● 作者/Frank C. Sanchez, Weilun Lin, and Kent Korunka ● 譯者/李永悌 ● 審者/馬浩翔

應用非正規作戰原則於網路作戰中

Applying Irregular Warfare Principles to Cyber Warfare

取材/2019年第一季美國聯合部隊季刊(*Joint Force Quarterly*, 1st Quarter/2019)

非正規作戰在特徵、原則與理論方面皆與網路作戰甚爲相似，將非正規作戰原則應用於網路作戰將可獲得最大效益。本文參考麥考米克提出的網路鑽石理論模型，將網路行爲者分爲四類，從而發展出五種網路戰略。

2002年7月23日，美國肯塔基州坎貝爾堡(Fort Campbell)陸軍第101空降師第187步兵團第3營的士兵於阿富汗納瑞扎(Narizah)地區，在參與搜索與攻擊任務時建立衛星通訊，俾與重要的後方部隊取得進一步聯繫。

(Source: US Army/Todd M. Roy)

來自網際空間的威脅所在，超越陸、海、空與太空領域的實體限制。不同於這些傳統領域的是，其助長的威脅難以預測，具有適應、變形與複製能力，且不具國籍與樣貌。[1] 在面對網路上由不露面、無國界，有時甚至無國籍的敵人所發起之網路威脅時，部隊的挑戰在於應採取何種因應態度。這些敵人出現在不受傳統戰爭規範與規則所侷限與約束的領域中，且軍隊在這些領域大多沒有實務經驗。為確保美國能維持在網路上的優勢，並能預見、迅速因應與反制網路上的威脅，美軍的網路戰略與戰法必須有所調整，並將非正規戰法與混合戰納入其作戰能力。

儘管網路相當重要，國家領導人、戰略家及軍事計畫人員仍難以理解如何將網際空間作戰(Cyberspace Operation, CO)化為國家政策工具以納入國家安全中。其中一項重要缺失來自於領導人對於網路為何及在網路領域可達成何種效果，欠缺經驗與基本認識。與被視為「數位原民」(digital native)年輕世代不同的是，大部分國家與軍事領導人及軍事計畫人員皆被視為「數位移民」(digital immigrant)。數位原民一詞由普倫斯基(Marc Prensky)所提倡，意指在數位科技應用伴隨之下成長的世代，而「數位移民」則指在數位科技問世之前(約於1980年代)出生，後來才接受數位科技應用的世代。[2] 儘管數位移民缺乏網路知識，但其中有許多人深知非正規作戰(Irregular Warfare, IW)與特種作戰的價值及重要性。許多非正規作戰與網路作戰(Cyber Warfare, CW)間的共同點，可為美國領導人建立遂行網際空間作戰的基礎，俾維持在網路上的優勢。

非正規作戰與網路戰具備相似之特質、原理與理論，將非正規作戰應用在網路戰上可獲取最大效益。(Source: USN/Gary Nichols)

早期的網路權理論家通常會提倡三個重要術語：網際空間、網路權與網路戰略。[3] 在網路領域已趨成熟之時，網路理論家與思想家仍未給予上述術語適當定義。瞭解非正規作戰有助於獲得網路作戰的基本知識。透過強調非正規作戰與網路作戰兩者相似之處，並提供運用非正規作戰原則進行、定義及整合所有跨領域與軍種網路作戰的重要架構，美國領導人將可開始理解網路權如何能普遍提升美軍網路部隊效能。

非正規作戰與網路作戰的關連

特種作戰在美軍擁有悠久、聞名及多樣的歷史，例如包括

羅傑斯突擊隊(Roger's Rangers)、奧克角突擊行動(assault of Pont-du-hoc)，以及鷹爪行動(Operation Eagle Claw)等。美陸軍退役上校塞萊斯基(Joseph Celeski)提到，美聯合特戰大學(Joint Special Operations University)特戰部隊武力研討會(Special Operations Forces [SOF]-Power Workshop)認為特戰部隊為「多重與跨領域部隊，可於不同層級遂行或支援傳統或非正規作戰，獲致或支援軍事與政治成果。」[4] 該研討會成員列出以下特戰部隊作戰環境的特質：

