作者/Jennifer Leigh Phillips　譯者/黃文啟　審者/黃依歆

網路領域的戰術用兵：支配敵人

Tactical Maneuver in the Cyber Domain: Dominating the Enemy

取材/2019年第二季美國聯合部隊季刊(*Joint Force Quarterly*, 2nd Quarter/2019)

網路領域係未來戰場的一部分，將來部隊在問題界定和設計戰役時，必須能具體看出網路領域和其他領域間的野戰與戰術介接面，方能將網路領域的戰術用兵融入聯合兵種多領域作戰，以利掌握未來戰場優勢。

2018年12月14日於夏威夷檀香山，美國佛羅里達大西洋大學所設計的自主式水面載具「制霸梟鷹」(Owltonomous)於美海軍研究室所贊助的「海洋機器人X挑戰賽」中與群雄競技。(Source: USN/John F. Williams)

在步兵排肅清街道時，史塔克利(Stokely)下士一過街角就遭到附近住宅高樓群中某制高點狙擊手射擊。先前這條街早已因為不明爆炸而陷入混亂，因此史塔克利可以看到狙擊手射擊那棟大樓的每層窗邊都有民眾探頭窺看。在數度設法消滅這名狙擊手未能成功後，這個排終於確認出其位置所在。該狙擊手就躲藏在這棟建築六樓的邊間。由於極可能造成該地區百姓傷亡，這支部隊一直沒有要求火力支援。現在聯合終端攻擊管制員(Joint Terminal Attack Controller, JTAC)開始要求火力：「網路01，這裡是L63，立即制壓座標211432，二棟，六樓，西南角，辨證碼TANGO UNIFORM，完畢！」對方立即回應：「這裡是網路01，立即制壓，座標211432，二棟，六樓，西南角，完畢！」一會兒之後，聯合終端攻擊管制員的網路遠距作戰影像強化接收器螢幕上就出現一名手持步槍的人，正背對著攝影機鏡頭。「L63，這裡是網路01，目標確認，要求確認是否立即制壓。」「這裡是L63，確認！」狙擊手旁邊的電視機突然爆炸，整個房間滿是碎玻璃和破片。這場爆炸擾亂了狙擊手，這讓該部隊能快速通過街道，持續朝目標位置前進。

想像一下，如果戰術小組能規劃一項不僅整合空中和地面支援，甚至還包含「網路」領域即時待命火力的突擊行動，將是怎樣的情景？在獲致節約兵力、降低成本、減少實際間接傷害等方面，真的充滿無限機會。為有效在未來戰爭中與敵競爭，美國必須充分掌握在網路領域內外用兵的能力以掌握主動權，藉此打亂敵人的認知決策能量。欲在網路領域獲致野戰及戰術層級用兵的戰果，美軍必須在準則、戰術和訓練等方面超越既有能量。

戰術網路用兵概念來自於認清物聯網將全面普及化的事實，其在未來二十到四十年必定充斥於人們日常生活的每個面向。物聯網將深入廣大城鎮地區和空曠鄉間，幾乎可以連結到目前世界上許多「孤立」的偏遠地區。

過去一直被視為美國軍事行動優勢的龐大實體戰力，已快速成為一種負擔。在近接和深遠作戰網路領域範圍內的擾亂性武力運用和操縱，已能透過戰術與野戰層次的網路用兵達到奇襲和震撼效果。未來軍事行動已不太可能任由人們選擇決戰時空。美軍或許認為自己可以主宰網路領域的戰略用兵，但商業、民間和系統性影響都將迫使戰術層級的軍事單位不得不在網路領域發揮攻勢效能。未來前線部隊在執行各類型軍事行動任務時，勢必會與物聯網進行互動。

當面對像俄羅斯或中共等具備科技均勢實力的敵人時，軍事人員很可能在認知、實體和/或虛擬面向上處於劣勢。因此，針對網路領域的概念性思維，必須揚棄目前對於戰略層級決策的堅持，轉向讓網路與聯合兵種在戰術和野戰用兵方面完全融合，使其成為達成國家和戰略目標的必要條件。美國的國防機制必須在適切戰術能力和實務教育方面進行投資，使美軍人員能在整體多領域戰法下有效執行網路領域的用兵任務。

