合作關係。不論如何，哈瑪斯在這些行動中展示了高超的網路作戰能力。這種能力並非一朝一夕產生，過去十年間，哈瑪斯發展出一套精密的網路能力，並取得了一些顯著勝利。2013年，哈瑪斯開始其網路作戰行動，使用包括色情影片在內的網路釣魚手段，利用人們因影片性質而不願回報遭到威脅的心理。[8] 至少自2017年開始，哈瑪斯便利用虛假的交友檔案來吸引以色列國防軍(IDF)人員下載含有惡意軟體的圖片，讓哈瑪斯間諜可以透過這些人員的手機，竊取有關以色列國防軍武器、部隊及設施等資訊。[9]

在2018年FIFA世界盃足球賽期間，哈瑪斯開發了一款應用程式來利用球迷對賽事的關注。這款應用程式本應讓使用者追蹤比賽結果，但它也包含了針對以色列國防軍人員的惡意軟體。[10] 這使哈瑪斯可以遠端控制手機的鏡頭和麥克風，取得有關以色列國防軍部隊、基地、裝備及行動等資訊。與哈瑪斯

相關的駭客在使用社交工程手段方面也顯得十分老練，尤其是在像WhatsApp這種熱門通訊應用程式上探誘資訊。[11] 遭駭的以色列國防軍裝置似乎提供了大量詳細情報，幫助哈瑪斯成功進行了2023年10月7日的襲擊。[12]

以色列國防軍並未對哈瑪斯的網路活動掉以輕心。正視相關網路活動並將其視為威脅局勢中一個嚴重的要素。2019年5月，以色列國防軍對哈

資安意識傑夫(Cyber Awareness Jeff)是美國國防部的資安意識挑戰活動(Cyber Awareness Challenge)知名角色之一(也是最多人嘲仿的)，其與搭檔緹娜(Tina)一起出現在這個挑戰中。儘管網路安全意識在近期確有改善，但這項挑戰活動仍有許多精進空間。該活動應逐年自我完善，帶來新的技能和意識，並向官兵展示對手真正的威脅和戰術，以帶來更好的參與效果。圖片文字為「(網路)威脅是真的，不要讓傑夫失望」。(Source: USN on X)

瑪斯的網路作戰指揮機構進行了轟炸，以回應一次大規模的網路攻擊企圖。[13] 隨後在2021年，以色列也針對加薩地區的哈瑪斯網路設施進行打擊，包括儲存設施和網路戰人員的藏匿點，並直接針對這些網路戰人員進行攻擊。[14]

微處理器下無新事

先進的網路工具和「零日」漏洞(Zero-Day，沒有修復方案的安全性漏洞)正被賣給出價最高的買家。[15] 曾經專屬於國家安全局等機構的工具，如今透過蓬勃發展的灰色市場，落入了流氓國家、犯罪集團及恐怖組織手

中。例如墨西哥的販毒集團，他們利用以色列NSO公司所開發的強大間諜軟體Pegasus和其他網路工具來威脅集團內部人員、記者及社運人士。[16]

恐怖組織多年來一直在運用網路戰術來實施或支援其行動。2009年，伊朗支持的伊拉克什葉派武裝分子駭入美軍MQ-1掠奪者無人機(Predator)的視訊訊號，取得與美軍操作人員相同的存取權限。[17] 自2012年起，駭客團體敘利亞電子軍(Syrian Electronic Army)的駭客駭入媒體公司相關帳戶，並利用這些平臺推廣他們偏好的敘利亞內戰敘事並散布假訊息。[18]

發生於2013年的事件也許是最具影響力的駭客行動，當時敘利亞特工取得美聯社 (Associated Press)的推特(Twitter)帳戶權限，並發布了一則關於白宮發生爆炸的推文。儘管該推文被迅速揭穿，卻也短暫導致美股下跌，造成實質但短暫的經濟影響。2015年1月，與ISIS相關的駭客短暫接管了美軍中央司令部(Central Command)的推特帳戶。[19] 雖然這讓美軍顏面無光，但該行動的軍事價值有限，因為軍方很快便恢復對該帳戶的控制，該行動似乎也未能支援該組織在其他領域的行動。

將網路行動整合納入更廣泛的軍事行動有其難度。2022年俄羅斯入侵烏克蘭後，許多專家指出，儘管俄羅斯據稱擁有部分世上最先進的網路能力，也在2014年併吞克里米亞後在烏克蘭進行了多年的實戰演練，但俄羅斯卻似乎無法將網路作戰效果與地面或空中行動相互協調配合。[20]

與美軍等行為者所能夠達成的可能效果相比，雖然哈瑪斯在其攻擊時的網路整合規模與範圍並不令人印象深刻，但仍值得關注。值得注意的是，哈瑪斯並不需要滲透以色列國防軍安全網路來取得所需情報；它針對的是更大範圍且更脆弱的攻擊面，也就是瞄準以色列國防軍官兵隨身攜帶的裝置，相關裝置以色列網路安全機構尚未提供防護。這應該視為一個警訊，即其他組織將透過提升其網路能力，以在未來作戰中攻擊軍方廣大而脆弱的網路弱點。

對全球的網路攻擊行為者而言，他們並不會區分積極參與衝突的人和坐在家裡滑手機的人。當官兵境外部署時，那些惡意行為者將鎖定美陸戰隊員與美海軍官兵及其眷屬進行間諜活動，並想辦法在任何可能的地方削弱單位能力。

強化個人能力

美海軍部網路戰略中的第一行動主軸認為網路安全訓練必須加以改善。

[21] 人為錯誤是組織遭受網路攻擊的首要途徑，美陸戰隊和海軍的工作人力規模龐大且組成多元，無疑是與其他組織相比(若不是更具吸引力的組織)更具吸引力的攻擊目標。

過去幾年中，美國國防部年度網路安全意識挑戰的改進是值得讚揚的，但該計畫仍然不夠完善。[22] 首先，訓練需要自我完善，並每年導入新技能和意識；但事實卻不然，這些訓練往往只被視為機械性的例行公事，甚至有更多人覺得這種訓練很麻煩，快速在網站上用滑鼠點一點就交差了。即便使用者深知網路基礎知識的重要性，許多人也難以投入到抽象的「如果……會怎樣？」情境中。然而，向官兵展示針對他們進行攻擊的真實威脅和戰術，則較可能引起更高度的參與，比如「俄羅斯組織對烏克蘭使用了哪些技術？以色列士兵如何被哈瑪斯相關的網路團體攻擊？」人類天生更容易對明顯可能影響自己生活的事物感興趣。澄清目前所教授的概念(如網路釣魚連結、虛擬私人網路[VPN]等)，以及敵人如何利用這些概念來攻擊美國使用者間之連結，將能強化官兵的理解與警覺。

除了改善訓練外，美海軍部應與網路安全暨基礎設施安全局(Cybersecurity and Infrastructure Security Agency)及廠商密切合作，產生各種可供官兵在個人裝置上使用的有效網路安全工具，並將這些工具納入訓練。[23] 只告訴官兵從交友軟體下載圖片可能包含惡意軟體是不夠的，他們必須具備可以隨手使用的工具來保護自己。這些工具應包括虛擬私人網路服務，以便官兵在出國執行任務與休假時能更安全地使用網路。這些工具種類繁多，但對其能力和侷限性的理解不足，可能使官兵面臨風險。準備簡單的工具包，以及使用時機與方法的基本知識，就可以大大增強部隊的網路安全性。

另一個潛在的簡易改進措施是提供防毒軟體保護。如果向任何一位指揮官報告：部隊人員大多缺乏工作所需的個人防護裝備（Personal Protective Equipment, PPE)；這些指揮官會非常擔憂。政府提供的裝置都配有商用防毒軟體，因為政府認為這些電腦對設定防禦基線具有重要意義。讓每個人的裝置(包括個人裝置)使用防毒軟體是一種簡單卻有效的改進措施。然而，有案例證據表明，官兵的個人電腦和行動裝置並不具備足夠的「網路個人防護裝備」。

美國國防資訊系統局(Defense Information Systems Agency)提供一套「家

用計畫」(Home-Use Program)，官兵可以在一臺裝置上免費獲得一年的McAfee防毒軟體保護。[24] 這是一個好的開始，但很多人擁有多臺裝置，而且大多數人在第一年後將不會續訂此種防護。許多美陸戰隊員及美海軍官兵都知道這些軟體的重要性，但他們可能不願或無法支付維護個人裝置服務的年度費用。防毒軟體保護應該免費提供所有官兵，作為其公發防護裝備的一部分。此措施將在駐地和部署環境中設置新的防護基線，減少網路攻擊面。有鑑於美海軍部的裝置與人員規模，這項措施無疑將所費不貲，但這種龐大的資安漏洞幾乎勢必會在未來造成更高的成本。

敵動，我也動

要使網路空間達到百分之百的安全，或期望完全符合最佳實踐是不可能的。即便每位官兵都成為完全認證的網路安全專家，他們仍然是人類，只要是人就會犯錯。然而，減少目前的安全漏洞規模和深度是值得大量投資的。敵人絕對非常樂意運用連接官兵隨身裝置來取得軍事優勢，因此提升大眾的網路安全值得投入時間和資源。考量到網路在資訊環境中的關鍵角色，透過改進所有官兵所接受之訓練、提供他們保護自己所用的實際工具，以及提供基本網路個人防護裝備來保護網路空間，是至關重要的。

作者簡介

W. Stone Holden為美陸戰隊少校，現任職於美陸戰隊第29航空大隊，從事安全合作及情報蒐集管理任務，以及管理各種專案，運用尖端科技解決不同的威脅。

Reprint from *Proceedings* with permission.

註釋

1. Daniel Byman, Emily Harding, and Michael Leiter, “Hamas’ October 7 Attack: The Tactics, Targets, and Strategy of Terrorists,” Center for Strategic and International Studies, 7 November 2023.
2. MWI Podcast, “Understanding Hamas—From Tactics to Strategy,” West Point Modern War Institute, 14 November 2023.
3. *Summary of the 2023 Cyber Strategy of the Department of Defense* (Washington, DC: Department of Defense, September 2023); Department of Defense, “DOD Announces Release of 2023 Strategy for Operations in the Information Environment,” 17 November 2023; and Department of the Navy, “The Department of the Navy Releases Inaugural Cyber Strategy,” 21 November 2023.
4. Omer Yoachimik and Jorge Pacheco, “Cyber Attacks in the Israel-Hamas War,” *The Cloudflare Blog*, 23 October 2023.

5. Colin Demarest and Tzally Greenberg, "'Hacktivists' Join the Front Lines in Israel-Hamas War," C4ISRNet, 31 October 2023.
6. Blake Darche, Amen Boursalian, and Javier Castro, "Malicious 'RedAlert—Rocket Alerts Application' Targets Israeli Phone Calls, SMS, and User Information," *The Cloudflare Blog*, 13 October 2023.
7. Sam Sabin, "Hackers Make Their Mark in Israel-Hamas Conflict," Axios, 10 October 2023.
8. Simon P. Handler, *The Cyber Strategy and Operations of Hamas: Green Flags and Green Hats* (Washington, DC: Atlantic Council, November 2022), 12–13.
9. MWI Podcast, "What Was Hamas Thinking?" West Point Modern War Institute, 23 October 2023.
10. Handler, *The Cyber Strategy and Operations of Hamas*.
11. "Hamas Using WhatsApp to Hack Israel Soldiers," *Middle East Monitor*, July 2019.
12. Michele Groppi and Vasco da Cruz Amador, "Technology and Its Pivotal Role in Hamas's Successful Attacks on Israel," Global Network on Extremism and Technology, 20 October 2023.
13. Judah Ari Gross, "IDF Says It Thwarted a Hamas Cyber Attack during Weekend Battle," *Times of Israel*, 5 May 2019; and Israel Defence Force, twitter.com/IDF/status/1125066395010699264, 5 May 2019.
14. Eviatar Matania and Lior Yoffe, "Some Things the Giant Could Learn from the Small: Unlearned Cyber Lessons for the U.S. from Israel," *Cyber Defense Review*, Winter 2022.
15. 「零日」(Zero-Day)漏洞是一種電腦漏洞，存在於安全研究人員或電腦公司一無所悉的情況下，這代表著他們沒有任何時間來修復這個問題。
16. Cecile Schilis-Gallego and Nina Lakhani, "'It's a Free-for-All': How Hi-Tech Spyware Ends Up in the Hands of Mexico's Cartels," *The Guardian*, 7 December 2020; and Alan Feuer and Emily Palmer, "An I.T. Guy's Testimony Leads to a Week of Cyber Spy Intrigue in El Chapo Trial," *The New York Times*, 13 January 2019.
17. Mike Mount and Elaine Quijano, "Iraqi Insurgents Hacked Predator Drone Feeds, U.S. Official Indicates," CNN, 17 December 2009.
18. J. Dana Stuster, "Syrian Electronic Army Takes Credit for Hacking AP Twitter Account," *Foreign Policy*, 23 April 2013.
19. David C. Gompert and Martin C. Libicki, "Decoding the Breach: The Truth About the CentCom Hack," RAND Corporation, 3 February 2015.
20. Gavin Wilde, "Cyber Operations in Ukraine: Russia's Unmet Expectations," *Cyber Conflict in the Russian-Ukraine War* (Washington, DC: Carnegie Endowment for International Peace, December 2022).
21. *2023 Cyber Strategy* (Washington, DC: Department of the Navy, November 2023), 5-6.
22. Department of Defense, "Cyber Awareness Challenge 2024."
23. 資訊系統稽核人員認證(CISA)網站上提供了一份免費網路安全工具清單，範圍從基礎到高階不等。然而，這些工具的宣傳不足，且缺乏如何使用這些工具的訓練。請參見www.cisa.gov。
24. Defense Information Systems Agency, "Antivirus Home Use Program (AV HUP)."

回目錄→


(Source: DVIDS)

● 作者/Alfredo Rodriguez III ● 譯者/蕭光霈 ● 審者/丁勇仁

加速培養網路領導幹部

Accelerating Cyber Leader Development: A Call to Action for Service War Colleges

取材/2024年第一季聯合部隊季刊(*Joint Force Quarterly*, 1st Quarter/2024)

網路專業領導幹部發現所屬機關經常遭受網路攻擊，每日數以百萬計的入侵網路事件，使我方投票系統乃至於社群媒體發文等各個層面皆受到干擾。愛沙尼亞於2007年發生網路攻擊、伊朗納坦茲(Natanz)鈾濃縮設施遭受一連串網路攻擊，以及2014年索尼影業(Sony Pictures)公司於資料遭駭等事件，不過是少數成為媒體標題的冰山一角。時至今日，網路空間同時兼具科技發展之機會與弱點。銀行業、公用事業及醫療保健電子化，似乎各行各業益發依賴數位裝置構成之網路以儲存、處理及分析數據。然現實情況卻令人惶恐不安，國家在這片險象環生之網路領域上隨波逐流，將作戰領域數據之儲存、處理及分析任務交付未完成準備的網路專業高階領導幹部。本文宗旨係專為美國國防部所屬高階網路專業領導幹部之養成提供建言，俾能在此危機四伏之作戰空間中取得勝利。

儘管美國在此領域擁有良好防禦能力，但針對美國之攻擊從未止歇。

2019年7月25日，美海軍戰爭學院於美國羅德島州紐波特(Newport)舉辦前進防禦：2019年重大基礎設施兵棋推演(Defend Forward: 2019 Critical Infrastructure War Game)的相關參演人員。

(Source: USN/Tyler D. John)

數位戰場上的攻方，不必在乎法律制裁。在戰略競爭的時代，中共積極竊取智慧財產，持續在經濟與軍事上追平美國。俄羅斯與其代理人(傀儡)公然破壞民眾對於美國選舉過程嚴整性與民主制度之信心。[1] 美國基礎建設不斷受到刺探，罪犯利用全球網路之便，盜取民眾個人與公司行號資產。這般環境能使軍事力量在傳統思維下毫無用武之地。瞭解網路如何形塑世界的一方，就能調整做法、準則及作業模式，確保其軍事力量能夠迎接挑戰。美國網路空間日晷委員會(Cyberspace Solarium Commission)委員金(Angus King，緬因州無黨籍參議員)與蓋拉格(Mike Gallagher，威斯康辛州共和黨眾議員)曾合撰公開信，強調如此岌岌可危之情況，彼等寫道：「現況是美國每日無時無刻不在遭受攻擊。現況是美國之力量與責任刻正緩慢流失與捐棄。吾等要求中止此一惡化現象。」[2]

當前態勢

美國2019年《國防授權法》(*National Defense Authorization Act, NDAA*)中首設美國「網路空間日晷委員會」，以解決在網路空間遭遇之挑戰。該委員會係為國家層級上之初步做法，俾研擬戰略手段，保衛美國抵抗恐會招致嚴重後果之網路攻擊。[3] 日晷委員會之報告討論國家在網路專業人才之招募、養成與留用等政策，以及擴大其公職任用遴選上之執行情形。美國國防部網路戰略(Cyber Strategy)同樣寫道：

> 國防部將調整其制度文化，讓各階層人員皆熟悉網路空間領域，並能將所學融入日常工作之中。領導幹部及

其幕僚必須「通曉網路知識」，以瞭解其決策在網路安全上構成之意涵，並為尋找運用網路空間領域之良機做好準備，以換取戰略、作戰及戰術上之優勢。[4]

2023年8月7日，美陸戰隊網路戰大隊與網路空間作戰營之軍、文職人員於網路旗23-2(Cyber Flag 23-2)演習中彼此較勁。 (Source: US Marine Corps/Brian Stippey)

在網路空間中採取之行動，應無異於其他領域之行動；換言之，各軍種必須要為網路專業軍官建立特業軍職專長。這些軍官將領導如何運用網路空間以協助聯合作戰，或提供相關諮詢。提供訓練精良、技術到位之士官兵與准尉位階人員係為當下重點，各軍種針對規劃網路專業軍官之養成，亦可比照辦理。與其他領域相同，網路空間需要的是循各自經管養成之聯戰專業軍官，俾於出任高階指揮職與高司幕僚職，做好領導統御之準備。[5] 目前美國國防部發布之網路人力出版品，係用以建立網路人力之標準，並作為組建相關作戰部隊之參用基礎。前述出版品係國防部建立網路職務專長號碼之權威參考，亦是美軍律定能在網路領域中執行作戰、支援及領導任務之人員資格的參用基礎。在國防部網路人力框架(DOD Cyber Workforce Framework, DCWF)範圍內，各軍種目前將承擔網路專業人員養成與資格審定之責。尤值一提，前述出版品係用以律定從事網路專業職務之領導幹部角色，以及授權相關人員發展。

為實踐美國國防部網路人力框架，國防部如何能在專業軍事教育(Professional Military Education, PME)基礎上，養成高階網路專業之軍職與文職領導幹部？如何讓這群高階網路專業領導幹部做好準備，以運用網路空間與資訊相關能力，支援因勢利導之聯合作戰、戰略發展及其他國家安全行動，或提供相關諮詢？國防部將前述問題委託蘭德公司(Rand Corpora-

tion)進行研究，檢視其在聯合專業軍事教育第二階段(Joint PME Phase II)與研究所層級上，針對網路空間主題所實施之教育制度做法。[6] 是項研究出版時，適逢作者為本文進行之研究告一段落，研究報告建議中的擴訓做法，與本文所見略同。

各軍種戰爭學院應配合國防部網路人力框架，施行網路空間戰略研究班教程，以養成網路專業領導幹部。這種先期探路做法，可為網路專業軍官塑造聯合專業軍事教育與未來經管發展之體系。美國國家與國防戰略、聯合專業軍事教育指導，以及美國國防部網路空間人力指導綱要皆須配合調修，以開設是項教程。本文係以國家之角度說明網路空間，描述國防部目前施行之網路空間人力指導綱要，然後詳述目前聯合軍事專業教育體系最適於養成未來網路專業領導幹部之原因。本文結論中提出，各軍種戰爭學院可藉由設立網路空間戰略研究班教程，以達成國防部要求，並能協助國防部在此競爭激烈的網路空間作戰領域中克敵制勝。

