作者/Aric A. Ramsey　譯者/劉慶順　審者/劉宗翰

重視網路火力

A Call for Cyber Fire

取材/2019年7月美國海軍學會月刊(*Proceedings*, July/2019)

網路戰的攻守運用得宜，將是戰爭獲勝的加乘因子。為了達成此一目標，美軍應著手強化訓練與整合、發展基礎準則及釐清法律權限等作為，才能有效因應未來的挑戰。

美國網路國家任務部隊(Cyber National Mission Force, CNMF)在2018年5月達成「全負荷作戰能力」(full operational capability)，並在全軍部署133個網路作戰團隊。[1] 這些團隊主要由目前已正式成為統一作戰司令部(unified combatant command)的美國網路司令部(U.S. Cyberspace Command, USCYBERCOM)負責管制，並將某些管制權分別賦予五個軍種網路司令部。[2] 這些團隊的任務範圍從完全攻勢乃至完全守勢，並視其奉命作戰的主要層級及受支援司令部而定。大體而言，從網路國家任務部隊自2013年開始發展以來，國家級網路司令部即與軍種級網路司令部並行運作，以確認在新作戰領域中遂行網路作戰的方式。

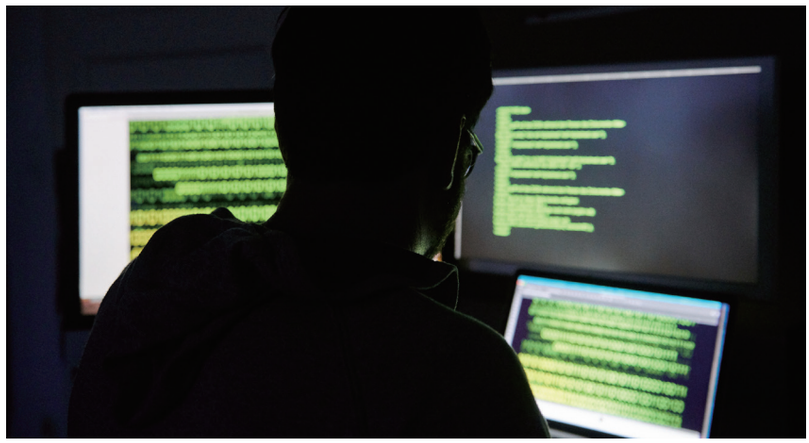
在完成將部隊與裝備置於一個統一司令部下的目標後，吾人必須將重點轉移至尚未發展成熟的運用概念、改善正規訓練、將網路能力整合至傳統部隊，以及在戰術層級運用此種能力等方面。在這個過程中，網路國家任務部隊支援傳統作戰的責任亦不能遭到忽略。

攻勢網路作戰屬高度機密。然而，粗略觀察被普遍歸咎於俄羅

在加州二十九棕櫚樹基地(Twenty-nine Palms)「陸戰隊空地戰鬥中心」(Marine Corps Air Ground Combat Center)的機械化突擊課程期間，第12陸戰團第1營營部火力支援官波利斯(Conrad Polys)少尉要求火力支援的情形。在當前作戰環境中，訓練戰術領導幹部尋求網路支援至關重要。(Source: USMC/Jacob Wilson)

斯對烏克蘭發動之網路攻擊，至少提供美國探索敵人可能性的窗口。最引人注目的例子，或許是俄國在2015年12月對三家烏克蘭能源公司發動的協同攻擊，這次攻擊影響七個11萬伏特及二十三個3萬5千伏特的變電所，並導致橫跨三個地區的22萬5,000名用戶失去電力。[3] 該次攻擊經過精密的規劃與協調，這可從對備份系統發動的支援攻擊與客戶服務線路遭到濫用獲得證實。在初期攻擊後，又發動旨在切斷目標地區電源的攻擊，隨後又進行消除管理電腦及破壞變電所內管制重要功能實體設施的攻擊。要達到等量的破壞與混亂，雖然需要大量的傳統彈藥，然而毫無疑問的是，預備性「網路火力」(cyber fires)將在未來為敵兵力提供重大優勢。

吾人可以合理認為美國網路國家任務部隊具有的網路能力，並不亞於對烏克蘭施加網路戰的對手。然不同於對手的是，美國並沒有機會針對面積與烏克蘭同樣大小的國家，進行整合網路能力與傳統作戰的測試。因此，傳統部隊指揮官對於網路國家任務部隊的完整能力欠缺根本理解，網路國家任務部隊能整合傳統武力，並藉由攻勢與守勢網路作戰支持其機動計畫的機會也極為有限。為運用此種新型態戰力，俾利為所有層級的戰爭提供最佳支援，美軍必須盡速發展其集體思維、訓練、資源及法律基礎。


