於網路領域之戰術作為－宰制敵人 (Tactical Maneuver In The Cyber Domain)

譯者／朱子宏中校

作者/ Phillips, Jennifer Leigh

提要

一、美陸軍訓準部於 2018 年 12 月發行《美國陸軍多領域作戰 2028 願景》，將多領域分為地面、海洋、空中、太空以及網路等五大類，然而網路領域之戰術作為仍然受到政策與法規之限制。

二、美國在發動任何軍事行動之前，均會考量國際法、國際公約或者是國際人道主義等，使其師出有名，然而網路領域的戰術作為，成為了美軍未來軍事行動的必須考量之面向。

三、網路領域之戰術作為，可以突破傳統戰術作為，用兵上達到節約與集中之原則，並且在戰術層級與戰役層級創造出不對稱作戰的戰略效果，進而克敵制勝，主宰戰場。

關鍵詞：多領域作戰、網路作戰、不對稱作戰、非線性作戰、正義之師。

前言

美陸軍訓準部於 2018 年 12 月 6 日發行了《美國陸軍多領域作戰 2028 願景(The U.S. Army in Multi-Domain Operations 2028)》，將戰場區分地面、海洋、空中、太空及網路等五大領域，其中網路領域之應用包含了電磁活動、資訊流通以及人文操控等內涵，進而可以透過網路領域發展出電子戰、資訊戰、輿論戰、法律戰以及心理戰等。[1]

然而，雖然美軍在武器科技與戰術戰法雖然大多數都是領先集團之一。但是，美國身為一個世界大國，想要達成其戰略目標，進而謀求國家安全與利益的同時，也必須扮演著世界模範生的角色。因此，雖然美軍擁有先進的戰機、龐大的航空母艦群，或者是精良的坦克車等，但是唯獨在網路作戰上受限於政策、道德以及國際人道法、武裝衝突法及接戰規定等，無法大刀闊斧的執行戰術作為。在進入本文之前，先看一段小故事：「當排上執行街道掃蕩，史多克利下士轉進街角時，遭到來自公寓大樓群中制高點處的狙擊手射擊。在不明爆炸物爆炸時，街道上早已是一片混亂，史多克利下士見到許多人蝟集於各樓層的窗戶旁邊，同時也是狙擊手射擊處。經過了幾次嘗試制壓狙擊手的行動失敗後，單位確認了狙擊手的位置。狙擊手位於街角公寓大廈的六樓。單位因考量可能在此區域造成民眾傷亡的潛在因素，無法使

[1] TRADOC Pamphlet 525-3-1, The U.S. Army in Multi-Domain Operations 2028(Washington, DC, Department of Army, December 6, 2018), pp.vi-viii.

用實體火力支援。聯合前進攻擊管制官(Joint Terminal Attack Controller, JTAC)請求火力支援：『網域一號，這是 L63，請求對座標 211432，第二棟建築物西南角六樓進行立即制壓。辨證碼為 TU，完畢。』對方回應：『這是網域一號，立即對座標 211432，第二棟建築物西南角六樓進行立即制壓，完畢。』片刻過後，圖像在聯合前進攻擊管制官操控中的網路螢幕載臺上呈現，一個持有步槍的男子正背對著監視器設備。『L63，這是網域一號，目標已確認，請求確認立即制壓之要求。』『這是 L63，確認無誤。』位於狙擊手附近的電視設備爆炸，玻璃及碎片飛遍整個房間。爆炸干擾了狙擊手，使得整個小隊得以快速通過街道，繼續前往目的地。」

本文

看完上述的故事，想像一下當戰術層級之部隊執行突襲作戰時，得以整合空中、地面以及網路空間火力攻擊的可能性，進而達成節約兵力、減少成本並且降低實體的附加傷害，這對於未來的戰爭可以創造出無窮的機會。為了能於未來戰爭中有效地與對手競爭，美國必須具備網路空間中以優勢的戰術作為來瓦解敵人認知決策能力，進而奪取先制。為了達成在網路領域中戰役與戰術層級作戰的成功，美國軍隊需要於現行的準則、戰術及訓練上多挹注資源與心力。