> 作戰環境錯綜複雜，特點為不穩定且狀況不明；暴力行為、影響力與制衡作用通常以間接方式進行，包括微妙且狡詐的低層級行動。[5]
>
> 環境風險高且極度敏感，遂行行動時有極高的個人與政治風險。[6]
>
> 非正規作戰環境以國內與次國家(substate)政治暴力行為為特點，再加上叛亂、顛覆、暴力政治行動及恐怖主義。[7]

第3-05號聯戰出版品：《特種作戰》(*Special Operations*)將特種作戰環境描述為「敵對的、阻絕的、或政治上與/或外交上敏感的環境……並……具有以下其中一項或數項特性：具急迫性、祕密或隱密本質、低能見度、與當地部隊合作或透過當地部隊行動、對地區熟悉度與文化專業知識的要求更高，以及較高程度的風險。」[8]

網路因其複雜性與行為者而與特種作戰有著相似之處。網路的全球新領域須仰賴連接資訊科技的基礎設施，包括所有自動化與網路化系統組件，藉以儲存資訊或內容流(content flows)。[9] 網路作戰係於實體網路、邏輯網路，以及網際空間領域的網路人物層次(cyber-persona layers)進行。[10] 連上網路的便利性讓個人行為者、犯罪組織與小型團體能夠以類似民族國家與跨國組織等層級在網路環境中從事活動。匿名與缺乏責任歸屬使網路行為者類似特戰部隊的隱密性或祕密性。

網路領域以不同於陸、海、空、太空等傳統領域的方式威脅區域與國家安全。[11] 因此，網路上居心不良分子，從個人駭客及犯罪集團乃至暴力極端主義組織與民族國家都有。不良分子基於利益、情報、阻斷服務或對重大基礎設施造成損害等理由，替個人或國家利益竊取資訊。在傳統領域中，此類行動相對可資識別，且較易歸類為戰爭行為，惟在網路上，網路攻擊的潛在意圖與責任歸屬實難以追究。

過去的思想家與戰略家已辨識出特種作戰與網路作戰間的一些相似點。特瑞亞斯(Eric Trias)與貝爾(Bryan Bell)曾撰文提到，「特種作戰固有的祕密本質類似遂行隱祕網路行動的便利性。」[12] 達根(Patrick Duggan)提出「網路作戰本質上就是人類作戰，並需要特戰部隊的獨特人類專業知識、非正規思維與審慎的不對稱作戰選項。」[13] 最值得注意的是，陳吉姆(Jim Chen)與戴納曼(Alan Dinerman)提出了架構，比較並對照傳統作戰與網路作戰間相似之處。相較於傳統作戰，陳吉姆與戴納曼參照其他作者的想法，創造出有助討論網路作戰能力的基礎模型。[14] 附表所示內容係改編自兩人的研究發現，其中包括用於比較並對照非正規作戰，藉以凸顯網路作戰與非正規作戰間的

附表：傳統、網路與非正規作戰

	傳統作戰	網路作戰	非正規作戰
目的（為何）	透過占有一段時間的地理位置優勢，以獲取政治、經濟、意識形態、社會及宗教優勢	協助獲取政治、經濟、意識形態、社會及宗教優勢；獲取佔有競爭優勢所需資訊	協助獲取政治、經濟、意識形態、社會及宗教優勢；獲取佔有競爭優勢所需資訊
戰略（如何）	運用公開與 / 或隱密行動；展現力量；幾乎無責任歸屬問題	運用公開與 / 或隱密行動；有責任歸屬問題	運用隱密行動；透過情報劃分責任歸屬
參與（何人）	諸如軍事或準軍事人員等部分人士	所有擁有連網裝置都可影響網路使用者	國家與非國家行為者，諸如恐怖分子、叛亂分子與犯罪網路等適應力強的敵人
目標（何物）	人類；主要是有形物體；直接影響人類生活	主要是如資訊等無形物品，或如資訊系統等有形物品；可實際在網路資訊方面間接影響人類生活	人類；主要是有形物體；直接影響人類生活
空間（何地）	有限度的地理位置	一旦連上線，地理位置即無遠弗屆	全球
持續時間（何時）	時間有限	持續進行，惟每次攻擊時間通常短暫	時間極為有限
準備時間（何時）	時間相對較長	時間相對較短	時間相對較短
代價（何物）	高昂	相對較不昂貴	相對較不昂貴
特質（何物）	相對更為透明	相對不透明並採隱密模式	相對不透明並採隱密模式
責任歸屬（何物）	相對容易釐清	可能難以究責	相對難以釐清
交戰規則（何物）	相對明確	不明確	不明確
印象（何物）	必然嚴重或殘酷；明顯	若非攸關生死的情況則較不嚴重；有時沒有感覺	若非攸關生死的情況則較不嚴重；有時沒有感覺
損害（何物）	嚴重的實體傷亡	嚴重的資訊損失	有時嚴重
直接影響對象（何人）	部分人士 / 產業	所有連上受影響網路的人士 / 產業	部分人士 / 產業
影響依據（何地）	地理位置	網路連線	地理位置
嚇阻功效（何物）	明顯有力	限於當前	輕微
優勢（何物）	可達成	難以達成	難以達成
結果 / 成果（何物）	明顯	可能不甚明確	可能不甚明確
勝利者（何人）	可明確識別	可能難以判定	可能難以判定
復原時間（何時）	相對長	相對短	相對短

