作者/Natalie R. Alen, Gregory M. Eaton, and Jaime L. Stieler　譯者/黃文啟　審者/丁勇仁

因應俄羅斯混合作戰之道：網路戰略納入私部門網路能力

The New "Cyber" Space Race: Integrating the Private Sector Into U.S. Cyber Strategy

取材/2023年第2季聯合部隊季刊(*Joint Force Quarterly*, 2nd Quarter/2023)

美國若想在大國網路競爭中取得優勢，不僅須強化跨部會合作，亦需一套能有效融合私部門創新力量的統一作爲，以進行嚴謹分工的國家網路戰略，進而達成其國家戰略目標。

(Source: Shutterstock)

2022年12月7日，第136網路安全支隊威脅研究員王中士於薩爾瓦多向該國網路安全部門提報新的重點項目，其中包含人工智慧與網路弱點辨別。
(Source: US Air National Guard/Victoria Nelson)

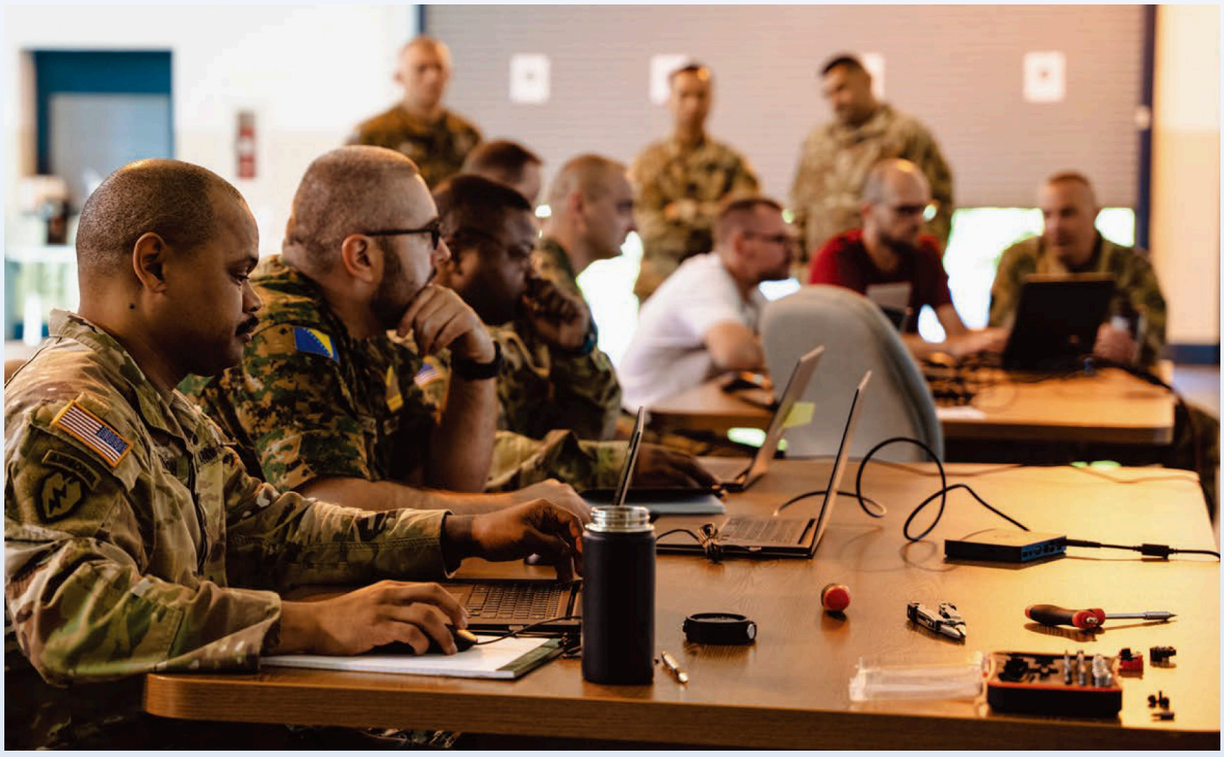
目前俄羅斯網路戰力顯示出該國愈來愈擅於將網路力量融入整個社會，成為一個完全成熟的國家權力手段。俄羅斯網路活動已能融合殺傷性行動與較強之資訊領域攻擊，遂行美軍稱之為混合型戰法的持續且低強度之攻勢戰役。俄羅斯軍方將網路與其他「愛國」非國家行為者結合，從事包含運用駭客和疑似與俄國安全機關有直接關係或受其控制的犯罪組織。沃茨(James Wirtz)博士強調，「俄羅斯以遠超過其他新興網路圈行為者的能力，似乎已經設計出整合網路戰與大戰略的方式，用以達成其政治目標。」[1]

俄羅斯崛起成為網路大國，以及克里姆林宮運用網路戰做為國家權力手段所造成的影響，美國政府與軍事領導人絕非渾然不知。然而，問題仍在於：美國究竟從俄羅斯身上學到什麼？美國如何調整其國家戰略，將網路力量融入其國際競爭與衝突的整體社會做法？智庫學者

