● 作者/Thomas Parker and Warren Parker ● 譯者/黃文啟 ● 審者/馬浩翔

善用既有的網路戰準則

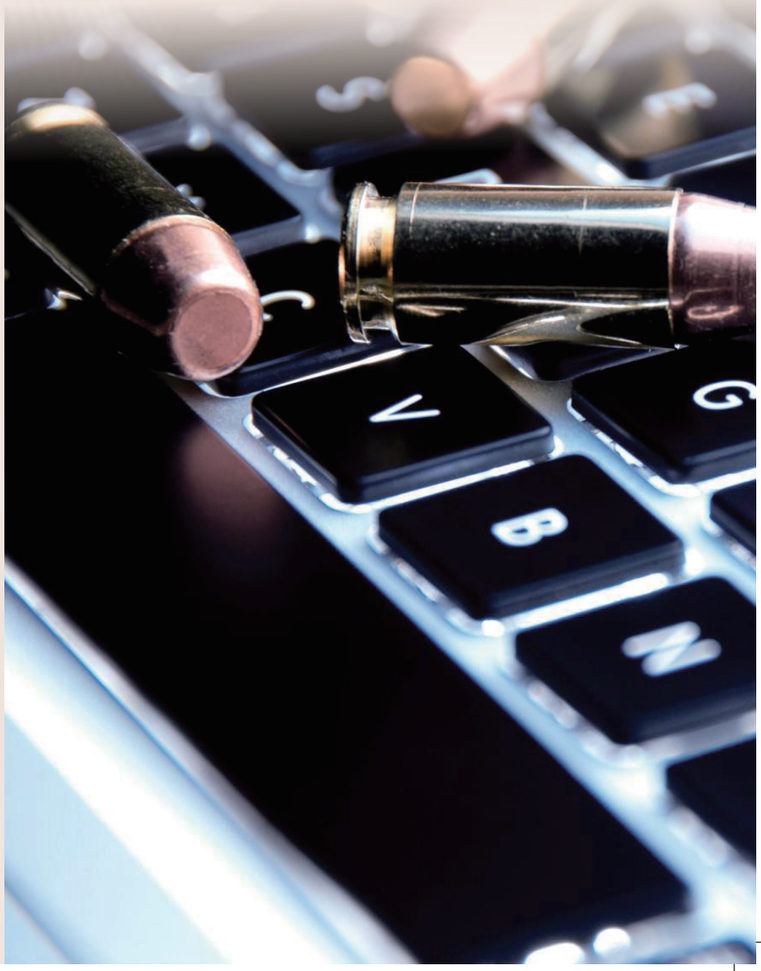
Cyber Warfare Doctrine Already Exists

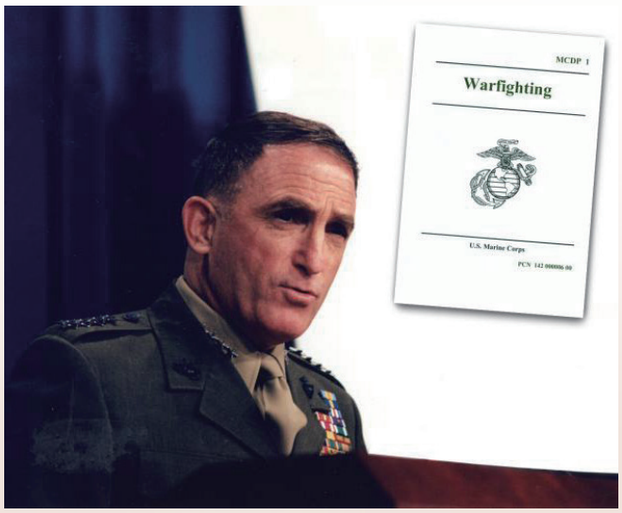
取材/2019年2月美國海軍學會月刊(*Proceedings*, February/2019)