Source: Adapted from Jim Chen and Alan Dinerman, "On Cyber Dominance in Modern Warfare," in *Proceedings of the 15th European Conference on Cyber Warfare and Security*, ed. Robert Koch and Gabi Rodosek (Reading, UK: Academic Conferences and Publishing International Limited, 2016), 54.

若能師法特種作戰、非正規作戰與特戰部隊等高度仰賴專業化及裝備的部門，美國的網路戰作法將可獲取最高效益。(Source: MSN/ Ashley Lawrence)

相似處。儘管本表並未全然囊括各項作戰的所有面向與特質，卻足可說明網路作戰與非正規作戰間的極度相似處。

儘管本表列出諸多相似點，但重要的是認識網路作戰與非正規作戰間的差異。其中一項重要差異：低個人風險，是網路作戰的最大優勢。網路攻擊幾乎可在任何一處進行，還能讓攻擊者雖處在民族國家地理邊界範圍內，卻依然安全無虞。網戰的低個人風險，與特戰部隊人員在高度競爭環境中或深入敵後遂行任務，其中所承擔的高個人風險，兩者形成鮮明的對比。進入網路的便利性，且只要採取適當步驟隱藏身分即難以究其責任等特性，能進一步說明網戰的低個人風險。

特種作戰中的許多核心活動可完全融入網路任務的情況中。攻勢網路作戰類似特種作戰的直接行動、反制大規模毀滅性武器、軍事資訊支援作戰及特別偵察任務等意圖。同樣地，特種作戰的國外內部協防(foreign internal defense)與安全部隊協助任務等意圖，則類似守勢網際空間作戰。[15] 儘管在識別與追查網路攻擊行為者、目標網攻效果及流向某國或群體的資訊時，其繁複的程序相當重要，但民族國家對其公開參與的必要性卻並非同等重要。網路行動應支援尚未被偵察到的入侵行動，其監視、破壞穩定與操弄潛力可產生的功效，遠比立即摧毀或破壞來得更長久。

若能師法特種作戰、非正規作戰與特戰部隊等高度仰賴專業化及獨特戰術、技術、程序和裝備的部門，美國的網戰作法將可獲取最高效益。非正規作戰本質上與「具高適應性的行為者」有關。歐提斯(Rain Ottis)與羅倫茲(Peeter Lorents)曾撰文提到，「網路為彼此互連的資訊系統，以及透過這些系統進行互動的人類用戶所構成之時變性(time-dependent)組合。」[16] 兩人強調，事實上「網際空間係人類基於人類目的所創造之人造空間」，必須要能瞭解與影響人類的思想和行為。[17]

其他非正規作戰原則應用於網路

基於前述相似特性，下一個合乎邏輯的步驟就是融合特種作戰與非正規作戰的術語，以建立

有關網路作戰的思維與理論基礎。柯(Nicholas Co)在〈將特種作戰原則應用於網路〉(*Adapt Special Operations Principles to Cyber*)一文中建議，以美陸軍沙克撓(Sid Shachnow)上校於1980年代中期制定的「美軍特戰部隊信條」(SOF Truths)，作為支援未來網際空間成功作戰的指導原則。[18] 特種作戰的構想係建立於個人、小型部隊與先進科技的基礎上。美軍特戰部隊信條第1條認定，賦予特種作戰決定性優勢的是人員而非裝備。特戰部隊是一群訓練有素的人員，能應用高度專業的技能，配合彈性、創意、創新與獨特能力以達成各類軍事選項的國家目標。[19] 除了這些論述外，該文章亦介紹了其他數則引用自特戰部隊領域的構想與術語。