附圖：網路空間戰略研究班必修課程提案

附註：藍色部分代表一般課程內容。綠色部分代表特業課程內容。本圖由作者自製。

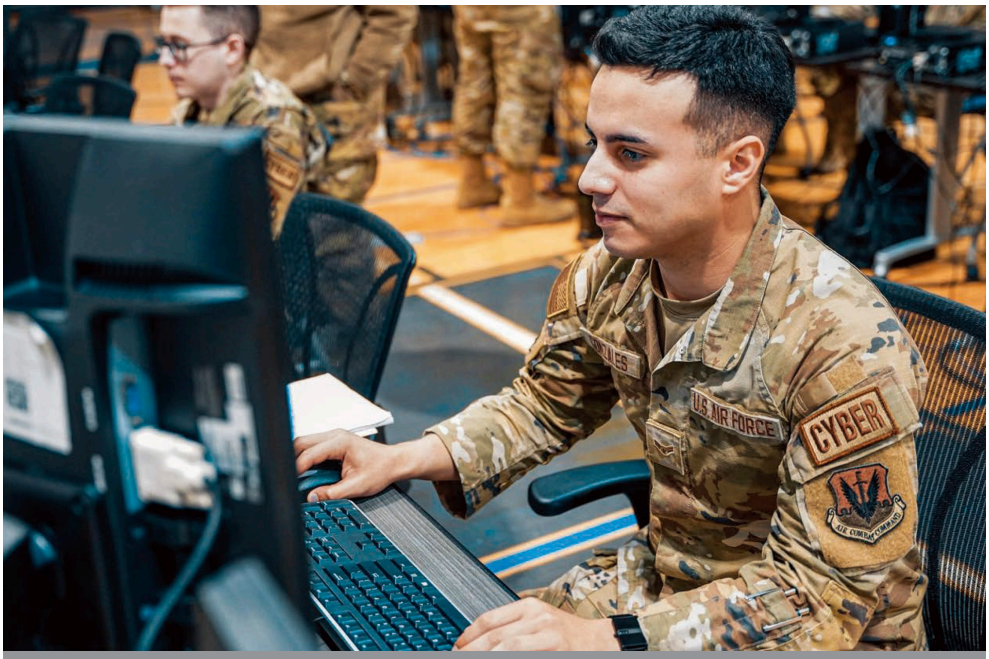
領域統御在網路空間上之挑戰

國家與國防部之觀察角度。全球數位連結為人們帶來龐大經濟成長、科技優勢，以及改善生活品質。美國網路空間日晷委員會報告中說明人們更加緊密相連與數據交換所形成之弱點。報告指出網路世界需要相當程度之數據安全、韌性及可信度，而此非政府或民間單方面得以具有完善設備來提供。[7] 網路世界讓對手得以運用特定工具遂行脅迫、破壞、間諜及勒索等活動，俾在數位、經濟及社會層面上超越我們。

網路作戰之力量與涵蓋範圍正逐步成長，其他國家與非國家行為者能夠在不投入軍隊或表明意圖的情況下，對美國施壓。《國家安全戰略暫行指南》(*Interim National Security Strategic Guidance*)將網路世界形容為「具有危機與良機之科技革新」領域，而此即全球強權國家研發與運用新興科技之賽場。[8] 《2035年聯合作戰環境》(*Joint Operating Environment 2035*)中描述未來採取科學、技術及工程領域上之手段，是能讓敵人在科技上得以與美國並駕齊驅，並能挑戰美國利益之做法。[9] 在2035年發生的戰爭，將是運用武力在阻絕全球公域(Global Commons)與爭奪網路空間之競賽。《資訊環境中之聯合作戰概念》(*Joint Concept for Operating in the Information Environment*)中將其濃縮為一個核心主題，以解決前述挑戰，並達成持久不墜之戰略成果。[10]

為取得勝利，聯合部隊必須將網路空間融入作戰藝術之中，以規劃專以發揮軍事任務中資訊層面之作戰行動。[11] 領導幹部必須瞭解軍事任務與資訊力量中，有關「獲取、處理、分發與運用數據以強化作戰力量」[12] 涉及之網路空間與資訊層面。要能瞭解透澈，需要各軍種將實體與資訊力量結合教育訓練管道，讓網路專業領導幹部做好準備，成為跨界多領域之戰士。作戰環境之創新做法與資訊力量持續整合，能讓各級指揮官掌握更多能將軍事力量發揮極致之選項。[13] 網路專業領導幹部在此環境中扮演之角色，是要能全心全意投入此變化多端的環境與跨足全般領域進行整合。目前各軍種戰爭學院對於高階網路專業領導幹部實施之教育，必須達成此項要求。

今日處境。網路空間日晷委員會報告明述美國政府處境欠佳，無法以必要之速度與靈活度在網路空間中領先群倫、維護美方利益。[14] 報告指出美國政府受到工業時代的官僚體系、法律及規範所束縛。[15] 聯邦政府



2023年5月12日，美空軍第83網路作戰中隊(83rd Network Operations Squadron)上等兵岡薩雷斯(Aden Gonzales)參加第688網路空間聯隊於美國德州聖安東尼奧(San Antonio)舉辦之第4屆凶猛地獄三頭犬(Savage Cerberus)年度戰術演習。(Source: DOD/Nadine Wiley De Moura)

欠缺具備網路專業之公職人員，正使美國在此方面的努力大打折扣。報告中引述資料顯示，美國政府尚有超過3萬3,000個網路專業之人員缺額。[16]

招募與留用網路專業人才遭遇困難，亦對各軍種造成嚴重影響。留用與培養善用網路工具的人員非常重要，因此2022年會計年度《國防授權法》即要求美國國防部，針對聯合教育體系現行網路與資訊戰教程進行整體評估。《國防授權法》明確指導國防部評估目前深造教育單位有無實施適當課程，且該單位是否為合宜之施訓機構。[17] 此時要將網路空間定位為作戰領域，就需採取嶄新戰略態勢，以盱衡全局之視野，檢視此瞬息萬變之網路世界。

該委員會之主要建議集中在人力資本之範疇。第1.5項建議指出，美國必須招募、養成及留用能夠建構網路防禦體系，以及能靈活、有效運用國家力量中所有與網路空間相關工具的網路人力。[18] 與此項建議格外相關的是強化國家標準暨技術研究院(National Institute of Standards and Technology)角色，並運用在全國廣為施行之國家網路安全教育倡議(National

Initiative on Cybersecurity Education, NICE)建立之人力框架。此框架說明執行網路安全工作的基本必要任務、知識及技能，亦是能讓機構組織養成網路安全專業人力之基礎，並能幫助這些機構採取適當教學活動以提升人員知識與技能。具體來說，國家網路安全教育倡議所制定之框架，係為現行美國國防部培養網路人力所要求之組織原則，對高階網路專業領導幹部更是如此。然而，為達成這項教育義務，各軍種除在專業軍事教育列有可選訓之密集課程與網路認證課程外，各軍種至今皆未提出針對專為養成大部分高階軍、文職官員之戰爭學院相關專業教程。

美國國防部目前之要求。近於2018年發布之《國家網路戰略》(National Cyber Strategy)，強調培養優秀網路安全人力係為安全優勢。內容寫道美國將「全面培育廣大人才，同時向海外最傑出優秀且認同我國價值觀念者招手」。[19] 這項戰略強調聯邦政府必須運用國家網路安全教育倡議框架，將網路安全專業人力之遴選、招聘、養成及留用作業建立標準。在網路領域上能夠成功致勝，有賴於美國國防部能否培育出高素質人力，以養成能夠整合嶄新能力、運用新興做法之領導幹部。該項戰略發布時，國防部在資訊保證(Information Assurance)部門外，尚欠缺專為解決網路人力之全面性指導。

所以，美國國防部如何養成網路專業人才，如何配合國家網路安全教育倡議？國防部網路人力戰略的焦點之一，即為發行美國防部第8140號出版品，用以說明國防部各級單位之網路人力管理。前述出版品說明要求重新評估幕僚充員、調整人員之網路空間工作職掌(已納入國防部網路人力框架)，以及留用合格人員。國防部與美軍網路司令部(U.S. Cyber Command)合作，將網路空間工作職掌與資格需求完整結合，納入重要的國防部網路人力框架。國防部第8140號出版品區分為三份彼此關聯之指導綱要、指導及手冊。[20]

- 2020年10月5日，頒布美國國防部第8140.01號指導綱要《網路空間專業人力管理》(*Cyberspace Workforce Management*)。
  - 賦予國防部網路空間人力管理委員會(Cyberspace Workforce Management Board)職權。
  - 建立網路人力之要件。
  - 確立國防部部內業務與職掌。
  - 制定網路空間專業人力之定義。

- 2021年12月21日，頒布國防部第8140.02號指導《識別、追蹤及呈報網路空間人力需求》(*Identification, Tracking, and Reporting of Cyberspace Workforce Requirements*)。
  - 提供對於國防部網路人力框架所列職務，進行識別、追蹤與呈報之指導。
  - 確認軍、文職需求。
  - 提供整體網路空間專業人力養成需求之基準。
- 2023年2月15日，頒布國防部第8140.03號手冊《網路空間人力資審暨管理專案》(*Cyberspace Workforce Qualification and Management Program*)。
  - 律定網路空間人力資審之職責與程序。
  - 說明在基礎(學科)、實作(能力)與持續培養/資審之要求。
  - 適用範圍涵括軍、文職及約聘人員。

美國國防部第8140號出版品處理網路人力各層面之問題。網路空間人力包含組建、維護、運作、防衛及保護國防部與美國網路空間資源之人員；遂行相關情報活動之人員；使未來作戰得以進行之人員；以及能在網路空間中或透過網路空間投射力量之人員。

美國國防部網路人力框架係為一全面標準化做法，以述明國防部之網路專業職務皆要達到適才適所。此項框架讓各軍種能夠識別、追蹤及呈報網路專業人員與其資格是否符合《2015年聯邦網路安全人力評估法》(*Federal Cybersecurity Workforce Assessment Act of 2015*)之要求。即將發行的國防部第8140號手冊將會列出國防部網路人力框架中54項職掌之工作項目，以及專業知識、技巧及能力(Knowledge, Skills, and Abilities, KSA)。此54項專長職務分布於下列5項領域：

- 網路資訊科技。
- 網路安全。
- 網路效果。
- 網路情報。
- 網路推手(Cyber Enablers)。[21]

雖然網路專業領導幹部之職務非常重要，但是未來一般高階文官與上校階軍官亦可能出任網路政策與戰略規劃之職務，或任何支援重要網路與科技方案之採購與專案管理之工作。國防部網路人力框架透過國防部網路

人力框架更新(DCWF Refresh)方案進行調修，並為更多擔任數據處理與人工智慧的網路專業領導幹部律定專長號碼。[22] 這些職務為3位數的專長號碼，普遍稱之為「網路專長號碼」(Cyber Coding)。

依據美國國防部第8140號文件，網路專長號碼係為協助識別、追蹤及呈報擔任網路專業職務及使用經過授權之人事與人力資料庫人員。新設之專長號碼將能代表該項職務工作項目與相對應之熟練程度。目前相關作業仍在進行，各軍種僅針對所屬網路人力進行初步編碼。2021年，國防部有超過12萬的軍、文職職位列入網路專長號碼；然美陸軍、網路司令部及其他少數單位仍在透過其人力系統進行相關編碼作業，因此尚未列入統計。[23] 儘管數字不完整，前述報告數字仍足可顯現國防部網路人力之規模。

美國國防部網路人力框架與網路專長編碼工作，代表美國防部需要將網路人力管理進行標準化作業。每項網路專業職務皆列有其定義、主要與附帶工作項目，以及專業知識、技巧及能力，說明達成其重要業務職掌與評估其熟練程度必要之條件。[24] 網路專業領導幹部不能免除前述之要求。從同一份國防部網路專長號碼報告中推測，有超過700個職位號碼為網路專業主管(Executive Cyber Leader)。美陸軍一旦完成相關作業，相關數據將會激增。對於要讓高階網路專業領導幹部資格符合國防部第8140號文件之要求，確實顯而易見。就算目前欠缺美陸軍最終編碼總數，前述內容代表美國防部整體的高階網路專長職務不但種類繁多，數量亦持續增加。另外，各軍種除運用國防部網路人力框架管理網路人力之培養與職務表現外，且皆奉行指導，確認符合規定為達成任務整備的要件之一。[25] 身為國防部培育領導幹部搖籃之聯合專業軍事教育，目前已做好調整以迎接是項挑戰。

聯合教育與網路。聯合專業軍事教育正不斷琢磨作戰藝術與科學，特別是擁抱與整合科技，以圓滿達成任務。2020年，參謀首長聯席會議(Joint Chiefs of Staff, JCS)針對專業軍事教育之願景與指導，明述戰爭特質與行為之變化，需要「持續整合發揮國家力量之手段與支持國家目標之影響力……並且更深入瞭解對敵我雙方革新與未來科技潛在之意涵」。[26]

今日環境需要對發揮力量之資訊手段、必要之網路能力及不斷演變之科技進行深入研究。因此，參謀首長聯席會議之願景明白陳述專業軍事教育必須讓結訓人員具備充分知識與技能，服役時能夠成為「在強權競爭與革

2023年8月11日，負責網路空間防禦作戰(Defensive Cyberspace Operations)的美陸戰隊後備部隊直屬大隊(Force Headquarters Group)網路空間作戰操作員麥卡曼(Joshua Mackaman)下士，於美國內華達州拉斯維加斯(Las Vegas)舉辦之國際資訊安全會議(DEF CON 31)電腦網路駭客競賽中協助民間參賽者。(Source: US Marine Corps/Jonathan L. Gonzalez)

新科技條件下之戰事瞬息萬變情況中運籌帷幄」的聯合作戰領導幹部、資深參謀軍官及戰略家。[27] 美國國防部首席資訊官(Chief Information Officer, CIO)於其因應國防部網路戰略之行動主軸(Lines of Effort, LOE)中附和這項任務。其行動主軸第8項：維持網路人力，殊值關注。此行動主軸負有特殊目的，係要強化國防部網路教育品質連貫性，相關次目標簡述如次：

- 第8-5-2項：藉由融入實際與相關之個案研究，強化聯合專業軍事教育院校實施之網路空間課程。
- 第8-5-3項：發展相關概念，以擬定領導階層之網路戰略發展及計畫作為框架，納入聯合或軍種主辦之功能性課程中。
- 第8-5-4項：將網路任務、職務角色與責任，融入必要之領導統御訓練計畫與課程之中。[28]

各軍種戰爭學院要實現前述目標，發展方向就須符合美參謀首長聯席

會議主席(Chairman of the Joint Chiefs of Staff)對於軍官專業軍事教育之指示。在2020年5月發布之指示中，說明在六項聯合學習領域(Joint Learning Areas, JLA)中採取的成果導向(Outcome-based)做法。美國國家與聯合網路願景與國防部首席資訊官行動主軸之意圖，可就其中三項聯合學習領域詮釋。

- 第三項聯合學習領域：從競爭、衝突到戰爭的漸進過程。此項指導說明聯合作戰領導幹部運用其對於戰爭本質與特徵的知識，來判定影響美國利益之挑戰，評估可行之最佳兵力手段以達成國家安全目標。[29] 網路科技對戰爭演進與全球競爭貢獻良多。高階網路專業領導幹部必須改變目前網路態勢，因應已改變之戰爭特質。此聯合學習領域確符美國防部網路戰略之行動主軸第8-5-2項所述，且可達成其要求。
- 第四項聯合學習領域：安全環境。此項指導說明對於構成威脅、機會及風險的創新與科技部隊所採取之評估。[30] 高階網路專業領導幹部獲得授權，針對網路威脅與機會，發揮領導統御作為與提供相關諮詢。聯合學習領域可支持美國國防部網路戰略之行動主軸第8-5-2項與第8-5-4項，因為高階網路專業領導幹部必須瞭解，在克服安全環境持續變化中，自身所扮演的角色。
- 第五項聯合學習領域：戰略與聯合計畫作為。此項指導說明聯戰軍官負責在衝突全程中，研擬全領域(All-domain)計畫。[31] 依先前討論之諸多國家與聯合戰略所示，網路係為作戰領域。高階網路專業領導幹部必須在計畫作為全程為此領域負責。美國國防部網路戰略之行動主軸第8-5-3項符合所求，且藉由此聯合學習領域可達成其目標，因為網路領域遍布於其他所有領域之戰術、作戰及戰略層次。

美參謀首長聯席會議主席之指導，將美國國防大學資訊暨網路空間學院(College of Information and Cyberspace, CIC)列為網路空間專業領域高階領導幹部之唯一學府。然僅此一所學院既無法因應演變中之安全環境，亦不切合國防部第8140號文件與近期專長編碼上之網路人力需求。網路領域急速擴張，並如先前強調，遍布於其他所有領域之戰術、作戰及戰略層次之中。[32] 網路空間的學習，不能僅限於少數獲選就讀資訊暨網路空間學院的人員。依據蘭德公司2021年之研究，國防部估計僅能完成聯合專業軍事教育第二階段軍事需求之62%，導致網路與資訊專業軍官僅能接受通識專業軍事教育。[33] 於資訊暨網路空間學院接受聯合專業軍事教育第二

階段結訓的學員人數比例，充其量也是少數。美陸軍戰爭學院、空軍大學與海軍戰爭學院並無特定教程培養網路專業領導幹部。藉由推行聯合學習領域，各軍種戰爭學院可依國防部網路戰略，刻意培養領導幹部以達到要求，並能配合國防部2022年會計年度《國防授權法》對於軍種戰爭學院實施網路專業教育之評估。目前編入聯合專業軍事教育第二階段通識教程之網路主題課程已然不足。

網路專業領導幹部之定義及相關建議

為讓高階專業軍事教育符合國家政策文件設定之要求，以及美國國防部第8140號文件建立之框架，須將網路專業領導幹部職務予以定義。目前在國防部網路人力框架下對於網路專業領導幹部職務之簡述，係前述相關建議之參考基礎。亦即網路專業領導幹部遂行決策職權，以及建立願景與方向，供單位網路與相關政策、資源及/或作戰參據，同時肩負擬定影響任務成功之風險相關決策之責。

綜合現有聯邦政府網路專業領導幹部必須具備之專業知識、技巧及能力，以及資訊暨網路空間學院之學習成果，有助於建立研議中的網路專業戰略研究教程之基準。[34] 針對研議教程之建議學習成果如次：

- 評估國家安全環境，置重點於網路空間作戰及相關新興科技對國家力量所有工具構成之影響。
- 能將聯戰準則之觀點，納入網路空間作戰與戰略。
- 分析網路空間作戰、科技、理論、法律及政策等重要層面，用於研議國家與軍種戰略、聯合作戰及其他國防部行動。
- 對網路能力與運用的潛在弱點，以及對聯合作戰構成威脅、機會及風險的創新與科技部隊，進行評估並降低相關影響。
- 有關網路能力運用，採取戰略領導統御、決策及道德行為原則。

與任何教育計畫相同的是，均衡傳授知識之深度與廣度就是挑戰。上述學習成果，一方面是為均衡必備之專業知識、技巧與能力設定方向，以形塑與保護網路環境，另一方面則是用戰略領導統御奠定基礎，以影響軍種壁壘之文化與軍事戰略。

此建議可在各軍種所屬教育單位之網路資源與專家協助下進行。除此之外，是項建議可用於活化資訊暨網路空間學院，使其成為卓越中心(Center of Excellence)，並能支援教程研擬，提供研究機會，並成為軍種

戰爭學院之合作伙伴──此係另一項與蘭德公司研究所見略同之結論。[35] 是項建議所涉範圍廣泛，得以彈性實施；且其內容足夠詳盡，得以迅速施行。建議中並無須更換或刪除原本緊湊的聯參指導課程，只須在某特定教程單元，縮小範圍置重點於網路空間與資訊。這與現行之太空、海事、國安及其他不同類型班次並行，且亦殊途同歸：在需要劃分專業、個別養成之領域中培育出高階領導幹部。