網路戰的型態已臻成熟，此時需要制定準則以支持決策流程，而網路戰準則的概念需與時俱進，即可爲此領域提供一個如何思考的重要基礎。

在越戰結束後，當時美陸戰隊必須回答關於其在未來衝突中角色定位的根本問題。布魯金斯學會(Brookings Institution)曾在1976年主張陸戰隊應更新其在第二次世界大戰時期的兩棲突擊戰術，以求與時俱進。[1] 後來接踵而至的是一連串辯論，主要討論陸戰隊是否應維持現狀，但這種作法恐讓這支部隊遭致邊緣化的風險，或是採取一個新途徑，但可能會斲傷陸戰隊兩百年來所維持的特有文化。[2] 一方堅持機動式作戰，另一方則是主張持盈保泰，認為只須更新武器裝備並持續在《艦隊陸戰隊教範手冊》(Fleet Marine Force Manual)內容中正式修訂戰爭的屬性即可，諸如此類主張的論點往往尖苛不諱並直指艦隊，不管是在《美國陸戰隊月報》抑或遠征作戰高級班和陸戰隊指參學院的講堂上，都對這項議題議論紛紛。[3]

這類爭論最後在1989年告終，因為當時陸戰隊司令格雷(Alfred M. Gray)上將簽署了一份開創性的準則出版品，即第1號陸戰隊準則出版品：《作戰》(Warfighting)，這本手冊言簡意賅，內容正好超過一百頁，同時具有深遠寓意，[4] 其目的在於描述戰爭本質、戰爭理論、戰備及如何遂行作戰。在1997年時，另一位陸戰隊司令克魯拉克(Charles C. Krulak)上將更新了第1號艦隊陸戰隊教範手





美陸戰隊克魯拉克(Charles C. Krulak)上將授權發行第1號陸戰隊準則出版品：《作戰》，此作為無意間為網路戰準則奠定基礎。(Source: US Naval Institute)

冊，即現在的第1號陸戰隊準則出版品：《作戰》，內容指出作戰「不僅是行動指導，而且也是一種思維方式。」[5]

《作戰》準則概念不受時間影響，同樣能運用於當代網路戰，並為此一新領域提供一個如何思考的重要基礎。克魯拉克特別指出，「陸戰隊不能停滯不前，必須在不斷成長的經驗、理論進展及改變中的戰爭面貌等基礎下，持續向前邁進。」[6] 克魯拉克對陸戰隊準則所持的願景是需與時俱進，他也同時重視網路戰能力的發展，因為這對陸戰隊與海軍這兩個軍種均至關重要。

傳統的作戰準則與網路

克魯拉克在其所提出的「三面向戰爭」(three-block war)概念中認為，最底層的單位須在壓力與複雜情境下做出即時決策。[7] 他重視戰鬥中人的因素，並認為戰略下士(strategic corporal)這種初級幹部的影響力會比高階幹部來得大。克魯拉克的概念涉及了城市的三個面向，陸戰隊員須執行維和與人道救援作戰行動、反叛亂，以及進行同步或是前仆後繼的高密集衝突行動。然今日戰爭的作戰模式出現了第四面向：網路。

在新興且發展迅速的網路戰領域，運用陸戰隊準則可說是一個機會，同時也是一項挑戰。陸戰隊員思考、訓練、計畫作為及執行作戰行動等方式，正好可以為海軍的網路準則提供一個範本。《作戰》準則有三個部分與網路戰息息相關：一、攻勢與守勢作戰行動的本質兩者不可分割；二、機動作戰是一種手段，是為了要開創缺口並利用敵人的弱點；三、聯合兵種作戰方式是要讓敵人沒有獲勝可能。