克拉默(Franklin Kramer)、史塔爾(Stuart Starr)及溫茲(Larry Wentz)在《網路力量與國家安全》一書中主張：

> 網路力量現已成為全球生活基本事實。在政治、經濟及軍事事務方面，資訊與資訊科技提供並支持所有作戰活動的關鍵環節。美國國家安全作為已開始將網路納入戰略考量因素。然而，這些作為才剛剛起步。重要結論為……美國必須針對網路發展與運用建立一套有效的國家與國際戰略架構，將其納入整體國家安全戰略之中。[2]

雖然美國政府致力改善網路安全與韌性，以增加國家遭受網路攻擊的存活力，但是為了建立美國網路優勢，現在必須開始將私部門與較廣泛的資訊領域戰略相整合。隨著克里姆林宮發展與運用網路戰之手段逐漸成熟，美國也必須能採取整體社會做法，結合私部門與公部門之能力(包含美軍的專業能力)，並將之投入此新時代的網路大國競爭中，並進而藉此取得優勢。然而，私部門抗拒與美國政府資訊共享及合作，仍是成功落實國家網路戰略的障礙。為了克服此一障礙，政府領袖們必須檢視上一次美國如何因應全新出現的國際競爭領域，以成功整合公-私-軍



2022年6月29日，第169網路防護小組人員，以及波士尼亞(Bosnia)與赫塞哥維納(Herzegovina)武裝部隊官兵於馬里蘭州勞瑞「卡斯丁大兵戰備中心」(Private Henry Costin Readiness Center)共同執行網路對抗演習。

(Source: US Army National Guard/Tom Lamb)

隊組織，以遂行國家權力。

俄羅斯整體網路力量的起源

俄羅斯的網路攻擊（包含分散式阻斷服務(DDoS)攻擊及對重要基礎設施與網路的攻擊）已在新聞上廣泛報導多年。這些表面上為非國家行為者所發動的網路攻擊與入侵行為，疑似是由克里姆林宮所指導與控制。2007年，俄羅斯聯邦安全局據信就是愛沙尼亞各銀行、媒體集團及政府機關遭到分散式阻斷服務攻擊的幕後黑手，這場攻擊行動可算是以網路戰作為遂行政治影響力脅迫工具的首度運用案例。[3]

2008年，俄羅斯附隨團體(包含名為「俄羅斯商業網路」的犯罪組織)在俄羅斯發動地面侵略前，阻斷了喬治亞政府的通信、銀行、運輸公司及電信服務公司。[4] 此外，俄羅斯「激進駭客」(Hacktivist)網站公布了一張喬治亞網站的清單，供其他駭客進行攻擊，內容包含攻擊指引及可供下載的惡意程式。[5] 俄羅斯國防部後來成立了專門從事資訊戰的正式部門，以整體社會範圍有效整合軍事戰力與非國家行為者，以進行網路與影響力作戰。

莫斯科的惡意網路活動仍在持續進行，而其為爭取克里姆林宮利益而運用網路戰做為國家權力手段的慣常行為，已對美國在網路大國競爭中造成重大挑戰。

得自克里姆林宮的經驗教訓

或許從俄羅斯運用整體網路戰所獲得最重要之經驗教訓並非科技方面而是組織方面：亦即採用統一協調機關有效整合俄羅斯的國家、軍隊及非國家行為者在所有資訊作戰範疇的各種戰力。據美國智庫海軍分析中心(CNA)研究指出，俄羅斯軍事理論家甚至並未使用「網路戰」(Cyber-warfare)這個名詞。[6] 相反地，網路戰被視為更通用性名詞「資訊戰」(Information Warfare)的其中一環，而莫斯科當局視資訊戰為一種手段，可從事：

> 協助國家主宰資訊環境……且可納入整體政府作為的一環，以及配合其他俄羅斯或蘇聯軍事準則的遵行者所熟悉較傳統的資訊戰武器手段共同運用，包含假訊息行動、心理戰、電子戰及政治滲透等。[7]

此一觀點獲得作家雷契夫(Yavor Raychev)的支持，雷氏特別強調網路戰的概念在俄羅斯及美國的政治軍事思想上有多項重要差異。[8] 雷契夫表示，美國人視網路戰為現代混合戰爭的一環，其融合傳統戰、非正規戰及網路戰。[9] 但雷氏指出，「在俄羅斯傳統中，在蘇聯瓦解前，『混合戰』一詞指的是政治戰與資訊作戰。」[10] 此種情況衍生出的問題是，美國政府應採取何種戰略作法，將資訊領域融入網路國家權力手段，以結合軍隊與私部門的各種能力。

現有美國網路戰略與公-私夥伴關係

產業界與美國政府在網路防護與計畫的公部門與私部門夥伴關係始於柯林頓政府時期，且相關合作仍在持續擴大。[11] 相較於俄羅斯軍方運用違法非國家行為者協助與執行其網路戰力，美國