野戰與戰術層級主動權的掌

2018年7月17日於美國德州聖安東尼奧(San Antonio)聯合基地，美空軍第558飛行訓練中隊中隊長(左)正和遙控飛機駕駛班學員討論如何利用T-6飛行模擬器來實施訓練任務。(Source: USAF/Bennie J. Davis III)

握，必須能充分利用網路行動癱瘓敵軍認知鏈路。時間和空間因素也對情報、指管及後勤等構成各種挑戰。今日在網路領域上採取線性和戰略被動的作法，無法肆應用兵方面的戰術與野戰協調需求。為了在實體、虛擬與認知等面向上獲致打贏戰爭所望創造的條件，必須重新強調網路領域和實體空間的跨界互動特性，以利精進聯合作戰準則、野戰用兵作為和各種戰術、技術及程序(Tactics, Techniques, and Procedures, TTP)。克服各種認知障礙，以了解此種跨界互動特性，必須透過聯戰部隊教育、訓練、模擬和演訓驗證，才能有利於統合作為，同時也要審慎質疑並挑戰美軍對於網路領域既有概念上的偏頗想法。網路領域的三項關鍵特質，將迫使美軍必須在聯合兵種多領域用兵上強化整合網路空間的各項考量因素：包含互動式複合系統；實體、認知和虛擬範疇

的交集；以及透過適當整合網路領域的戰術用兵行為，作為所有戰爭行為階段野戰布局手段，獲致非線性、以小搏大的戰略效果。[1]

網路空間戰術用兵的作戰考量因素

用兵：戰術用兵的各種要素必須在網路領域與其他領域之間善用虛擬、實體和認知關連性，進而透過多領域用兵作為達成野戰與戰術層級目標。未來分散式作戰行動的勝利，取決於配合其他領域遂行連續或同步整體行動時，能否在網路領域具備快速用兵之能力。美軍必須跳脫完全將重點置於遂行網路領域攻勢與守勢行動所需工具的僵化認知，轉而將重點置於透過能真正充分整合認知、虛擬與實體等網路領域面向的聯合兵種多領域用兵，以作為奪取主動權，達到宰制敵人的目標。第1號陸戰隊準則出版品：《作戰》(*Warfighting*)闡明如下：

> 勝利鮮少取決於有效率地落實程序和技術，主要取決於了解敵人系統的特質。用兵取決於速度與奇襲，而非能否集中兵力打擊敵人弱點。節奏本身就是一種武器，且通常為最重要的。用兵(不像打消耗戰)的成功通常與所投入之力量不成比例。然而，正因為相同的理由，若是採取無效用兵作為，就有極大的機會遭遇災難性挫敗。[2]

在營級(含)以下階層，戰術部隊必須有效對敵人發揮震撼與奇襲效果，而網路領域在某些特定情況下，可能是達成上述目標的最有效手段。美軍部隊目前已開始整合機器人、無人飛行載具、人工智慧及其他戰力。全軍部隊雖然已在聯合兵種用兵作為中融入網路領域，但目前僅有少數專業人員真正了解網路領域與其他領域之間的互動關係──亦即兩者間的介接面。美軍所有人員需更熟知網路領域和其他領域交互作用，才能澈底達成目前多領域用兵的典範轉移。顯然，網路並非用於取代其他形式的用兵和火力作為，而是在美國遂行軍事行動的作法之一。

今日企業界所擁有的大多數科技都是用於協助測度、規劃和利用網路環境。若將這些科技應用在野戰與戰術層級軍事目的，必須清楚掌握網路領域用兵作為，事實上與軍事任務攸關之人文及實體範疇有著實體和時間上的重疊。凡是能支持用兵作為的活動，亦適用於火力作為考量，且必須在準則和訓練上進行大量投資，以了解支持這些行動所需之後勤與情報需求。明確地說，後勤考量因素必須涵蓋各層級支援和結構管理需求項目，並將最新且新興的科技整合至分散網路環境。然而，網路領域相關用兵理念和概念必須優先於科技工具和軍品解決方案之投資。

