作者/Paul M. Nakasone　譯者/黃國賢　審者/馬浩翔

網路部隊的戰略構想：遂行持續作戰

A Cyber Force for Persistent Operations

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

美國在網路上的戰略與作戰型態正處於轉型的關鍵時刻。美國網路司令部正逐漸發展成熟，並轉變成爲戰鬥部隊，也將其兵力組成模式移轉爲經常性戰備策略，期能與網路上的敵人打持久戰，並於戰爭中發揮致命戰力。

1954年，來自哈佛大學、年僅27歲的杭廷頓(Samuel Huntington)問了美海軍一個問題，「請問貴軍種展現何種功能，讓社會有義務維持這支軍隊？」他在《美國海軍學會月刊》提出此篇影響深遠的文章中，主張一支軍種──或任一軍事元素──其存續之基礎在於遂行國家政策。杭亭頓將此稱為軍種的「戰略構想」(strategic concept)，藉以說明軍事武裝力量打算如何、何時，以及於何處保護自己的國家，進而讓公眾的支持獲得正當性。[1]

杭廷頓當年提出的疑問引起相當迴響，因為美軍在第二次世界大戰結束後，海軍便面臨其存在目的為何之危機。這支軍種曾於歷史上最大的衝突事件中協助盟軍取得勝利。但同盟國最終竟是以如此壓倒性實力戰勝軸心國，以至於到了1954年時，美海軍竟然已然到了航遍天下無敵手的境界。如此一來，美海軍長久以來矢志成為國家第一道防線的戰略構想不再那麼令人信服。此外，美國的戰略假定也因為核子戰爭的預期心理，而重新形塑其外交與國防政策。儘管沒有任何敵人能夠從海上進犯美國本土，但有一個敵國──蘇聯──卻能從空中投射氫彈摧毀這個國家。美海軍向來以「海洋」為導向的傳統，並以此作為組建強大艦隊的正當理由，在面對歐亞大陸的地面核武力量時，似乎顯得無相關性。

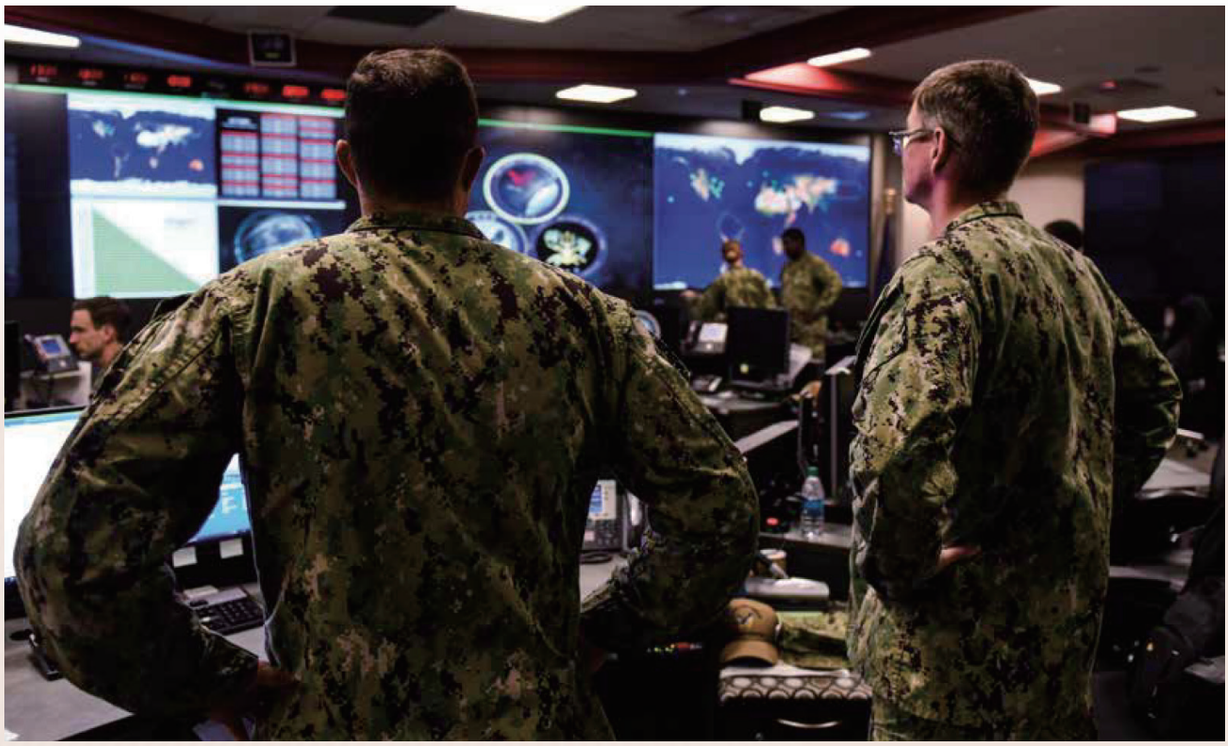
其後，美海軍發展出一種「越洋」(transoceanic)的戰略構想，將該軍種以往海上競逐的戰略方針，轉型為橫跨全球各大洋，並將武力投射至遠方的各大陸地區。為因應威脅及國家政策的改變，美海軍調整戰略構想的作法，以確保公眾的

