軍文交織的美國網路防護體系

杜貞儀

網路安全與決策推演研究所

壹、前言

美國網路戰略目標，在於透過改變攻擊者行為、阻絕利益、強加成本建立重層網路嚇阻（Layered Cyber Deterrence），降低重大網路攻擊事件的頻率與嚴重程度，以及對美國國家力量及影響力的傷害。[1]作為少數具備攻勢能力的國家，以往對於美國網路戰略落實的關注，多半在於網路司令部（USCYBERCOM）的形成、整合及形成戰力，如何從前身——戰略司令部（USSTRATCOM）所屬的全球網路作戰聯合特遣部隊（Joint Task Force- Global Network Operation, JTF-GNO）及網戰聯合職能編組指揮部（Joint Functional Component Command- Network Warfare, JFCC-NW）合併，並進一步升格為獨立的單一司令部，較少著墨其軍文交織的面向。雖然美軍已將網路空間作戰（cyberspace operation）明確定義為攻勢網路作戰（Offensive Cyber Operation, OCO）、守勢網路作戰（Defensive Cyber Operation, DCO）以及國防部資訊網路維運（Department of Defense information network（DODIN）Operation）三部分。[2]但屬守勢作為的網路防護，過去較不受外界關注。

然而，隨著網路威脅樣態變化，網路司令部起初以因應伊斯蘭國恐怖攻擊的任務目標與內容，也需逐漸調整、轉向，以對未來的大國競爭做好準備。當美國情報體系指控俄羅斯在 2016 年美國選舉期間進行一系列的干預，試圖影響選舉結果時，美網路司令部在積極防護作

[1] Cyberspace Solarium Commission, “Cyberspace Solarium Report,” March 2020, https://www.solarium.gov/report.

[2] 網路空間任務定義出自“Joint Publication 3-12: Cyberspace Operation,” Joint Chief of Staff, June 8, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf。關於 JTF-GNO 於反恐任務的角色，請另參杜貞儀〈美國網路任務部隊目標標定與效益評估〉,《國防情勢月刊》第 152 期。

為的任務與角色，才逐漸為人所知。2018 年底美國土安全部下新設之網路與基礎設施安全局（Cyber and Infrastructure Security Agency, CISA）成立，整體網路防護體系勢必進行跨部會的整合。

尤其 2020 年底一系列的網路安全事件，更加凸顯跨部會以及公私協力的重要性。包括 SolarWinds 這樣極具針對性、本質上為接近國家層級間諜行為的供應鏈攻擊，以及微軟 Windows Exchange 遭駭事件中，國家行為者的輕率攻擊行徑，與作為關鍵基礎設施的「殖民管道」（Colonial Pipeline）公司遭勒索軟體攻擊，一系列事件的影響層面極廣，現有之美國政府網路防護體系顯得窮於應付。由網路司令部為主體、代表美國國防部及軍方在網路空間執行任務，以及負責境內安全的國土安全部及其網路與基礎設施安全局間，其各自在美國網路防護體系的角色與任務範圍是否須重新檢視，還有哪些可能的改善方向，也是後續檢討的重點。

本文將由美國網路安全體系的防護層面進行探討，並以其軍文交織的特色進行介紹，從中呈現軍方在境內網路防護任務能夠扮演的角色，以做為我國國家網路安全政策方向參考。

貳、美國網路安全體系建構

一、美國網路安全體系建構及網路司令部編制

美國政府的網路安全體系，起初由情報及執法機關組成，包括法務部所屬的聯邦調查局，以及國家安全局（National Security Agency, NSA）。依照 2006 年美《網路作戰之國家軍事戰略》（*National Military Strategy for Cyberspace Operations*）的定義，美軍在網路空間作戰的主要角色有三，分別是：保衛國家、國家級事件應變以及關鍵基礎設施防護。[3]而在網路司令部 2018 年升格為獨立的單一司令部時，與主掌訊