則是運用美國境內具崇高地位企業的才智與專業能力，推動公部門與私部門重要基礎設施網路安全方面的共同合作。美國「2018年國家網路戰略」(2018 National Cyber Strategy)要求「聯邦政府與私部門全面性的科技進步與行政效率提升」，以確保網路空間安全。[12] 同樣地，美國國防部2018年「網路戰略」(Cyber Strategy)也確認有必要透過跨部會與私部門夥伴關係提升美國重要基礎設施韌性。[13] 美國國土安全部透過網路安全暨基礎設施安全局(Cybersecurity and Infrastructure Security Agency, CISA)主導此項作為，藉由公部門與私部門的夥伴關係，以建構更堅強的防衛與韌性。[14] 例如，網路安全暨基礎設施安全局負責督導各項資訊共享計畫，諸如具產業針對性的資訊共享與分析中心(Information Sharing and Analysis Centers, ISACs)及資訊共享與分析組織(Information Sharing and Analysis Organizations, ISAOs)。這些非營利且是會員參與型的組織，都是由私部門重要基礎設施所有權人所成立，為政府與產業蒐集、分析及傳遞各種網路威脅資訊，以推動更有效的網路安全資訊共享，以及強化私部門間之合作與資訊分享。[15]

雖然這些夥伴關係對改善美國的網路防護已具成效，但外界仍然大力呼籲政府與私部門企業應擴大整合，以進一步發展美國私部門、公部門及國防部門的網路能力。在過去幾年間，美國網路司令部司令兼國家安全局局長仲宗根(Paul Nakasone)上將積極推動與科技公司的夥伴關係，強調私部門與矽谷才是創新思維的最前線。[16]

前網路司令部司令兼國家安全局局長羅傑斯

美國國土安全部「網路安全暨基礎設施安全局」主導跨部會與民間夥伴合作，提升國內關鍵基礎設施韌性。2019年，時任國防部長艾斯培(Mark Esper)親臨該局第二屆年度國家網路安全峰會致詞。

(Source: US DoD)

(Mike Rogers)上將認為，美國在政府與私部門關係方面並未採取效果最佳的做法。目前，美國的合作方式是公部門與私部門都是置重點於對內工作，且只有在發現某件重要事情時才會彼此通報。羅傑斯上將提倡美國應跨出共同合作走向相互整合，使政府與私部門無時無刻地在互利夥伴關係上推動網路安全合作。[17] 政府與私部門科技公司融合一體的夥伴關係，象徵邁向強化聯盟關係並吸引新夥伴關係的動能，此亦為2018年美國國防部「網路戰略」的戰略行動主軸。[18]

此項戰略要求盟邦及其他重要夥伴更廣泛的資訊共享，以強化集體網路行動的效能，並建立可信任的私部門夥伴關係。雖然這項戰略可推動資訊共享，但針對資訊共享與解密使用的速度仍

然有令人憂慮之處。在提供給美國國家情報總監的備忘錄中，多位聯合作戰司令就曾對過度加密有關對手之情報導致資訊共享與傳遞能力喪失，以及情報獲得速度太慢的情況表達憂心。[19] 這項備忘錄說明跨部會、盟國及重要夥伴們在資訊共享方面遭遇的多項重大挑戰。假如美國之目的是要推動政府與私部門充分運用矽谷創新作為的夥伴關係，則分享資訊的速度與範圍仍需要更進步的做法。