網路作戰的概念來自於對物聯網(Internet of Things, IoT)興起之認知，在未來 20 年到 40 年之間，物聯網將會遍布各個角落。物聯網將會存在於大型都會區域，並逐步擴展至農村，以及鏈結到人們認為未與世界接軌的區域。在以往，美國軍事作戰所留下來的龐大實體足跡是一種優勢，但是現在卻成為了一種責任。在戰術層級與戰役層級的網路作戰中，軍事行動將未必能夠由我們選擇時間與地點，然而在近接與深遠作戰中運用部隊干擾與操縱網路領域之戰術作為，可以使對方驚慌失措。美軍也許會發現他們雖然能夠於網路領域中管控部隊的戰略運用，但是對於商業、民間及系統的影響，將會迫使戰術單位於網路領域中採取攻勢作為。

當面對科技水平如俄羅斯或中共之敵人，軍隊可能在認知、實體及虛擬層面上處於劣勢。因此，針對網路領域的概念發想必須跳脫依賴戰略層級決策的困境，進而在戰役層級與戰術層級作戰中整合網路能力與聯合兵種部隊，來達成國家與戰略目標。我們的國防體系必須在戰術能力以及人員教育上進行適切的投資，使其在多領域作戰下的網路空間內無往不利。

戰役與戰術之主動仰賴網路作戰的運用，進而擾亂敵人的認知鏈結。時空因素也帶給情報、指揮管制及後勤方面的挑戰。今日於網路領域中採取傳統的線性戰略將無法滿足戰術及戰役層級作戰之需求。為了能夠在實體上、虛擬以及認知層面中作戰勝利而達成所望戰果，必須針對跨越網路領域及實體空間的面向修訂準則，改善作戰訓練及戰術、技術與程序(Tactics, Techniques, and Procedures, TTPs)。克服認知障礙，並且具備跨域思考之能力，同時

也需要透過聯合部隊之教育、訓練、模擬與試驗來不斷地探詢與挑戰我們在網路領域概念上的成見。下列三個關鍵的屬性使美軍強化其聯兵部隊在多領域作戰中網路空間的整合：一套互動複雜的系統；實體、認知及虛擬的交集；與非線性(Nonlinear)、不對稱(Disproportionate)戰略效果，欲於作戰全程達成此目的，可透過戰役設計過程中，適切整合網路領域中的戰術作為。[2]

網路空間之戰術作為應考量的因素

一、兵力運用

戰術作為之要件必須掌握網路領域與其他領域間在虛擬、實體及認知上的鏈結，進而藉由多領域作戰達成戰役及戰術目標。未來作戰的成功仰賴於網路領域中迅速的作戰節奏，同時也是跨領域作戰中逐步與同步整合的一部分。我們必須摒棄在網路領域中著重在運用工具採取攻防的固有觀念，轉而朝向在多領域作戰中整合實兵部隊與網路領域中對認知、虛擬及實體層面的操控，奪取先制權，進而宰制敵軍，依據海軍陸戰隊準則第一號，作戰篇所述：「成功不僅只仰賴在程序與技術的優異表現，而是瞭解敵軍體系的特性。作戰仰賴速度與出其不意，若不如此，我們無法集中戰力攻擊敵弱點。速度就是武器-往往是最重要的因子。機動作戰之勝利不同於消耗戰，通常仰賴不對稱作戰之成效。然而，同樣地若無法妥善運用機動作戰的特性，極有可能帶來毀滅性的失敗。」[3]