[3] "National Military Strategy for Cyberspace Operations (U)," Joint Chiefs of Staff, December 2006, https://www.hsdl.org/?%20abstract&did=35693. (Unclassified version with redacted)

號情報的國家安全局共享空間、人力與資源，形成「身兼雙職」（dual-hat）的架構，以此加速網路司令部發展，也展現出網路安全與情報密切相關的本質。

網路任務部隊（Cyber Mission Force, CMF）是網路司令部的直屬戰力，依 2012 年經參謀長聯席會議核可的編制，共有 133 支部隊，約 6200 名人員。各部隊依照其職掌與任務，共分為：網路防護隊（Cyber Protection Team）：負責國防部資訊網路（DODIN）防護並在遭到入侵時進行反應；國家任務隊（National Mission Team）負責偵測敵方網路活動、阻止攻擊並反擊；戰鬥任務隊 （Combat Mission Team）則是進行戰鬥網攻行動，以支援網路司令部及各作戰指揮部（Combatant Command）的優先任務；最後則是為國家及戰鬥任務隊提供任務分析與計畫支援的網路支援隊（Cyber Support Team）。[4]

目前網路司令部編制的 133 支網路任務部隊，分別編入直屬網路司令部的國防部資訊網路（Joint Force Headquarters- DOD Information Networks）聯合部隊指揮部、網路聯合部隊指揮部（Joint Force Headquarters- Cyber）、網路國家任務部隊指揮部（Cyber National Mission Force Headquarters）、與各軍種的網路指揮部及各區域作戰指揮部（見圖 1）。[5]其中陸軍常備役共有 41 支網路任務部隊，加上屬預備役之陸軍國民兵的 11 支網路防衛隊，以及陸軍後備役的另外 10 支網路防衛隊，使來自陸軍的網路任務部隊，成為美國網路戰力的最主要構成

[4] 關於美國網路司令部網路任務部隊如何藉由演訓驗證、形成戰力，請參考杜貞儀，〈美國網路任務部隊與訓練環境發展〉，《國防情勢月刊》第 146 期。

[5] "DOD Training: U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Forces," U.S. Government Accountability Office, March 6, 2019, https://www.gao.gov/assets/700/697268.pdf.

單位。[6]