攻守勢作戰行動相互配合

根據最新版的第1號陸戰隊準則出版品《作戰》，其內容指出網路戰涉及各種作戰行動，旨在保護與防禦關鍵資訊、電腦及網路設備，同時避免這些設備遭敵方所利用。[8] 如同其他作戰領域，攻勢與守勢不僅互為補強，兩者亦不可分割。在作戰層面上，資深軍事領導人必須做好萬全的因應準備，以利當面對敵人採取損害美國利益的行動，或是敵人於美國在敵網路領域採取攻勢行動後所做出的回應。在戰術層面上，侵略者也需要對相同戰術做好防禦之因應準備，因為別人同樣會採取「以子之矛，攻子之盾」。任何以防禦為主的計畫，註定是一個失敗的戰略，因為敵人在對美國攻勢做出反應時，就已喪失優勢的取得。簡言之，不斷將各種弱點極小化可說是相當短視近利。速度、行動流暢度及奇襲等概念的設計，必須用來塑造敵人的世界觀。

在守勢網路安全挹注大量投資，就足以掌控網路空間，克魯拉克如果聽到這種說法，一定會覺得很可笑。當他還是陸戰隊司令時，其授權出版的準則就體現了攻勢遠景，「進攻是防禦不可或缺的一部分。」[9] 麻省理工學院電腦科學與人工智慧實驗室史羅比(Howard Shrobe)副教授也認同以下看法，美國設置了制式化的安全分層機制，但這也導致架構上存有弱點。我們在無意間創造了戰術缺口，況且這種機制並無法處理不斷演進的威脅。[10]

在新興且發展迅速的網路戰領域，運用陸戰隊準則出版品可說是一個機會，同時也是一項挑戰。(Source: USMC/Tojyea G. Matally)

守勢網路投資雖然使領導人感覺更有安全保障，同時可以冒較低作戰風險。然而，當防禦科技與守勢作戰行動成為主要選項時，就會產生有限的行動方案與受侷限的機動能力。在人力資本與科技的投資必須平衡發展，但在網路的攻守勢方案之間，未必一定要平衡以對。一個常見的提問是，何謂夠安全的網路。但其實這個問題問錯了。更適切來說，大家該問的其實是這兩個問題：第一，何者是國家與軍種層級的網路戰略？第二，海軍該如何投資以達成戰略目標？一旦能回答這兩個問題，就能決定網路要做到何地步才算安全。

民間產業不斷在網路安全上挹注大量資金，原因是渠等只能仰賴守勢作為，像是〈電腦詐欺與濫用法〉(Computer Fraud and Abuse Act)等類法律限制，

壓縮了民間公司保護自身的攻勢選項，反而對那些攻擊者有利。在實體世界中，各國政府已同意民間公司僱用武裝警衛以保護資產與生命安全，以避免遭受武裝竊取與恐佈分子的威脅。

民間公司不被允許發動攻勢網路行動，而網路空間自警行為(cyberspace vigilantism)也會產生許多潛在的危險後果。然而，許多實體公司並無法遂行攻勢網路行動，此部分形成了一個重大的不利因素。[11] 鑑此，美軍必須藉由聯合兵種作戰方式，準備好網路空間的因應之道。

網路領域的機動作戰

機動作戰可提供海軍與陸戰隊團隊所需的靈活度與速度，以因應敵人在任何領域的行動，同時取得制敵先機，這種方式同樣也適用於網路空間。機動作戰的概念已在實體戰場上運用數千年了。在網路空間中，作戰指揮官一旦利用奇襲、欺敵、速度及靈活度等方式來提升機動能力，他們就能對敵人迎頭痛擊，使之吞下敗果。已故前美空軍上校波伊德(John Boyd)所創立的「觀察、指導、決心、執行」(Observe-Orient-Decide-Act, OODA)這一套決策循環模式，可做為在網路領域上思考機動作戰的一個可用架構。[12]

機動作戰可提供海軍與陸戰隊團隊所需的靈活度與速度，以因應敵人在任何領域的行動，這種方式同樣也適用於網路空間。(Source: USMC/Tojyea G. Matally)