火力：只要能獲得適當權限並建立指揮管制架構，網路領域的火力申請會類似於其他領域。在「部隊接觸時」透過網路摧毀或啟動虛擬/實體連結裝置以達致命性效果，此種手段可稱之為密接網路支援任務，其不見得會像空中密接支援能由肉眼看到實際效果。各種戰術必須運用建立一套類似網路的「火力申請」協調程序，以結合電子戰和資訊作戰。[3]

火力支援可透過作戰中心編設的網路小組提

供，或由美國網路司令部或聯戰指揮部所屬聯合網路中心提供深遠火力支援。在這些向上申請支援作為缺乏加密與可靠通信的條件下，未來戰術單位也必須盡諸般手段以擁有在自身網路領域建制火力支援的能力。至於遂行直接戰術網路火力任務的能力，來自於小組本身而不是本文一開始所述的「網路01」等向上申請作為時，並不會減少那些支援該小組的各類型單位在前述虛擬環境中，監控戰術網路直接火力效應的責任。

事先律定之網路空間協調程序與接戰規定，則用於防止網路效應超出範圍，以免網路領域環境鄰接部分所進行的戰術用兵作為發生意外狀況。任務執行前已確認為可採取網路用兵作為的環境，可能不見得恰好就在戰術單位進行實體用兵的特定作戰責任區域。即便在通

戰術單位未來須在自身網路領域中建置火力支援的能力，以利密接網路支援任務。(Source: USAF/Taylor Phifer)

信中斷或通信品質不佳的環境中，前述指定向上申請單位仍可監控網路環境外的溢出效應，以確保聯戰特遣部隊指揮官和/或兵種單位指揮官能充分了解網路領域環境發生的種種變化。

指揮管制：一如前述有關用兵與火力的考量因素，計畫與作戰部門人員必須發展出類似空域管制機制(Airspace Control Mechanism)的作為。然而，劃分地理疆界並不足夠，因為支援物聯網的應用軟體和網路架構，不見得會像支援用兵和火力任務所操作的裝置或程式一樣，會位於同一城市、地區或國家。在網路領域整合戰術用兵的作戰行動指揮管制，便成為減少非預期後果的基本要件。

決策人員必須檢討各種能擴大聯戰特遣部隊以下階層，戰術部隊指揮官權限的機會，以遂行網路領域用兵的攻勢和守勢任務。此種權限擴張應包含審慎分析現有接戰規定及《武裝衝突法》(Laws of Armed Conflict)的適用性，以檢討網路領域的兵力運用方式。針對軍隊如何擴充權限，以及在後勤方面如何協助被動與非傳統機制從事即時監控、溝通與協調，以促成未來更多元指揮管制的作法，乃是有必要進一步深入研究的議題。

正義戰爭考量因素：羅特瑞(Gregory J. Rattray)曾針對有關網路領域用兵問題提出一個有趣的想法，其對於軍隊接戰規定方面的影響，或許值得深入考量。羅氏明確提出所謂微兵力(microforce)的概念，在此種概念下「運用非暴力數位攻擊以達成政治目標的行為，必須視為新型態戰爭行為之一部……此一方面的相關議題就是某項武器在攻擊時所能發揮的能量有多大。」[4] 先不論數位攻擊是否真的代表一種全新的戰爭行為，認清網路領域行動是一種能量或暴力的形式，對於引述正義戰爭理論相關內容適用性具有相當助益。或許目前動能與非動能武力的概念必須進行調整，才能認清武力就是一種暴力行為，不論此種武力的效應是否可由肉眼或感測器加以判別。如本文一開始所提之例證，透過網路領域的戰術用兵發揮制壓敵人的效果，存在著直接對非戰鬥人員造成無辜的間接傷害，或原本用於軍事目的手段對民間網路不小心造成破壞的可能性。