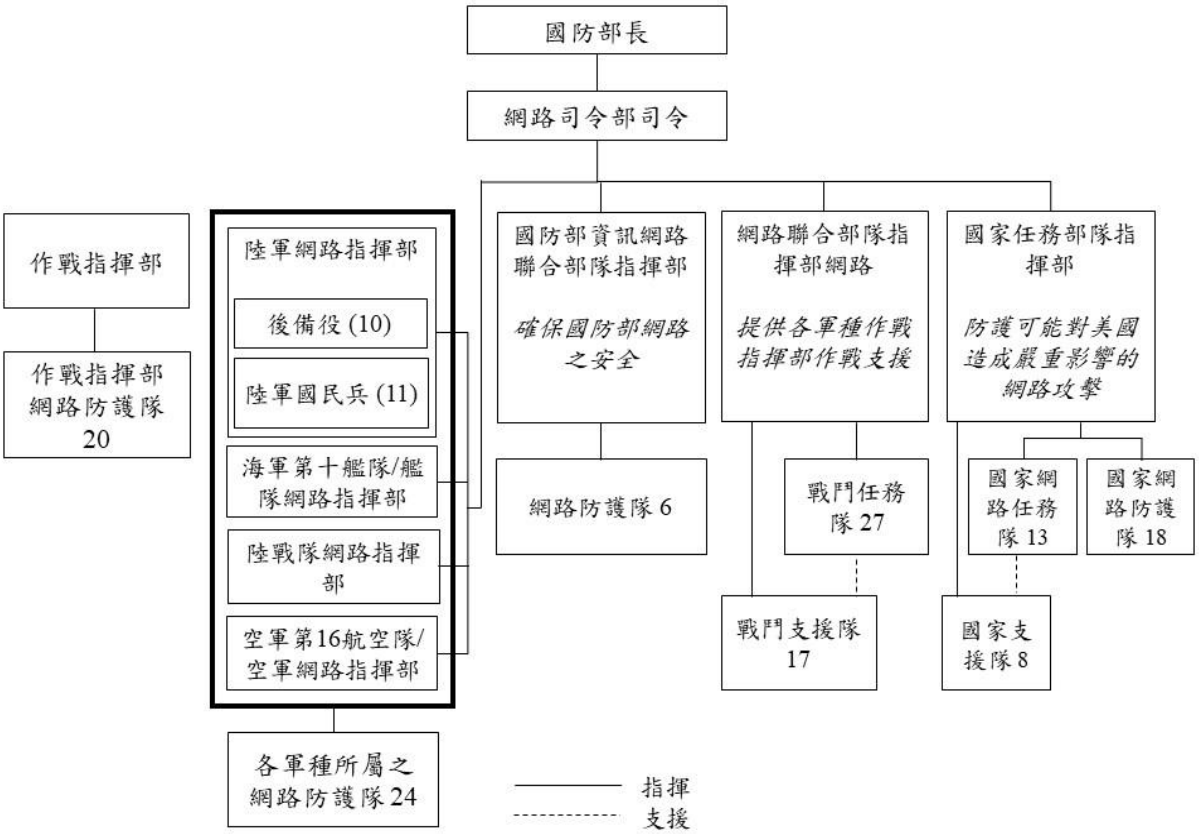

圖 1、美國網路司令部編制及網路任務部隊配屬

資料說明：單位/役別後數字表示所屬網路任務部隊數目，預備部隊之陸軍後備役、國民兵以括弧表示。

資料來源：作者翻譯自美課責審計署報告（見註 5），並參考 2019 年美國空軍第 16 航空隊（Sixteenth Air Force）復編之相關新聞更新單位名稱，見 “Sixteenth Air Force (Air Forces Cyber): Legacy 2021,” June 2021, https://www.16af.af.mil/Portals/80/16%20AF%20Legacy%202021%20(V20210607).pdf?ver=5v8vlCX5WM3PjV_4Pdsr3Q%3d%3d 。

二、國土防衛架構下的網路防護

雖然網路空間沒有明顯疆域，但為了明確定義網路作戰的範圍，美國防部在《聯戰準則 3-12：網路空間作戰》（*Joint Publication 3-12: Cyberspace Operation*）中，仍將網路空間劃分為藍、紅、灰三個部

[6] “DOD Fact Sheet: Cyber Mission Force,” U.S. Army Cyber Command, February 2020, https://www.arcyber.army.mil/Info/Fact-Sheets/Fact-Sheet-View-Page/Article/2079594/dod-fact-sheet-cyber-mission-force/.

分。其中藍色代表美國、其任務夥伴或其他美國防部受命防護的區域。雖然美國防部的現行命令僅防護美國防部網路，但網路部隊亦須為接獲請求時，防護其他美國政府單位、或美國與盟國的關鍵基礎設施進行準備。紅色則是敵方所控制的網路空間，其餘不符合紅或藍兩者定義的區域，則列為「灰色」網路空間。[7]