2018年8月29日，美陸軍第1騎兵師第2裝甲旅級戰鬥部隊(Armored Brigade Combat Team)士兵於德州胡德堡(Fort Hood)進行徒步電子作戰訓練。(Source: US Army/Carson Petry)

首先，將用在非正規作戰的相對優勢構想應用在網路作戰。美海軍麥克雷文(William McRaven)上將在其著作的《特種作戰》(*Spec Ops*)中把「相對優勢」(relative superiority)一詞定義為，「發生在由一般規模較小的攻擊部隊對抗較大規模或防禦精良的敵人時，獲得決定性優勢的情況。」[20] 如前所述，由於連上網路相當方便，且僅需冒極低的個人風險，因而能讓規模小至如個人駭客的勢力，於潛在時間點壓制或對抗防禦精良的敵人。目前普遍存在的誤解就是全球網路優勢或主導權不僅有可能存在，也容易維持。布萊恩特(William Bryant)引述了知名網路專家利比奇(Martin Libicki)的論點提到，「網路主導優勢不具意義，因此並非為網路作戰人員的合適作戰目標。」[21]「2035年聯合作戰環境」(Joint Operating Environment 2035)文件所預示的未來安全環境中充滿了漏洞，其中可直接連上武器系統，而軍事作戰行動遍及全球，範圍可涵蓋個人工作站、伺服器或控制器晶片組。[22] 網路係由數不盡的裝置組成，其廣大與多變的特性讓維持全面性網路優勢成為不可能的事。此種風險無時無刻都存在，任何人都有可能失去相對優勢。美國網路司令部(U.S. Cyber Command)近期發布的「司令部願景」(Command Vision)即強調此論點並指出，「新漏洞與機會隨著新網路地形(cyber terrain)的出現而不斷產生。沒有目標會保持靜態，沒有攻勢或守勢能力能維持永久效能，也沒有永遠的優勢。網路地形可做到良好的防禦，但仍持續處在危險中。」[23] 美空軍在其第3-12號準則文件：《網路作

2018年2月20日，美國俄亥俄州萊特派特森空軍基地(Wright-Patterson AFB)空軍技術學院(Air Force Institute of Technology)的學生於上課期間聆聽教授(圖右)解說駭客技術。(Source: USAF/Al Bright)

戰》(*Cyber Operations*)中將「網際空間優勢」(cyberspace superiority)一詞定義為「在不受干擾的情形下，在(或透過)既定時間與領域中於網路進行作戰的作戰優勢。」[24] 此一定義非常貼近麥克雷文對於相對優勢將在「交戰關鍵時刻」達成的論述。[25]

其次，「優勢」一詞暗指對敵人投射某種形式力量(網路權)的能力。惟美國國防部尚未定義網路權一詞，定義最接近為美空軍的「網路兵力應用」(cyberspace force application)，亦即「在(或透過)網路進行戰鬥作業，針對已驗證目標採取決定性行動，以達成軍事目標與影響衝突的進程與結果。」[26] 謝爾登(John Sheldon)對網路權的定義論述如下，「於和平與戰爭時期為我方優勢操控戰略環境認知，同時讓敵方無法有效理解相同環境的能力。」[27] 透過將特戰部隊的構想與術語應用於前述定義上，本文將提出以下定義作為進一步思考與討論網路權的跳板。在戰略層級上，於國家和平時期與各式衝突中，網路權為了達成國家安全目標，在(或透過)網路進行與影響活動之各式網路能力總體實力。在作戰與戰術層級上，網路權則是透過科技作為爭奪資訊完整性、機密性、安全性與可用性手段的敵人遂行網路作戰，從中獲得控制權與相對優勢。