即便美國自網路領域濫觴便享有整體優勢，但美國的對手在基礎領域中亦羽翼漸豐。(Source: US Army/Bill Roche)

信心與國會的支持。美海軍此項新戰略角色，一直延續至冷戰結束，對美國維持該軍種助益良多，不但發揮圍堵蘇聯的力量，同時也確保美國(及其盟邦)的海上武力夠壯大，甚至強大到蘇聯從未認真考慮想要組建一支足以與美國匹敵的海軍艦隊。[2]

當美國被問道「請問美國網路司令部展現何種功能，讓社會有義務維持這支軍隊？」司令部可以回應網路部隊的戰略構想已然由「反應式部隊」進化為「持久型部隊」。這支持久型部隊將對抗那些處心積慮在網路空間中傷害美國人及美國利益的敵人。這支部隊旨在減少那些足以資敵於網路空間中作戰的基礎設施和各種資源。隨時間推進，一支持久型部隊將作業範圍擴大至美國及友邦，同時提高那些加駭於美國的敵軍所需付出的代價。為了保護國家重大的公共及私人機構免於受到持續在網路空間中演進的威脅，我們的相關作業行動切不可流於片面。

吾等非但不可無視於重大的網絡防禦任務，更如同在面對其他不同面向的衝突般，須主動採取向敵方主動出擊的策略。一支持久型部隊不像其他部隊只能受限於分散的監視行動，其擁有更多機會遏阻敵方不軌之意圖，並且保護美國人民。持久性不應被誤用於為接戰而接戰；反之，其應當被視為一種策略，授權美國網戰部隊遵循國家領導者所設定的目標，來獲致更多的決定性結果。如同在近期公布的《2017年國家安全戰略》及《2018年國防戰略》報告所述，此等演進使得美國網路司令部正隨著戰略環境及國家政策的改變而有所調整。



2018年9月27日，在馬里蘭州密德堡(Fort Meade)美海軍艦隊網路指揮部作戰中心駐足觀看螢幕的第10艦隊官兵。
(Source: USN/Samuel Souvannason)

網路空間與強權競爭

全球化與互聯式的網路自九一一事件之後呈現最大的戰略進展。無論是從內部、透過或源自網路從事各類活動與作戰行動，如今世界各國均擁有更多手段來擴大自身力量，同時降低或奪取他國力量，並且在「不至於引發武裝衝突」的前提下，透過競爭獲取戰略優勢。美國的敵人已然領略此要領，並以子之矛攻子之盾。

當網路空間於1990年代走向全球化後，其基礎似乎很快和西方價值觀不謀而合。基於此等理由，社會互動、經濟交流、科技進程，乃至於軍事作戰的步調都變得更加快速，並且確實對獨裁者形成威脅，他們深怕抓在手中的權力會被受到數位時代功能賦予權力的公民社會所顛覆。這些獨裁者心中的恐懼在2011年發生的阿拉伯之春中一覽無遺。為了回應此種發展趨勢，擁有網路能力的政府部門將行動針對之對象提升至對付自己人，甚至是美國民眾。他們針對各種反對觀點展開全球性的監控手段，並且竊取前所未見、數量龐大的各種智慧財產與個人隱私資料，甚至干擾民主程序的進行，將各種關鍵基礎設施暴露在高度風險下，進而侵蝕美國國力。個別看來，敵軍所採取的方式似乎互不相關，但在日積月累下，一