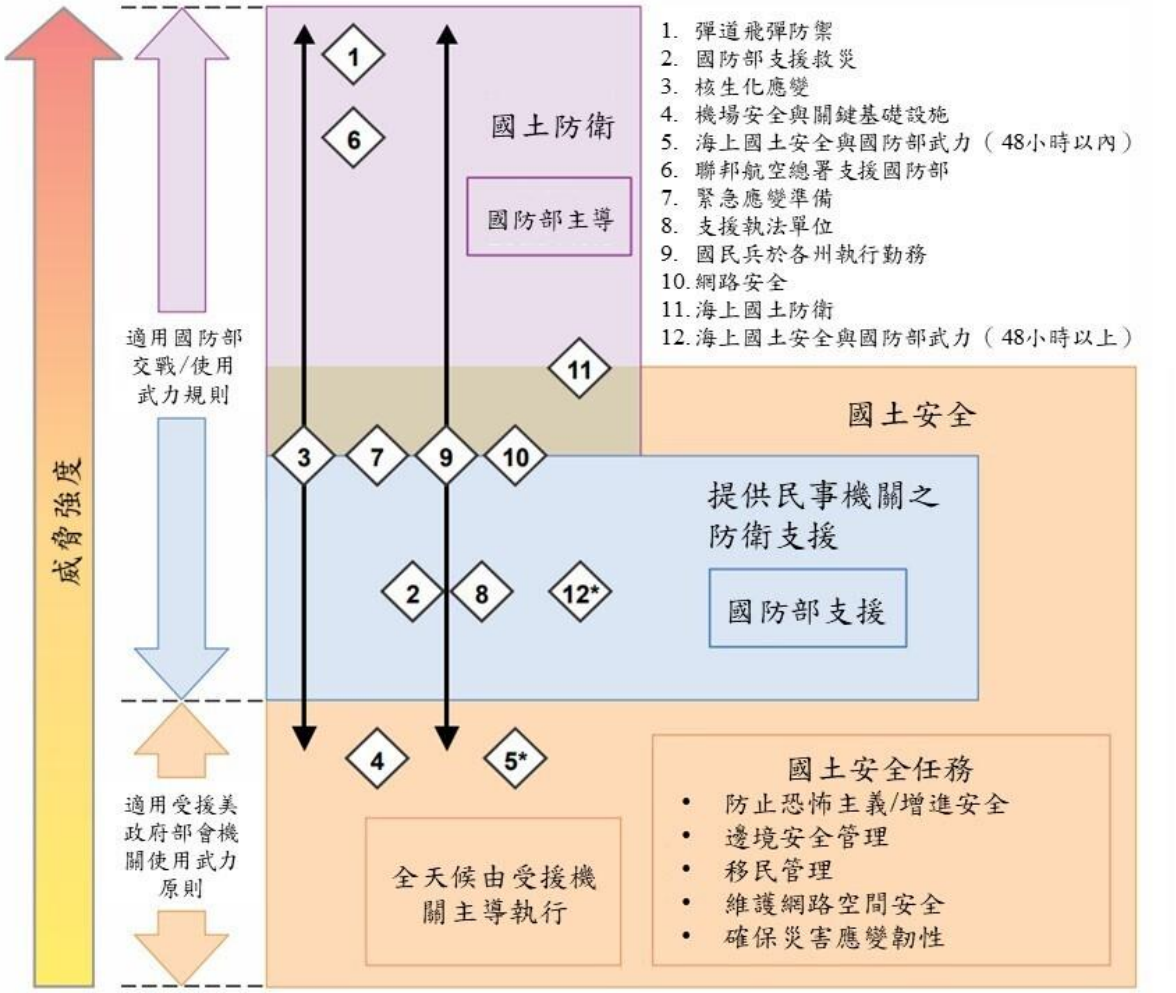

圖 2、美國土防衛、國土安全、提供民事機關之防衛支援間關聯圖

資料說明：網路安全為項目 10，威脅強度略同於緊急應變準備，並適用美國防部交戰/使用武力規則。

資料來源：翻譯自《聯戰準則 3-28：提供民事機關之防衛支援》(*Joint Publication 3-28: Defense Support to Civil Authorities*)

美國既有的國土防衛架構是基於核生化防護、彈道飛彈防禦及反恐等需求而建立的（圖 2），在此架構下，潛在威脅警示、干擾並且擊

[7] "Joint Publication 3-12: Cyberspace Operation," Joint Chief of Staff, June 8, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

退威脅以及保障任務完成（mission assurance）三個部分由國防部主導，而在提供民事機關之防衛支援（Defense Support to Civil Authorities, DSCA）中，國防部另外亦須就救災、執法、緊急應變準備等任務支援其他政府單位。[8] 就如美軍對由執法單位主導的緝毒行動（Counter Narcotics Operation）提供支援，美軍支援國內的網路防護工作，亦同樣以 DSCA 的架構為基礎。[9]