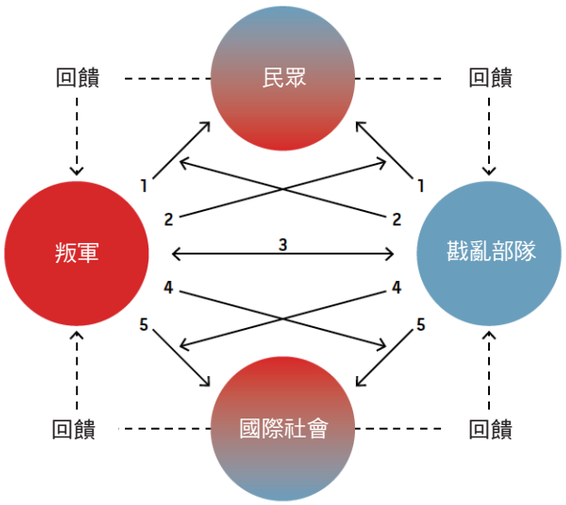
網路戰略的非正規架構

當前網路戰略中有許多觀點與架構。由於戰略必須預期作戰環境的變化，作戰環境對戰略亦將有所影響。[28] 美國國防部可利用網路威脅的主要面向，諸如威脅行為者、內部威脅、供應鏈弱點、對美國國防部發展其網路作戰策略能力的威脅等。[29] 部分策略僅針對網路防禦或網路安全，而其他戰略本質上則為攻勢。麥考米克(Gordon McCormick)的「戡亂鑽石理論模型」(Counterinsurgency Diamond Model)原理與理論，可作為發展網路戰整體戰法與戰略的架構。就本文而言，在簡要說明麥考米克模型的內涵與架構後，即可將其整體前提應用於網路。如圖1所示，威爾森(Greg Wilson)簡要說明了該模型的運用與互動：

> 鑽石理論模型所建立的全面性架構，考量國家或地主國

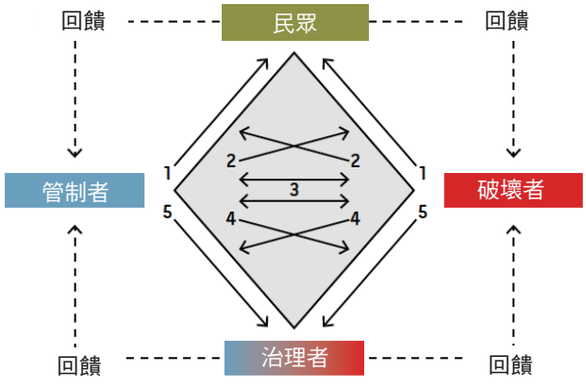
政府、叛亂或恐怖分子、當地人民，以及國際行為者或贊助者間的互動。國家或地主國政府的目標在消滅叛亂分子，或將其成長與影響力限制在可控制範圍內。叛亂分子或恐怖分子的目標則是將規模發展至足以摧毀國家的管控機制並取代現有政府，或迫使政府在政治上做出某種形式的讓步，以達成其所欲之目標。為發展有效戰略，一個國家必須先瞭解其相較叛亂分子所擁有的優勢與劣勢。國家通常擁有由武裝部隊與警察組成的既有安全體制，對叛亂分子有兵力上的優勢，惟在資訊方面則處於劣勢。此種資訊劣勢的產生係因叛亂分子或恐怖分子分散各地且藏身在當地群眾之中，故難以偵知與標定。[30]

圖1 麥考米克的戡亂模型



(Source: Gordon H. McCormick, "Seminar in Guerrilla Warfare," Naval Postgraduate School, Monterey, CA, 2003.)

圖2 網路鑽石理論模型



(Source: Adapted from McCormick's Mystic Diamond Model [McCormick, "Seminar in Guerrilla Warfare," Naval Postgraduate School, Monterey, CA, 2003].)

圖2所示的網路鑽石理論模型(Cyberspace Diamond Model)係以麥考米克的戡亂鑽石理論模型為基礎，透過優質治理、改善安全環境及透明度(與究責有關)來促進網路的資訊正當性(information legitimacy)。由於作戰環境中的所有行為者對資訊的正當性都能接收與感知，資訊正當性即是網路衝突的核心。國家領導人與軍事專業人員應運用此一網路鑽石理論模型，以制定網路戰的戰略方針。惟此架構亦可實施在作戰與戰術層級，協助軍事將領與計畫人員將戰略指導轉化為作戰計畫。

管制者。管制者是在目前網路或資訊通訊科技(information communication technology, ICT)上具有部分影響力或管理權限的人士。管制者的例子範圍囊括網路管理員及國家政府。一般而言管制者係單一主導力，惟民間企業、組織或國家亦可提供額外能力來強化管制者。管制者必須整合民事、軍事、外交、資訊、經濟、科技與財經等所有國力工具。這些力量包含但不限於決策者、軍隊、執法機關、情報機關、基礎設施供應商及網路安全人員等。管制者係以破壞者的認知來界