在營級(含)以下的單位，部隊必須有效地使敵人驚慌失措，網路領域之戰術作為可能在某些情況下成為最適合的手段。美軍近來整合機器人、無人飛行載具(Unmanned Aerial Vehicle, UAV)、人工智慧(Artificial Intelligence, AI)及其他能力，聯合兵種部隊已經與全軍的網路領域完成整合。但是，真正的問題在於整合網路領域及其他領域的專才目前卻非常稀少。全軍需要針對可以整合網路領域與其他領域的人員進行更高等的教育，如此才能扭轉既有的多領域作戰概念。顯而易見地，網路不是用來取代兵力以及火力，而是成為作戰任務的之一部。

現今許多商業科技支援繪製、覆蓋及運用網路環境。為了於戰役或戰術層級運用這些科技來達成軍事目的，必須清楚瞭解網路領域中有利於達成軍事任務的人文與地理面向。這些作為足以支援作戰外，也能夠應用在火力運用構想及滿足任務中後勤與情報需求，但是這些都必須仰賴準則編纂與人員訓練的投資。明確地說，後勤考量事項要涵蓋建築支援與指令管理之需求，這些新興科技必須整合入網路環境中。然而，未來在網路領域執行作戰相關的概念之前，必須先滿足硬體的需求。

二、火力運用

---

[2] The term phase specifically refers to the phases of an operational plan as articulated in Joint Publication 3-0, Joint Operations (Washington, DC: The Joint Staff, January 17,2017), V-6.

[3] Marine Corps Doctrine Publication 1, Warfighting (Washington, DC: Headquarters Department of the Marine Corps, June 20, 1997), p.38.

在網路領域中提出火力支援要求，和其他領域一樣，須具備適當的權限與指管架構。所謂的網路密支任務，係藉由網路，在部隊接敵狀況之下來摧毀或是啟動一條界於虛擬與實體之間的鏈結，進而造成致命的效果。雖然網路密支任務不會比運用空中密支攻擊所造成的效果來的明顯，但是仍將需要結合電子戰及資訊戰等手段建立相同的火力支援要求。[4]

網路領域之火力支援可以透過作戰中心附屬的網路單位提供或者經由美國網路指揮部或是聯合部隊指揮部(Joint Force Command, JFC)下轄的網路中心提供深遠火力支援。在未與上述單位建立起安全無虞的通聯方式下，未來戰術單位必須儘可能地於網路領域中運用其建制火力支援。這項能力著重於提供來自於建制單位的直接網路火力支援任務，而非上級網路火力支援單位，正如小故事中的「網域一號」，它將無法分擔協助故事中遭敵分散的單位，僅能負責透過虛擬層面監控火力射擊效果。

先期建立之網路空間協調程序及接戰規定，是用來減少於網路領域執行戰術作為時溢出或產生之後果。在執行任務之前，適合網路作戰的環境未必會與戰術執行單位實際作戰的區域相重合。即便在沒有通訊或是通訊受阻的環境下，前述的網路作戰單位可以監控網路環境外的效果，確保聯合特遣部隊指揮官或是部隊指揮官可以掌握網路領域環境的改變。

三、指揮與管制

無論是兵力運用還是火力運用，計畫人員及執行人員需要發展與空域管制類似的管制機制。然而實體的地境未必能夠滿足其需求，當藉由操控設施與程式來協助作戰以及射擊任務時，其網路架構未必與物聯網坐落於同一個城市、地區或是國家。整合網路領域中戰術作為的指揮與管制對減少意外後果是非常重要的。

決策者應當審時度勢，適度授權聯合特遣部隊之下級單位指揮官於網路領域中執行攻擊及防禦。權力下授前應謹慎分析接戰規定(Rules of Engagement)與武裝衝突法是否適用於網路作戰。更進一步地檢視軍隊如何利用被動式及非傳統的監控、通訊及協調作為來協助後勤支援，進而提供指揮官多元的選項。