關鍵基礎設施安全則由美國土安全部統籌，並依照關鍵基礎設施特性進一步分為 16 類，各由不同的機關主管與協調。美國防部在關鍵基礎設施安全防護上，具有雙重角色，不僅是聯邦政府的一員，也是國防工業（Defense Industrial Base）關鍵基礎設施的協調機關（Sector-Specific Agencies, SSA）。作為聯邦政府的一員，美國防部在部會層級必須對國防關鍵基礎設施進行威脅辨識、排序、評估、復原及防護的工作，並與其他政府部會機關合作，保護所有關鍵基礎設施及資源。作為國防工業關鍵基礎設施的協調機關，除與公部門合作外，也需要與私部門進行協調。

參、挑戰與未來展望

一、網路防護跨部會合作的實例與挑戰

在網路司令部成立後，就關鍵基礎設施網路防護相關作為，對內分享事件應變情報，對外則持續接戰（Persistent Engagement），以對駭客團體強加攻擊成本的方式，嚇阻進一步攻勢，目前已有兩項公開實例。首先是針對 2020 年美國選舉，有 2016 年俄羅斯干預的前例在先，網路司令部與國家安全局共同成立選舉安全組（Election Security Group），並與聯邦調查局、CISA 進行交換情報。與國民兵的合作，則

[8] "Joint Publication 3-27: Homeland Defense," Joint Chief of Staff, April 18, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_27.pdf.

[9] "Joint Publication 3-28: Defense Support to Civil Authorities," Joint Chief of Staff, October 29, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_28.pdf.

設有仿照醫療後送資料的「資安 9 項」（Cyber 9-line），以結構化的方式擬定狀況回報格式，加速情報分享，讓各州國民兵部隊能夠取得網路司令部的情報並加以運用（圖 3），並在美國大選多州同時舉辦總統候選人初選的「超級星期二」（Super Tuesday）等關鍵時刻提供支援。