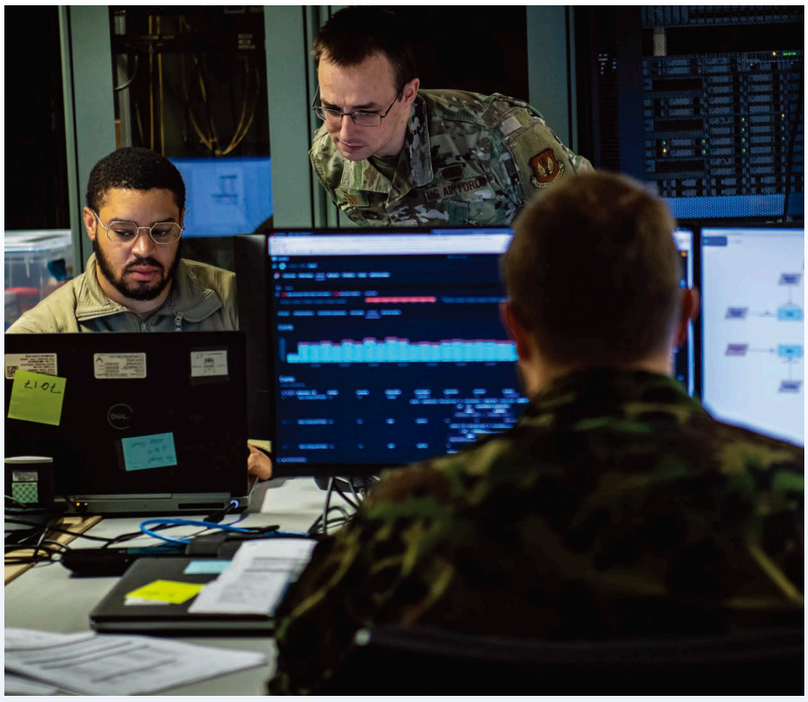
科技大廠、美軍，以及資訊領域

在美國，多數網路架構、作業及專業能力都深植民間市場。[20] 情況雖然如此，但美國目前對於網路行動的做法，尚未具有能有效整合私部門的專業能力。為在對抗俄羅斯極權體制的競爭中獲勝，一套能呼應美國民主價值及有效對抗敵人的均衡整體社會做法有其必要。如雷契夫所言，「可以推論西方世界對於網路戰的觀點，主要仍以軍事為重點且偏重技術層面。西方世界視網路戰為現代作戰型式中廣泛網路衝突背景下的一部分，但卻鮮少瞭解其社會面向。」[21] 雖然各方專家可以不認同雷契夫對於美國政府在網路互動全般背景認知的看法，但顯然此種網路行動的軍事觀點，以及並未與軍事思考做法充分融合的無盡民間資源，兩者間仍存在許多落差。

「美軍聯戰準則5-0聯合計畫作為」(*JP 5-0, Joint Planning*)內容記載參謀首長聯席會議主席認為若要成功運用軍事力量支持美國的利益，則必須與其他三大國家權力手段緊密協調：外交、資訊及經濟手段。[22] 而跨部會協調在眾所皆知的「3D」中——建立外交(Diplomatic)、發展(Development)及國防(Defense)以擬定計畫及執行作戰——是美國交流政策與其獲致成功的關鍵要素。透過跨部會協調尋求在資訊領域擴大整合公、私部門夥伴關係的概念，已經提高了其在網路競爭與作戰新時代的適用程度。

跨部會合作的原則詳載於「美軍聯戰準則5-0」等軍事準則，而美國國家安全會議也持續促成所有國家權力手段方面之整合，達成統一作為所必須的「相互瞭解與合作」。[23] 然而，大型科技公司一直不願意與美國政府在網路議題上充分合作。此舉限制了公部門與私部門實體在使用網路領域及對其進行保護的統一作為。如同崔夫諾維(Darko Trifunović)博士所言，史諾登(Edward Snowden)洩密事件所曝光的那些從事美國網路力量任務的頂尖科技公司，對此事件的處置方式就是讓自己遠離「政治服從或參與國家分配的網路戰任務」。[24] 除此之外，某些私部門企業放棄國家網路安全防護計畫，轉而另行為自己尋找提供網路防護的替代解決方案。據卡內基國際和平基金會(Carnegie Endowment for International Peace)表示，「愈是足智多謀且老練的私部門實體正不斷加碼其自身解決網路威脅的作為。除了各式各樣的安全措施外，愈來愈多的公司轉而尋求網路保險政策的風險挑戰機制。但網路保險的現有保障範圍卻只能提供有限、不確定且僅是臨時性的解決方案。」[25]

網路安全暨基礎設施安全局是在2018年成立於國土安全部轄下的獨立聯邦機關(類似聯邦應急管理署)，此舉就是美國政府希望成立一個負



2022年5月12日，德國蘭斯坦基地舉行為期2週的「無聲獵殺」(Tacet Venari)網路演習，參演官兵正在分析元數據以辨識網路可疑活動。(Source: USAF/Jared Lovett)

責整合所有聯邦文職機關網路安全事務的統一組織，以及提供公部門與私部門保護重要基礎設施網絡合作的嘗試。[26] 然而，自網路安全暨基礎設施安全局成立後，該局就一直受到隱私權倡議人士及諸如蘋果與亞馬遜等大型科技公司的普遍批評，因為該局容許資料可供其他公司或美國政府運用。[27] 國土安全部督察長辦公室的一份內部報告在結論指出，資料共享仍需要許多精進作為。[28] 2021年5月12日為改善美國網路安全所公布的行政命令，目的就在於解決各部會、機關及私部門間更廣泛資訊共享的需求，但網路安全暨基礎設施安全局與私部門在隱私權及相互合作方面，仍存在許多問題。[29]