網路戰攻守運用得宜，將是戰爭獲勝的加乘因子。 (Source: AP/達志)

強化守勢網路作戰為首要之務

不論是政軍界與媒體圈都著迷於攻勢網路作戰可望產生的效應，而攻勢網路作戰在各種公開及未公開的國家衝突，以及在全球犯罪活動中發揮效應的例子更助長此種迷思。這些能力儘管令人印象深刻，但美國仍必須將守勢網路作戰列為其在網路空間領域的首要任務。從來沒有任何火力型態本身就具有決定性，包括經由網路空間投射的火力在內。假使攻勢網路作戰無法達成支援傳統作戰的預期效果，但守勢網路作戰若成功阻絕對手影響友軍作戰網路的能力，任務就極可能獲致全面成功。儘管守勢網路作戰沒有如此吸引人，也不值得以頭條新聞報導，但它在網路空間需求層次架構中的首要地位卻是極為明顯的。守勢網路作戰對於「任務確保」(mission assurance)而言極為重要。

訓練能負起全責的軍官

從現在起的十年內，不論是

海軍與陸戰隊的作戰與戰術層級指揮官，都不太可能曾在其職涯先前任何階段受過網路作戰的充分洗禮。因此，除了指參學院現有少數有關網路戰的PowerPoint簡報外，還必須進行正規教育，使各級指揮官都能具備在網路作戰領域運用攻勢與守勢網路作戰的技能。一旦完訓，這些幹部就必須為其無法在控制範圍內適當運用網路能力的過失負起責任。

一名未做好側翼防衛的步兵營營長將遭到撤職的命運，但若同樣情況發生在步兵營的重要作戰資訊技術網路時，營長卻甚至連口頭警告之類的處罰都不會有。這兩種情況之所以未受到相同方式的處罰，僅是因為尚未有直接導致生命損失的網路危機。網路戰爭不是巫術，況且對於未具備資訊學位的人而言，掌握功能層級的網路戰爭也不是件太過複雜的事。美軍絕不能讓軍事幹部對可用來攻防的強大網路力量保持繼續無知狀態，尤其是某些營級與軍艦幹部。

有效的訓練也必須切合實際。這意味著網路戰部門必須與其他作戰要素共存，必須走出其敏感分隔資訊設施內的小隔間。由於美國對手已經證明其網路火力的有效性，因此美軍顯然需要如同陸戰隊營級部隊之海軍艦砲、火砲及航空軍官的網路連絡官。[4]

這些網路火力連絡官與負責投射網路作戰效益的網路部隊，都必須接受切合實際的訓練，而這些訓練不僅要求其能在與傳統部隊整合時展現能力，並促使其能更深入理解受支援指揮官之作

為因應現代網路的發展趨勢，各級指揮官或學官都必須具備網路作戰的技能。(Source: AP/達志)

戰構想的時機與節奏。這必須針對城鎮戰的訓練環境進行廣泛改造，並應仿效近鄰競爭對手的工業與現代城市網路環境。此外，每次演習都必須整納入網路假想敵部隊，以深入模擬真實的作戰環境。美軍必須竭盡所能發掘及利用友軍系統的缺失，以營造中斷情況與危機感。這將能教導各級指揮部勿過度依賴各種作戰功能的網路致能能力，同時也可協助通信人員識別及改善其防衛態勢的缺失。不論是對網路國家任務部隊或是各級指揮官及其幕僚而言，擬真環境都是必要的，因為前者必須接受訓練才能在嚴酷條件下遂行作戰，而後者須直接體驗網路的能力與限制，以創造運用與對抗網路作戰的實質效能。

基礎準則實屬必要

由於網路戰發展過於快速，使得詳細與技術性概念運用的時效性刊物遭到忽視。由於吾人對網路空間的認知已遠超過戰爭領域，因此對於網路支援通用詞彙與現實期待就顯得更加殷切。這些刊物應區分為公開及機密版，並應詳盡說明攻勢與守勢網路作戰的適當應用。步兵在論及火力支援計畫與支援其防禦多人操作武器的位置時，長官與下屬都為機動計畫提供堅實的參考架構。在戰術任務分配完畢後，奉命攻佔及肅清目標的連級部隊即可瞭解如何為每項任務做好準備與任務成功的樣貌。然而，就網路戰而言，來自網路司令部與各軍種的戰術指導極為稀少，導致聯合通信的內部混亂，並使得濫用網路能力的機會大增。

即使像是網路空間領域的標準作戰術語與圖解這樣的基本套件，對網路作戰詞彙的標準化作業皆極具助益。[5] 此外，若再加上正式的指揮官訓練，將會開始改變美軍因應網路戰的軍事文化。然而，有太多尚未成熟理解數位世代戰爭的幹部，仍漫不經心地認為網路及通信軍官的工作「過於技術性」。