定，惟後者在影響局勢時能感知外部力量的存在，因此這些外部力量亦成為管制者的一部分。而管制者在界定破壞者時也是如此；惟因感知範圍涵蓋全球，管制者的舉證責任往往更大。追究責任歸屬是管制者需要克服的最大障礙。

破壞者。破壞者為中斷或干擾網路資訊可用性、安全性、機密性或完整性的人類、機器、政府與罪犯。主動或被動支援破壞者的任何人與事物本身也是破壞者。自願的破壞者與受脅迫而提供支援的破壞者間往往沒有明顯區別。例如在僵屍網路(botnet)中未經所有人同意而遭受惡意控制的電腦，即可視為受脅迫(非自願)破壞者。破壞者利用民眾的信任獲取支持或施以控制。

民眾。民眾係由網路用戶或使用資訊通訊科技的人類或機器組成。儘管支援可能出自受脅迫的民眾，但民眾在提供超出必要範圍的更多支援前並不會被視為破壞者。在前述兩種鑽石理論模型中，民眾皆可成為力量來源。惟在網路上，作戰環境的範圍遠超出地理邊界，民眾可以是全球、區域或個人的系統用戶。

治理者。儘管網路欠缺一般法治與傳統的治理概念，本文仍依據聯合國教科文組織的定義來引用治理一詞。聯合國教科文組織將治理定義為，「設計來確保責任歸屬、透明度、回應性、法治、穩定性、公平與包容、授權及廣泛參與的結構與程序。」[31] 聯合國教科文組織亦稱治理為「遊戲的標準、價值與規則」以及「公民與利害關係者所進行之互動，並參與有關文化與體制環境的公共事務。」[32] 治理者為網路鑽石理論模型中的行為者之一，係由外部民族國家、國際組織與其他未發揮直接或間接支援管制者與破壞者功能的團體所組成。與民眾類似的是，身為治理者的成員在為任何一方提供支援前皆保持中立；一旦提供(或被視為提供)支援，即成為管制者或破壞者。網路行為者重視或理解組織及實體的正當性。諸如美國國家標準暨技術研究院(National Institute of Standards and Technology)、維基解密(WikiLeaks)或超文件通訊協定(Hypertext Protocol)等，皆為民眾所重視或理解的治理者實例。

制定網路戰略與回饋

管制者與破壞者在進行每次行動時，必須考量行動對民眾與治理者所接收資訊的已知正當性可能造成何種影響。依網路鑽石理論模型所示與編號，管制者與破壞者在網路衝突的過程中將全數運用以下五種策略；惟如前所述，力量來源主要為民眾。網路讓管制者得以把重點放在運用網路攻擊，以進行對抗破壞者的直接行動。然而值得注意的是，管制者必須認清維護民眾資訊的安全性、可存取性、完整性與機密性的重要。因此，基於這兩股勢力必定會執行各項戰略的各要素，重點將置於戰略1與戰略5。

戰略1：民眾支持。在圖2中，由於管制者與破壞者皆需仰賴大眾支持以獲取成功，戰略1的意圖在於獲取力量來源(亦即民眾)的支持。儘管一般而言管制者在資源、人員與網路方面具有強大優勢，卻往往欠缺有關破壞者的特定情報。因此，管制者需要民眾支持，俾獲得辨識

2016年5月30日，位於美國華盛頓州雷蒙德市(Redmond)微軟公司總部遊客中心。(Source: Coolcaesar)

破壞者所需之情報。這就類似非正規作戰中戡亂部隊或叛亂分子與民眾間的互動。管制者透過網路的優質治理、改善安全與社會經濟條件來提升資訊正當性。管制者的目標則在維持其自身作戰環境的控制、資訊正當性及民眾信任。確保與維持民眾的支持將使管制者耗費大量資源、時間、能力與人力。