在戰場上掌握全般狀況至關重要。一般而言，網路網絡的概念涉及諸如在家收看網飛(Netflix)、進行金融交易、在工作上收發電子郵件，或是各個指揮官在戰場上彼此傳送資料。不過網路領域也包含更大範圍的各種裝置、網絡及平臺，諸如各種控制系統、物聯網裝置及社群媒體等。社群媒體平臺現在已成為大量傳送訊息與假訊息的管道，這甚至是十年前所始料未及的。網路領域的複雜度也逐漸增加，因為該領域的變動性與時俱增。[13] 惡意行為者在這個複雜的網路領域中伺機而動，因此海軍與陸戰隊團隊必須對此一領域瞭若指掌，才能徜徉其中。

重視網路的領導人必須思考除了科技以外的整體環境。網路環境複雜度增加的原因，來自於大量形形色色的行為者。國家與非國家行為者、機器人、人工智慧、民間企業及公家機關等都是構成非線性環境的因素。不過戰爭的各項根本之道並未改變，即使網路交戰步調與複雜度提升，但狀況覺知仍對網路操作者至關重要，因為這些人要準備好因應各項惡意行動，同時將攻勢行動的附帶損害降至最低。

預判敵人在網路空間的各種活動，除了需要虛擬駐留外，有時甚至也要實施實體駐留。海軍與陸戰隊團隊之所以能成為適格的遠征部隊，是因為官兵打從從軍的第一天起就不斷接受訓練。網路作業人員在其專屬領域上，亦必須運用相同的

施訓模式，美軍需將這些作業人員放到名實相符的職位，並賦予其行動的自由與能力，進而遂行達成戰略、作戰或戰術目標所需「速度、聚焦及出奇不意」之效用。[14] 一旦覺知狀況，網路操作者必須是已備便好能執行決策循環步驟中最後兩項「決心、執行」的階段。

於此同時，網路操作者須孰悉科技。網路戰領導人亦要研讀孫子兵法的各種概念，像是欺敵、速度、行動流暢度、奇襲及形塑敵人的世界觀。網路戰的領導人──從基層乃至五角大廈高層──必須跟得上科技的發展，並使之成為網路行動的加乘因子。各領導人必須確保麾下網路操作者，有機會接受所有專業軍事教育。如此一來，重視網路的領導人就能擁有適切稱職之兵力，並向作戰指揮官提供各種選項，使敵人無法順利執行作戰與戰術作為。

包含網路在內的聯合兵種作戰方式

網路行動無法獨自發揮效用或僅躲在高安全門之後。大家必須視網路為在傳統聯合兵種作戰方式中的另一項武器選項。熟悉科技與戰術的領導人，必須也要能熟練地將網路整合至計畫作為與作戰行動之中。網路戰不能再被視為是另一種蒐集情資的戰爭模式，勢必要將之提升成與其他戰爭領域相同層級。

作戰目標永遠是去瓦解敵人的凝聚力，作法是針對敵人弱點施以聯合打擊。對海軍而言，這意味著資訊戰部隊必須展現其能駕馭網路領域並在其中移動自如，以利支援傳統作戰行動。因此，傳統作戰部隊必須時時備便以支援網路作戰行動。

大家或許不清楚何時與如何因應敵人在網路空間中的行動，況且戰爭因為在動能與非動能行動的廣大範圍下，變得更為複雜。這些包含在推特上散播網路謬論的敵人、阻斷網路流量、攻擊與破壞實體系統，以及在網路上的蓄意破壞行為。對國家安全領導人而言，或許最大的挑戰是去決定責任歸屬與如何因應。責任歸屬很困難，因為網路上的活動是匿名的，同時各個機構也不太願意向外公開證據。因應的決策取決於採用國力(外交、國際、軍事或經濟)中的某種手段，或是結合屬於國力的各種手段以構成最佳比例。[15] 鑑於上述複雜度，若要在軍種層級執行國家與國防部的網路戰略，將是一件具挑戰性的任務。[16]