假設此一觀點認為網路領域應視為與其他領域同等的環境，有助於釐清網路領域考量因素與正當戰爭手段(jus in bello)原則的關連性。正當戰爭手段對於美國軍隊而言，攸關正義戰爭理論的西方道德與哲學傳統，以及構成國際人道法律的各種國際協議與條約等。

各種機會來臨

前線部隊進行網路戰術用兵作為整合，置重點於透過攻勢用兵達成所望目標。美軍應設法從孤狼行為汲取經驗，以作為未來網路領域戰術用兵的依據，而非僅強調個別行為者的威脅和孤狼所能構成潛在不成比例的效應。這些教訓亦可作為遂行網路領域戰術性攻勢行動時所須考量的克制之必要條件，正因為此一複合性系統內部各環節的互動有可能造成不成比例的潛在後果。

了解網路領域是一個複合式體系：軍事計畫作為是一項解

決問題的演練。當面對某項軍事想定或挑戰時，計畫人員必須設計出某種依據有效和完整問題界定以獲得成功的作法。未來的計畫人員必須構思所有領域戰術行動的背景，包含互動式網路和網路領域構型。根據傳統軍事計畫作為的假設，只要將指揮官的指導和任務轉化為各種目標和各部隊戰術任務，計畫人員就能在所有領域採同步或連續性作法，進行兵力派遣和執行作戰任務。然而，適切計畫作為需要審慎分析這些領域對於人類認知和所有領域環境條件影響的多面向本質。

戰術層級軍事計畫作為融合網路領域似乎將威脅到簡約原則。當代戰略著作和論述對於網路領域過度戲劇化的描繪，似乎已經蒙蔽了在此一領域問題解決方法的清晰思路。然而，網路領域是一個具有互動特性的複合式體系，今日已經有多種有效技巧，可建立對網路空間領域多面向關連性和層次的了解。透過嚴謹探究網路空間虛擬、實體和認知面向間的關連性(介接面)，軍事計畫人員可望獲得各種機會，找出網路空間與其他戰術行動配合的同步及縱深特質。密切掌握更廣泛野戰與戰略層級目標是所有計畫作為的基本要件；計畫作為融合網路領域亦無例外。

在網路領域戰術用兵作為成功獲致簡約性的關鍵要件之一，就是跳脫對軍品解決方案的依賴，並優先將重點放在本文所論述的各種想法和概念，以利逐漸建立對網路領域的共同認知。雖然共同作戰圖像、電腦網路防護和電腦網路攻擊工具，都將是遂行網路領域戰術用兵作為的需求要項，在從事軍事行動上對此一領域所具複雜性的共同及全般了解更是必要條件。在功能性解決方案分析中列入「準則、組織、訓練、物資、領導統御、人事、設施及政策」(doctrine, organization, training, materiel, leadership, personnel, facilities and policy, DOTMLPF-P)等考量因素，是本研究重要的後續走向。今日美軍聯戰部隊已被迫聚焦在建立基準性的網路領域共通知識，因為此種背景知識已被視為讓軍事計畫與作戰單位人員了解網路環境，並得以在此一環境從事成功戰術用兵作為的必要條件。

雖然美國國防部的資安訓練已成為教導所屬官兵保護自身在網路領域各項活動的標準工具，但目前仍無統一的必要訓練項目，用於建立整個聯戰部隊進行網路領域溝通的共同詞彙和語言。雖然「中階發展教育」(Intermediate Developmental Education)可提供美軍軍官認識網路領域概念，但此種訓練的內容太少，也不能快速讓戰術部隊建立低階軍官和基層士官兵所需要的計畫作為能力。採取統合性作為打破網路領域的「神祕面紗」，可以直接促進官兵在計畫作為與命令撰擬方面的明確性。