四、正義戰爭的考量

Gregory J. Rattray 提出了一個關於在網路領域用兵的有趣想法，也許對於未來在運用軍事接戰規定時有所助益。他特別指出了微型部隊(Micro Forces)的構想，即是「運用非暴力型的數位攻擊來達成政治目的，必須被視為一種新興的戰爭型態…這裡的爭議在於武器攻擊當下釋放出的能量。」[5]先把數位攻擊是否呈現為一個新的作戰型態的問題擱在一旁，先瞭解網路領域的所有行動均屬於一種能量或暴力行為，將有助於正義戰爭理論之運用。也許當前對

[4] Per Field Manual, Tactics, Techniques, and Procedures for Observed Fire (Washington, DC: Headquarters Department of the Army, July 16, 1991), p.6-30, calls for fire consist of six elements sent in three separate transmissions. While additional elements or subelements may need to be adopted for real-time cyber support in a close combat situation, the practical coordination mechanisms would remain the same.

[5] Gregory J. Rattray, Strategic Warfare in Cyberspace (Cambridge: MIT Press, 2001), p.20.

於動能攻擊與非動能攻擊的認知上需要調整，無論是否可由肉眼辨識其效果，均應被視為一種暴力行為。正如同開場小故事所描述，網路領域中戰術作為所造成的效果有可能對非武裝人員造成不預期的直接傷害，或是在民用網路上為達成軍事目的而造成的溢出傷害。

假設對於網路領域的認知被視為與其他的領域相同，能夠協助釐清網路領域作戰應考量之戰爭手段正當性下。戰爭手段正當性運用在美國軍隊之中，除了考量道德及西方傳統正義戰爭理論哲學，也包含了國際人道法的國際協定與條約。

機會出現

整合部隊與網路領域的戰術作為，透過攻勢作戰來達成目標。強調個別行為者的威脅性及孤狼式攻擊所帶來的潛在不對稱作戰效果，我們更應該尋找並學習孤狼式的攻擊經驗，來因應網路領域的戰術作為。因為複雜系統內的交鋒所帶來的潛在後果，可以透過這些經驗協助瞭解網路領域中攻勢作戰的重要限制條件。

一、瞭解網路領域為一個複雜系統

軍事計畫作為是用來解決問題。當呈現一項軍事想定或挑戰時，計畫人員必須設計一條以成功為基礎的有效途徑來界定問題所在。未來計畫人員必須擘劃出所有領域的戰術行動內容，包含了網路領域中的互動式網路與指令。傳統軍事計畫作為係依據指揮官指導事項與任務目標及戰術行動來進行闡述，計畫人員能夠以同步或者是連續的方法來執行跨領域的作戰。然而，合宜的計畫需要謹慎分析這些領域所有的影響面向，包含了人文觀點與環境狀況。

將網路領域整合入戰術計畫中似其違背了作戰的簡單原則。有鑒於浮誇的戰略文獻與語言有助於釐清網路領域中的問題。但當此領域屬於一個互動型的複雜系統，現在我們可藉由高效率的技術來發展我們對網路空間領域中多面向鏈結與層次的認知。經由對網路空間領域中的虛擬、實體及認知層面的連接與鏈路進行嚴謹的調查，軍事計畫人員希望能夠達成在網路領域中與其他戰術行動同步且深入的整合。密切掌握更好的作戰與戰略目標是所有計畫中重要的一環；將網路領域整合入計畫之中更是不可或缺。

未來成功要素之一是在網路領域中執行簡單易懂的戰術作為，此舉仰賴物質解決方案及優先著眼在網路空間中對於共同資訊分享的革新想法與概念。當共同作戰圖像(Common Operating Picture, COP)、電腦網路防禦(Computer Network Defense, CND)與電腦網路攻擊(Computer Network Attack, CNA)成為網路領域執行戰術作為的要素時，對於在複雜的網路領域中所執行的軍事行動有著全盤且完整的瞭解是非常重要的。整合準則、組織、訓練、物資、領導統御、人員、設施及政策(Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, and Policy, DOTMLPF-P)等考慮事項，為解決方案分析重要的一環，也是後續整合作為的一部分。軍事計畫人員與執行人員必須具備對網路領域的基本認知，包含瞭解網路環境，且能於網路環境中成功的執行戰術作為能力，成為了現今聯合部隊的基本且重要之著眼。