美國網路整合的數位兵力

將私部門融入美國網路國家權力戰略的可能解決方案之一，是在資訊領域保護美國國家安全的「3D」中增加第四根支柱──亦即數位。新的第四個「D」不僅可以運用美國政府與美軍的網路防護及網路作戰能力，作為大科技公司網路資訊與創新的介面，同時仍可維護私部門的獨立性。一如美國國際開發總署(U.S. Agency for International Development, USAID)在美國外交政策所扮演的角色是「3Ds」中「發展」兵力之主導機關，一個獨立且由文人主導的機關，可以運用保護重要基礎設施的各種夥伴關係與投資項目，在資訊領域促進美國的網路利益及經濟繁榮。一個新的「數位」機關也可以做為聯邦政府在網路科技研究發展及科技轉移專案的管道。冷戰時期所採用的類似公部門與私部門夥伴關係模式，就是成立諸如國家科學基金會(National Science Foundation)及國防先進研究計畫局(Defense Advanced Research Projects Agency)等機關。研究發展方面的聯邦預算挹注，促成了各種新的科技與技術能力問世，因而得以建立各種新產業，讓聯邦政府與私部門可同時獲益。[30] 政府類似

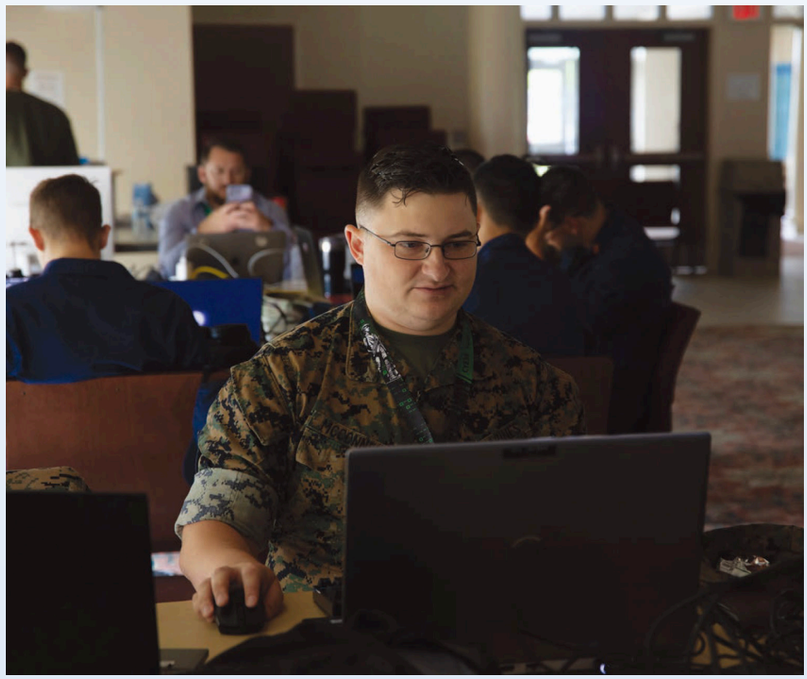
的主導性數位主軸，不僅可以維持資訊領域的投資與創新，同時還能強化其他國家權力手段，並提供讓美國公部門與私部門協調最大化所需之組織能量，以因應與俄羅斯的網路力量競爭。

真正整合第四個「D」(亦即數位兵力)的概念，也需要確保在競爭全期明確區隔民間與軍事活動的能力。[31] 如同2018年，4,000名谷歌公司職員提出之訴願，要求「一個說明谷歌或其合約商都不得發展戰爭科技之明確政策」所示，美國網路科技界有許多人對於致力爭取美國網路優勢如果代表直接支援美國國防部達成其目標，將會感到相當不安。[32] 不僅如此，武裝衝突法的目標「區分原則」在平民參與資訊領域時之直接敵對行為的適用範圍仍有爭議。[33] 成為第四個「D」的數位兵力必須針對所有美國網路科技活動提供必要的隱私、監督及協調。同時，其亦須在民間能力與政府或軍事目標之間做出明確劃分，同時讓美國政府的地位可更有效以一套開放性整體社會做法在資訊領域對俄羅斯及其他民族國家進行競爭。此種組織的進步需要研擬提供私部門公司各種誘因的權限，以克服隱私權與資料共享的顧慮，諸如補助金、有限責任保護，以及網路安全研究管道等諸多事項。[34]