先期要做的是於各軍種戰爭學院設立(或復編)一位網路專業主管。該名網路專業領導幹部將會成為推動網路領域教育之傑出內部推手，致力提升高階網路專業領導幹部學習成果，協助結訓人員具備國防部網路人力框架中所列之網路專業領導幹部職務資格，並與軍種內、外之網路專業教學人士協力合作。該班次應招收涵蓋具備網路、資訊、太空、採購及資訊科技專長之軍官與文職人員，以兼容並蓄，俾讓國防部網路人力框架編列專長號碼之所有高階網路專業領導幹部完成工作準備。此班次以戰爭學院現行聯合戰略與領導統御課程為基礎，增加網路空間與資訊戰呈現之獨特觀點與挑戰。該班次可增列學習網路空間之作戰環境，以及美國國家與國防部之網路戰略，亦尋求納入網路科技能力、法規、政策及資訊分析等課程。課程中亦可納入赴各軍種、國防部與國土安全部之網路作業設施、研究實驗室，以及業界合作伙伴等地點進行短期參觀見學。參觀見學及與業界合作伙伴、其他聯邦政府機關的建教合作，可讓學員能夠符合《國防授權法》所述，擴大與國防部部外單位接觸往來，以探索各式各樣網路能力與手段。[36]

此班次召訓之學員，會依所屬軍種要求提交研究報告，並將學習重心置於網路與資訊領域之挑戰。此一專業班次，能夠訓練學員在戰爭學院課程的兵棋演習期間，提供網路分析與專業知識。本文提議之網路空間戰略研究班必修課程如附圖所示，尚須借助各軍種網路專業單位調修，以及資訊暨網路空間學院提供建言。採行本文之建議可確保達成所有學習目標，畢業生亦能達到國防部網路人力框架列舉對各軍種網路專業領導幹部之要求。

結語

網路空間逐漸改變戰爭與全球競爭演變之方向。起初旨在擴大思想與互動之數位環境，而今卻是用以阻撓美國主權行使所有國家力量的工具。宣

稱網路空間對其他所有作戰領域具有破壞性的效果，這不過是輕描淡寫。克勞塞維茨(Carl von Clausewitz)曾提出警訊：「所有計畫作為，尤其是戰略計畫，必須關注當代戰爭之本質。」[37] 第二次世界大戰法國學者布洛克(Marc Bloch)曾寫道「理論家深陷於歷史教學的錯誤」，以及「參謀學院散播著腐化的氣息」，批判性地銜接克勞塞維茨，乃至於現代美國防部高階官員之抨擊。[38] 美國國防部必須順應潮流並發揮創意，否則就會發現自己要面對的是更虎視眈眈且靈活敏捷之行為者。

美國國防部網路戰略之行動主軸與第8140號出版品，闡述了建立網路人力管理所需之治理方式與架構，以及為相關人員的資格與培育提供基礎。高階聯戰網路專業領導幹部之養成，對在此方向之努力相當重要。由於其至關重要，國防部網路人力框架將其列為一項網路專業領導幹部職務。領導者建立文化，我們必須確保高階網路專業領導幹部熟稔各個領域所涉及之科技、風險及戰略性網路應用。各軍種戰爭學院要定位為領導國防部養成高階網路專業領導幹部之學府，以達成指導綱要要求；並尋求解決之道，以培養每一新世代網路專業領導幹部，以在此不斷改變地作戰領域旗開得勝。

為加速讓我方現有部隊轉型成能在網路競爭與衝突中取勝之兵力，聯合部隊應超越快速採購船艦、戰車及戰機之範疇。聯合部隊必須展現堅定不移、源源不絕之承諾，專注於培養未來高階網路專業領導幹部，藉以形塑網路作戰領域，將之融入各領域之戰略、作戰及戰術階層。期許各軍種戰爭學院能夠藉由建立特定之網路空間戰略研究科班，成為在此領域中之開路先鋒。

本文作者感謝美空軍戰爭學院寇金斯(Mark D. Coggins)上校博士、洪恩(Carl J. Horn)博士與卡梅納(Gene C. Kamena)教授就本文主題與概念提出細心之批評與建議。

作者簡介

Alfredo Rodriguez III是美陸戰隊副司令(主管資訊)轄下人力處軍種網路人力專案經理。

Reprint from *Joint Force Quarterly* with permission.

註釋

1. Angus King and Michael Gallagher, co-chairs, *Cyberspace Solarium Commission Report*

(Washington, DC: U.S. Cyberspace Solarium Commission, March 2020), 8, https://cybersolarium.org/wp-content/uploads/2022/05/CSC-Final-Report.pdf.
2. Ibid., 1.
3. Ibid.
4. *Summary: Department of Defense Cyber Strategy* (Washington, DC: Department of Defense, 2018), 5, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.
5. Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Force Quarterly 73* (2nd Quarter 2014), 14, https://ndupress. ndu.edu/JFQ/Joint-Force-Quarterly-73/Article/577499/the-joint-force-commandersguide-to-cyberspace-operations/.
6. Quentin E. Hodgson et al., *Educating for Evolving Operational Domains: Cyber and Information Education in the Department of Defense and the Role of the College of Information and Cyberspace* (Santa Monica, CA: RAND, 2022), iii, https://doi.org/10.7249/RRA1548-1.
7. *Cyberspace Solarium Commission Report*, 1.
8. *Interim National Security Strategic Guidance* (Washington, DC: The White House, March 2021), 8, https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.
9. *Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World* (Washington, DC: The Joint Staff, July 14, 2016), 3, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joe_2035_july16.pdf?ver=2017-12-28-162059-917.
10. *Joint Concept for Operating in the Information Environment* (Washington, DC: The Joint Staff, July 25, 2018), 8, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf.
11. Ibid.
12. Ibid., viii.
13. Ibid., 9.
14. *Cyberspace Solarium Commission Report*, 16.
15. Ibid., 15.
16. Ibid., 16.
17. National Defense Authorization Act for Fiscal Year 2022 (NDAA FY22), Pub. Law 117-81, 117th Cong., 1st sess. (December 27, 2021), 489.
18. *Cyberspace Solarium Commission Report*, 43.
19. *National Cyber Strategy of the United States of America* (Washington, DC: The White House, September 2018), 17, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
20. William Hess and Alfredo Rodriguez III, "USMC DOD 8140 OPT Presentation," USMC DOD 8140 Working Group, Headquarters Marine Corps, Washington, DC, June 14, 2021, 4.
21. "DOD CIO Cyber Workforce Management," Defense Workforce Council presentation, Pentagon, Washington, DC, August 2021, 3.
22. "DOD CIO Cyber Workforce News," *Defense.gov*, October 2020, https://dodcio.defense.gov/Portals/0/Documents/Cyber/WorkforceNewsletterOctober2020.pdf.
23. 美國防部首席資訊官辦公室人力管理處處長強生(Patrick Johnson)於2021年10月7日提供筆者之電子郵件; Department of Defense Inspector General (IG), *Audit of the Department of Defense Recruitment and Retention of the Civilian Cyber Workforce* (DODIG-2021-110) (Washington,

DC: Government Publishing Office, August 2, 2021), i, 2, 8, 11–12, 26, 28.美國國防部督察長之報告刪除了相關數字。強生於電子郵件中提供可公開之數字。

24. Department of Defense Instruction 8140.02, *Identification, Tracking, and Reporting of the Cyberspace Workforce Requirements* (Washington, DC: Department of Defense, December 21, 2021), 9.
25. Ibid., 6.
26. *Developing Today's Joint Officers for Tomorrow's Ways of War: The Joint Chiefs of Staff Vision and Guidance for Professional Military Education and Talent Management* (Washington, DC: The Joint Staff, May 1, 2020), 3, https://www.jcs.mil/Portals/36/Documents/Doctrine/education/jcs_pme_tm_vision.pdf?ver=2020-05-15-102429-817.
27. Ibid., 4.
28. "DOD CIO Cyberspace Strategy Lines of Effort, LOE 8 Summary," Department of Defense CIO, October 4, 2019, 3.
29. Chairman of the Joint Chiefs of Staff Instruction 1800.01F, *Officer Professional Military Education Policy* (Washington, DC: The Joint Staff, May 15, 2020), 26.
30. Ibid., 25.
31. Ibid.
32. Joshua A. Sipper, "It's Not Just About Cyber Anymore: Multidisciplinary Cyber Education and Training Under the New Information Paradigm," *Joint Force Quarterly* 100 (1st Quarter 2021), 53, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2497154/its-not-just-about-cyberanymore-multidisciplinary-cyber-educationand-training/.
33. Hodgson et al., *Educating for Evolving Operational Domains*, 28.
34. Carl J. Horn, "College of Information and Cyberspace Update," National Defense University, August 7, 2019, 6.
35. Hodgson et al., *Educating for Evolving Operational Domains*, 37.
36. NDAA FY22, 492.
37. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1989), 220.
38. Marc Bloch, *Strange Defeat: A Statement of Evidence Written in 1940* (New York: Norton, 1999), 125.

回目錄→

2023年12月30日，美國海岸防衛隊破冰船北極星號(Polar Star)在南極大陸麥克馬多峽灣(McMurdo Sound)破冰航行。

(Source: US Coast Guard/ Jeremy Burgess)

● 作者/John B. Kelley, Christopher J. Sarton, Scott A. Curtice, and Charles C. York III

● 譯者/李永悌 ● 審者/黃坤銘

南極：競爭、合作或共存

The Other Arctic: Competition, Cooperation, or Coexistence?

取材/2024年第二季美國聯合部隊季刊(*Joint Force Quarterly*, 2nd Quarter/2024)

希望南極大陸能因各國在此致力推動科學研究，樹立國際合作典範，成為純淨且耀眼的和平大陸。

——美海軍伯德(Richard E. Byrd)備役少將

1959年，為確保科學自由與各國皆可進入南極大陸，共有12個國家簽署《南極條約》(*Antarctic Treaty*)。迄今，全球簽約國總數增至56國，其中有半數以上國家(29國)獲得協商國(Consultative Party)地位，可透過《南極條約》協商會議(Antarctic Treaty Consultative Meeting, ATCM)決定未來南極大陸保護措施與運用規範。[1] 60多年來，《南極條約》體系(Antarctic Treaty System, ATS)為全世界科學研究、生物多樣性保護及區域旅遊提供和平穩定環境。

2018年12月26日，中共第35次南極考察任務研究人員展開南極泰山研究站第二階段工程。
(Source: Xinhua/Liu Shiping)

隨著氣候變遷不斷為兩極地區開創契機，國際社會日漸憂心未來重軍事與經濟而輕忽保護工作者，可能會以不負責任方式開發南極地區。[2] 美國、盟國與夥伴國對中共在南極大陸的活動甚為關切，這些國家更憂心南極可能成為軍事競爭而非全球合作之場域。

各國有充分理由憂心，但也並非無計可施，可以參考過往史料與國際規範深入研究。聯合部隊將按例與跨部會、跨政府機關進行跨國合作，透過全政府行動、重新與志同道合協商國協商，以及鼓勵各國在維護南極大陸獨特地位前提下，試圖與中共進行國際合作，維持美國在南極的獨特地位。

深入瞭解美「中」在南極的所作所為與雙方利益後，聯合部隊的任務就逐漸明朗。本文透過文獻(相關文章、書籍及出版品)回顧，深入研究聯合部隊如何支持美國南極戰略。本研究透過競爭與歷史規範角度，由內而外檢視美「中」雙方對南極的目標、投入、介入及行動。

背景與戰略利益

二十世紀上半葉，阿根廷、澳大利亞、智利、法國、紐西蘭、挪威及英國等七國宣稱在南極大陸擁有領土主權。然而，這些主張皆未獲國際認可。[3] 1959年，美國提出《南極條約》，並由當年在南極進行研究工作的12個國家進行簽署，以避免未來他國聲索主權，確保世界各國都能進入南極地區。[4] 此後簽署國的數量增加至56個，但只有符合《南極條約》協商會議要求，於南極大陸「進行實質研究活動」的國家，才能獲邀成為協商國。只有協商國能在會中投票表決重要政策與相

關決策，例如即將於2048年修正的《馬德里議定書》(*Madrid Protocol*)。[5]

南極活動主要規範架構包含《南極條約》與《南極條約》體系下的附加議定書。該條約禁止從事軍事活動，並規定軍事裝備僅可用於協助科學研究、後勤及搜救任務。[6] 除《南極條約》體系外，尚有數紙附加議定書、公約及另外三個主要規範文件。1991年簽署的《南極條約環境保護議定書》(*Protocol on Environmental Protection to the Antarctic Treaty*，亦即《馬德里議定書》)將南極大陸界定為「致力和平與科學的自然保護區」。[7] 1972年簽署的《南極海豹保育公約》(*Convention for the Conservation of Antarctic Seals*)則保護海豹免受狩獵與其他經濟活動影響。[8] 1980年簽署的《南極海洋生物資源保育公約》(*Convention on the Conservation of Antarctic Marine Living Resources*)內容涵蓋磷蝦、有鰭魚類及其他海洋生物資源保育與「合理利用」。[9]

由於開採礦產資源會破壞環境，《馬德里議定書》明文禁止相關活動。南極大陸有近98%的表面被冰層覆蓋且有多數區域不宜人居，礦產與能源也因鮮少地層暴露而難以獲得。由於陸地上覆蓋極厚冰層，開發南極大陸資源極具挑戰性。[10] 此外，南極大陸裸露岩層的面積約等同美國科羅拉多州，惟南極陸地總面積卻大於美國與墨西哥國土面積總和。進行採礦或探勘計畫的後勤工作相當艱鉅，而氣候嚴峻與通行不易也導致部分裸露的大型岩塊迄今杳無人跡。[11]

儘管如此，專家認為南極大陸冰層下可能蘊含大量礦產──可能有2,000億桶石油與5,000億噸天然氣──而且隨著氣候變遷，極地地區逐漸撥雲見日，開採這些資源的成本可能逐年降低。[12] 隨著科技進步，《南極條約》體系規範力道逐漸不足──尤其中共對這片大陸的興趣與日俱增，美軍聯合部隊在支持維持南極獨特地位的國際行動中扮演日益重要的角色。

中共的行動、活動及利益

中共在南極大陸與周邊海域擁有數項合法目標、義務及活動。中共南極科學研究活動一直相當頻繁，並在30年間設立長城、崑崙、泰山及中山四處基地，接著2024年2月，第五個秦嶺基地開始運作。[13] 自1988年以來，中國大陸南極考察隊向南極研究科學委員會(Scientific Committee on Antarctic Research)提出以下學科的研究活動：

- 氣象學

- 電離層
- 地磁學、地質學及地理學
- 測量與製圖
- 生物學
- 人類生理學
- 海洋水文學與化學。[14]

產生有效且可靠的科學工作是在南極地區「暢行無阻的門票」(Coin of the Realm)。一個國家的科學研究數量與品質將左右該國《南極條約》協商會議的地位與影響力。[15] 只有南極地區研究與活動符合《南極條約》協商會議要求的國家，才會受邀成為協商國，而只有協商國才能投票表決組織政策與決策。[16] 1983年，中共簽署《南極條約》，並於1985年成為《南極條約》協商會議協商國。[17]

此後，中共竭盡全力與其他地區《南極條約》體系成員國建立關係，並提升南極地區行動能力與能量。中共透過官方機構中國極地研究中心安排南極大陸活動，該機構負責監督中共南極研究站各項科學研究。[18] 藉由這些努力，中共擴大參與南極治理、在戰略要地建立研究站、簽訂長期支援協議，以及藉由科學發現與站點命名贏得聲望等手段，逐步建立其國家影響力。[19] 截至目前為止，中共仍公開表示遵守《南極條約》體系制度，同意其他附加議定書與公約，並將保護範圍擴大涵蓋海洋生物資源與禁止採礦。[20]

2018年起，中共以國內法律規範人民在南極大陸行為，適用對象不僅涵蓋科學家，也包含遊客與其他民營企業。[21] 2017年第40屆《南極條約》協商會議期間，中共首度發表名為《中國的南極事業》白皮書，該文件指出：「中國政府一貫支持《南極條約》的宗旨與精神，堅決維護《南極條約》體系穩定。」[22] 鑑於中共公開支持南極事務，簽署諸多具法律約束力的協議，中共堪稱是支持《南極條約》體系制度與遵守國際規範的模範生。

國際社會對中共追求南極利益的憂心之處，非關公開政策與承諾，而是對於國際規範與協議抱持修正主義態度──由其在北極與南極地區的所作所為即可見一斑。[23] 中共在國際上的所作所為與灰色地帶政策已損及國家信譽。一帶一路倡議與對發展中國家進行強制經濟投資等發展計畫，都使中共蒙受國際批評。此外，南海與南太平洋因領土與自然資源爭議而日

益緊張，促使澳大利亞與紐西蘭等主要南極地區周邊國家檢討、修正對「中」國防政策。[24]

觀察人員發現，中共未經同意架設衛星地面站、高頻雷達站及興建疑似為軍事用途的飛機跑道，這些行徑加深各國擔憂。其中，多數工程位於阿戈斯冰穹(Dome Argus)的崑崙站──南極大陸最高處，可一覽無遺極地軌道上所有衛星。[25] 紐西蘭坎特布里大學(University of Canterbury)政治與國際關係學教授暨南極門戶研究中心(Gateway Antarctica)研究助理布雷迪(Anne-Marie Brady)表示，過去20年來，中共皆未依要求，每年定時向《南極條約》協商會議提報共軍南極活動概況。[26] 布雷迪列舉兩項實例，首先是2007至2008年，共軍專家前往南極大陸建立首座高頻雷達站，接著是為中共北斗衛星系統建造地面站。[27] 中共均未將前述兩項活動納入《南極條約》協商會議正式報告。儘管《南極條約》並未明文禁止這些活動，但也確實顯示中共企圖在科學研究站部署軍民兩用關鍵技術，過程中行事低調，避免引起國際社會關注。

2023年3月3日，美國海岸防衛隊破冰船北極星號完成部署任務、支援2023年深凍行動(Operation Deep Freeze 2023)後，接續造訪美國的南極央凡爾島(Anvers Island)帕麥研究站。

(Source: US Coast Guard/ Aidan Cooney)

《南極條約》體系第七條律定，落實《南極條約》體系，仰賴觀察員自由進入南極大陸研究站、設施與裝備、所有船舶及飛機等區域，以及進行空中觀察及發出必要探勘通知。[28] 實際上，惡劣氣候與會員國進入限制繁多，就算突擊檢查確認科學研究作業也極為困難。而且聯合部隊亦可如在南海或東歐一樣，利用監視裝備強化南極潛在熱點或危機事件稽核作為。此外，1985年與1998年，國際法期刊曾論及《南極條約》體系薄弱執法機制，並點出該條約可能遭到推翻或置之不理，成為鞭長莫及的灰色地帶。[29] 未來，這些問題可能關係重大，因此美國必須整合資源，強化南極地區相關作為。

中共亦試圖利用《南極條約》協商會議架構，限縮前述條

約監管機制，藉此鬆綁自身行動限制，擴大國家利益。近期，中共代表團提議在崑崙研究站建立南極特別管理區(Antarctic Specially Managed Area, ASMA)，主張額外保護基地周圍環境，限制其他國家未經中共同意與協調情況下參與活動。中共前述行動讓各國更加懷疑前述管理區的主要用途。[30] 幸好，以美國為首的主要盟友與協商國成員，拒絕中共代表團提案，防止其試圖改變南極特別管理區行為準則的行徑。[31]

除了當前應對氣候變遷相關作為與全球定位系統衛星發展外，任何相關軍事運用至少都要數十年光景才能擴及南極大陸，而禁止開礦活動的《馬德里議定書》也要等到2048年才會修正。但是，瞭解中共影響力對南部大陸的長期效應不能拖延數十年。中共建造具有軍民兩用研究站，為未來戰略重地與擁有大量海洋生物資源(亦即漁業與磷蝦)地區的影響力奠立基礎。[32]

中共透過可信與顯而易見的科學投資，強化自身南極治理地位與影響力，當作改變當前《南極條約》體系規範的敲門磚。提升國家地位與影響力有助於左右重大區域問題風向，譬如《南極條約》體系的南極海洋生物資源養護委員會(Commission for the Conservation of Antarctic Living Marine Resources)就「合理運用」一詞的解釋權。中共反對劃定全新海洋保護區，表面上是為了防止其他《南極條約》體系成員擴大領土主張。阻止增設海洋保護區也讓這些區域可以「合理運用」，包括有限度商業捕魚。[33] 除了憂心海洋生物資源，礦產資源開採方面亦令人擔憂——中共可能透過2048年《馬德里議定書》修正時建議開放南極開採，甚至可能申請提前特別修正，要求更早開放。由於修訂議定書需要四分之三協商國同意，中共長期影響力日益增長後，可透過國家威望、影響力，甚至經濟脅迫來取消或至少放鬆礦產開採保護限制。[34]