當沒有任何一個單位嘗試著在網路領域中打造出聯合部隊通聯時共通的語言，國防部資訊安全確保訓練變成了教育現役人員如何在網路領域中保護他們自身的活動的基礎工具。當深造教育期間為學官引進網路領域概念時，這些訓練顯得為時已晚且不足，無法為部隊養成年輕的計畫軍官及士官。大家能夠齊心協力揭下網路領域的神秘面紗，將能使計畫與命令寫作更為清楚。

最後，戰役設計應該也要將正義戰爭原則納入網路領域的運用。無數的政策、適法性及接戰規定程序將會持續地影響網路領域中的戰術作為。1988 年釋出莫里斯蠕蟲的康乃爾大學學生羅伯特莫里斯，所帶來的潛在負面影響就是一個計畫不周且缺乏風險管控的例子。莫里斯釋放蠕蟲當時是為了計算網路的大小。然而，莫里斯於蠕蟲中安裝的隨機測試措施，起初是為了確保能夠成功地突破系統防護，進而大量的複製。因此，所有被蠕蟲侵入的電腦系統因為超載而全部癱瘓。正如同文章所討論的，戰術、技術與程序，以及管制的措施必須包含減少風險協議來減少意外產生的負面影響。更明確地說，為了從避免民眾顛覆當地政權到提供部隊位置，進而干擾村落或城鎮的無線網路技術或是全球互通微波存取網路，也有可能對所有人民造成一些負面的影響，如干擾醫療警報系統、居家照護監視系統，或者是其他維持生命功能的儀器。當民防及民間網路設施仰賴網路骨幹設施，工具及戰術、技術與程序必須著眼在設施與網路分類與識別協定，盡可能減少不必要的附加傷害。

在沒有廣泛及具體的專業知識協助下，要克服複雜網路領域中分析與問題解決的既有觀念並非易事，也有可能會危害統一指揮的軍事原則。軍事計畫小組在解決問題的過程中，針對問題的診斷及向高級長官清楚，且簡要地解釋面臨之挑戰是必備條件。此外，高級長官必須孰悉網路領域中存在的風險、假定事項及機會。最後，指揮官必須信賴戰術階層的部隊追求行動自由時，能夠妥善處理風險。網路領域亦是如此，但是當指揮官不瞭解網路領域時，將會面對到更多的風險。

二、運用網路領域中實體、認知及虛擬的交集

未來計畫作為需要計畫者洞悉網路領域中認知、實體及虛擬層面之特性，才能同步與實體領域如地面、海洋、空中及太空共存與互動。有效地呈現軍事作戰中的問題，須呈現出網路與其他領域間的鏈結，分辨運用這些鏈結的機會，以及提供周詳的機制來掌握優勢，做為後續攻勢作為或守勢作為。

超級工廠蠕蟲的案例中，很清楚的解釋如何於網路領域中運用虛擬與實體的鏈結，導致伊朗納坦茲核子設施中的鈾氣離心管損壞。[6] 如同莫里斯蠕蟲，超級工廠蠕蟲目的很單純，但是設計者將超級工廠的影響範圍限定於納坦茲的鈾氣離心管。有效的界定問題及謹慎辨識

[6] For a detailed case study on the Stuxnet worm, see 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), p.212–231

虛擬與實體層面的鏈結，使我們瞭解其目的在於限制伊朗的核設施發展。問題界定可以有效地協助設計者操控虛擬層面，進而在實體層面上達到所期望效果。此外，此蠕蟲起初並未受到伊朗政府偵獲，而且當機械(實體)故障時，初始研判是機械故障或者是失靈。超級工廠成功地在網路領域中運用虛擬層面的行動對實體跟認知層面上產生影響。