旦發生狀況，他們就會擁有決定性的優勢。

強權競爭的局面重現引發甫出版之《國家安全戰略》作者群不禁感嘆，儘管「整體而言美國在政治、經濟及軍事上仍保有優勢，然而其他行為者卻早已悄然執行長程計畫來挑戰美國，並且更進一步引發各種反對美國及其盟友的各種議題。」根據《國家安全戰略》所述，全世界愈演愈烈的政治、經濟與軍事競爭，已然對美國的安全與繁榮造成挑戰。在這場競逐爭勝的場域卻已移轉到網路中，並且從公開競爭演變為不舞刀動槍的競逐。

原始概念

美國網路司令部於2010年開始運作，當時美國國防部資訊網及國家關鍵基礎設施，所遭受的主要網路威脅為刺探與干擾。即便美國自網路領域濫觴便享有整體優勢，但美國的對手即便是在基礎領域中，亦羽翼漸豐。當時美國網路司令部的主要任務為透過探知對手的能力發展狀況，以維持美國既有優勢。美國網路司令部成立初期將重點置於保護國防部網路，並支援特別是部署在伊拉克及阿富汗的地區作戰指揮官。因此，美國網路司令部在當時是一支「回應型部隊」──遂行反恐作戰，並針對各種危機發生的想定提供傳統部隊計畫性支援，以及維持作業能量以回應恐對關鍵基礎設施「造成嚴重後果的攻擊事件」。

2013年可視為此戰略的轉折點，而原先的戰略構想也變成不合乎現況發展的過氣觀點。敵人如今已具備令人感到驚訝的能力，不但能夠持續攻擊關鍵基礎設施與政府網路，甚至擴及包含美國國內、外的學術界。長久以來，透過網路竊取智慧財產原本就很常見；但如今各種心懷不軌的活動卻開始讓聯邦政府及民間企業付出高昂的代價。敵人小心翼翼地以不會引發美國武裝回應的方式從事這些活動。此種攻擊案例包含伊朗於2012至2013年針對財政部門所發動的阻斷服務攻擊及2014年對金沙賭場發動的網路攻擊；北韓於2014年針對索尼影視集團發動網路攻擊；中共於2015年干擾GitHub源代碼託管網站，並於同年竊取美國聯邦人事管理局的安全相關資料。俄羅斯亦自2015年起將其所從事的各種網路活動拉高至肆無忌憚的程度，包含介入美國及其盟邦的選舉活動，以及資助烏克蘭電力系統網路攻擊事件。這些活動證實了先前的相關臆測，亦即網路上的各種活動將隨著時間的積累而重創某國的資源與國力。

如今實力匹敵者或不分軒輊的敵人正持續在網路空間中猛烈攻擊美國。這些是計畫性的活動而非單一駭客或偶發事件，而具有計畫性。網路空間讓敵人得以運用各種新管道，透過不至於引發武裝回應的方式，採取持續、非暴力性質的行動，侵蝕美國軍事、經濟與政治力量，繼而產生日積月累的戰略影響。換言之，全球的力量分配如今已能在無須引發武裝衝突的前提下實現。因此回應式部隊的戰略構想──將美國網戰部隊當做動能衝突的後援單位，或是在網路攻擊事件發生後做出回應──如今已然面對如同杭廷頓當年對1945年之前美國海軍戰略構想所做出的批評相同狀況。更糟的是，此種狀況衍生的效應為此等過時戰鬥構想給予敵人有可趁之機，讓他們更想

2018年5月10日，一群圍在電腦前的美空軍士兵正在德國艾因西德霍夫(Einsiedlerhof Station)航空站，參加首次以網路為主的「沈默狩獵」(Tacet Venari)演習。(Source: USAF/Blake Browning)