美國的行動、活動及利益

儘管許多研究戰略競爭學者直指冷戰為聯合部隊極地利益的濫觴，但真正歷史卻更綿遠流長。美國欲瞭解、投資及探索南極大陸的心願已醞釀200年之久。一位名叫帕麥(Nathaniel Palmer)的美國海豹獵人最先發現南極半島。[35] 此事促使美國國會委派美海軍威爾克斯(Charles Wilkes)上尉，率領美國探索中隊(U.S. Exploring Squadron，或稱威爾克斯探險隊[Wilkes Expedition])探察這片大陸並繪製地圖。[36] 1838年，探險隊自漢普頓錨

地(Hampton Roads)出發，繪製1,500餘浬的南極海岸線圖，發現280座島嶼，並證明南極是世界第七大洲。[37] 惟當時美國國內爆發數起事件，導致十九世紀無法從事進一步探索，但威爾克斯探險隊仍為後續80年間的16次探險活動奠定基礎。這些由澳大利亞、比利時、英格蘭、法國、德國、日本、挪威、蘇格蘭及瑞典的探險活動相輔相成，1911年，人類終於抵達南極點。[38] 這些活動也成為迄今許多國家聲索南極大陸主權的基礎。

1928年至1930年與1933年至1935年，伯德(Richard Byrd)出資進行南極探險，為美國二十世紀南極科學活動揭開序幕。第二次世界大戰期間，南極大陸研究活動停擺，但1946年至1947年，美海軍南極發展計畫(Navy Antarctic Developments Project，又名跳高行動[Operation Highjump])是目前為止規模最大的南極探險活動，總計動用超過4,700名海軍與陸戰隊人員、44名觀察員、13艘船艦及數架飛機。此次探險範圍超過100萬平方英里，其中半數前所未及，並進行空拍以利後續繪製地圖。然而，該活動建立的研究站大多不適用於科學研究。[39]

第二次世界大戰餘波及美蘇聯冷戰擴大，讓南極大陸落入全球戰略競爭範疇。到了1958年，鑑於核子衝突不斷升高，南極大陸主權爭奪不斷，再加上國際地球物理年(International Geophysical Year, IGY)小有成就，促使美國時任總統艾森豪(Dwight Eisenhower)邀請12個國際地球物理年參與國家，齊聚華盛頓起草《南極條約》。[40] 當時訂定的條約不僅有效建立南極國際規範，也排除(但未解決)各國領土與主權爭議。[41] 同樣重要的是，《南極條約》這種務實架構，可避免美蘇對抗，保留各自戰略優勢。[42] 超級大國參與及運用聯合部隊以促進美國利益的架構，已在南極驗證成功，並成為當前美「中」競爭典範。

《南極條約》與後續協定後來統稱為《南極條約》體系。這些協定塑造與鞏固美國當前南極政策，堅守下列四項原則：

- 美國不承認任何各國領土主張。
- 美國保留未來該地區運用權利。
- 南極大陸僅可用於和平目的。
- 各國都能自由從事科學研究與其他和平活動。[43]

美國根據《南極條約》體系精神與授權，責由國家科學基金會(National Science Foundation, NSF)擔任美國南極計畫(U.S. Antarctic Program, USAP)管理機構，聚焦南極科學研究。[44] 美國國家科學基金會經營三處全年無休

阿蒙森·史考特南極研究站(Amundsen-Scott South Pole Station)。
(Source: Cmichel67)

的科學研究站：麥克默多站(McMurdo Station)、阿蒙森·史考特南極站(Amundsen-Scott South Pole Station)及帕麥站(Palmer Station)。這些研究站每年平均為3,500名科學家與支援人員提供協助，研究範圍涵蓋各類學科，包括天文學、大氣科學、生物學、地球科學、環境科學、地質學、冰川學、海洋生物學、海洋學及地球物理學等。[45] 此外，研究船帕麥號(R/V Nathaniel B. Palmer)——研究能量媲美科學船隊——可容納的科學家比船員還要多。[46]

美國透過參與《南極條約》體系涉入南極事務，並由國務院海洋與極地事務辦公室(Office of Ocean and Polar Affairs, OPA)居中協調政策。[47] 該辦公室與美國國家科學基金會密切合作，每年率代表團參加《南極條約》協商會議，並與《南極條約》秘書處(Antarctic Treaty Secretariat，總部設於布宜諾斯艾利斯[Buenos Aires])保持密切聯繫，秘書處則負責《南極條約》締約國間的溝通聯繫。[48] 此外，美國海洋與極地事務辦公室根據《南極條約》第七條與《南極條約環境保護議定書》第十四條規定，檢查外國研究站、設備及入境船隻，確保所有會員國都能進入南極並強化《南極條約》體系規範。[49] 而在這些層級之下，還有許多官方的聯合、跨部門、學術及商業支援組織。

美國國防部的作戰支援組織包括：

- 聯合特遣部隊南極支援隊(Joint Task Force－Support Forces Antarctica, JTF-SFA/深凍行動[Deep Freeze])提供後勤支援，以及監督海軍、空軍、空軍國民兵、空軍後備役指揮部及海岸防衛隊人員。
- 第109空運聯隊(自紐西蘭提供LC-130滑橇式運輸機空中支援)。

- 第62空運聯隊(以C-17運輸機提供自紐西蘭至麥克默多研究站的空運支援)。
- 海岸防衛隊太平洋地區破冰船行動(航道清掃與燃料補給作業)。
- 海軍資訊戰中心(天氣預報、空中交通管制及基地作業)。[50]

然而，全政府戰略方針在南極地區似乎並非常態。跨部會行動僅限於美國南極計畫、聯合特遣部隊南極支援隊，以及其他運輸與後勤單位間的協調工作。2019年，美國太平洋空軍時任司令布朗(Charles Q. Brown, Jr.)上將指出，區域內大國競爭最後可能會蔓延至南極大陸，美國應考慮於北極與南極地區部署必要軍事能量。[51] 惟三年後，美國印太司令部的態勢，並未針對作戰司令部的戰略責任區(南極大陸)的戰略競爭，採取聯合、跨部會、跨政府及跨國的整體作為。[52]

此外，2022年，美國國防部向國會提交的《中共軍力報告書》(*Military and Security Developments Involving the People's Republic of China*)中，全書196頁篇幅僅提及南極3次。該文件提及海岸防衛隊全新破冰船，評論南極研究站太空支援能力，僅用三句話簡單帶過中共不斷增加地區能見度與調整戰略。[53] 相較之下，報告中有194次提及臺灣、45次提及一帶一路倡議、40次提及南海，南極大陸在美「中」全球競爭中似乎鮮少獲得關注。[54]

號召行動

過去50年，以科學研究需求為基礎的美國南極計畫對美國的貢獻卓著。目前，中共不斷挑戰國際秩序既有規範，美國必須重新審視原有做法。首先，美國政府各部會首長應體認，中共將南極大陸視為沒有主權歸屬的灰色地帶。[55] 其次，儘管北極與南極氣候相似，但國際地位卻截然不同。南極大陸事務遵循《南極條約》體系，而北極則受《聯合國海洋法公約》(*United Nations Convention on the Law on the Sea*)管轄。美國政府必須以不同方式應處。

2022年，美國國防部成立北極戰略與全球韌性辦公室(Arctic Strategy and Global Resilience Office)，確保美國北極利益。[56] 若美國政府採取相同思維，南極事務恐將分散美國力量，因為此舉代表美國對南極具有軍事目標。鑑於美國受《南極條約》體系規章約束，國務院海洋與極地事務辦公室自然會繼續居中協調美國南極政策。依據美國國務院政策，國家科學基金會主導美國南極計畫，遂行常態性活動，聯合部隊應如何透過全政府

方針進行整合，以確保長期戰略競爭要素，為未來預做準備？

萊克(Art Lykke)戰略理論說明目的、方式及手段間的「三腳凳」關係，一旦失衡必會產生風險。[57] 而美國在南極運用類似架構時，卻只有國家科學基金會美國南極計畫、國務院海洋與極地事務辦公室兩項要素。以美國國防部當作架構中的第三足，將軍事觀點納入政策與研究，將有助於避免美國未來利益面臨戰略風險。國防部可提供反對修改南極國際規範的獨特觀點與資源，除了能夠觀察與識別惡意行為，還可瞭解全盤戰略場景。此外，聯合部隊能夠訂定應變計畫，並可依環境變化與任務優序滾動式調整相關計畫，這是國務院或國家科學基金會所欠缺的能力。美國總統辦公室的科技政策辦公室(The Office of Science and Technology Policy)負責內閣層級南極議題的討論，並提供總統相關決策資訊。[58] 該諮詢部門可藉多方討論，整合研究、政策及軍事觀點，納入美國決策資訊。

執行層面，則可建立美國聯合部隊與南極地區利害關係人的直接聯繫管道。例如，聯合特遣部隊南極支援隊與國家科學基金會相距數千英里，且兩者之間有諸多官僚機構。儘管國家科學基金會極地計畫辦公室有兩個軍職職務(空軍國民兵與國防部聯絡官)，但該辦公室位於國家科學基金會地球科學局(Geosciences Directorate)內，導致聯絡官無法向國家科學基金會領導階層傳達戰略競爭資訊。

為提升行政效率，美國聯合部隊應向美國國家科學基金會主任辦公室及美國國務院海洋與極地事務辦公室派遣更多聯絡官。建立更健全的聯絡機制亦符合美國總統第6646號南極相關事務備忘錄(President’s Memorandum Regarding Antarctica)的要求。[59] 如此一來軍人就能即時向部會主管說明南極行動的戰略意涵，並就南極大陸周邊相關行動訂定跨部會因應措施。這些國務院增設職務可強化軍事顧問功能，並聚焦戰略競爭與聯合部隊協助跨部會工作能力。

儘管上述三足鼎立做法可降低風險，但與其他《南極條約》體系成員進行戰略合作，亦可確保美國國家利益。長期以來，美海軍與美空軍不斷戮力支持研究工作。如前所述，1946年至1947年，海軍跳高行動支援部分初期南極科學研究，該行動積極促成水文、地理、氣象、地質及電磁領域研究。[60] 這些軍事研究支援可當成美軍與他國軍隊合作窗口，極具價值。藉由軍方協助的研究與《南極條約》體系成員攜手維護共同利益，合作雙方都能更瞭解南極大陸活動，也有助於建立雙方互信。

美國特別適合此種做法；目前29場《南極條約》協商會議中，有16場係與美國有同盟關係的盟友舉行，而其他幾場大多是與聯合部隊有密切軍事關係的長期合作夥伴。[61]《美國國家安全戰略》與《國防戰略》皆強調強大盟國與夥伴國是打擊世界獨裁主義的主力，也是維護世界秩序的基石。因此，加強美國與《南極條約》體系成員邦誼，將有助於避免違反現行體制或試圖改變南極大陸科學研究的不當舉措。[62]

未來，南極大陸也是美「中」良性互動的媒介，藉此建立互信，共享《南極條約》界定的中立地理區。然而，當前國際局勢不斷升溫，這種互動看似遙不可及，但冷戰期間美蘇也採用類似溝通機制，有效應對危機與研議軍備管制。1958年《萊西－扎魯賓協定》(*Lacy-Zarubin Agreement*)被視為穩定冷戰局勢的關鍵，該協定透過科學與技術交流促進人際關係、降低敵意，以及鋪陳後續外交作為。[63]

美「中」若以南極科學支援名義進行軍事合作，即可讓各國瞭解現況，體現科學至上宗旨，並確保軍事行動皆以和平為目的。這些合作行動亦符合南極與《南極條約》體系相關規範，確保各國國家利益。許多研究站的補給任務必須仰賴軍方運輸裝備、破冰船及天氣數據。上述任務可透過多國行動付諸實行，美「中」武裝部隊也能互相合作，攜手支援南極科學研究。前述研究環境杳無人跡且有國際監督，這樣一來，不僅可促進雙方合作，也能避免北冰洋軍事競爭的類案再現。

結語

美國在南極大陸必須降低風險，避免他國強化影響力企圖改變現狀，也應把握南極獨特地位，掌握契機。2022年，《美國國家安全戰略》提到：「除非美國瞭解競爭日益白熱化如何衝擊合作，以及合作的需求如何影響競爭……否則美國無法在大國競爭勝出。美國未來戰略不僅要能處理這兩項問題，還要能瞭解彼此關係並相應調整戰略。」[64]

近期，中共戰略亦提倡「人類命運共同體」與「為解決世界問題貢獻中國智慧與力量」等構想，同時還指出「中國二十一世紀的重要目標就是實現民族復興，建設現代化強國」。[65] 惟中共未在官方聲明中提及的是引領「人類共同未來」，改變現狀以符合中國利益。[66] 美「中」雙方不僅意識到，雙邊合作才能解決跨區域問題，同時亦受困於大國競爭影響與限制，尤其印太地區緊張局勢升溫導致情況更加惡化。中共對美國圍堵政策有所

顧忌，而美國則對中共以修正主義與專制獨斷處理區域問題感到憂心。此情況導致世界各國專注針鋒相對的議題，大幅減少實現世界共同體與穩定外交交流的相關作為。

鑑於政策與行動為現行國際秩序與規範的基礎，美國必須在既有架構內維護國際規範與確保自身南極利益。無論是明天、2048年或是更遙遠的未來，美國都必須採取行動，確保其他國家保有自身利益，享有行動自由。結合美國國務院、國家科學基金會及國防部等三大支柱的全政府方針，整合《南極條約》體制資源，以確保美國南極政策、南極科學研究及國防部戰略行動相互支援，俾杜絕惡意影響，以及防範有心國家片面毀約。面臨左右南極大陸命運的時刻，美國至少必須確保各國能夠透過選票維護自己利益，不受中共左右或脅迫，並避免中共在當地的活動弱化國際決策。

過往，美國對南極戰略競合並不陌生。冷戰期間，《南極條約》協商會議成員透過強化科學主權、獻身南極和平利用及承認《南極條約》體系合法性等方式，避免南極大陸衝突與促進合作。儘管冷戰後，美國可能不再聚焦前述重點，若能同心協力，美國仍坐擁必要機構、政策及資源，即可再次實現此一目標。中共試圖合法化以自身為中心的修正主義作為，主導南極國際治理主導地位，此舉已對《南極條約》體系構成全新威脅。[67]

在美國過往70年的領導下，鑑於多數《南極條約》協商會議成員皆對科學合作、增進人類福祉及和平利用南極做出深遠承諾，《南極條約》體系已備妥應付中共的諸般作為，但也容易受到現代戰略競爭的衝擊。總而言之，南極大陸的戰略地位，端賴美國是否有能力整合官方作為，激勵與引領包含中共在內的國際社會，共同實現南極合作願景。

作者簡介

John B. Kelley美空軍上校為美空軍空中機動司令部(Air Mobility Command)安全主任。

Christopher J. Sarton美海軍中校為聯合與聯盟作戰學校(Joint and Combined Warfighting School)第二階段聯戰專業軍事教育(JPME II)教官。

Scott A. Curtice美陸軍少校為國防威脅防治局(Defense Threat Reduction Agency)大規模毀滅性武器反制計畫官。

Charles C. York III美陸軍少校為美軍運輸司令部聯合機動官(Joint Mobility Officer)。

Reprint from *Joint Force Quarterly* with permission.

回目錄→

(Source: USAF)

● 作者/David Roza ● 譯者/余振國 ● 審者/丁勇仁

搜救與高端作戰，孰輕孰重？

Rescue and the High-End Fight

取材/2023年5月美國空軍暨太空軍月刊(Air and Space Forces Magazine, May/2023)

這就如同過去20年裡美空軍的搜救任務：會有兩架HH-60G鋪路鷹(Pave Hawk)直升機在沙漠上空低空飛行營救地面人員，而兩架A-10疣豬(Warthog)攻擊機則是同時在上空盤旋，以提供空中密接支援(Close Air Support)，還有一架HC-130J負責指揮和管制。

2023年2月，當時搜救人員正於內華達州測試和訓練場接受訓練，相關訓練一部分是友軍「藍軍」部隊對戰敵方「紅軍」飛機模擬空戰，以及另一部分是紅旗 23-1 操演(Red Flag 23-1)模擬地對空威脅。第55救難中隊飛行員特納(Timothy Turner)上尉表示，他們參與的部分是：「我們如何在大規模空戰下戰鬥，以及我們如何在具有高度防禦和威脅環境中執行人員救援(Personnel Recovery)」。

過去20年來，美空軍在伊拉克、阿富汗及其他地區的反叛亂衝突中多次運用鋪路鷹直升機執行任務。但在這些戰鬥中，敵人並未取得制空權，如果美國與中共或俄羅斯發生衝突，那麼情況就不會是這樣了，因為這兩

個國家都擁有先進的戰鬥機及地對空飛彈系統。

2022年，美空軍部長肯達爾(Frank Kendall)在決定要削減空軍搜救直升機數量以汰換鋪路鷹機隊後指出：「當我們進行反叛亂行動時，在此種情況下我們會失去飛行員，現在需求已有所不同。」肯達爾同意將HH-60W快樂綠巨人2式(Jolly Green II)直升機的採購計畫削減成為75架，而不是原計畫的113架，之後國會將採購總數提高到85架。

肯達爾在某次接受《美國國防新聞週刊》(*Defense News*)採訪時表示：「就是有些地方你不會乘坐直升機，在那個現實狀況中，乘坐直升機根本行不通。」

直升機飛行高度低、速度緩慢，沒有吸收雷達波的匿蹤能力，很容易成為整體防空系統目標，而且其航程不足以跨越印太戰區。

HH-60兵器官兼美國空軍暨太空軍協會(AFA)米契爾航太研究所(Mitchell Institute for Aerospace Studies)國防研究員金瑞(Michael Kingry)中校在航太優勢(Aerospace Advantage)播客(Podcast)上表示：「如果開戰第一天你在臺灣海峽駕駛直升機，那裡會是一個非常危險的作業地點。但同樣地，在西太平洋上也沒有什麼神奇的界限，如果你跨越了這條界限而且又不是駕駛第五代戰鬥機，那就可能立即遭到攻擊。」

事實上，美空軍搜救人員認為，若有適合的設備，HH-60W可以有效地擔任太平洋作戰中的偵察工具、通信中繼站點、運輸工具、武器平臺及救護直升機。但是，這需要較多的支援並減少的官僚的干涉，該裝備才能在戰鬥中發揮潛力。搜救人員表示，這個平臺依然還有升級的空間。

HH-60G兵器官兼第305救難中隊指揮官麥克唐納(Brough McDonald)中校在接受《美國空軍暨太空軍月刊》(*Air & Space Forces Magazine*)採訪時問道：「為什麼我不在我的直升機上安裝火箭、飛彈和非動能作戰裝置呢？」他說：「直升機和救難機隊有機會最大限度地提高整體戰鬥空軍的殺傷力與存活力。如此一來不是只有戰鬥人員保護我，而且還包括『我能幫戰鬥人員做些什麼？』」

沒有跨不過的海洋

美空軍搜救人員常面臨的問題是距離，他們曾經從離岸數百英里的船隻上救起人員，涵蓋範圍如同美國大西洋沿岸到西非的部署區域。

HH-60G兵器官洛薩克(Brandon Losacker)中校表示，即使是戰鬥機也需

要空中加油才能飛越太平洋廣闊的空域。雖然HH-60W不補充燃油的作戰半徑比戰鬥機短得多，但直升機不需要跑道即可著陸，這代表操作人員幾乎可以在西太平洋數千個島嶼中的任何地方設立補給站。

美空軍第33救難中隊的HH-60G鋪路鷹搜救直升機可提供戰鬥搜索和救援能力，協助確保日本防禦能力，並維持印太地區自由與開放。圖中所示為第33救難中隊於2023年4月從日本沖繩北部的一個偏遠著陸區出發執行訓練任務。

(Source: Raymond Geoffroy)

洛薩克說：「這為我們提供了遠距離行動的靈活性，可以配合參與較大規模的空中戰役。只要有一塊露出海面的岩石，它大到足以讓HH-60著陸，那麼這裡就可以成為警戒位置。」