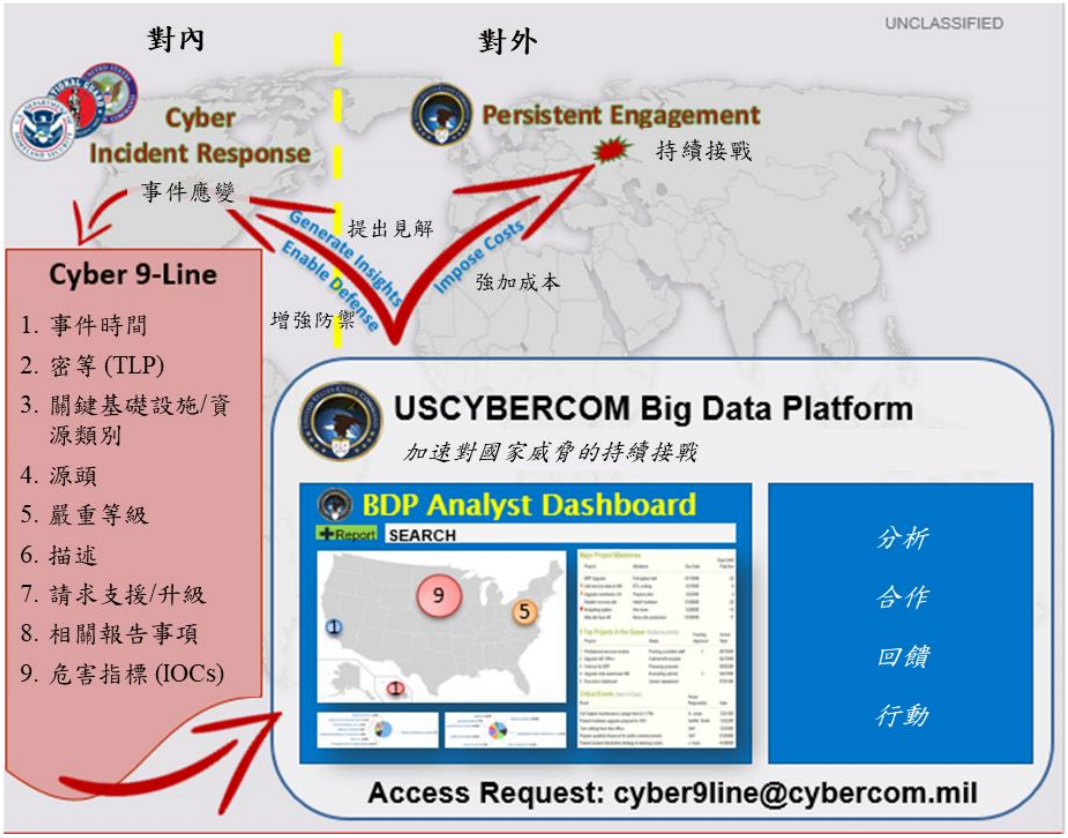

圖 3、「資安 9 項」與網路防護的內外分工

資料來源：美國網路司令部

在 2020 年的新冠肺炎疫情下，這樣的協作機制亦在網路防護上扮演極為重要的角色。由於預期駭客將試圖取得新冠肺炎疫苗開發資料，為支援美政府加速疫苗開發生產的「曲速行動」（Operation Warp Speed），美國土安全部的 CISA 藉由前節敘述之 DSCA 機制，請國民兵及陸軍後備役網路部隊提供醫藥產業之網路安全支援。這也顯示美軍在境內網路安全防護的角色，並不僅限於各級政府機關，在必要時，

協調機關亦能依照既有機制向美國防部提出申請，支援屬於私部門的關鍵基礎設施提供者。[10]

不過，美國防部與國土安全部在網路防護的合作關係，其實仍面臨挑戰。美國防部總督察長曾就十年來雙方合作的概況進行調查，發現美國防部與國土安全部雖然就網路安全合作簽有備忘錄，但並無依照備忘錄制定實施計畫。從幾項實例來看，既有機制似乎能夠運作，不過由於缺乏明確定義雙方角色、責任、里程碑以及完成日期的實施計畫，就保護國家關鍵基礎設施而言，雙方仍可能基於認知差異而影響整體合作。即便 2020 年影響許多聯邦政府部門以及私部門單位 2020 年的 SolarWinds 事件，與明文規定的合作實施計畫無關，本次事件也已彰顯國防部與國土安全部合作因應所有網路威脅時的重要性。若有更具體之規範作法，將能夠幫助雙方達成其維護網路安全的共同目標。[11]

二、建立聯合網路防禦協作機制並提供所需資源因應威脅

基於過往的合作經驗，CISA 依據《2021 財政年度國防授權法》（*National Defense Authorization Act of 2021*, NDAA）所賦予的權限，於 2021 年 8 月宣布成立聯合網路防禦協作機制（Joint Cyber Defense Collaborative, JCDC），以此匯集公私部門協力合作，以共同抵禦關鍵基礎設施的網路威脅，從而引領國家網路防禦計畫的制定。從公開資料中揭示 JCDC 的主要目的，在於藉由這項新的合作機制，協調跨聯邦部門、各州地方政府、民間或組織等合作夥伴，來識別、防禦、檢測和應對涉及國家利益或關鍵基礎設施的惡意網路攻擊，尤其是勒索軟

[10] Paul M. Nakasone, "Posture Statement of General Paul M. Nakasone, Commander, United States Cyber Command, Before the 117th Congress Senate Armed Services Committee," United States Senate Committee On Armed Services, March 25, 2021, https://www.armed-services.senate.gov/download/nakasone_03-25-21.

[11] "Audit of the Department of Defense's Implementation of the Memorandums Between the Department of Defense and the Department of Homeland Security Regarding Cybersecurity and Cyberspace Operations (DODIG-2021-100)," Department of Defense Office of Inspector General, July 12, 2021, https://www.dodig.mil/reports.html/Article/2691902/audit-of-the-department-of-defenses-implementation-of-the-memorandums-between-t/.