既有準則依然有效

美陸戰隊在1989年完全接受機動作戰。與許多人士所持之的恐懼相反，機動作戰並未因此弱化陸戰隊文化，反而是直接對戰場成功做出貢獻。當大家檢視《作戰》準則內容時，網路戰與遠征作戰並無根本上的不同，而遠征作戰是海軍與陸戰隊的核心任務。網路戰的型態已臻成熟，此時需要制定準則以支持決策流程、科技發展路線，以及最重要的是進行人力資本投資。海軍與陸戰隊必須培養瞭解網路空間複雜本質的領導人，而渠等必須發展一支速度與節奏都符合要求的機動兵力。網路作戰必然同樣適用於聯合兵種作戰方式的計畫作為。

許多人的迷思是認為網路空

間的成功可以單靠投資科技。但所有海軍軍官一定要瞭解波伊德的名言，「機器無法打仗，但人可以，因為人會使用心智。」[17] 國家的網路戰領導人必須清楚明白根本道理，不管科技如何進步，都不會減少人類意志、獨創力的重要性，以及不管是在實體或是網路戰場上的創新力。

註：本文為網路徵文比賽第一名得獎作品。

作者簡介

Thomas Parker 係美馬里蘭州休特蘭 (Suitland) 海軍網路戰發展大隊的首位輪機值更官，他近期轉調至位於華盛頓特區的海軍海上系統指揮部。

Warren Parker 係湯瑪斯 (Thomas Parker) 的父親，2001 年自陸戰隊退伍，目前為三星戰略規劃公司 (3StarStrategicPlanning) 的合夥人，現居南卡羅來納州博福特 (Beaufort)。

註釋

1. Martin Binkin and Jeffrey Record, “Where Does the Marine Corps Go from Here?” review by Andrew J. Pierre, *Foreign Affairs* 54, no. 4 (July 1976).
2. Fideleon Damaian, “The Road to FMFM 1: The United States Marine Corps and Maneuver Warfare Doctrine, 1979-1989,” master’s thesis, Kansas State University, 2008.
3. S. W. Miller, “Winning through Maneuver Warfare: Part 1, Countering the Offense,” *Marine Corps Gazette,* March 1980.
4. Fleet Marine Force Manual 1, *Warfighting,* U.S. Marine Corps, 1989.
5. Marine Corps Doctrinal Publication 1 (MCDP 1), *Warfighting,* U.S. Marine Corps, 1997.
6. MCDP 1, *Warfighting,* 2.
7. Charles Krulak, “The Strategic Corporal: Leadership in the Three Block War,” *Marine Corps Gazette,* January 1999.
8. Marine Corps Doctrinal Manual 1-0, *Marine Corps Operations,* U.S. Marine Corps, 2011.
9. MCDP 1, *Warfighting.*
10. Howard Shrobe, “We’re Hosed and We’re All in this Boat Together: Governments, Industry, Academia All Have a Role to Play,” lecture, *Hack-The-Machine,* Cambridge, MA, 23 September 2017.
11. Nicholas Schmidle, “The Digital Vigilantes Who Hack Back,” *The New Yorker,* 7 May 2018.
12. Jeffrey N. Rule, “A Symbiotic Relationship: The OODA Loop, Intuition, and Strategic Thought,” Strategy Research Project, U.S. Army War College, 2013.
13. Peyton Price, Nicholas Leyba, Mark Gondree, Zachary Staples, and Thomas Parker, “Asset Criticality in Mission Reconfigurable Cyber Systems and Its Contribution to Key Cyber Terrain,” *Proceedings of the 50th Hawaii International Conference on System Sciences,* 2017, 6042-51, scholarspace.manoa.hawaii.edu/handle/10125/41893.
14. MCDP 1, *Warfighting.*
15. Jeff Farlin, “Instruments of National Power: How America Earned Independence,” Strategy Research Project, U.S. Army War College, 2014.
16. National Cyber Strategy of the United States of America, WhiteHouse, September 2018, www.whitehouse.gov./wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
17. Nancy Wesensten, Gregory Belenky, and Thomas J. Balkin, “Congnitive Readiness in Network-Centric Operations,” *Parameters* 35, no. 13 (spring 2005), 94-105, ssi.armywarcollege.edu/pubs/pa rameters/articles/05spring/wesenste.pdf.