美空軍搜救人員曾經在防空威脅下營救作戰人員。越南戰爭期間，雷達導引的防空火砲、地對空飛彈及近距離小型武器火力都是實質威脅，然而空軍搜救人員仍然利用精湛的技能設法成功營救了3,883人。1992年，歷史學家小蒂爾福德(Earl Tilford Jr.)在《東南亞搜索和救援》(*Search and Rescue in Southeast Asia*)一書中將此歸功於「科技進步、創新及想像力」。

麥克唐納還指出，即使在今天，直升機機組人員通常還是會解救遠離目標區域的倖存者。

麥克唐納解釋道：「飛行員從飛機上逃脫跳下的地方，就是我要去的地方。前往這種地方所遇到的問題，與開戰第一夜在中國海灘上遇到的問題有所不同。」

不再孤單，也不再害怕

由於沒有飛機可以獨自完成所有任務，所以美空軍會使用其他類型飛機形成戰力組合來掩護所有盲點。在紅旗操演中，戰鬥機提供空中密接支援，其他機種負責指揮和管制，而HH-60則負責艱辛的搜救行動。

特納說：「大家都已知道過去20年來是如何執行搜救，但現在所遭遇的衝突與我們在紅旗操演中模擬的完全不同。我們

可能無法單槍匹馬、無所畏懼地完成任務。我們需要融入整個美空軍的保護傘下，以大型團隊的方式採取行動。」

儘管如此，直升機機組人員還是有一些技巧可用來應付先進的威脅。麥克唐納說：「雖然我所飛的並非低可偵測性機種，但我們的飛行高度很低，這在做法上不一樣。敵人先進的現代長程地對空飛彈(SAM)，它們是用以攻擊高空飛行的超音速戰鬥機。此種防空系統，並不適用於飛行速度如同高性能摩托車及飛行高度略等於地表植被的直升機。」

麥克唐納表示，事實上，美空軍搜救直升機機組人員刻意藉美國最先進的雷達實施訓練，來將自己的生存能力提高到最大。快樂綠巨人二式經過改良的雷達警示接收器套件，可以較快地為機組人員提供更多資訊，加快他們的決策速度，並使他們在對抗敵人時更具優勢。

然而，新型HH-60直升機戰力仍有進步空間。雷射干擾器可以對付紅外線導引威脅，而電子反制措施莢艙可以擾亂對手通信，並有助於將直升機隱藏在無線電雜波中。美空軍在建造HH-60W直升機時沒有為上述裝備提供機身外部掛載點，洛薩克認為這是「一個嚴重的設計疏忽」。但這些直升機還是可以透過添加掛載點來支援此類設備。

洛薩克說：「我們沒有尋求創新的方法來使用現有科技，而是透過相對廉價的改進方式來提高我們現役平臺的存活力。還有許多科技沒有妥善利用。」

「以空軍的方式處理問題」

美空軍官員認為85架的快樂綠巨人二式機能提供足夠搜救能力。

美空軍發言人史堤芬尼克(Ann Stefanek)說：「透過提供國防部唯一的專門戰鬥搜索和救援部隊，空軍致力於支援聯合部隊的人員搜救。隨著國防部將注意力轉向針對同級對手，空軍被迫要為其優先項目做出困難決定，但空軍相信計畫中的85架直升機機隊未來可為美軍提供必要戰力。我們是根據在與近乎同級競爭對手發生衝突時的需求來構建未來部隊。」

為了一場不同類型的戰爭進行準備，美空軍正在探討如何訓練飛行員在前往較不具爭奪性的接載地點時，能夠長時間獨自生存。美空軍也在物色自主電動垂直起降(Electric Vertical Takeoff and Landing, eVTOL)飛機，這種飛機可能會用來搜救被擊落的飛行員，而不會使空軍搜救人員身陷危險之中。

2022年11月，一架美空軍HH-60G鋪路鷹直升機在美國中央司令部責任區內執行直升機空對空加油（Helicopter Air-to-Air Refueling, HAAR）任務，從一架隸屬於第1遠征救難大隊的HC-130J戰鬥王二型機接收燃油。鋪路鷹直升機的主要任務是在敵方環境中不分晝夜進行人員搜救行動，以便在衝突期間救回陷入敵區人員。直升機空對空加油作業可延長部隊的作戰時間，使搜救裝備能在空中滯留的時間更長。(Source: Daniel Asselta)

但無人救難載具可能無法接載受傷飛行員，而且自主電動垂直起降平臺可能還需要再等幾年後，才會被軍方視為有能力去執行這種任務。

麥克唐納說：「我們目前唯一有的，就是這型老但實用的載具了。這是我們唯一的選項。所以那種『該型機存活度不高』的批評……難道要我們在接下來20年或更久都沒有任何可用的搜救飛機嗎？」

電子反制莢艙、輕型導引火箭及雷射干擾器有助於HH-60W直升機減低先進威脅的傷害，但這些裝備可能只是這類升級的開端。

麥克唐納說：「如果能採用創新的想法，並以美空軍與空軍官兵的觀點來處理問題：讓這架飛行器在面對殲-20(J-20)、薩姆-20防空飛彈(SA-20)時能夠存活。嘿！兵器官，擬定新戰術；工程師，發揮創意。最後你會發現，『哇，我們能創造出真正有搞頭的東西了。』」

與過去呼應

洛薩克認為問題不在於這種直升機無法執行任務，而是美空軍沒有盡

力提供裝備使其發揮功能。洛薩克說：「空軍現在已經陷入了循環論證，他們認為直升機無法存活，所以沒有對其存活力進行足夠投資，這造成直升機無法存活的觀點似乎是事實。」

這種模式就曾經發生在美空軍搜救圈。2019年，洛薩克在空軍大學發表的一篇論文中指出，空軍在韓戰結束後，因為認為核戰不需要執行傳統搜救，就將搜救人員從1萬2,000名飛行人員刪減成1,465名。空軍之後在越戰期間倉促重建搜救勤務，但其後在考慮與蘇聯開戰時，讓搜救勤務又再次萎縮。

《沙漠風暴作戰中的戰鬥搜索和救援》(*Combat Search and Rescue in Desert Storm*)一書中記載，1980年代中期，美空軍委員會曾決定不購買用於搜救計畫的HH-60，一名軍官回憶起此事時說道：「當時我說『等一下，你們這麼做會嚴重傷害到搜救勤務。』委員會的人回復：『如果我們把所有的錢都拿去買H-60，就沒有錢購買戰鬥機，這麼一來也就沒有任何戰鬥機飛行員需要被解救。』所以HH-60就沒了。」

美空軍從1982年開始採購MH-60G用於特種作戰，後來又添購HH-60G用於搜索和救援。現在隨著鋪路鷹機隊的使用壽命已接近終了，其接替裝備也面臨類似的困境。

2019 年，洛薩克寫道：「美空軍內部有一個強烈的想法，認為在未來與同級對手發生的任何戰爭都會是極度致命的，而導致不用執行戰鬥搜救(Combat Search and Rescue, CSAR)。」但是，他認為：「我們有義務做出有搜救意願的姿態，並為我們的飛行人員提供援助。」

麥克唐納也同意，數學總是很難證明其合理性。他說：「如果這是一個保險的價值主張，這並不合理。如果桌上有1美元，你會用來製造一架無法被擊落的噴射機，還是不要製造噴射機，而投資搜救部隊以執行任務？」

麥克唐納建議不要將戰鬥搜救視為一種保險，而是將其視為美空軍戰力套裝系統中多功能且支持空中戰力的元素。直升機可以充當「天線農場」，在敵飛彈射控涵蓋範圍內將資訊轉發至定翼機；直升機可以在簡易基地防禦時提供火力支援；直升機可以協助應處大規模傷亡，就如同2020年伊朗飛彈襲擊期間在伊拉克所做的那樣。麥克唐納指出，幾十年來，空軍搜救直升機在美國中央司令部的作戰區域中已經證明了其多用途能力，其中包括最近該司令部充當彈性戰鬥部署(Agile Combat Employ-

鋪路鷹直升機在過去的20年裡一直頻繁出勤，但美空軍領導人擔心該裝備無法在與中共或俄羅斯的戰鬥中存活。圖為2022年8月，第301救難中隊的HH-60G鋪路鷹直升機在「遠方地平線」(Distant Horizon) 演習期間，自夏威夷布拉德肖陸軍機場(Bradshaw Army Airfield)起飛。(Source: Darius Sostre-Miroir)

ment)的測試實驗室。

「我們需要做出決定」

搜救座右銘──「我們所做所為，都是為了讓他人活下來」──這是美空軍搜救人員要牢記在心的。

特納說：「我們不會放棄任何人。如果今天沒有成功救回，我們明天、後天會再嘗試去救。我們一定會繼續努力，並以此為傲。」

洛薩克表示，如同美陸軍及美海軍醫護人員，都會與美陸戰隊人員並肩作戰，但是美空軍搜救人員並非如此，陸軍派遣步兵執行任務時醫護人員會陪同實施支援，陸戰隊員無醫護人員陪同亦不可單獨部署。洛薩克補充道：所以，對空軍而言，不能在沒有搜救人員支援情況下，派遣戰鬥機飛行員與中共戰鬥。

洛薩克說：「如果我們領導階層的評估是搜救團隊無法運作，然後呢？

如果不是我們，那麼是誰？」

洛薩克認為美空軍搜救與攻擊戰鬥單位願景應該擁有足夠的資金和授權以探討現有的實驗科技，其中包括電動垂直起降航空器，並將之運用於重大演習進行測試，以加速開發及節省多年試驗。

洛薩克表示：「如果我們想提高速度來滿足需求，那麼就必須做出深思熟慮的決定，來接受更大的風險。」洛薩克認為可以透過挑選非常成熟、經驗豐富的飛行員加入這樣的單位來降低風險。

麥克唐納說：「我的同袍們，他們不是輸家，他們也不服輸。如果只發給他們打包繩和泡泡糖，他們也會自己想出完成任務的辦法，因為我們這行就是這樣。我想我之所以會為此感到苦惱，因為我知道我們的任務派遣和要求，以及與同級對手作戰的狀況和結果，儘管如此，你們還想減少裝備採購數量？」

美空軍預算戰略是以造成敵人的傷亡為主，但洛薩克堅定地認為，搜救仍是減少空軍人員傷亡且保護被擊落空勤人員的重要能力。

洛薩克說：「判斷一個國家認真備戰的關鍵指標，就是該國將野戰醫院及血庫派遣支援前線。空戰也是如此。除非你表明已經準備好並願意流血犧牲，否則一切都只是空洞的劍拔弩張表象，幾乎沒有一點真正的嚇阻力。」

回目錄→

美陸戰隊軍官候補生兼律師Alexander L. Nowinski在美國加州沙加緬度募兵站留影。陸戰隊律師須完成法學院、軍官候補學校及後續培訓，方能執業。
(Source: DVIDS)

● 作者/Sean K. Price ● 譯者/黃文啟 ● 審者/黃坤銘

美陸戰隊辯護律師制度簡介

Marines Defending Marines: Why Marine Defense Counsel Are Essential to the Marine Corps Justice System

取材/2024年3月美國陸戰隊月報(*Marine Corps Gazette*, March/2024)

2023年8月3日，美軍上訴法院(軍法體系中的最高法院)因美陸戰隊一般軍事法院影響實體權利，駁回殺人罪判決。[1] 上訴法院此舉係因某位陸戰隊上校違犯被告選任辯護律師的權利。在此情況下，「駁回」意指軍事法院將永遠無法進行審判程序，委員會成員(陪審團)也永遠聽不到證人對於事情發生始末的證詞，也無法做出終局判決。不僅如此，由於這項駁回是「實體權利受到影響」，所以不會有終局判決，原因是政府不能重啟軍法審判。起訴動作劃下句點且永遠結束。這對於軍法制度而言就如同是A級意外事故或船隻擱淺。審判前，因為政府不當舉措導致一項受到高度關注的殺人案被駁回，證明陸戰隊軍法體系真的出了嚴重問題。

畢竟，一個無法透過審判程序裁定非法殺戮(殺人罪)控訴──不論結果

為有罪或無罪──的司法體系，就沒有資格稱之為司法體系。以非法手段取人性命，咸認為人類最嚴重的犯罪行為，而設立司法制度的初衷就是為了審判此種罪行。正因為美陸戰隊從事合法殺人工作，一套無法裁定軍人致人於死行為是否合法的軍法制度，就已經完全背離設立宗旨：換言之，未能履行《軍事審判教則》(*Manual for Courts-Martial*)所闡明「為武裝部隊伸張正義、嚇阻不當行為、促進合宜責任歸屬、協力維護良好秩序與紀律，進而提升軍事體制效率與效能，最終達到強化美國國家安全目的」之責。[2] 然而，悲劇卻真的發生了。陸戰隊軍事法院對嚴重犯罪行為的判決，在委員會成員尚未聽取案情事證前就被駁回，就只因為某個陸戰隊軍官沒有尊重被告尋求辯護律師的權利。

在美國訴吉爾美(United States v. Gilmet)的個案中，一個擔任軍法官的上校對被告辯護律師(一名陸戰隊上尉)表示，美陸戰隊辯護律師「可能自認受到法律保護，但其實並非如此」。[3] 這名上校還說，「你認為自己得到保護，但那不過是個法律虛構故事」。[4] 接著這名上校還告訴被告辯護律師，「我知道你的身分與你承辦的案件，你也沒有得到保護」。[5] 最後，這名上校在結束前聲稱，因為美陸戰隊軍法官人數少，晉升委員會以後會知道辯護律師「做過」什麼事，長此以往，那些擔任辯護律師的軍官都無法順利晉升。[6] 這個事件發生在2021年11月，就在軍法審判預定開始前。這名上校言談中明確點出，那些表現優異的軍法官辯護律師，未來發展都會受限──軍法官反倒應該不要認真辯護，想方設法儘快結案才是上策。

美陸戰隊辯護律師與美國其他辯護律師一樣，都有責任「在辯護期間忠於委託人、展現超然專業……最終仍須為當事人爭取最大利益」。[7] 這項為當事人爭取最大利益的職責，完全不考量美國政府、陸戰隊或任何特定指揮部利益，就是擔任陸戰隊辯護律師這項工作與軍種內其他職務截然不同之處。美國國會與各軍種都明文規定，所有軍法辯護律師都應受到保護，方能安心為當事人爭取最大利益。然而，在這個案件中，一名擔任軍法官的陸戰隊上校竟公然宣稱這些保護措施純屬「法律虛構故事」──亦即辯護律師保護僅限於書面形式，實際上根本沒有。因此可想而知，被告自然會擔心上尉辯護律師不會為自己爭取最大利益。

就軍事檢察官而言，他們未能說服軍事法院審判長，這名上校的行為不會造成被告辯護權利受到損害(「合法權利受到損害」是法律名詞)。

[8] 因此，2022年2月，軍事審判長依據軍法，以合法權利受到損害為由駁回所有控訴罪名。[9] 2023年8月(近18個月後)，美軍上訴法院支持這項裁定。因此，殺人罪將永不審判。未來完全不會有任何軍法法院會對這個案件真相做出最後判決。

美陸戰隊軍法官擔任辯護律師，在軍法體系中扮演要角。(Source: Santiago G. Colon Jr.)

這個結果對美陸戰隊軍法體系有何意涵？對於被告而言，這可謂是某種形式的勝利(此人遭到控訴數年，但最後不會有任何判決結果)。[10] 但就另一方面而言，尤其是對美陸戰隊與軍法界來說，卻形同遭到起訴。陸戰隊軍法體系無法處理一起眾所矚目的極端嚴重案件，只因為某位陸戰隊軍官違反美國軍人應得到有效辯護的憲法賦予權利，而這名軍官必然曾宣誓支持與捍衛美國憲法，甚或可能多次參與類似宣誓儀式。本文並不關切美國訴吉爾美案遭駁回後是否會翻案──美軍上訴法院已對本案做出裁定，而美國政府也未向聯邦最高法院提出上訴。美軍上訴法院並未裁定，這名陸戰隊上校的個人說法，並非只是個人對陸戰隊辯護律師工作的觀點，反倒側重這名上校言詞對於被告與辯護律師關係的損害。[11]

美陸戰隊辯護律師是否真的普遍因為充分辯護，導致個人職涯發展受限，本文並不打算深入探討這個實務問題。當然，這個問題還是十分重要。不過更重要的問題是，此種情況是否真該如此。奉派為陸戰隊員辯護的律師，將因為在工作上表現稱職而衝擊個人職涯發展，真的應該是如此嗎？答案是否定的。陸戰隊需要──且應當獲得──稱職的辯護律師。

基本上，美陸戰隊員應重視與尊重優良辯護工作，理由有二。其一，美國司法體系(包含軍法體系)有賴稱職辯護律師才能發揮功能。因此，陸戰隊若無稱職軍事辯護律師就無法成為真正的軍法體系。其二，陸戰隊辯護律師身負憲法義務，必須

確保當事人最大利益。希望某個陸戰隊軍官不要善盡法律職責，反而從事職務以外的工作，完全違背自身原則。

美國司法體系辯護律師職責

美國刑事司法體系的基本理念為，被告可在律師協助下，針對政府控訴為自己辯護。此項權利明確載入憲法條文。美國憲法第六號修正案敘明：「在所有刑事起訴案中，被告應享有權利……聘請律師協助為自身辯護。」求助律師在本質上是十分寶貴的基本個人權利，同時也可協助確保政府採取正確行為，並確保法院針對特定案件獲致正確結果之功能性目的。由於美國司法體制是源自於英格蘭「彈劾主義制度」，與歐洲大陸的「糾問主義制度」截然不同。

彈劾主義制度仰賴檢辯雙方的有效攻防。因此，審判前數週到數月間，檢方與辯方會充分調查案件內容，避免讓對方在審判過程取得戰術優勢(事實上，頂尖檢察官與刑事調查人員通常都會針對辯方如何反制特定論據或證據項目進行兵棋推演，並據以強化調查成果)。針對法院參考確定罪刑的事項，都會傳喚證人、蒐集證據，以及審前申請的辯論。開庭聲明與結辯論點都會經過演練與修訂。對於檢辯雙方而言，那都是極度耗時且激烈的過程，但雙方都是受彈劾主義制度驅使，必須尋找與探究終局判決有關之所有證據。正因為此種檢辯攻防，才能確保法院可以取得做出此項判決之全部證據。

有時可能因為證據明確，抑或政府提供的審前判決十分寬大，甚或兩者同時存在，使得被告決定接受協商以終結案件。在此種案件中，被告志願協商的合法性，取決於被告是否依據律師案件調查與審理風險評估結果所提供之最佳建議。同時，也有可能是因為辯方審理前所發現的證據或問題，導致檢察官無法起訴被告，進而放棄個案。因此，專業獨立且為被告爭取最大利益的辯護律師，不但是為被告服務，同時也幫助政府省下無意義的審判時間與花費。然而，若是無法在審理前達成協議，接續就會由軍事審判官或審判委員會組成的軍事法院進行審理。

審理過程中，負有說明被告犯罪事由職責的軍事檢察官必須提供證據，包含證人證詞與證物，說服法院起訴罪名罪證確鑿。辯護律師可以對檢方證人提出後續質問(交叉詰問)，以發掘其中不合理，檢驗證人記憶精確性與回溯事件的能力，同時舉證不利於政府控訴的事實。接著辯護律

師可以(但非絕對必要)提出辯方立場(這是辯護律師可以獨立取得證據的理由。事實上，美國憲法第六號修正案保障被告有權「以義務性程序傳喚對其有利之證人」)。當檢察官與辯護律師對法官或陪審團提出證據後，雙方都有機會說明證據意涵──哪些證據可靠、哪些證人可信，以及法院應做出何種判決。唯有此時，法院才可判決被告是否有罪，但別忘記，依據美國憲法，除非檢方能提供毫無合理質疑的事證，否則被告都應推定無罪。

美海軍陸戰隊法律服務支援組(Legal Service Support Section, LSSS)辯護律師Peter Rush在晉升中尉後受到祝賀，其任務為協助處理日常行政與軍事司法問題。(Source: DVIDS)