在戰略考量下授權使用超級工廠蠕蟲發動攻擊，除了計畫、蠕蟲(病毒)發展及執行外，更包含了由一位技巧純熟的專家來擴展網路攻擊效果。以色列政府在決定如何中止伊朗納坦茲核設施發展的問題時，計畫人員需要窺見運用網路領域中的虛擬鏈結，跨越實體領域進而達成實質的效果。因此，在網路領域中的認知層面上同時思考攻擊者及被攻擊者的想法，更能影響對方認知層面。超級工廠蠕蟲展現出於網路領域內運用適當的戰術作為，符合節約與集中的作戰原則。

以色列在超級工廠蠕蟲達成節約原則係跨領域的戰場情報準備(Intelli- gence Preparation of Battlefield, IPB)。這個例子亦凸顯網路領域中介於技術與人文考量的鏈結。當地緣政治效應與伴隨之效應造成更大的難題時，用來辨識適合的鏈路模控學便成為重要的科學方法之一。[7]在符合決策者「行動前景」的範疇中，決心運用網路領域作為解決方案，成為精確解決以色列問題的選項。[8]

藉由對軍事準則、訓練與戰術的修正，行動規範可以使執行戰術作為時減少對民眾造成意外的附加傷害，且維持攻勢動能。今日即便在網路不發達的國家，電話及無線網路科技的廣泛運用(及在缺乏技術整合的網路環境，或是運用如藍芽一對一連接的設備)，不僅能開創奪取先制之機會，更能拓展戰術優勢作為。在道德規範與節約原則的考量之下，也許針對一棟公寓大樓中的正在對單位射擊的武裝人員進行空中炸射是無法讓人接受的。但是，或許可以藉由連網的電視，或是電話來進行被動的觀察。假如單位能夠確認敵火來源，無論是運用鏈結導致電力短路，使電話中的電池過熱導致小幅度爆炸，或是開啟電視讓對方分心等作為來造成實質影響，進而達成癱瘓敵人的目標，未來都可能成真。

網路領域中的戰術作為，唯有將其納入聯合兵種多領域作戰之戰術作為，才能有發揮的空間。但目前可以確定的是，美軍現今的用兵及科技尚不允許這個場景出現。但是，在準則、組織、訓練、物資、領導統御、人員、設施及政策持續地修訂下，未來得以滿足這些需求。

非線性、不對稱的戰略效果在戰術層級體現

在美軍聯合準則 3-0，聯合作戰篇(JP 3-0 Operations)中敘述「指揮官執行「網路作戰」來維持網路空間的行動自由、達成聯合部隊指揮官的目標、拒止敵人行動及輔助其他作戰行為。」

[7] Horst W.J. Rittel and Melvin M. Webber, “Dilemmas in a General Theory of Planning,” Policy Sciences 4, no.2 (1973), p.155–169.
[8] Ibid 8.

[9] 然而，大多數的軍事論述仍然著重於戰略網路運用，或是僅以網路為中心的思考模式，而非將其視為一個多領域作戰之一部。當領導者及戰略任務主導了戰事中的領導統御、訓練、計畫及動能作戰，往往會產生一個趨勢，就是因網路領域的「獨特性」而將其單獨劃分出來。但是，戰場上所有的戰術行動均應支撐戰略指向。戰術及戰役層級的網路作戰可為軍隊帶來潛在的非線性與不對稱的戰略效果。

為瞭解戰術階層的網路作戰願景，非線性、不對稱的戰略效果一詞應該被納入解決問題的內涵中。軍事計畫者須同時就科學及人文因素中尋求解決問題之方案。戰爭的目的在於摧毀敵人的意志及拒止敵人續戰的慾望與能力。人類意志可以藉由網路領域來傳達與影響。政策制定者不可小覷網路領域之戰略控制，鎖定個人意志的戰術作為變得至關重要。在發掘對方的弱點時，同時可以將我們的弱點轉為優勢。為了能夠有效地達成此目的，我們需要改變對網路領域的既有概念，而俄羅斯在面對 2008 年喬治亞危機時，在網路領域的戰術作為，為未來遵循多領域作戰原則，並將網路領域整合其中提供了可貴的經驗。