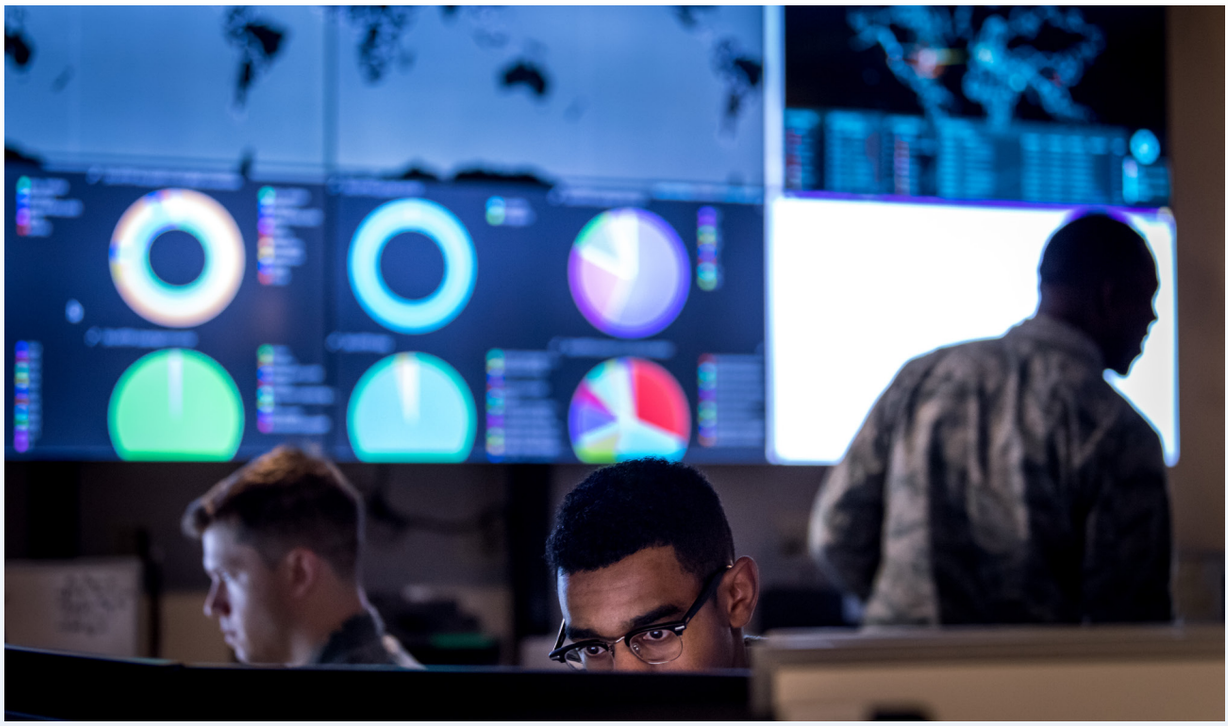
整合資訊領域

建立一個第四「D」組織以整合政府與私部門活動，同時區隔民間與軍事目標，是在大國網路力量競爭時代達成統一作為的必要條件。某篇文章指出：

> 各國政府擁有獨特能量，可以幫助資訊共享與相互間之交流。此種作為將可幫助創新鐵三角——亦即公部門、私部門及學界——的關係重建，並鼓勵各界間之相互瞭解，而這是打破限制政府與高科技公司彼此合作之文化藩籬的必要步驟。[35]



2022年6月13日，美陸戰隊第8通信營負責防衛性網路空間行動——內部防護措施的網路戰作業士麥康納(Ian McConnell)中士於康乃迪克州耐安提克市聶特營基地(Camp Nett)所舉行之網路洋基22(Cyber Yankee 22)演習中研擬網路駭攻計畫。(Source: USMC/Ashley Corbo)



國家網路戰略應充分整合軍民資源、共享情資，攜手對抗敵對勢力。圖為2017年12月2日，馬里蘭州空軍國民兵第175網路作戰大隊第275網路作戰中隊作業實況。(Source: USAF/J.M. Eddins Jr.)

所幸，美國政府在60多年前為了處置另外一個來自俄羅斯的國家安全領域挑戰，已經為此種型態的組織設計了一套模式。1957年，蘇聯發射第一顆人造衛星──史普尼克號(Sputnik)。此舉激起了後來世人熟知的太空競賽，並促使美國產生在短期內動員政府與私部門能力投入太空領域的需求。[36] 因此美國在1958年成立國家航空暨太空總署(National Aeronautics and Space Administration, NASA)，負責持續督導美國的太空計畫，整合民間與軍方的各種能力。成立國家航空暨太空總署所依據的國家航空暨太空法(National Aeronautics and Space Act)，「同意該機關與產業界及教育機構簽訂合約，並要求最大程度可能之可行與適切資訊傳遞」。[37] 原始法條第103節第b段原文引述如下：

> 美國國會進一步宣布此類活動(航空與太空)應由美國政府所監督之管制航空及太空活動之文職機關負責，並應受其指導，除了……武器系統發展、軍事作戰或防衛美國專屬或主要相關活動。[38]

此種型態的立法與組織安排完全呼應中曾根與羅傑斯上將對於資訊領域應與私部門進行更廣泛之整合與資訊共享，但私部門不參與任何網

路司令部或美國國防部所屬單位從事之軍事網路活動。

澈底革新：網路安全暨基礎設施安全局版本

網路安全暨基礎設施安全局在成立之時，原本想像其應該是類似「國家航空暨太空總署」的解決方案；然而，在成立的最初四年間，仍然未能符合大眾的想像，或是像國家航空暨太空總署當年那樣激發私部門的積極參與。處理資料隱私權及資料共享的各種初期挑戰，大幅削弱了網路安全暨基礎設施安全局充分讓私部門融入美國網路戰略作為方面的效能。為了讓該局成為能在網路領域整合美國政府與私部門各項作為的數位組織，遵循國家航空暨太空總署的相同發展路線對其所有助益。