這套制度的某些特點必須特別說明。首先，法院的工作並非調查案件──但這卻是歐洲式糾問主義制度的運作方式──而是依據檢辯雙方提供的證據與主張審理案件。[12] 事實上，美國司法體系因為結構性問題不能調查案件。美國司法機關(包含軍法機關)根本沒有人員與資源執行調查。真正負責取得證據呈送法院的是檢察官與辯護律師(但同樣地，辯方律師也可完全不呈送證據，而僅針對檢方證據進行辯護)。負責詰問完成宣誓的證人者，也是檢察官與辯護律師。在審理前耗時數月──有時甚至長達數年──調查案件者，也是檢察官與辯護律師。

此種檢辯攻防不僅保障法院可依據充分證據做出判決，也是確保判決結果適法性的基本要件，大眾也對檢辯雙方致力求勝深具信心。所有「必須」考量的每一項證據與論點都「已經」仔細思量，因此，檢辯雙方在審理過程都會用盡合法手段蒐集證據，支持有利論點。但若是被告沒有適合的辯護律師，這套制度就無法產生合法判決，因為那意謂著其中一方並沒有積極爭取自身權益。此種情況就彷彿拳擊手收受賄賂放棄比賽，或假想敵在兵棋推演中任由對手痛擊。假如某一方放棄競爭，就不會有人信任比賽結果的正當性。事實上，假如被告辯護律師在審理中未善盡職責，上訴法院就會駁回原判決。[13]

正如同美國司法體系其他機關，軍法體系也採取彈劾主義制度。美國國會賦予被告「指派代表為自身辯護的權利」。[14] 軍官代表美國政府擔任公設辯護人與被告的辯護律師。[15] 美國《軍事審判統一法典》(Uniform Code of Military Justice, UCMJ)進一步要求代表政府與被告的軍方律師必須「具備履行職責的相應能力」。[16] 因此要求軍法審判的檢辯雙方必須有能力為委託人發聲，不僅可履行國會要求，維護被告指派律師為其辯護之憲法權利，亦可落實彈劾主義制度內涵。

話雖如此，但軍隊畢竟是(必然是)一個階級制度組織。一名低階士官兵怎麼會對中尉或上尉軍法律師有信心，認為律師能為自己挺身而出，對抗高階軍官，包含將被告移送法辦的直屬指揮官？但這確實正是許多軍職被告一開始對律師與當事人關係的感覺。所以，美國國會也顧慮到這種情況：《美國軍事審判統一法典》嚴禁使用「未授權手段……影響軍法審判」。[17] 軍事法院應該透過彈劾主義程序，依據法律與證據做出判決，不得因為外在行為者(或許位居高位者)以非法手段介入，影響審判過程、左右判決結果。

為達此目的，美國國會亦明文禁止使用晉升或派職為手段，阻止該名軍官善盡辯護律師職責。[18] 國會深知，每位軍事辯護律師均隸屬各軍種，因此，若是辯護律師善盡職責反倒會遭受懲罰，則無法適切捍衛當事人權利，並在彈劾主義制度中充分參與競爭──當然當事人也相信委任律師會全力辯護。吉爾美案中，那位上校的說詞恰好突顯這個問題。

回顧吉爾美案，那名上校告訴辯護律師，法律只不過是一種形式。上校說詞中提到：「你認為自己得到保護，但那不過是個法律虛構故事。」[19] 這段話的背後意涵是：「如果你積極為當事人辯護，就會惹禍上身，不論美國國會或憲法怎麼規定。」美軍上訴法院判定，此舉侵害被告委任律師協助之權，因為該名上校「導致被告辯護律師認為，如果自己繼續積極為被告辯護，個人在陸戰隊的未來發展將受到損害」。[20] 由於美國政府並沒有即時糾正，導致彈劾主義程序不完備，因此本案不繼續審理。[21]

對一個眾所矚目的殺人案件來說，這是一個難堪結局，但吉爾美案已經結束。現在的問題是未來該如何改進。事實上，如果這名上校的說詞確實反映美陸戰隊領導幹部的想法，那真的必須有所改變。陸戰隊必須重視與尊重所有案件的辯護工作，而陸戰隊員應該擁有一組強大的辯護律師團隊提供諮詢。有效辯護工作是適切發揮陸戰隊軍法體系功能的基本要

件，想想陸戰隊指揮官使用這套制度的頻率，就可以瞭解前述制度的必要性。2022會計年度，總共召開206場陸戰隊一般與特別軍事法庭(Special Court-Martial, SP-CM)，以及113場簡易軍事法庭(Summary Court-Martial)。[22] 美海軍人數約為陸戰隊二倍，但同一時期軍事法庭開庭場次卻遠低於陸戰隊：總共只有181場一般與特別軍事法庭，以及寥寥可數的9場簡易軍事法庭。[23] 這些數字明顯可見陸戰隊指揮官非常重視軍法體系。但如同吉爾美案的判決所示，陸戰隊不應該存在那種辯護律師無法好好為當事人辯護的制度──辯護律師應在彈劾主義制度中全力以赴。

美海軍軍事法庭開庭場次雖遠低於陸戰隊，卻也透過謀殺委員會(Murder Board)整備機制，協助軍種辯護律師完成各項抗辯整備 。
(Source: USN/Ayana Pitterson)

陸戰隊員捍衛陸戰隊員

為了遵循美國國會與美國總統對於軍法體系應有稱職辯護律師的法定要求，美軍各軍種成立軍事辯護律師主管機關。陸戰隊辯護服務組織(Defense Services Organization, DSO)就是陸戰隊專責機構，負責提供陸戰隊員與任職於陸戰隊各指揮部的海軍官兵此項服務。[24] 不論任何時間，陸戰隊辯護服務組織大約都有60位陸戰隊軍法官，而因為這些軍法官都隸屬陸戰隊，所以可說是世界上最好的辯護律師──「只要允許他們善盡職責」。

現在的美陸戰隊辯護服務組織是一個新成立機關──2011年9月，依據修訂後的《陸戰隊法律行政教則》(*Marine Corps Manual for Legal Administration*)成立。[25] 這項改革「賦予陸戰隊辯護服務組織更大督導管制權限，能更深入督導所屬執行狀況，以及調整辯論律師分派權責」。[26] 這些改變是希望「有效建立陸戰隊辯護服務組織與辯護職掌的獨立性」。[27] 為達此目的，陸戰隊辯護服務組織所屬督導律師有權派遣辯護律師為特

定當事人進行辯護，[28] 督導辯護律師負責考核辯護律師，[29] 而且辯護律師的兼辦業務不可「與辯護律師法定職務與律師—當事人道德規範衝突」。[30] 陸戰隊辯護服務組織編組與保護措施，旨在確保陸戰隊員憲法與法律所賦予的權利，充分發揮獨立組織的功能。

美陸戰隊辯護服務組織成立宗旨只有一個──就是為陸戰隊員辯護，而組織信條就是「陸戰隊員捍衛陸戰隊員」。除了戰鬥任務外，沒有人像陸戰隊辯護律師那樣全心全意為陸戰隊員奮戰。這是因為陸戰隊辯護律師的使命──以及唯一的任務──就是保護陸戰隊員。對於陸戰隊辯護律師來說，「任務優先、心繫官兵」(Mission First, Marine Always)完全不衝突，因為保護陸戰隊員就是辯護律師的任務。

因此，美陸戰隊辯護律師與當事人的關係非常特殊且別具意義。在律師—當事人保密要求下，陸戰隊辯護律師與通常為低階士官兵的當事人，可以建立一種無人可比的坦誠透明互動。這種陸戰隊軍官與士官兵的關係，在其他單位是不存在的。不僅如此，由於辯護律師依法必須為當事人爭取最大利益，因此為當事人奮戰的熱誠絕對不會因顧慮體制或政府利益而受影響，完全不像其他軍官與陸戰隊員的一般袍澤情誼。這項工作獨一無二：陸戰隊辯護律師只追求一個目的──也是唯一目的──為陸戰隊員辯護。

前述目的讓美陸戰隊領導幹部就算沒有懷疑，也會多少感到有一些挫折感。陸戰隊辯護律師的職責，往往迫使其站在各級指揮官與軍法體系檢察官的對立面。但那正是辯護的特性，而非問題。陸戰隊軍法體系有賴辯護律師積極對抗，面對某位對當事人採取不利行動的指揮官與檢察官。雖然，這在某些案件中令人煩惱，但對於整個體系的正常運作是必要的。辯護律師在相關案件中使政府的意圖受挫，諸如在審判中贏得無罪開釋，其實正是軍事辯護律師為軍法體系做出最大貢獻的地方。司法體系的滔天大罪，就是將無辜之人予以定罪。

千萬別誤解。美陸戰隊所有辯護律師確實都有崇高且沉重的責任，盡力捍衛無辜陸戰隊員，但這並不代表陸戰隊各級指揮官與軍事檢察官故意追訴無罪之人。如同陸戰隊辯護律師一樣，他們也是滿懷赤誠、克盡職責且深具榮譽感的軍官，但任何政府體系都會出錯。即便所有政府機關都謹慎小心、克盡職責且為民服務，無辜的人還是可能成為被告。在這種駭人的情況下，陸戰隊辯護律師就是被告最好的朋友，也是檢察官最可怕的敵

人。

美陸戰隊辯護律師若失去領導人的尊重，以及陸戰隊辯護服務組織與《軍事審判統一法典》律定的編組與保護措施，就無法充分為陸戰隊員辯護。證諸於吉爾美案，假如陸戰隊領導高層將前述規範視為「法律虛構故事」，則世界上所有編組與保護措施都會失去意義(然而諷刺的是，吉爾美案中那位想要破壞軍法體系的上校，最終可能都會導致起訴被駁回，反倒讓被告坐收漁利)。

美陸戰隊辯護律師都是執行美國憲法所賦予職責的軍官。這並不代表各級幹部「有義務」在某些案件中同意辯護律師的立場。但各級幹部必須以開放的胸襟，認真傾聽陸戰隊辯護律師的說法並予以尊重。陸戰隊辯護律師並沒有選擇：他們「在道德上有責任」為當事人奮戰。不僅如此，若無辯護律師，各級幹部所望的司法體系也會蕩然無存。

美陸戰隊員的卓越表現享譽全球，陸戰隊軍官在為同袍辯護時也應有同樣表現。為陸戰隊官兵奮戰到底的辯護律師，正好體現陸戰隊的核心價值。任何領導幹部都不應對此大打折扣。

作者簡介

Sean K. Price現為美陸戰隊司令派赴國家地理空間情報局(National Geospatial-Intelligence Agency)研究員，曾任軍事檢察官、辯護律師及司法顧問職務。

Reprint from *Marine Corps Gazette* with permission.

註釋

1. *United States v. Gilmet*, 83 M.J. 398, 401 (C.A.A.F. 2023). 具體來說，這名被告被以「違反合法命令、非自願誤殺、過失殺人及妨礙司法等違犯美國《軍事審判統一法典》第92、119、134及131b條」的罪名。作者並未在本案擔任軍法官或督導職務。
2. United States Department of Defense, *Manual for Courts-Martial, United States (2024 Edition)* (Washington, DC: 2023).
3. *Gilmet*, 83 M.J.
4. Ibid.
5. Ibid.
6. Ibid.
7. United States Department of the Navy, *JAG Instruction 5803.1E, Professional Conduct of Attorneys Practicing Under the Cognizance and Supervision of the Judge Advocate General* (Washington, DC: 2015).
8. *Gilmet*, 83 M.J.
9. Ibid.
10. 最顯著的是，同類型的另一個案件中，兩名涉及相同事件而遭起訴的陸戰隊員，審理結

束後，殺人與傷害行為獲判無罪，此事希望顯示出本案被告原本也應該可以在審判中獲得有利判決。然而，本文並非關切相關控訴背後的事證處理過程；因為被告尋求律師的權利未獲尊重，所以這些事證也不會被採納。

11. *Gilmet*, 83 M.J.
12. 《軍事審判統一法典》確實賦予軍事審判官與軍事法庭成員有限權力，可以詰問證人甚或取得證據。UCMJ art. 46(a) (2016); MCM, R.C.M. 913(c)(1). 但此一權力鮮少使用。幾乎所有軍事法庭引用的證詞或提供的證據都來自軍事檢察官或辯護律師。
13. *Strickland v. Washington*, 466 U.S. 668 (1984); United States v. Green, 68 M.J. 360 (C.A.A.F. 2010).
14. UCMJ art. 38(b)(1) (2019).
15. UCMJ art. 27(a)(1) (2019).
16. UCMJ art. 27(b)(2), (c) (2019).
17. UCMJ art. 37(a)(1) (2019).
18. UCMJ art. 37(b) (2019).
19. *Gilmet*, 83 M.J. at 401.
20. Ibid.
21. Ibid.
22. Headquarters Marine Corps, *U.S. Marine Corps Report on Military Justice for Fiscal Year 2022*, (Washington, DC: 2022). 這是軍事法院「審判」的案件數量，意指做出有罪或無罪判決的案件，而不包含審理中或遭到駁回的案件。
23. U.S. Navy, *U.S. Navy Report on Military Justice for Fiscal Year 2022*, (Washington, DC: 2022). 2022會計年度，美陸戰隊常備部隊總編制為17萬6,556員。*USMC FY22 Military Justice Rep.*, 15. 2022會計年度，美海軍常備部隊編制員額則為34萬8,521員。*Navy FY22 Military Justice Rep.*
24. Headquarters Marine Corps, *MCO 5800.16–V3, Legal Support and Administration Manual* (Washington, DC: 2018).
25. Headquarters Marine Corps, *MCO P5800.16A Ch 6, Marine Corps Manual for Legal Administration* (Washington, DC: 2011).
26. Ibid.
27. Ibid.
28. *MCO 5800.16–V3*, The LSAM superseded the LEGADMINMAN.
29. Chief Defense Counsel of the Marine Corps, *Policy Memorandum 3.2, Submission of Fitness Reports for DSO Marines* (Arlington, VA: 2014).
30. *MCO 5800.16-V3*.

回目錄→


(Source: AI-generated)

● 作者/Matthew Bruzzese ● 譯者/李昭穎 ● 審者/謝榕修

中共以中間人規避美政府出口管制

PRC Use of Middleman to Circumvent US Government Export Controls: The Case of Suzhou Rebes Electronic

取材/2024年7月12日美國詹姆斯頓基金會網站專文(*China Brief*, July 12/2024)

前言

隨著美、「中」戰略競爭加劇，美國政府更為警覺，試圖防止敏感技術遭中共非法取得，進而對中國大陸採取反制措施，包括於美國工業暨安全局(Bureau of Industry and Security)實體名單中增列中共機構，以及對於遭查獲違反出口管制措施者，強化執法與法律行動(聯邦公報，2022年12月19日；Defense One，2021年6月8日)。雖然如此，遭制裁的中共實體仍持續想方設法，以規避上述措施，並取得推動中共軍事現代化所需的關鍵外國技術。相關規避方式包括運用不加掩飾的人頭代購者自美國獲取所需技術，這些技術對中共而言原本是無法取得的。近期兩名中國大陸公民遭指控，企圖藉人頭公司代替中共遭制裁實體，購買關鍵半導體製造設備，此舉顯示對任何希望

蘇州瑞貝斯電子科技有限公司製作美企業Micro-Coax產品文宣介紹旗下產品，涵蓋軍用通信、衛星、雷達及航空等領域。(Source: Suzhou Rebes Electronic)

規避美國出口管制法的潛在走私者而言，代購仍為不二法門(美國司法部，2024年4月25日；騰訊，2024年4月30日)。

2022年10月，《華盛頓郵報》(*The Washington Post*)指出，美國科技遭用於推動中共極音速武器計畫(華盛頓郵報，2022年10月17日)。該篇報導揭露中共運用中間人的情況，這些技術顯然係透過人頭代購者取得途徑，由美國移轉至中共飛彈研究機構，但代購者卻以看似合理的說法，相當敷衍地否認技術最終流向。然僅須稍經查閱中間人官網，即可發現其毫不掩飾所銷售的軍方對象。

該篇報導指出：「華天海峰(Hifar)科技股份有限公司絲毫不隱諱向中國飛彈機構銷售軟體與諮詢服務之舉，並在其網站中將逾50個軍事機構與供應商列為『合作伙伴』，其中包括中國航天空氣動力技術研究院、中國空空導彈研究院、中國運載火箭技術研究院、中國火箭軍及中國空氣動力研究與發展中心。」

《華盛頓郵報》的案例引發憂慮，且非僅此一例。中共藉相同的方式採購雷達、通信及其他軍工產品所需的關鍵組件，此點顯示藉由貌似無害的中間人採購，可能是規避出口管制經常使用的手段。

進口美國技術轉售中共國防企業

蘇州瑞貝斯電子科技有限公司(Suzhou Rebes Electronic Technology，以下

稱瑞貝斯)係一家成立於2006年的中國大陸公司，專門生產射頻(Radio Frequency, RF)與微波組件，用於行動通信、衛星通信、量子計算、雷達及其他用途(瑞貝斯，2023年2月)。與極音速飛彈相比，瑞貝斯所銷售的先進電纜配線等組件也許較不引人注目，但對於任何需要高速與可靠資料傳輸的設備而言，卻是關鍵組件。其中包括軍用航空、衛星、雷達、防空系統、通信系統、高性能電腦等其他應用領域。簡而言之，在嚴苛或惡劣的環境下，這些電纜組件可迅速可靠地傳輸大量資訊，為現代戰爭不可或缺的能力。雖然許多銷售對象遭美政府列入黑名單，瑞貝斯毫不隱諱地自美採購許多此類組件，並售予中共國防企業與共軍研究機構。

瑞貝斯聲稱與多間美國公司具合作關係，進口並在中共轉售相關產品(瑞貝斯，2023年2月)。瑞貝斯亦聲稱其為部分美國公司的中共官方代表，相關美國公司有許多是射頻、微波電纜組件領域的行業領導者(Marki Microwave，2023年2月)。此等行業領導者還向美軍供應產品，宣傳其在現代戰鬥中的可靠與堅固性。[1] 瑞貝斯官網文件內容顯示，至少一部分自美國進口的產品確實為軍規電纜(瑞貝斯，2023年2月)。[2]

對於這些自美國進口產品的軍事潛力，瑞貝斯並未低調處理，反而在向中共客戶行銷時，提及其軍事用途。瑞貝斯介紹一間美國公司電纜，稱其適用於「軍用通信、雷達、飛彈導引、衛星及航空」領域(瑞貝斯，2023年2月)。在行銷另一間美國公司產品時，指出可用於「衛星、相列雷達、電子戰及信號情報」等用途(瑞貝斯，2023年2月)。而在第三間公司宣傳其產品時，指稱該產品適用於超級電腦，而該產品目前限制對中共出口(K&L Gates，2022年10月21日；瑞貝斯，2023年6月)。造訪後者產品網站發現，其用於美國克雷(Cray)超級電腦(美國國防部與武裝部隊使用)，並運用於F-35第五代戰鬥機與戰斧飛彈(Tomahawk Missile)等一系列先進武器(Custom Interconnects，2023年6月)。

刪除新聞稿反倒凸顯產品軍事用途

瑞貝斯曾明確指出，許多自美國進口的產品最終均銷往中共軍方用戶。例如在其官網遭刪除的新聞稿中，提及該公司慶祝成功向共軍通信部隊銷售ka頻段電纜組件，運用於「雷達項目」(瑞貝斯，2021年6月)。雖新聞稿起初聲稱設備為自行產製，但於下一段卻指出其所有電纜均自美國與歐洲公司進口，甚至特別提及其中數間公司名稱：「線纜全部採用Micro-

瑞貝斯公司為Marki Microwave產品製作廣告,介紹其在衛星、相列雷達、電子戰及信號情報等領域之用途。(Source: Suzhou Rebes Electronic)

Coax、Times、Gore、Harbour、ATM、Tensolite、Huber+Suhner及IW等公司進口電纜。」

接著,瑞貝斯聲稱已與多間中共主要國防企業簽訂電纜組件供應協議,其中包括軍用電子企業集團子公司的中國電子科技集團公司、軍用航空企業集團的中國航空工業集團公司、航太與彈道飛彈巨擘子公司的中國航天科技集團有限公司及中國航天科工集團有限公司。確切而言,其所指的是中國電子科技集團公司第十、十三、十四、二十二、二十九、三十八、五十四及六十三研究所(從事軍用電子產品開發);中國航空工業集團公司的瀋陽與哈爾濱子公司、中國航天科技集團有限公司第五、八及九研究院,以及中國航天科工集團有限公司第二研究院。該公司亦聲稱與兩所共軍學術機構(國防大學與海軍工程大學)、數間與共軍機構關係密切的民間學術機構簽訂協議,後者包括「國防七子」之一的北京航空航天大學,此七所形式上的民間大學因與國防機構關係密切而聞名,並負責中共大部分的軍事研究(澳大利亞戰略政策研究所,2019年11月25日)。