雖然有人認為俄羅斯針對喬治亞網路基礎設施的戰術，作為其地面作戰戰略之一部，並非戰術層級。但是，在作戰中運用網路攻擊奪取先制，並達成節約兵力的價值是有目共睹的。雖然俄羅斯政府未正式承認其針對喬治亞民間及政府網路設施實施大規模電腦網路攻擊，但是，很明顯地達成了俄羅斯所望之軍事目標。電腦網路攻擊避免了對方準確預測俄羅斯地面作戰的兵力大小與指向，也遏止了觀察人員、軍事單位及資深政策專家的相互通聯。於網路領域之攻擊使對方不僅且缺乏資訊，且無法掌握戰局，使其無法於第一時間有效地應對俄羅斯的入侵。此外，此攻勢也利用部分民眾的親俄情懷，使得其對於俄羅斯入侵的本質、意圖以及強度感到困惑。隨著戰役發展，俄羅斯在網路領域的作戰強度、時效及規模，依據俄羅斯計畫人員的需求做出改變。

網路領域首先必須被視為一個有機的環境，拒止、欺敵、間諜活動、攻擊或者機動等都比關注在網路領域的行為更加重要。人類會藉由網路領域影響他人或受他人影響，正如同他們在地面、海洋、空中及太空一樣。人們在網路領域的活動正如同他們走在地面上或者是航行跨越海洋。在未來的世界上，網路領域將十分普遍，它將連結人類、設備與被動及主動等多層網路。

網路領域的作戰不是新的概念，我們日常藉由操控網路領域中的實體、虛擬以及認知層面及產生互動。執行軍事作戰時，當網路領域的戰術作為成為聯合兵種多領域作戰的途徑之一，此概念必須更深入地在軍事準則與戰術中去探究及闡明。對部隊針對網路領域進行有效的教育是培育未來計畫者、執行者及領導者來說是非常重要的，因為它們可以掌握這個領域。未來的部隊必須能夠洞悉網路領域及其他領域在戰役與戰術上的鏈結，尤其是他們為了達成

[9] Joint Publication 3-0, Joint Operations (Washington, DC: The Joint Staff, January 17, 2017), III-9.

戰略軍事及國家目標時所做的問題確認與戰役設計。當網路領域在民間與軍事生活中普及，對於網路領域具有共同的認知，將成為軍事部隊面對未來挑戰時所踏出的第一步。

結論

在前言所敘述的小故事，運用既有的監視器材進行被動的監視，或者是運用網路或電路啟動設備或產生爆炸，導致敵人分心或受傷。這些場景以往只能在美國好萊塢的動作或科幻電影中出現。然而，隨著網路的普及與科技的發達，這些場景也許都會發生在許多人身邊。尤其是人工智慧結合網路的發展，不僅有機器人、無人載具或者是到現今蔚為風潮的無人駕駛功能，更使得上述事件發生的機率提高。

許多國家往往在執行戰術作為時，只考量兵力運用、火力運用與指揮管制等面向，往往忽視了法律與道德層面的考量。然而，美軍近年發展多領域作戰之概念，在網路領域中的戰術作為必須考量許多因素，如：道德規範、國際人道法律、武裝衝突法與接戰規定等，美軍在網路領域中似乎無法大展拳腳。又因為美軍許多軍官對於網路領域之作戰的觀念不甚清楚，或者是缺乏相關人才，因此許多高級長官或決策者，往往將網路領域之作戰獨立出來，反而缺乏了跨領域整合的作戰概念。