第一項步驟是將網路安全暨基礎設施安全局從國土安全部分離，賦予該局更高的作業獨立性，並增加該局的能見度，以及提高做為美國政府網路安全或數位環節代言人的公共地位。前網路安全暨基礎設施局局長克瑞布斯(Christopher Krebs)曾公開主張將該局從國土安全部分離並成為一個獨立機關，以給予私部門及其他有關對象一個與政府共同合作打擊網路威脅的明確可見「大門」。[39]

第二，網路安全暨基礎設施安全局應具有更大的預算權限，以資助網路研究發展，並透過合約與補助金提供私部門參與所需誘因。雖然該局目前督管重要基礎設施防護資訊共享的相關產業論壇，諸如資訊共享與分析中心及資訊共享與分析組織等，但該類論壇的參與及加入會員仍然嚴格限制為志願性質，而網路安全暨基礎設施安全局也僅給予專案支持。一個獲得財務力量的新網路安全暨基礎設施局，可以繼續管理並運用這些既有關係，同時可以透過取得補助金專案與研究發展預算，提供更大的參與誘因。

最後，一個全新獨立且重塑形象的網路安全暨基礎設施局可以成為「網路卓越中心」，藉由網路資訊、網路專業能力，以及政府、學界及產業最佳做法的蒐集與傳遞，並同時將攻擊性網路目標予以區隔。這個讓外界有新想像的網路安全暨基礎設施局，可以成為培養美國網路人才的磁吸中心，不僅增加既有訓練專案，也可創造實習與休假研究機會、研究助理職務，以及由科技公司補助之在職主管專案等方式，加速美國政府與產業界的網路人才成長。透過與美國政府其他部會，以及與軍事部門的輪換式任職機會，亦可以「交織歷練」培養人才，並為贏得大國網路競爭所需的統一作為，建構相關之專業組織。

今日，多數美國網路人才與能力都在私部門。一套成功的國家網路力量戰略必須能整合這些資源，一如俄羅斯已充分展現的例證，同時還應維持美國獨有特質。在美國針對政府與私部門能力進行有組織且彈性的整合作為時，需要一種可促進資訊共享及統一作為的做法，以支持國家利益，且同時能防範隱私權顧慮問題，並且維護做為美國價值基礎之結社自由。重新打造網路安全暨基礎設施安全局成為類似國家航空暨太空總署的組織，專門負

責整合公部門與私部門在網路發展與運用的活動，可以提供建立政府與私部門統一作為的可能手段。此舉將使美國政府得以運用整體社會做法，同時確保私部門網路科技公司可以與資訊領域的直接敵對行動保持完全區隔。

作者簡介

Natalie R. Alen美陸戰隊後備中尉為人力及後備事務部門後備事務處程式資料官主管。

Gregory M. Eaton美海軍後備上校為國防後勤局聯合後備兵力分配聯合作戰機構主管。

Jaime L. Stieler上校現任美空軍第480情監偵聯隊作戰處長。

Reprint form *Joint Force Quarterly* with permission.

註釋

1. James J. Wirtz, "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy," in *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015), 31, available at <https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf>.
2. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, *Cyberpower and National Security* (Washington, DC: NDU Press, 2009).
3. Michael Connell and Sarah Vogler, *Review of Russia's Approach to Cyber Warfare* (Arlington, VA: CNA, September 2016), 13, available at <https://apps.dtic.mil/sti/pdfs/AD1019062.pdf>.
4. John Markoff, "Before the Gunfire, Cyberattacks," *New York Times*, August 12, 2008; Connell and Vogler, *Review of Russia's Approach to Cyber Warfare*, 18.
5. Connell and Vogler, *Review of Russia's Approach to Cyber Warfare*, 17.
6. Ibid., 3.
7. Ibid.
8. Yavor Raychev, "Cyberwar in Russian and U.S.A. Military-Political Thought: A Comparative View," *Information & Security: An International Journal* 43, no. 3 (2019), 354.
9. Ibid., 351.
10. Ibid., 349. Emphasis added.
11. Madeline Carr, "Public-Private Partnerships in National Cyber-Security Strategies," *International Affairs* 92, no. 1 (2016), 43–62.
12. *National Cyber Strategy of the United States of America* (Washington, DC: The White House, September 21, 2018).
13. *Department of Defense Cyber Strategy* (Washington, DC: Department of Defense [DOD], September 2018).
14. "Protecting Critical Infrastructure," Cybersecurity and Infrastructure Security Agency (CISA), September 7, 2021, available at <https://www.cisa.gov/protecting-critical-infrastructure>.
15. "Information Sharing and Awareness," CISA, February 16, 2022, available at <https://www.cisa.gov/information-sharing-and-awareness>.
16. Mark Pomerleau, "U.S. Cyber Command's Top General Makes Case for Partnering With Tech Firms," *C4ISRNET*, August 25, 2020, available at <https://www.c4isrnet.com/cyber/2020/08/25/us-cyber-commands-top-general-makes-case-for-partnering-with-tech-firms/>.
17. Ryder Ashcraft, "Admiral Mike Rogers, USN (Ret.)," *DOD Reads: What Are You Reading?* podcast, April 26, 2021, available at <https://anchor.fm/dodreads/episodes/Admiral-Mike-Rogers--USN-Ret-eubfn6>.
18. *Department of Defense Cyber Strategy.*
19. Betsy Woodruff Swan and Bryan Bender, "Spy Chiefs Look to Declassify Intel After Rare Plea from 4-Star Commanders," *Politico*, April 26, 2021, available at <https://www.politico.com/news/2021/04/26/spy-chiefs-information-war-russia-china-484723>.
20. Max Smeets, "U.S. Cyber Strategy of Persistent Engagement and Defend Forward: Implications for the Alliance and Intelligence Collection," *Intelligence and National*