在網路空間中嘗試各種戰略方案，不斷對美國發動攻擊。為了發揮戰略效應，在網路中持續採取行動變成常態，美國網路司令部因而需要新的戰略構想。

網路持久戰力

美國正在學習如何運用網路能力提升2018年公布之《國防戰略報告》所稱美國的「競賽及戰時的任務」。無庸置疑的是，敵人也在學習中。他們也正在整合及運用各種不同的網路能力，使其能夠務實地結合自身的準則、戰略、組織文化，以及風險的容忍度。歷史殷鑑告訴我們，當衝突場景出現新戰力時，我們應當意識到此種新戰力必將隨著時間的推移而演進。舉例而言，戰車一開始就是用來支援步兵，迄今發展成為以貫穿敵人陣地為主要任務；而戰機則是從戰術偵察，演進成為戰略轟炸，迄今演變為無人情監偵系統。同樣的，作戰概念與戰略觀點也會隨著戰場經驗的積累而不斷演進並更趨於成熟。誠如克勞賽維茨所言，「戰爭藝術的基本知識才是經驗所在。」這意味著理論必須結合實務經驗。[3] 美國網路司令部已然瞭解想要與敵人在網路交戰的過程中克敵制勝，就必須不斷地尋求戰術、作戰，以及戰略方面的創新方案。此種持久力需要吾等在知識及行動上都能領先敵人，同時美國也必須能夠運用其在情報與作戰方面的優勢以達成此項目的。

2018年3月，美國網路司令部發布的《獲取並維持網路空間優勢》(Achieve and Maintain Cyberspace Superiority)文件中更新了該指揮部的戰略構想，以期能與美國國家戰略在網路空間競爭

方面的改變步調一致。[4] 該文件體認到復甦的強權競爭場域已然轉移至網路上，同時決定性的行動也能在低於武裝衝突的界線之下發生。因此，該指揮部的戰略構想希冀美國網路司令部能夠具備「持久的網路戰力」，而非「反應式網路戰力」，以期能夠從全球面向及持久不墜的戰力和敵人較勁與對抗，同時也能在既有之戰略上，以更有效率的方式和敵人作戰。

美國網路司令部的戰略思維隨著部隊與戰力而演進。該部正以下列方式加速變革：

- 美國的戰略觀點正在改變，不再認為危及國力的源頭僅限於戰爭及入侵領土。成功嚇阻傳統及核子戰爭的副作用在於，敵人如今已經透過網路空間重新調整操作方式，避免引發武裝回應，藉以重新形塑美國的政策選項。由於敵人迄今仍然認為能夠透過網路空間和美國進行對抗，同時也對美國的利益造成損害；同時從歷史來看，這樣的模式所須付出的代價最小，因此美國網路司令部必須在低於傳統動武的標準下進行作業，同時準備好在衝突中使用具備殺傷力的部隊。
- 美國正在與那些有可能在國外駭客活動中遭到鎖定的相關機構──尤其是國家關鍵基礎設施──在危機發生前建立關係；並且以持續共同作業模式，取代現行公務部門、各局處，以及民間機構間等橫向協調單位。此等關係的關鍵之處在於，能在敵人發動攻勢並提高自身防禦強度形成突破口前就挫敗其行動。理想狀況下，此種夥伴關係可讓吾等持久戰力能在惡意的網路行為變成攻擊事件之前即化解其危機。
- 美國必須「預先防衛」網路空間，如同其在實體領域上的防衛方式。海軍守在港口內就可以捍衛疆土，空軍亦不是只待在機場而已。渠等巡弋海疆及空域，戍守國土疆域，叫敵人無法越過雷池一步。此邏輯同樣適用於網路空間。如果僅限於國防部網路，則想要和敵人在網路空間中打持久戰，根本沒有勝算。為了保護重大軍事與國家利益，美軍同樣必須在敵人實際領土上採取行動。從以往反應式的觀點轉變為持久性的部隊，唯有預先防衛才能從敵方的衛戍能力中獲取我方的網路戰力，展現符合網路空間作戰環境的防衛態勢。
- 美國已不同以往強調在特定時間，於作戰「風險」下鎖定目標，同時確保這段時間的選擇權操之在我。美國將展現讓決策者持續維持最新選擇權的作戰方式。網路空間鎖定的目標本身就是電算與數據的「樣態」，其在數位資訊系統中的正常運作原本就處於不斷變化的狀態。為了利用新的弱點與機會，作戰行動的成敗乃在於能夠迅速調整那些未能奏效的戰力與戰術。
- 最後，美國正在確保我們的戰力、作戰節奏、決策程序，以及權責單位均能遂行綿密而持久的作戰。敵人與競爭者已對此受限且不定期的交戰方式採取網路侵略作戰模式，並已侵蝕美國的軍事、經濟與外交優勢。網路空間的戰略優勢來自運用──而非僅是掌握──網路戰力，以期在面對蓄意傷害美國之敵人時，能搶先獲得主動權。