最後，軍事設計還應考量如何融入各種和網路領域有關的正義戰爭原則。各式各樣的政策、法律考量因素和接戰規定程序仍持續影響網路領域中某些戰術的實用性。康乃爾大學生莫里斯(Robert Morris)在1988年所散布的「莫里斯蠕蟲」就是拙劣計畫作為與風險消弭手段所導致潛在負面影響

的例證。莫里斯散布該電腦蠕蟲的原意，是想計算當時網際網路的規模有多大。然而，莫里斯隨機植入電腦蠕蟲以確保其能成功滲透各種系統，卻造成蠕蟲大量複製並完全癱瘓其所進入的所有電腦系統。如前文所述，戰術、技術及程序和管控機制的應用範圍應包含風險消弭作業程序，以利限縮各種不預期後果。更明確地說，癱瘓某村莊或城鎮的WiFi或WiMax網路，以防止當地居民向地方政府機關通報戰術單位所在位置的作為，也可能擾亂醫療通報系統、安寧病患居家監控設備，或其他一般民眾所使用維生活動等所不樂見後果。隨著民防和民間網路基礎日益依賴通用架構骨幹，工具開發和戰術、技術及程序策擬必須置重點於，目標區隔手段和裝置與網路的識別作業程序，以利在最大可能範圍內限縮無辜間接傷害發生的情況。

若在缺乏廣泛與特定主題的專業知識下，想要克服網路領域分析和解決問題無疑是天方夜譚，這種缺失也會撼動軍事上統一指揮的原則。軍事計畫作業團隊解決問題時，必然包含深究問題性質及對高階領導幹部明確說明挑戰這兩大部分。除此之外，高階領導幹部必須充分了解網路領域所存在的各種風險、假設條件和機會。最後，各級指揮官必須有信心承擔給予戰術階層部隊行動自由的風險。網路領域已證明與其他領域一樣存在風險，但指揮官若不了解網路就必然會選擇較能避險的方式。

利用網路領域所有實體、認知與虛擬面向的交集：未來計畫作為需要計畫人員將網路領域的認知、實體和虛擬特質，視為與陸海空和太空等實體領域同時存在且同步進行互動的項目。軍事行動中欲充分說明界定問題，將包含找出前文所討論網路與其他領域存在之介接面、發掘運用這些橋樑的機會、同時提供周密機制，以利在攻勢或守勢任務中運用這些橋樑。

震網(Stuxnet)電腦蠕蟲造成伊朗納坦茲(Natanz)核子設施內鈾氣體離心機實體損害的個案，就是透過網路領域利用虛擬與實體介接面功能的最明顯例證。[5] 一如莫里斯電腦蠕蟲，震網蠕蟲有一特定目標，但設計者讓震網蠕蟲只針對某些規格，希望將效果侷限於針對納坦茲核子設施內的那些鈾離心機管。有效界定問題和審慎確認虛擬與實體面向的關連性，是確認遏止伊朗擴大其鈾濃縮計畫所望手段的必要步驟。此一問題界定作為，使設計人員得以透過虛擬世界的操縱作為，獲致實體面向中的所望效果。此外，伊朗政府最初還完全未偵測到這個電腦蠕蟲的存在，當機械(實體)問題開始出現時，其原本還認為是發生了實體缺陷或故障。因此震網電腦蠕蟲透過網路領域的虛擬行動，獲致實體和認知上的雙重效果。

雖然震網電腦蠕蟲攻擊係依據戰略優先訴求進行授權，但其計畫作為、電腦蠕蟲開發和任務執行等卻需要戰術層級重點作為，包含由技術精熟的專家團隊進行廣泛網路間諜活動。在界定問題以決定如何癱瘓納坦茲鈾濃縮作為時，計畫人員必然已經想出如何在網路領域中找出那個虛擬介接面，以獲致實體效果。就此一方面而言，認知與網路領域交互作用，可同時從攻擊者和受害者的身上看到。尤其，震網電腦蠕蟲攻擊事件