Security 35, no. 3 (2020), 450.
21. Raychev, "Cyberwar in Russian and U.S.A. Military-Political Thought," 353.
22. Joint Publication 5, *Joint Planning* (Washington, DC: The Joint Staff, December 1, 2020), xv, available at <https://irp.fas.org/doddir/dod/jp5_0.pdf>.
23. Ibid., I-24.
24. Darko Trifunović and Zoran Bjelica, "Cyber War—Trends and Technologies," *National Security and the Future* 21, no. 3 (2021), 76, available at <https://doi.org/10.37458/nstf.21.3.2>.
25. Ariel E. Levite, Scott Kannry, and Wyatt Hoffman, *Addressing the Private Sector Cybersecurity Predicament: The Indispensable Role of Insurance* (Washington, DC: Carnegie Endowment for International Peace, October 2018), available at <https://carnegieendowment.org/files/cyber_insurance_formatted_final_web.pdf>.
26. Cynthia Brumfield, "What Is the CISA? How the New Federal Agency Protects Critical Infrastructure," *CSO Online*, July 1, 2019, available at <https://www.csoonline.com/article/3405580/what-is-the-cisa-how-the-new-federal-agency-protects-critical-infrastructure-from-cyber-threats.html>.
27. Graeme Caldwell, "Why You Should Be Concerned About the Cybersecurity Information Sharing Act," *TechCrunch*, February 7, 2016, available at <https://techcrunch.com/2016/02/07/why-you-should-be-concerned-about-cisa/>.
28. Jordan Smith, "CISA Aims to Improve Cyber Threat Data Sharing Problem," *MeriTalk*, October 9, 2020, available at <https://www.meritalk.com/articles/cisa-aims-to-improve-cyber-threat-data-sharing-program/>.
29. "Executive Order on Improving the Nation's Cybersecurity," The White House, May 12, 2021, available at <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>.
30. David H. McCormick, Charles E. Luftig, and James M. Cunningham, "Economic Might, National Security, and the Future of American Statecraft," *Texas National Security Review* 3, no. 3 (Summer 2020), 56, available at <https://tnsr.org/2020/05/economic-might-national-security-future-american-statecraft/>.
31. Joint Doctrine Note 1-19, *Competition Continuum* (Washington, DC: The Joint Staff, June 3, 2019), 2–3, available at <https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn1_19.pdf>.
32. Scott Shane and Daisuke Wakabayashi, "'The Business of War': Google Employees Protest Work for the Pentagon," *New York Times*, April 4, 2018.
33. David Wallace, Shane Reeves, and Trent Powell, "Direct Participation in Hostilities in the Age of Cyber: Exploring the Fault Lines," *Harvard National Security Journal* 12 (2021), 186, available at <https://harvardnsj.org/wp-content/uploads/sites/13/2021/02/HNSJ-Vol-12-Wallace-Reeves-and-Powell-Direct-Participation-in-Hostilities-in-the-Age-of-Cyber.pdf>.
34. Michael Daniel, "Incentives to Support Adoption of the Cybersecurity Framework," Department of Homeland Security, August 6, 2013, available at <https://www.dhs.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework>.
35. McCormick, Luftig, and Cunningham, "Economic Might, National Security, and the Future of American Statecraft," 58.
36. "The Birth of NASA," National Aeronautics and Space Administration, March 28, 2008, available at <https://www.nasa.gov/exploration/whyweexplore/Why_We_29.html>.
37. W.D. Kay, *Defining NASA: The Historical Debate Over the Agency's Mission* (Albany: State University of New York Press, 2005), 6.
38. *National Aeronautics and Space Act of 1958*, H.R. 12875, Pub. L. 85-568, 85th Cong., 2nd sess., July 29, 1958, available at <https://history.nasa.gov/spaceact.html>.
39. Suzanne Smalley, "Ex-CISA Chief Krebs Advocates for Standalone Cyber Agency. Experts Say That's Impractical," *Cyberscoop*, August 12, 2022, available at <https://www.cyberscoop.com/cybersecurity-experts-say-cisa-cannot-stand-alone/>.