反觀 1988 年康乃爾大學的學生羅伯特莫里斯為了學術研究所釋放出莫里斯蠕蟲造成了電腦癱瘓；以色列為了破壞伊朗針對核子設施的擴張，所放出的超級工廠蠕蟲，導致其機器設備故障及停止運作;又或者是俄羅斯於 2008 年針對喬治亞事件時大規模的癱瘓其網路作為等。顯現出透過網路領域進行攻擊導致實體設施損壞或者是造成心理層面的恐慌是可行的，若能夠在符合道德規範及政策法規的前提下，在網路領域執行相關的戰術作為更可以為其他領域的之作戰塑造有利的環境。

不論哪一個國家未來要進行多領域作戰，在傳統地面、海洋及空中無法佔領優勢時，太空及網路或許可以成為了扭轉優劣態勢的關鍵領域。然而，太空領域之作戰可能需要高額的投資與尖端的技術才有可能呈現效果。因此，針對網路領域的軟硬體發展及相關科技技術人才的培育與投資，相形之下較為經濟實用。若是能成功運用網路領域之特性，成功鏈結其他領域，又或者是利用網路領域在虛擬層面之操控，為實體層面之傳統作戰及認知層面之心理作戰奠定勝基，除了能夠符合孫子兵法中所述：「凡戰者，以正合，以奇勝。」更能成為未來新興戰爭型態的一部分。

本軍目前雖然依據國家軍事政指導成立資通電軍，惟未來網路作戰、資訊作戰與運用電磁活動進行干擾與反制作為將遍布所有層級。從文中得知，連身為軍事強國的美國，僅具少數專長或專業人員，且著重於戰略階層之網路攻防作為，無法同時顧及戰術或是戰鬥層級之網路作戰。據此，首先建議本軍可仿效美軍多領域特遣部隊，於各旅、營級單位建置具備網路作戰與電磁活動緊急反應小組(軍、文職搭配)，處理低強度、初階之網路作戰或電磁活動，

使具高階專長之資通電軍人員能夠專注於戰略階層的網路作戰。其次，本軍亦可就各單位管轄區域，建立軍用與民營之網路設備的相互備援機制，整合網路偵蒐能力，進而強化網路作戰中之戰場覺知與韌性。再者，建議本軍與各級演訓，妥善規劃並嵌入網路作戰、資訊作戰與電磁活動之科目，使本軍各級軍官能將網路領域之各項戰術作為視為作戰之一部。最後，建議本軍可以就現行國際法、國內政策與規範，針對網路作戰領域進行學術研討會或是座談會，廣邀各界網路政策與網路安全專家，使全軍建立面對網路作戰時應有的基本素養。

參考文獻

一、Field Manual, Tactics, Techniques, and Procedures for Observed Fire (Washington, DC: Headquarters Department of the Army, July 16, 1991).

二、Joint Publication 3-0, Joint Operations (Washington, DC: The Joint Staff, January 17, 2017).

三、Marine Corps Doctrine Publication 1, Warfighting (Washington, DC: Head- quarters Department of the Marine Corps, June 20, 1997).

四、Morton, Chris “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).

五、Phillips, Jennifer Leigh “Tactical Maneuver in the Cyber Domain-Dominating the Enemy” Joint Force Quarterly(Washington, DC) 93, 2nd Quarter 2019.

六、Rattray, Gregory J. Strategic Warfare in Cyberspace (Cambridge: MIT Press, 2001).

七、Rittel, Horst W.J. and Melvin M. Webber,“Dilemmas in a General Theory of Planning,” Policy Sciences 4, no.2 (1973).

八、TRADOC Pamphlet 525-3-1, The U.S. Army in Multi-Domain Operations 2028(Washington, DC, Department of Army, December 6, 2018).

譯者簡介

朱子宏中校，美國色岱爾軍校 2007 年班、美國陸軍指揮參謀學院 2018 年班、政治大學戰略與國際事務所碩士、美國陸軍指揮參謀學院軍事理論碩士，曾任排長、測量官、教官、連長、外事連絡官，現在國防大學陸軍指揮參謀學院教官。