2017年8月31日，太平洋上，派遣至網路指管通情部門的射控員，正在太平洋上的美利堅號(USS America, LHA-6)兩棲突擊艦，於飛彈甲板上檢查海麻雀地對空攔截飛彈。(Source: USN/Alexander A. Ventura II)

網戰部隊的價值

資深政治及軍事領導者認為，美軍必須有能力在武裝衝突的界線之下與敵人較勁。此項概念明確陳述於《國家安全戰略》中：「我們的任務在於確保美國能維持軍事優勢；並且能夠結合其他國家力量元素，做好保護美國的準備，因應美國國家安全所面對的特定挑戰。」[5] 實力匹敵者正不斷採取行動，試圖尋求能夠攻擊美國的戰略優勢，因此目前沒有任何軍事需求比網路空間來得更為重要。為達此目的，美國網路司令部將採取下列措施：

- 在敵人所在之處採取預先作業。此為網戰部隊的主要任務，也是美國網路司令部預先防衛的概念。此項概念的目的在於限制敵人影響或控制我方的範圍。美國無法承擔遭到敵人突破其網路系統或攫取資料(智慧財產與個資)。如果只能在「藍區」(blue space)進行防衛則必敗無疑。反之，我們應當保持滴水不漏的機動能力，橫跨所有相互連結的戰場，範圍遍及全球，並且具備持續形塑戰場的能力，以創造有利於我，不利於敵的作戰優勢。
- 確保聯合部隊能夠安全且可靠地遂行作戰任務。美國網路司令部主要任務為防護國防部資訊網(DODIN)，包含指揮、管制、通信，以及聯合部隊的資料匯流。其幾乎在美軍任何作戰階段均發揮作用。基於防護美國國防部資

訊網的任務，美國網路司令部自2010年成立以來，在美軍所有軍事行動中均扮演間接、但具有強力支持作用的角色。國防部依賴愈加安全且密不可分的資訊網路，以滿足其全方位的作戰需求，並且「因為過去及當前網路司令部的相關作業」而能發揮必要功能。

打造具備持久力的網戰部隊

美國在網路空間上的戰略與作戰型態正處於轉型的關鍵時刻。網路空間代表著新的戰略環境，即便無需動用武裝衝突，國家力量也會在此戰略環境中遭到挑戰。高階政治與軍事領導階層已然體認到，美國國防部起初因應網路空間攻擊行為的方式──聚焦於韌性與回應行動──導致軍事行動中產生根本性的罅隙，並且因為將此等部隊列為支援部隊而錯過了下決定的時間點。

杭廷頓針對成功的戰略構想提出兩項重要因素：達成戰略所需的人力與物力資源，以及社會為了達成此戰略構想而將各項資源加以集結的組織架構。美國網路司令部正逐漸發展成熟，並轉變成為戰鬥部隊，擁有團隊、基礎設施、工具、進出管道及遂行任務所需的相關權責。該司令部也將其兵力組成模式，移轉為經常性戰備策略，期能與網路上的敵人打持久戰，並於戰爭中發揮致命戰力。該司令部基於作戰經驗及任務編組持續演進，將運用各種形式的小部隊，以無法預料的方式讓敵人撲空。

軍事單位的戰略構想是成功打贏這場戰爭的關鍵因素。正如杭廷頓在1954年發表的論文所示，軍事指揮官及部隊本身必須有能力讓文人領導階層及普羅大眾保持十足的信心，相信軍方已經設計出適切可行的戰略構想，並且具備相關技能，足可為國家遂行此等任務。依循此戰略構想所採取的持久作戰行動，理當隨著時間的推移，而讓美國網路司令部建立更多信心。

作者簡介

Paul M. Nakasone 上將為美國網路司令部司令，同時也是國家安全局局長及中央安全局局長。

Reprint from *Joint Force Quarterly* with permission.

註釋

1. Samuel P. Huntington, “National Policy and the Transoceanic Navy,” U.S. Naval Institute *Proceedings* 80, no. 5 (May 1954).
2. 蘇聯曾於1980年代建立強大的海軍，不過他們將這支軍隊用於控制國土周邊海域，以及保護他們的戰略飛彈潛艦──而非從事大西洋或太平洋的海上軍備競賽。
3. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976), 170.
4. *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command* (Washington, DC: U.S. Cyber Command, March 2018).
5. *National Security Strategy of the United States of America* (Washington, DC: The White House, December 2017), 3.