其中許多機構顯然均使用瑞貝斯所供應的高端電纜組件。例如,該新聞稿提及向中國電子科技集團公司第十四研究所供應產品,該所為中共最

重要的軍用雷達研究機構之一(環球時報，2020年1月12日)。該集團第五十四研究所亦致力於戰術通信與其他軍用電子產品研究(中共國務院國有資產監督管理委員會，2021年9月8日)。新聞稿中提及兩間中國航空工業集團公司子公司，即瀋陽飛機工業集團與哈爾濱飛機工業集團，分別產製許多共軍戰鬥機與直升機(美空軍中國航空航天研究所，2024年1月22日)。此外，中國航天科技集團有限公司與中國航天科工集團有限公司的子公司深入參與飛彈、防空系統及中共太空事業發展，顯示美國技術可能已流入中共部分或全部軍用終端產品的發展。

美國商務部將提供人工智慧晶片給中共軍事現代化計畫與軍事情報用戶的公司列入出口管制實體名單。圖為美國商務部。(Source: 達志/Reuters)

然最引發憂慮之處也許在於，該篇新聞稿聲稱瑞貝斯亦與「綿陽九院」簽署組件供應協議，而「綿陽九院」為中國工程物理研究院的隱晦代稱，該院係中共核武計畫的主要研究機構(瑞貝斯，2021年6月)；另一份新聞稿似乎證實瑞貝斯參與核武研究，並慶祝新合約使其「進入了我國國防領域高端的核工業領域」(瑞貝斯，2023年2月)。

結語

瑞貝斯官網與聲明表明，美國企業刻正向中共出售關鍵技術，並最終流向中共國防體系，現尚無證據顯示任何售予瑞貝斯產品的美國企業知曉前述二次銷售情況，且這些公司看似相當重視美國政府出口管制措施(Marki Microwave，2018年6月；ATM Microwave，2023年2月)。惟僅須克盡職責稍加調查，對其銷售對象即可具備更明確的認知，目前至少已有一間美國公司在其中共網站中，宣傳產品符合美軍同軸電纜的MIL-DTL-17軍規標準(Times Microwave，2023年2月)。[3] 這些公司可能認為，因瑞貝斯未納入任何美國出口審查名單，故銷售不會發生

問題。然該公司本身雖未列入清單，但與其合作的許多機構，包括中國電子科技集團公司、中國航空工業集團公司、中國航天科技集團有限公司、中國航天科工集團有限公司及中國工程物理研究院，均列入美國商務部的出口管制實體名單(國際清算銀行，2023年3月2日)。

中國大陸公司時常將中文視為「第一層加密」，用以發表公開聲明，惟聲明一旦經翻譯後，可能為其帶來麻煩。這些公司認為無人會將相關聲明予以翻譯。通常的確是如此，但當美政府開始更嚴格地執行出口管制措施時，瑞貝斯等案例則顯示，美政府於技術控管方面仍有很長的路要走。然而，運用有限的資源仍可對現況頗有助益。例如一位具中文能力者僅須連接網際網路，花費15分鐘，即可輕而易舉揭露事實，進一步發現美國出口技術在中共國防體系中的流向。雖然評估中共藉中間人規避出口管制的行為十分普遍，仍須進一步的調查工作，但在諸多的管制產品中數度出現類似案例，反映此為常見且可能有效之策略，故更應密切關注相關發展。

作者簡介

Matthew Bruzzese為美國藍路實驗室(BluePath Labs)資深中文分析師。

Reprint from The Jamestown Foundation with permission.

註釋

1. 請參閱以下例證：Ted Prema,“Powering high-performance, ultrareliable RF systems in military electronics,” Military Embedded Systems, 3 December 2021, https://militaryembedded.com/radar-ew/rf-and-microwave/powering-high-performance-ultrareliable-rf-systems-in-military-electronics; “GORE-FLIGHT Microwave Assemblies for Defense Aircraft,“ GORE, Accessed February 2023, https://www.gore.com/products/gore-flight-microwave-assemblies-defense-aircraft; “Micro-Coax, a Carlisle Brand,” CarlisleIT, Accessed February 2023, https://www.carlisleit.com/brands/micro-coax/; “Relentlessly Pursuing Discovery,” CarlisleIT, Accessed February 2023, https://www.carlisleit.com/markets/military-defense/; “Six cables available to support F-35 ramp rate to full production,” Harbour Industries, 21 January 2020, https://harbourind.com/latest-news/82-f-35-cables.
2. 瑞貝斯官網文件提及的產品被形容為MIL-DTL-17級，此為美國軍用標準電纜之官方名稱，請參閱“MIL-DTL-17 Requirements for Hi-Rel/MIL-SPEC Coaxial Cable Assemblies and a Note on RG Coax,” Military and Aerospace Electronics, 3 March 2019, https://www.military-aerospace.com/directory/blog/14059642/mildtl17-requirements-for-hirelmilspec-coaxial-cable-assemblies-and-a-note-on-rg-coax.
3. 英文版手冊網址： https://web.archive.org/web/20230217220131/http:/www.timesmicrowave.cn/uploads/PhaseTrackFamiliy.pdf.

回目錄→

(Source: DVIDS)

作者/Xavier Brunson and Cody Chick　譯者/章昌文　審者/謝榕修

金色眼鏡蛇軍演加強美國與印太盟友之關係

How Cobra Gold Helps the US Strengthen Its Indo-Pacific Partnerships

取材/2024年5月13日美國外交家雜誌(*The Diplomat*, May 13/2024)

南海爭議水域、烏克蘭戰爭及大國間日益升級的緊張局勢，都為美國強化其在印太區域的聯盟創造機會。從2022年開始，美國國防戰略確立以整合嚇阻做為強化聯盟的框架，為整體安全提供一個以對手為中心的做法。嚇阻成功的關鍵在於提供「整合保證」，這是一項透過安全合作向夥伴國與盟國提供「保證」的行動，可強化聯合、多國夥伴關係，進而能夠有效嚇阻對手。

正如佛林(Charles Flynn)上將與戴文(Tim Devine)中校近期在《美國海軍學會月刊》(*Proceedings*)，發表一篇談陸海一體化(Land-Naval Integration)的文章中所述：「陸軍因此透過歡迎其他利益相關者促進團結，幫助他們

建立更可靠手段，來支持陸上與海上的共同國家利益。以聯盟聯合部隊的方式行動，可讓美國及其盟國能夠採取齊一作為，達成共同目標。」

金色眼鏡蛇演習(Exercise Cobra Gold)就是一個明顯的個案研究，可闡明建立整合保證行動的重要性，並且在長期交流的關係中進行，此對理解區域挑戰與支持軍事關係至關重要。由於印太區域內部衝突風險可能升高，美國向區域夥伴國傳達共建安全合作的承諾，較諸以往更顯重要。

整合保證

整合保證是整合嚇阻的另外一面，嚇阻往往是威脅導向，著重在拒止，若有侵略行動時要承受懲罰或其他代價。再者，整合保證是夥伴國導向，與友好國合作，從根本上展現態勢、提供保護及支持美國人民與資源，此能建立真實信任與相互責任，為共同利益提供保障；整合保證深化外交、軍事、經濟、資訊及技術合作，進而可透過嚇阻，增強懲罰或拒止的能力。

整合保證將國家戰略中闡述的整合嚇阻做法轉化成可操作、最基本的架構，透過戰術與作戰層面實質專注於夥伴國與盟國，建立相互理解與人員作業互通性，以在戰略層面嚇阻敵人。在軍事戰役、聯合演習及安全合作中，藉由訓練與關係建立的同時，以一支可恃戰力部隊支持戰略目標，提供整合保證。

此項保證只能透過展現承諾來實現──承諾投入時間、資源及軍方人員支援盟國與夥伴國，以應對共同的機遇與威脅。整合保證是連結戰略框架與戰術層級相互瞭解之關鍵樞紐。

此外，整合保證是有效戰役行動的關鍵，冷戰期間步兵排能與北約盟國一起訓練，特別之處就是能瞭解彼此的全般意圖，而在相對和平的1990年代，別處部隊卻可能難以理解他們的聯盟訓練如何產生實質影響。儘管美軍多年來一直參與多國聯合演習，但行動重心都聚焦在具有目的性、逐步推進的交流，如此方能相互支援，並朝著明確的共同目標邁進。

此類保證以多種國家力量在各國間橫向交流，同時對高階領導者間之合作與戰術階層軍事人員的聯合訓練，提供縱向的良好互動。西點軍校的外國軍事院校交流計畫，就是在軍官職涯中如何透過像金色眼鏡蛇一類的年度演習，率先發展並持續培養關鍵軍方領導者關係，呈現整合保證的範

例。這些長期互動建立的友誼與私人聯繫，能幫助影響高階領導者的親美軍事政策與衝突時單位間之信任。在承平時期，美軍主要透過聯合演習競逐與夥伴國持續性合作，以建立整合保證。

金色眼鏡蛇網路演習期間，美國、日本及南韓軍事人員整合作業方法，以遂行聯盟數位防禦。Source: Cody Chick)

主要安全合作夥伴關係

2024年2月27日至3月8日，金色眼鏡蛇演習於泰國舉行，可做為促進軍隊間互動且產生較強整合保證的戰術平臺。最近一次的演習共有十國參加：泰國、美國、印尼、日本、馬來西亞、新加坡、南韓、中共、印度及澳大利亞。從新冠肺炎(COVID)疫情大流行以來，聯合多國演習日益增多，也為各國軍隊合作提供更多機會。

就戰術層面言，演習對展現承諾、建立作業互通性及戰備有其必要。從戰略層面來看，這表示區域內聯盟與國際事務的積極發展趨勢。在金色眼鏡蛇演習中，四方安全對話(Quad)成員國(美國、澳大利亞、印度及日本)，以及在2023年8月大衛營(Camp David)三邊安全協定高峰會中，展現與日本關係逐漸升溫的南韓亦派兵參加。合作的衡量標準之一，就是要確定某些國家在戰術階層有多少(抑或沒有)互動。

金色眼鏡蛇演習重點置於多國部隊指揮所演習(Multinational Force Command Post Exercise, MNF-CPX)、聯盟聯合野戰訓練演習、高階幹部專題討論會、人道援助及災難救濟(Humanitarian Assistance and Disaster Relief, HA/DR)。雖然近期金色眼鏡蛇演習，印度、中共及澳大利亞將參演科目侷限在人道與民事援助部分，然而，數項關鍵的金色眼鏡蛇演習活動，仍凸顯國家之間日益密切的合作。

金色眼鏡蛇演習大多是多國部隊指揮所演習，每個主要出

2023年8月18日，美國總統拜登於大衛營會晤南韓總統尹錫悅(左)及日本首相岸田文雄(右)，討論加強聯合國對北韓的制裁並阻止其非法資助武器計畫。
(Source: 達志/AP)

兵國家都參與其中。在多國部隊指揮所演習中，七國共同解決一場區域危機，目的在瞭解彼此能力與侷限、培養作業互通性及建立關係，此次演習強調的是多領域環境中大規模戰鬥作業與海上安全。指揮所演習對美陸軍的太平洋戰鬥行動方式並非疊床架屋，反之，「整體而言，棧道行動(Operation Pathways)聯合個人與戰術行動來解決作戰與戰略問題」。多國部隊指揮所演習提供一個觀察各國參謀間互動的機會，還提供軍事人員對當前安全挑戰的第一手描述，以及日益密切夥伴關係的深入見解。

日韓關係

為回應日益增長的區域威脅，日本與南韓之間關係持續回穩。在金色眼鏡蛇演習期間，兩國都參與公民援助計畫，南韓、泰國及美陸戰隊進行聯盟兩棲演習，三邊安全協定成員國也分享網路演習的成果。

除了金色眼鏡蛇演習之外，儘管日本與南韓因與中共的經濟關係而進行某種形式的戰術避險措施，但也都做出各種公開承諾，來提升與美國的安全合作。俄國對烏克蘭入侵，促使日本將其軍隊常態化，以增強其嚇阻侵略的能力與範圍。

同樣，北韓數量空前的新型尖端飛彈測試與中共在區域內日益升高的敵意，均顯示日本與南韓須要建立統一戰線。與過去十年截然不同的是，在2023年8月到12月間，日本、南韓及美國舉行30次三邊會談。由於各國已制定多年軍事演習計畫與針對任何潛在威脅的聯合警報系統，因此2023年8月的大衛營高峰會，才能建立最終機制。為回應北韓在2023年12月的飛彈發射，美國、南韓及日本舉行三邊軍事操演，其中包括美軍駐日韓的長程轟炸機與戰鬥機。

各方咸信，由於各國領導人安全利益一致，得以在戰術與作戰層面發展人道與軍事領域的整合保證，日本與南韓方能取得

卓越的進展。

競爭對手，齊心協力

多國民間與軍方團體正為人道救助與災難救濟行動做準備。
(Source: Cody Chick)

與諸多其他多國演習不同，泰國主導的金色眼鏡蛇演習，將諸多競爭者齊聚一堂，攜手演練公民援助、人道援助及災難救濟。在公民援助計畫期間，美國、泰國、馬來西亞及中共工兵部隊共同合作，在巴真武里府(Prachinburi Province)當地的一所學校新建一座多功能設施。軍事人員白天大部分時間都在建造設施，晚上則從事文化交流活動，以相互瞭解並建立同志情誼。在相對保守的軍事單位中，這些交流可讓戰士們瞭解文化差異與共通性的複雜程度。

美國參演部隊是由克拉克(Tyler Clarke)中尉領軍，他是夏威夷第871工兵連的美陸軍後備部隊軍官。克拉克從事木匠工作多年，慶幸有這樣的經歷。回顧這項計畫，克拉克表示：「每個人都表現出我沒料想到的盼望或興奮，想要相互瞭解與共同合作，尤其是那些年輕的士兵。我認為這種共同合作的難得機會不言而喻，而且他們真心想要認識彼此。」

儘管身處在泰國的一個小村莊中，來自四個國家的軍事人員卻藉由分享經驗建立袍澤之情，遠離政治緊張局勢所加諸的壓力，降低戰略層面的負擔並減少合作的阻礙。

泰國是美國的安全盟國且與中共有密切的經濟關係，此類活動凸顯了在可能的情況下交流合作的價值。不像在冷戰期間，敵國與盟國之間會有條明確的分隔線，今日大國競爭，是在一個更模稜兩可的環境中操作，夥伴國經常在競逐對手間權衡其利益。共軍與美國盟國之間在施工現場的互動，凸顯出平衡關係與擴大共同合作的機會。

雖然金色眼鏡蛇演習是由泰國居中協調，但卻代表美國與中共之間溝通管道的日益開放。競爭對手間之溝通，對緩解衝突與在該地區危機或人道援助與災害救濟之環境中進行協調至關

金色眼鏡蛇演習展現美泰長期友誼與多國合作促進區域和平與印太安全。圖為2024年3月8日實彈射擊演習後合影。(Source: DVIDS)

重要。

特種作戰部隊、安全部隊援助旅及州夥伴計畫的長期交流

在這些大型多國演習背後，是特種作戰部隊、安全部隊援助旅及州夥伴計畫(將美國各州國民兵與外國夥伴配對)的持久雙邊交流。

特種作戰部隊專注外國內部防禦，為安全合作做出重大的貢獻。他們在執行外國內部防禦的軍事部分保持領先，並與全世界進行交流。在金色眼鏡蛇演習中，美國特種作戰部隊、泰國特種部隊及日本特殊作戰群進行聯盟訓練。

在泰國，第一特種部隊大隊與泰國皇家陸軍特種作戰學校(Royal Thai Army Special Warfare Schoolhouse)密切合作，提供建議與協助。特種作戰部隊等單位的長期交流，展現對整合保證的信任與承諾。

同樣，安全部隊援助旅與夥伴國部隊維持長期交流，已超越了年度演習與各項活動，第5安全部隊援助旅曾在泰國士官學校與朱拉春高皇家軍事學院(Chulachomklao Royal Military Academy)，協助培訓接收新型車輛後的泰國皇家陸軍史崔克部隊。

整合重點發展學校與作戰部隊，為美國軍事支援建立世代保證。與夥伴國部隊保持聯繫，能夠推動大規模軍事演習，而一年中學到的教訓，可透過長期交流來重新培訓與提醒，使部隊能在來年完成更好的準備與達到更高水準的運作。

州夥伴計畫與金色眼鏡蛇演習緊密配合，增強區域重點的安全合作。金色眼鏡蛇演習期間，華盛頓州國民兵代表美國率先在人道援助與災難救濟中做示範。與領導者每一到三年就要更換的傳統軍事單位不同，國民兵部隊使軍隊領導者間可保有長期的關係，增添另一層的整合保證。華盛頓州國民兵聯合部隊指揮部參謀長阿克(Michael Ake)上校，過去14年來一直與其金色眼鏡蛇演習中的泰國夥伴相互配合。

針對州夥伴計畫的獨特功能，阿克表示：「我們(國民兵)軍人具備範圍廣泛的民間職業專業知識與經驗，這對任何任務都具增值作用──特別在人道援助與災難救濟之各項作為上。」

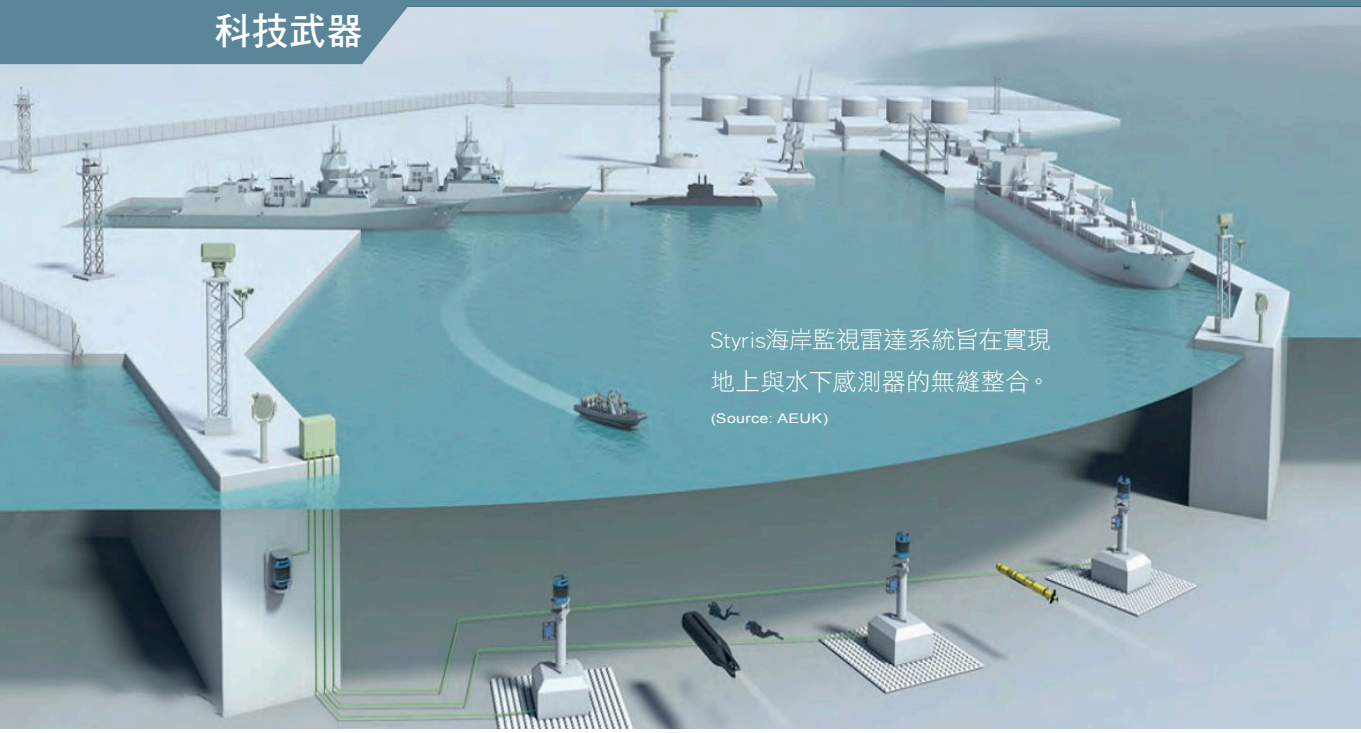
歐洲可清楚證明州夥伴計畫的潛力，正如特種作戰部隊一樣，2022年俄國入侵烏克蘭之前，美國國民兵透過州夥伴計畫在與烏克蘭部隊的訓練中發揮持續性的作用。