2018年4月，美陸軍快速反應能力辦公室(Army Rapid Capabilities Office)和電子戰暨網路計畫協調官(Project Manager for Electronic Warfare & Cyber)於德國格拉芬沃爾跟美陸軍第173空降旅第2騎兵團及其他接收單位共同合作，執行第18號聯合作戰評估。(Source: US Army)

若從兵力集中與節約的角度觀之，可看出在網路領域中進行戰術層級用兵作為的適切作法。

以色列當局在震網電腦蠕蟲攻擊事件中透過所有領域的充分戰場情報準備，達到節約兵力的目標。這個例證也凸顯出，網路領域技術與人文考量因素間的介接面。雖然確認適當介接面的模控(cybernetic)問題，基本上是一種科學方法，但希望達到的地緣政治效應和後續結果，卻屬於更高層次的「棘手性」問題範疇。[6] 利用網路領域機會的決策，之所以成為解決以色列當局問題的指定選項，就在於其符合決策當局可用「行動可能性」的範圍。[7]

一個適切擁有已確知介接面機會「地圖」的團隊，透過軍事準則、訓練和戰術的精進作為，可以在戰術用兵作為中保持攻勢，同時還能限縮對無辜的平民間接傷害。即便在今日最缺

乏網際網路連結的國家，行動電話和WiFi科技的廣泛運用(同時在缺乏此類科技整合網路的條件下，使用這些裝置仍然可以透過諸如藍芽等點對點連結進行彼此相連)仍能創造可奪取主動權並發揮戰術優勢的機會。雖然使用重量級空投彈藥攻擊某好戰分子射擊戰術小組的大樓恐怕不可行，但卻可以利用諸如電視和電話等彼此連結的裝置，被動窺視狙擊手進行射擊所在的房間情況。假如戰術部隊可以精確找出敵方火力的確切來源，運用電線短路而產生實體效果、以手機電池過熱製造低威力爆炸，或開啟電視進行擾亂等方式創造介接面，都會成為可能手段。如此一來便達到了消除敵人的目標。

網路領域的戰術層級用兵作為，只有將其視為聯合兵種多領域用兵作為的可行條件才有可能執行。美軍目前的兵力結構和科技當然無法使此種想定落實為事實，但重新調整準則和政策，就可以完全實現DOTMLPF-P解決方案，以滿足這些需求。

在戰術層級獲致非線性、不成比例戰略效應：第3號聯戰出版品《聯合作戰》(*Joint Operations*)明述，「各級指揮官得執行(網路作戰)以確保網路空間之用兵自由、達成聯戰部隊指揮官目標、阻止敵人獲得行動自由，以及促成其他作戰活動。」[8] 然而，多數軍事論述仍基於以網路為核心之考量因素，聚焦於戰略性網路或只專注於網路領域效應，而非基於真正多領域用兵作為的考量。雖然任務組合的領導統御與戰略是探討領導統御、訓練、計畫作為和戰爭中動能行動的主流，但有關網路領域的一致性趨勢仍是完全切割其應用，正因為該領域被認定之「特殊性」。但戰場上所執行的所有戰術任務，必須回歸其戰略目的。戰術和野戰層級網路用兵作為具有讓軍隊獲致非線性、不成比例戰略效應的潛力。

為了解此種戰術層級網路用兵的樣貌，「非線性、不成比例戰略效應」一詞，應從適切之問題解決背景去分析。軍事計畫人員在尋求解決各種問題時，都會涵蓋科學和人文因素。戰爭之目的在於擊垮敵人的意志，使其無法擁有持續作戰的欲望和能力。人類的意志可透過網路領域表達且受其影響。雖然政策制定者無法忽視此一媒體的戰略控制重要性，但打擊個人意志基本上就是戰術用兵問題──利用敵人的弱點，並讓我方弱點看來像是強項。為有效達成此一目的，必須在美方對網路領域的概念認知上進行改變。俄羅斯在2008年喬治亞危機時於網路領域進行戰術用兵的能力，提供人們運用可讓網路領域與未來軍事行動融合之多領域用兵原則的寶貴經驗。