戰略2：資訊破壞。如圖2所示，戰略2的意圖在於阻止或破壞敵人對民眾的控制。管制者的目標在於透過否定破壞者資訊的正當性，在破壞者與民眾間建立鴻溝，並阻止其接近與自由移動於民眾與作戰環境中的其他資源地帶間。破壞者必須試圖透過網路與資訊通訊科技來破壞資訊的正當性，或中斷、阻止管制者影響破壞者所仰賴的民眾與資源。與管制者攻擊破壞者資訊正當性的艱鉅任務相比，攻擊管制者資訊的正當性較為容易，因此戰略2對破壞者有利。透明度與責任歸屬是管制者成功的關鍵。與非正規作戰類似的是，叛亂分子較容易攻擊政府的正當性與控制權。

戰略3：直接行動。戰略3旨在打擊敵人、破壞其行動，並阻擋其持續衝突的意志與能力。管制者廣泛、全面且明顯的特徵，使破壞者得以確定管制者的活動與位置，進而增加管制者的個人風險。此類知識讓破壞者能夠依其選擇的時間與地點進行攻擊，因而有可能減少間接損害或責任歸屬。鑑於作戰環境無遠弗屆，管制者必須在能對破壞者進行有效行動前搶先取得情報。無差別攻擊(indiscriminate assaults)恐將降低資訊通訊科技治理的正當性，進而失去民眾的支持。政府於網路進行大規模資訊審查，即為無差別攻擊的實例。

戰略4：破壞互動。管制者與破壞者雙方皆需要公認的正當性，俾於戰略4中獲得支持與取得治理權。近期影子掮客(Shadow Broker，破壞者)洩漏美國國家安全局(National Security Agency)的機密與能力，其目的即在破壞美國政府(管制者)與微軟公司(治理者)間的資訊正當性。由於微軟公司負責為其產品提供漏洞、安全修補及修正程式，該公司擁有公認的治理能力。美國政府(管制者)運用網路鑽石理論模型時，必須攻擊影子掮客(破壞者)的資訊正

當性，同時強化與微軟公司(治理者)之間的關係、互動與信任。

戰略5：治理關係。戰略5說明在民族國家層級，治理者的正當性與強大的國際支持可產生公認的資訊正當性。在此層級中可透過舉國上下作為與堅強國際合作來強調此一論點。網路與資訊通訊科技的全球互連性，強度也不過如同其最脆弱且易受攻擊的鏈結。

回饋。在瞭解管制者與破壞者針對群眾與國際認知所發起行動而產生之成效時，回饋至關重要。回饋連結(feedback connections)讓管制者與破壞者雙方得以針對資訊正當性來評估網路作戰的成敗。雙方皆必須建立與維持回饋機制，俾評估其行動成效。

建議與結論

儘管美國已成立網路司令部，在此最新戰鬥領域中遂行任務與行動，仍難以精確瞭解網路及其內部行動情形。瞭解不足恐造成在執行或支援國家目標時，導致網路部隊與能力運用失算。網路理論家與國家領導人必須瞭解非正規作戰構想與理論可如何應用在網路作戰。其相似之處在於基本上兩者同樣具有複雜性、高適應性的行為者，以及不受傳統地理邊界限制的作戰環境。透

註釋

1. Patrick Lichty, *Variant Analyses Interrogations of New Media Art and Culture* (Amsterdam: Institute of Network Cultures, 2013), 54.
2. Marc Prensky, "Digital Natives, Digital Immigrants," *On the Horizon* 9, no. 5 (October 2001).
3. Sean Charles Gaines Kern, "Expanding Combat Power Through Military Cyber Power Theory," *Joint Force Quarterly* 79 (4th Quarter 2015).
4. Joseph Celeski, *A Way Forward for Special Operations Theory and Strategic Art*, Joint Special Operations University SOF-Power Workshop, August 2011, MacDill Air Force Base, 15.
5. Ibid., 15–16.
6. Ibid.
7. Ibid., 16.
8. Joint Publication (JP) 3-05, *Special Operations* (Washington, DC: The Joint Staff Staff, 2014), ix.
9. JP 3-12 (R), *Cyberspace Operations* (Washington, DC: The Joint Staff Staff, 2013), I-2.
10. Ibid.
11. Ibid., I-7.
12. Eric D. Trias and Bryan M. Bell, "Cyber This, Cyber That...So What?" *Air & Space Power Journal* 24, no. 1 (Spring 2010), 95.
13. Patrick Duggan, "Why Special Operations Forces in U.S. Cyber-Warfare?" *Cyber Defense Review*, January 8, 2016.
14. Jim Chen and Alan Dinerman, "On Cyber Dominance in Modern Warfare," in *Proceedings of the 15th European Conference on Cyber Warfare and Security*, ed. Robert Koch and Gabi Rodosek (Reading, UK: Academic Conferences and Publishing International Limited, 2016), 54.
15. JP 3-12 (R), *Cyberspace Operations*, vii.
16. Rain Ottis and Peeter Lorents, "Cyberspace: Definition and Implications," Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 268.
17. Ibid.
18. Nicholas Co, "Adapt Special Operations Principles to Cyber," U.S. Naval Institute *Proceedings* 143, no. 6 (June 2017), 58–59.
19. JP 3-05, *Special Operations*, I-2.
20. William H. McRaven, *Spec Ops, Case Studies in Special Operations Warfare: Theory and Practice* (New York:

過理解網路作戰與非正規作戰在特質、原則與理論的相似之處，戰略、作戰與戰術層級的領導幹部將可塑造其思維過程，並制定出一致計畫。

透過非正規作戰的視角，美軍幹部得以開始瞭解網路作戰可與傳統軍事作戰行動並行，或獨立進行。對國家與非國家行為者的網路作戰，應在常是未達公開戰爭門檻的長期區域與全球戰役中進行。[33] 此外，美國的網路戰略必須採取舉國上下與/或全國際聯盟(whole-of-international-coalition)的方針，俾於不斷變化的網路作戰環境中取得相對優勢。透過網路鑽石理論模型於戰略、作戰及戰術層級制定網際空間戰略，軍事領導人與計畫人員就可將網路領域的戰略指導轉化為作戰計畫。

作者簡介

Frank C. Sanchez海軍中校為美聯合參謀部聯J32部門(負責情監偵作戰)行動官。

Weilun Lin空軍少校為美中央司令部聯合網際空間中心(Joint Cyberspace Center)中亞及南亞科科長。

Kent Korunka陸軍中校為美運輸司令部(U.S. Transportation Comand)聯合遂行能力指揮部(Joint Enabling Capabilities Command)聯合規劃支援組(Joint Planning Support Element)聯合情報計畫官。

Reprint from *Joint Force Quarterly* with permission.

Random House, 1995), 4.

21. William D. Bryant, "Cyberspace Superiority: A Conceptual Model," *Air & Space Power Journal* 27, no. 6 (November–December 2013), 25, available at <www.airuniversity.af.mil/Portals/10/ASPJ/jthenals/Volume-27_Issue-6/F-Bryant.pdf>.
22. *Joint Operating Environment (JOE 2035): The Joint Force in a Contested and Disordered World* (Washington, DC: The Joint Staff, July 14, 2016), 36.
23. *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command* (Fort Meade, MD: U.S. Cyber Command, 2018), 4.
24. Air Force Doctrine Document (AFDD) 3-12, *Cyber Operations* (Washington, DC: Headquarters Department of the Air Force, July 15, 2010, incorporating Change 1, November 30, 2011), 50.
25. McRaven, *Spec Ops, Case Studies in Special Operations Warfare*, 4. Emphases by authors.
26. AFDD 3-12, 50.
27. John B. Sheldon, "Deciphering Cyberpower: Strategic Purposes in Peace and War," *Strategic Studies Quarterly* (Summer 2011), 95–112.
28. JP 5-0, *Joint Planning* (Washington, DC: The Joint Staff, 2017), III-2.
29. *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: Department of Defense, July 2011), 3.
30. Gregory Wilson, "The Mystic Diamond: Applying the Diamond Model of Counterinsurgency in the Philippines," in *Gangs and Guerrillas: Ideas from Counterinsurgency and Counterterrorism*, ed. Michael Freeman and Hy Rothstein (Monterey, CA: Naval Postgraduate School, April 2014), 15. To gain a better understanding of the Diamond Model, see Gregory Wilson, "Anatomy of a Successful COIN Operation: OEF-Philippines and the Indirect Approach," *Military Review*, November–December 2006.
31. United Nations Educational, Scientific, and Cultural Organization, "Concept of Governance," International Bureau of Education, available at <www.ibe.unesco.org/en/geqaf/technical-notes/concept-governance>. Emphases by authors.
32. Ibid.
33. *Achieve and Maintain Cyberspace Superiority*, 2, 7.