位於烏克蘭烏克蘭因卡(Ukrainka)的「翠普斯卡火力發電廠」(Trypilska Thermal Power Plant)。俄羅斯於2015年12月對烏克蘭電力基礎設施發動網路攻擊，造成大規模停電，證明網路戰會產生具體的軍事效應。

(Source: Wikimedia Commons)

法律權限必須加以釐清

網路的法律權限必須給予全面詳盡界定。網路「接戰規定」(rules of engagement, ROE)必須達到與正規軍事作戰同樣嚴謹的詳盡程度。在相對和平的狀態期間，攻勢網路作戰被視為是必須獲得最高軍事及政治領導人批准的戰略資產。經過設計後，這個過程將不容輕易變更且受到嚴格管制，以便在網路作戰意外影響及在預定目標外情況下，得以避免國際政治事件的發生。在對抗某些特定交戰國的全面作戰行動中，此種限制可能會加以放寬或取消。然而，運用網路火力仍存在首席軍

法參謀官與美國司法體系必須充分考量釐清的獨特法律複雜性。

美陸軍軍法總監(Judge Advocate General)指出，有許多法律專家都質疑現行的網路戰國際法欠缺明晰度。他們認為，此種不確定性顯著到足以讓人懷疑現行的武裝衝突法是否適用於網路作戰。[6] 確認法律權限及致力於修改相關國際法，使軍方能從容運用網路戰力，現在刻不容緩。此外，解決戰略與作戰層級的接戰規定困境，將可簡化複雜的指揮管制關係，降低運用網路兵力的不確定性，進而改善對作戰人員的支援。

這些法律必須慮及交戰方在遠程操作，以及實際座落在中立或甚至「友好」網路空間的目標。一旦發現敵對網路目標，在法律上即應准許在未經網路設施擁有者同意的情形下，對指定的軍事目標執行網路攻擊。若要使攻勢網路作戰對作戰人員獲得與傳統火砲或電子戰同樣的效率，就必須建立戰術網路接戰規定的基礎。

隨著美國及其對手對網路致能能力的日益依賴，同時藉由網路空間施加的混亂程度也正在急遽增加。[7] 儘管網路火力為美國提供在實施突襲前熄滅敵燈火，乃至破壞傳送至火砲瞄準線之數位射擊資料完整性等機會，但同時也將其作戰網路暴露在全球任何擁有筆電及網路鏈結者的面前。只有深入發展清晰、詳盡的網路準則，並將所有攻勢與守勢網路作戰能力充分整合至每次的訓練活動中，這些能力才能更全面的出現在戰術場景中。一旦經過整合與訓練，美軍將可在與敵人對抗時，隨心所欲充分運用其新增戰力。美軍敵人已經做到了這點，但美軍何時才能做到呢？

作者簡介

Aric A. Ramsey係上尉通信官，目前在美陸戰隊網際空間作戰群(Cyberspace Operations Group)服役。他畢業自密西根大學(University of Michigan)，擁有應用數學學位。

Reprint from *Proceedings* with permission.

註釋

1. U.S. Cyber Command, “Cyber Mission Force Achieves Full Operational Capability,” press release, 17 May 2017, www.defense.gov/News/Article/Article/1524747/cyber-mission-force-achieves-full-operational-capability/.
2. Executive Office of the President, “Elevation of U.S. Cyber Command to a Unified Combatant Command,” memorandum, 15 August 2017, www.federalregister.gov/documents/2017/08/23/2017-17947/elevation-of-us-cyber-command-to-a-unified-combatant-command.
3. Robert M. Lee, Michael J. Assante, and Tim Conway, “Analysis of the Cyber Attack on the Ukrainian Power Grid,” Electricity Information Analysis and Sharing Center, 18 March 2018, ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.
4. Sydney J. Freedberg Jr., “Rogers, Richardson, Neller Brainstorm Future Cyber Structure,” *Breaking Defense*, 24 February 2017, breakingdefense.com/2017/02/rogers-richardson-neller-brainstorm-future-cyber-structure/.
5. Eric D. McKroskey and Charles A. Mock, “Operational Graphics for Cyber-space,” *Joint Force Quarterly* 83, no. 4 (October 2016), ndupress.ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-83/Article/1130660/operational-graphics-for-cyberspace/.
6. U.S. Army Judge Advocate General, *Law of Armed Conflict Deskbook*, 5th ed. (Washington, DC; Government Publishing Office, 2015), www.loc.gov/rr/frd/Military_Law/pdf/LOAC-Deskbook-2015.pdf.
7. Jim Garamone, “U.S. Military’s Cyber Capabilities Provide Strength, Challenges,” *DoD News*, 22 June 2016, www.defense.gov/News/Article/article/810009/us-militarys-cyber-capabilities-provide-strength-challenges-official-says/.