長期交流對瞭解區域挑戰與支持軍事關係十分關鍵，在泰國，美國特種部隊透過50餘年的交流，與特種作戰部隊夥伴保持密切的聯繫；同時，第5安全部隊援助旅與州夥伴計畫統合傳統部隊整合保證作為。技術、作戰及人道層面的作業互通性雖已完成改善，但仍需與整合保證及共同瞭解結合。增加交流亦可能增加軍售，最終提升後勤補給中斷期間的作業互通性與裝備部署彈性。

結語

金色眼鏡蛇演習為區域夥伴提供一個建立軍事合作與作業互通性的平臺以促進整合保證，美國利用聯合演習與長期交流，作為在印太地區關鍵行動。整合保證可為夥伴國與盟國提供可信度、承諾及決心，這與建立有效嚇阻且具凝聚力聯盟的能力有直接關聯。透過印太地區聯合與多國層面的經常性交流，有助於建立穩定的夥伴接觸點，並維持部隊在地主國的持續駐留。儘管本質是戰術性的，但與時推移下，每次交流都會建立各世代間信任與公平，並讓區域夥伴為分享更大的戰略目標做出貢獻。

回目錄→



Styris海岸監視雷達系統旨在實現地上與水下感測器的無縫整合。
(Source: AEUK)

● 作者/Stefan Nitschke ● 譯者/周敦彥 ● 審者/謝榕修

強化關鍵基礎設施

Known Unknowns: Strengthening the Resilience of Critical Infrastructure to New Advanced Threats

取材/2024年1-2月德國軍事科技雙月刊(*Military Technology*, January-February/2024)

正如安全專家所普遍強調的，所有涉及保護關鍵基礎設施與裝備的機構及組織都應該進一步強化其網路聯繫，這可能包括蒐集(通過性能優異的感測器)、分析及判讀那些必須與其他部門單位之間分享的安全相關資訊。最佳例證是在潛水員偵測聲納技術(Diver Detection Sonar Technology)領域的最新發展，這將是在地區層級，尤其是在海洋安全環境中，打擊地方性恐怖主義與非法活動，所急需協調的一個重要元素。

針對威脅就是答案

在最先進的威脅中，有小型無人飛行載具(Unmanned Aerial Vehicle, UAV)或無人飛機。除了火箭、火砲與迫砲(Rocket, Artillery and Mortar, RAM)射彈之外，無人飛機也可以構成嚴重的安全威脅。無人飛機在任何商店都可以購得，但其自主性相當低。業界表示，迷你無人飛行載具

CR20海岸監視雷達可同時追蹤多達500個目標。

(Source: Belgian Advanced Technology Systems)

(Mini-UAV)能夠飛行24小時或更短時間，就情報而言，可以蒐集比微型無人飛行載具(Micro-UAV)更多的資訊。因此，必須保護關鍵基礎設施免於這些系統的入侵。紳寶公司(Saab)的長頸鹿4A(Giraffe 4A)雷達是一種解決方案，該雷達自2013年開始，在多次實際客戶測試中被用於偵測與追蹤非常小型的無人飛機。紳寶公司解釋，在實驗室中，Giraffe 4A雷達的偵測距離是該公司長頸鹿AMB(Giraffe AMB)雷達的兩倍。此外，還有網路攻擊，世界各地的大型政府機構與企業正疲於應付來自竊賊、敵對國家及駭客的網路攻擊，這給網路犯罪情報活動帶來額外挑戰。因此，這些發展可能引發對網路情報的新需求，包括網路反情報。網路情報的運用，像所有其他情報專業領域一樣──人工情報、公開性情報、信號情報、地理空間情資、測量與訊號情報──可以是理解網路攻擊性質與保存網路犯罪證據的第一步。然而，有警告指出，對於網路情報本質與運用，普遍缺乏資訊。歐洲各地安全組織也對最近的俄羅斯網路攻擊感到擔憂，於是發現情報的運用，包括蒐集、處理、整合、評估、分析及判讀有關外國、敵對或潛在敵對勢力與單位、實際或潛在作戰區域的可用資訊，是網路防禦的重要元素。

即時水上與水下安全

沿海設施的保護面臨著新挑戰。目前所有涉及港口或是碼頭的現代安全設備計畫，都明確顯示提高狀況覺知能力的需求。因此必須儘快考慮投資更適當的安全措施(包括水面與水下檢查/巡邏及更好的訓練程序)，以避免將來進行代價高昂的重新

建置，而這些都是業界現在可以提供的。

大約自2010年代中期以來就存在的範例是空中巴士國防與太空公司(Airbus Defence and Space)所提供的Styris海岸監視雷達系統。這是一套可擴充的感測器(包括攝影機、雷達、自動資訊系統、天氣感測器、無線電測向設備)，可融合來自各種感測器的數據，並生成即時的海事畫面。2018年，英國Atlas Elektronik公司表示，早期用於水下的監視系統「坦率地說，無法即時偵測與識別攜帶爆炸物的潛水員或蛙人，無論其使用開放式或循環式水肺」。該公司最初參與將重要水下專業知識引進該解決方案中的工作。因此，自2010年左右以來一直致力於導入潛水員偵測聲納──該公司的Cerberus Mod 2聲納──為操作人員提供監視與追蹤水面及水下目標的完整解決方案。Cerberus Mod 1聲納是由英國國防科技集團(QinetiQ)製造，並於2003年的水下國防科技展覽(Undersea Defence Technology, UDT)中亮相；2009年，QinetiQ水下部門出售給英國Atlas Elektronik公司，而Cerberus Mod 2聲納由其開發。

另一個解決方案是ATLAS海岸區域安全系統(ATLAS Security for Coastal Areas, ASCA)。該系統由德國Atlas Elektronik公司針對緊急需求所開發，可以配置為適合遠征作戰的機動系統，或作為保護海軍基地、港口、海上裝備及海岸線的陸基系統。ATLAS海岸區域安全系統以ATLAS海軍戰鬥系統(ATLAS Naval Combat System, ANCS)為基礎，是一套「有效的海岸防護系統」，得益於水下與水面感測器的部署彈性，可以提供最佳的態勢圖像，以滿足任何本地與區域需求。值得注意的是，該系統可以作為水面艦艇(例如巡邏艦艇)的核心系統，因此包含用於水下、水面或空中監視、偵測、追蹤、威脅評估及自動發出警報所需的軟體模組。戰鬥管理系統軟體還能夠下令各種自衛武器進行快速反應，打擊不對稱威脅，包括迫砲、火箭、汽車/卡車或快艇的地(水)面攻擊，潛水員搭乘人員運輸艇、袖珍潛艦或無人水下載具(Unmanned Underwater Vehicles)遂行的水下攻擊，以及自殺式攻擊。

另一個來自英國的例子是 Blighter Surveillance Systems Ltd.公司的Blighter Explorer Nexus系統，該公司是一家電子掃描雷達與感測器解決方案供應商。而此系統是一套完全整合的電池驅動可攜式雷達/攝影監視系統，可由徒步巡邏人員的攜行背包或由車輛快速部署，用於遠程邊界監視、臨時營區防護、前進偵察及其他秘密行動。Explorer Nexus系統可以

ULAQ武裝無人水面載具是新改良型一系列無人水面載具，專為執行海上安全任務。

(Source: ARES Shipyard and Meteksan Defence Industry Inc.)

偵測1.5公里處的匍匐前進人員及偵測8公里處的移動車輛。雷達會自動引導長程攝影機，使操作人員能夠識別所有目標。無線回傳鏈路可用於將即時感測器數據傳送到遠端位置，以便進行監控與戰略評估。

來自英國Sonardyne International Ltd.公司的水下入侵偵測技術──哨兵入侵者偵測聲納(Sentinel Intruder Detection Sonar，下稱哨兵)──可用於偵測從水中接近關鍵設施的不明潛水員與水下載具。根據該公司說法，哨兵是市場上最廣泛運用的水下入侵偵測聲納技術，具有經過驗證辨別真正目標與非威脅物體的能力，例如在各種作戰環境中的大型魚類或休閒遊艇。

以色列的DSIT Solutions Ltd.公司是Rafael Advanced Defense Systems Ltd.公司的子公司，負責銷售其AquaShield™水下安全系統。這是一套自主與自動化的高性能水下潛水員偵測聲納，旨在為高價值的沿海與海上裝備及位於海岸線與海上關鍵基礎設施提供持續水下安全保障。AquaShield™系統擁有先進信號處理演算法，能夠自動偵測、追蹤及鑑別所有類型水下威脅，且具有非常低的誤警率。數年前，總部位於倫敦的Energean能源公司選擇該系統來保護其浮式生產儲存卸貨(Floating Production Storage and Offloading, FPSO)平臺免受水下威脅。該浮式生產儲存卸貨平臺連接到Energean能源公司位於以色列外海的卡里什(Karish)和塔寧(Tanin)氣田。

業界表示，影像感測器、雷達可以發揮最大作用

業界有大量的機會來解決安全問題。現代的感測器能夠監控環境而使安全行動協調一致。因此，光電/紅外線與陸基雷達技術之多功能性持續吸引大量國際採購計畫並不令人意外。新型陸基雷達或光電/紅外線系統中的偵測器技術適合做為被

動目標偵測系統，能夠在完全黑暗與顯著背景雜訊的情況下尋找目標。根據比利時光電與雷達專家Belgian Advanced Technology Systems S.A.公司的說法，任何這些手段都會包括來自其他多個感測器的資訊整合。「可能包括光學目標指示器、雷達、雷射測距儀/指示器及車載紅外線搜索追蹤裝置與前視紅外線系統」，並結合安全即時數據鏈路、決策及導航輔助工具。該公司補充道：「在邊境與關鍵基礎設施周邊應被偵測的新威脅包括直升機、小型無人飛機及其他無人駕駛載具」，以及地面機器人載具。不僅如此，也要能偵測並摧毀火箭、火砲與迫砲射彈及其發射位置。

Blighter Explorer Nexus系統由Blighter B202 Mk2電子掃描微型都卜勒地面監視雷達、整合性可見光與紅外線熱成像相機、Windows人機介面、遮光目鏡及強固型筆記型電腦所組成。

(Source: Blighter Surveillance Systems)

法國的HGH Infrared Systems公司提供一種廣域監視解決方案，包括Spynel全景熱像儀與以Windows客戶端軟體為基礎的Cyclope偵測軟體。通過此一解決方案，圖像處理與數據分析軟體能夠實現即時360度熱成像影像，以強化海岸狀況覺知。HGH Infrared Systems公司在早前的訊息(2018年)中指出，他們保證能夠偵測、追蹤及識別多種威脅，包括木製船舶與游泳者。

然而，目前還沒有能夠適用於所有情況的方法。光電/紅外線感測器無法足夠準確地穿透雲層、灰塵、雨水或霧氣等遮蔽物來偵測目標。使用汞鎘碲(Mercury Cadmium Telluride, MCT)偵測器使得新型設備能夠使用微型冷卻器，而這些冷卻器不適用於使用銻化銦(Indium Antimonide, InSb)技術的設計。汞鎘碲偵測器傾向於在短波紅外線與長波紅外線波段發揮作用，並提升對煙霧與灰塵的穿透性。與早期系統相比，汞鎘碲偵測器能夠提供解析度高四倍的圖像。在邊際天氣條件(Marginal Weather Conditions)下，以4.5倍的距離(8.5公里)偵測小型目標(通常小於2.3乘2.3公尺)，還能在2至3公里或更遠距離識別與

Quadrocopter Surveillor S無人飛機被設計為一個堅固的載具平臺，適用於軍事與執法領域的高級監視應用。
(Source: RotorKonzept Multikoptermanufaktur)

辨認這些目標為友善物體，或將其與假目標區分開來。

這裡我們就要談到先進的雷達技術。德國的Hensoldt公司開發一款名為PrecISR™的多用途監視雷達，可提供合成孔徑雷達/地面移動目標指示器(Synthetic Aperture Radar/Ground Moving Target Indicator, SAR/GMTI)的相關功能，使偵察機操作人員能夠即時偵測與追蹤各種小型移動目標(例如可疑車輛)。PrecISR™雷達中的技術即使在可能干擾光電/紅外線感測器偵測結果的惡劣天氣條件下，也能確保對靜態與移動威脅可靠且準確的監視。Hensoldt公司的PrecISR™空中多用途監視雷達近期由位於盧森堡的CAE Aviation公司安裝在King Air B350飛機上。該合約是在PrecISR™雷達成功飛行展示中驗證其優異合成孔徑雷達/移動目標指示器能力後簽署的，合約內容包括Hensoldt公司與CAE Aviation公司共同參加瑞典Ocean 2020海洋監視演習。Ocean 2020演習(歐洲海上覺知開放合作計畫)由歐盟國防研究準備行動(Preparatory Action on Defence Research)提供經費，並由歐洲防衛局(European Defence Agency, EDA)負責執行，主要目的是通過整合無人系統，以及情報、監視、目標獲得及偵察相關裝備的傳統技術及新技術，來展示增強的海洋環境狀況覺知能力，包括「觀察、定位、決策及行動」等作戰任務。

再來是地面系統，以色列航太工業公司(Israel Aerospace Industries, IAI)開發ELM-2112FP持續監視植被穿透(Foliage Penetration, FOPEN)雷達，設計用來偵測以前在茂密樹葉與森林區域無法識別的威脅。該雷達由以色列航太工業公司的子公司Elta Systems公司研發，已經執行作戰部署數年，能夠在惡劣的天氣條件下與廣泛的覆蓋範圍內保護邊境及關鍵基礎設施。ELM-2112FP雷達可確保在目標與威脅進入森林地區時持續進行監視——而這些目標是傳統動態偵測雷達通常看不見的。該

雷達可以與其他部署雷達連接到相同的指揮管制系統──這項能力解決迄今為止由於植被與灌木叢造成的情報缺口。

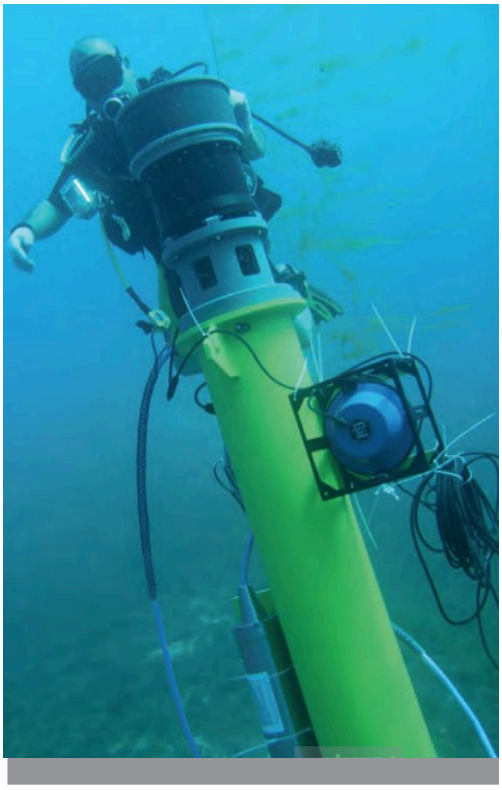
無人水面載具執行海上安全任務

維護海上安全是海軍的任務，包括保護國內港口、主要船隻及海上基礎設施免受各種威脅──從傳統攻擊到特種作戰及恐怖活動。首要的先決條件是持續的情報、監視與偵察，以維持狀況覺知與目標偵測，以及針對敵對活動接戰的目標分類與追蹤。這項任務與無人水面載具的部署非常契合。根據2021年美海軍部《無人作戰架構》(*Unmanned Campaign Framework*)指出，無人水面載具可在不危及人員生命的情況下執行各種海軍任務，並能夠執行高度耐久性與持續性的作戰──使用相對較低的成本，在理論上以可擴展之能力推進人類極限。

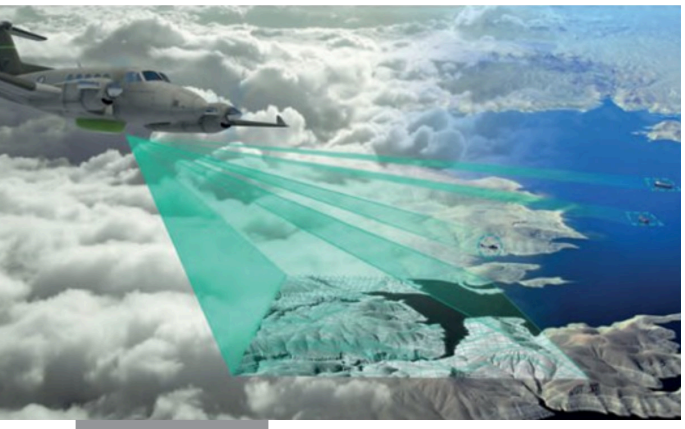
為此，土耳其的阿瑞斯(ARES)造船廠與Meteksan Defence公司經過密

ELM-2112FP持續監視植被穿透雷達能夠對利害區進行持續監視。

(Source: Israel Aerospace Industries)



ELM-2112FP持續監視植被穿透雷達能夠對利害區進行持續監視。 (Source: Israel Aerospace Industries)



PrecISR雷達將主動陣列與數位接收器技術的最新成果轉化為可擴展的高性能感測器，能夠安裝於各種空中載臺。(Source: Hensoldt)

集的研發活動成果，推出該國首個武裝無人水面載具計畫。2022年，Meteksan Defence公司總裁阿爾帕爾斯蘭(Selçuk Kerem Alparslan)向本刊的姊妹雜誌《海軍部隊》(*Naval Forces*)表示，此武裝無人水面載具是ULAQ系列的第一個原型載臺，首次成功從無人水面載具發射導引飛彈攻擊並摧毀水面目標，而且成功完成所有測試，包括口徑12.7公厘的武器系統。

結語

任何類型的關鍵基礎設施對於安全專業人員來說都是一個獨特的問題。有許多技術可用來協助保護關鍵基礎設施，此處包括無人載臺(無人飛行載具、無人水下載具、無人水面載具)、光電/紅外線攝影機及潛水員偵測聲納等三種。除此之外，越來越多的感測器被運用，並在控制功能中占有一席之地。這種方案包括以廉價但先進的載臺來搭載這些感測器，例如小型無人飛機或無人飛機(如德國RotorKonzept Multikoptermanufaktur公司的Quadrocopter Surveillor S無人飛機)，當有非法侵入風險時，愈來愈常被用來當做監視特殊利害區的載臺。這些系統可以觀察與追蹤慢速及快速移動的物體，如汽車、快艇或低空飛行的無人飛機──這些都是目前主要的威脅。

作者簡介

Stefan Nitschke博士是《海軍部隊》與《軍事技術與裝備》(Wehrtechnik)兩本姊妹期刊的主編，經常為《德國軍事科技雙月刊》撰稿。

回目錄→

本期詞語彙編

- 戰術、技術及程序(Tactics, Techniques and Procedures, TTPs)
- 阻斷服務(Denial-of-Service, DoS)
- 專業軍事教育(Professional Military Education, PME)
- 參謀首長聯席會議(Joint Chiefs of Staff, JCS)
- 參謀首長聯席會議主席(Chairman of the Joint Chiefs of Staff)
- 行動主軸(Lines of Effort, LOE)
- 空中密接支援(Close Air Support)
- 人員救援(Personnel Recovery)
- 戰鬥搜救(Combat Search and Rescue, CSAR)
- 人道援助及災難救濟(Humanitarian Assistance and Disaster Relief, HA/DR)
- 無人水下載具(Unmanned Underwater Vehicles)

數位化時代來臨，
國防譯粹月刊將於民國114年轉型電子版發行，
為您提供更即時的閱讀體驗，
並為地球節能減碳盡一份心力，
謝謝您。