儘管有人主張俄羅斯在其地面用兵行動中採取打擊喬治亞網路基礎設施的作為，並非由戰術層級單位進行，但透過此一行動中以先期網路空間火力奪取主動權並獲致節約兵力的效果，其價值卻十分明顯。針對喬治亞民間和政府網路基礎設施所發動的大規模電腦網路攻擊，雖然無法正式證明和俄國政府有關，但卻達成明顯的軍事目標。此項電腦網路攻擊使喬治亞無法精確判斷俄羅斯地面軍事行動的兵力和方向，並防止觀察人員、軍事單位和高層

決策專家彼此進行溝通和判斷。這場網路領域攻擊因而在模糊性和資訊缺乏的情況下，阻止外界對俄羅斯侵略行為採取有效的初期反應。除此之外，這次攻擊行動利用當地部分民眾支持俄羅斯的情緒，對俄羅斯入侵的真實本質、意圖和範圍造成混淆。隨著該次戰爭進展，俄羅斯在網路領域用兵作為的程度、時間和範圍亦隨之改變，以符合俄國計畫人員的軍事需求。

網路領域不應置重點於其範圍內所發生的各種行為，不論是阻斷、欺騙、間諜、攻擊或用兵，網路領域都應優先將這些因素視為一建制性環境。人類會影響網路領域且受其影響，一如在陸海空和太空領域。人們在通過網路領域時，與行經陸地或駛過海洋並無不同。在未來的世界中，網路領域涵蓋所有範疇，以被動和主動方式結合了人類、裝置和多層次的各種網路。

網路領域的用兵作為並非全新概念，因為我們每個人在日常生活中都與網路領域的實體、虛擬和認知面向互動並進行操控，另將網路領域的戰術用兵視為軍事行動中聯合兵種多領域用兵作為的一環，是一種必須更深入研究並融入軍事準則與戰術的概念。部隊在網路領域方面的有效教育，是培養未來計畫人員、作戰官兵和領導幹部的基本要件，如此這些人才能掌握網路領域。未來的部隊在從事問題界定分析和設計戰役計畫，以追求戰略層級軍事和國家目標時，必須能具體看出網路領域和其他領域間的野戰與戰術介接面。建立網路領域涵蓋所有平民和軍事生活的共同認知，是軍隊為此種必然未來做好準備的第一步。

作者簡介

Jennifer Leigh Phillips博士係美空軍後備役少校，以個人動員身分派任美空軍第607空中作戰中心情監偵處副處長。她同時於南加州大學擔任教育系助理教授。

Reprint from *Joint Force Quarterly* with permission.

註釋

1. 「階段」(phase)一詞係指特定作戰計畫所律定之各作戰階段。詳見Joint Publication 3-0, *Joint Operations* (Washington, DC: The Joint Staff, January 17, 2017), V-6.
2. Marine Corps Doctrine Publication 1, *Warfighting* (Washington, DC: Headquarters Department of the Marine Corps, June 20, 1997), 38.
3. 依據第6-30號陸軍野戰教範：《觀測火力之戰術、技術及程序》(*Tactics, Techniques, and Procedures for Observed Fire*, Washington, DC: Headquarters Department of the Army, July 16, 1991)，火力要求包含在三次報告中所列的六個部分。雖然在眞正的近接戰鬥網路支援，可能必須增加其他部分或補充，但實際協調機制仍然完全相同。
4. Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge: MIT Press, 2001), 20.
5. 針對震網電腦蠕蟲的詳細個案研究，詳見Chris Morton,"Stuxnet, Flame, and Duqu: The Olympic Games,"in *A Fierce Domain: Conflict in Cyberspace*, 1986-2012, ed. Jason Healey (Washington, DC: Cyber Conflict Studies Association, 2013), 212-231.
6. Horst W.J. Rittel and Melvin M. Webber, "Dilemmas in a General Theory of Planning," *Policy Sciences* 4, no. 2 (1973), 155-169.
7. Ibid.
8. JP 3-0, III-9.