體，同時建立事件應變框架，進而提升國家整體資安防護和應變能力。

JCDC 辦公室將由美國土安全部、司法部、網路司令部、國家安全局、聯邦調查局及國家情報總監辦公室（Office of the Director of National Intelligence, ODNI）組成。另外，JCDC 將與自願參與的夥伴合作、協商，包括州、地方、部落和地區政府、資訊共享與分析組織和中心（ISAOs/ISACs），以及關鍵資訊系統的擁有者和營運商，以及其他如微軟、亞馬遜、谷歌等私部門之服務提供商。甫成立之 JCDC，是否能夠自過往合作經驗中學習，釐清各方認知差異、角色、以及責任，將會是後續觀察的重點。

然而，美國土安全部需請求國防部支援，可能也反映文職單位缺乏足夠資源因應威脅的普遍問題。以往大型災害緊急應變，美聯邦政府基於《斯塔福德災害救援和緊急援助法》（*Stafford Disaster Relief and Emergency Assistance Act*）有系統地對州和地方政府提供災難應變的援助，包括動用聯邦基金。需求單位亦可經由 DSCA 機制向國防部提出支援請求，國防部則依法向需求單位報支開銷。[12]此《斯塔福德法》是否適用於網路攻擊所造成的災害，或另設網路安全事件應變與復原基金支應，有待進一步釐清。[13]但基於此法精神，美國防部提供原先任務以外的額外支援，均屬於有償服務（on reimbursable basis）。

最後，網路安全的核心在於人才，美國軍方有其固定培育體系，但文職人員則無，因而由人工智慧國家安全委員會（National Security Commission of Artificial Intelligence, NSCAI）提出設立聯邦數位學院

[12] 如新冠肺炎疫情宣布緊急狀態後的相關支援經費報銷概況，美國防部總督察長辦公室已有初步審計報告公開，詳見 Department of Defense Office of Inspector General, "Audit of the Reimbursement for Department of Defense Mission Assignments for Coronavirus Disease–2019 Pandemic Response in the U.S. Northern Command Area of Responsibility (DODIG-2021-091)," June 11, 2021, https://www.dodig.mil/reports.html/Article/2654551/audit-of-the-reimbursement-for-department-of-defense-mission-assignments-for-co/。

[13] Matt Lyttle & Yvonne Manzo, "When Cyber-Attacks Lead to Disaster, Does Stafford Act Apply?" Infosecurity Magazine, September 3, 2021, https://www.infosecurity-magazine.com/opinions/cyber-attacks-disasters-stafford/.

（Federal Digital Service Academy） 的倡議，並得到國際國防通信電子協會（AFCEA International）的支持，希望能夠藉由設立專注於網路安全與人工智慧的文官學院，來培育聯邦政府的數位、網路相關文職人才。[14]不過，拜登政府目前的網路安全政策規劃中，尚未提及人才培育部分，此可能因疫情與其他更急迫之議題，而未有機會進一步討論，但此仍將會是對於解決人力短缺的選項之一。

肆、結語

從美國網路防護體系的發展以及實際案例，可看出建構如民事機關之防衛支援（Defense Support to Civil Authorities, DSCA）的具體機制，是軍方參與關鍵基礎設施網路安全防護的基礎條件，並明確界定主導者、參與角色以及分工。確立情報分享機制，則能更有效的促進橫向聯繫以及情報運用。然而即使美網路司令部，其主要任務仍是對外持續接戰，尤其威脅情報有價，進行資訊分享與交換並提供實質支援，均有其成本，只有互利互惠的機制才能持續運作。對於與日俱增的網路安全威脅，無論災害緊急應變《斯塔福德法》未來是否涵蓋網路攻擊所造成的災害，或另設基金支應，美國拜登政府於建立聯合網路防禦協作機制、提供各級政府應變資源依據並強化政府相關人才培育的動向，仍值得持續觀察。

本文作者杜貞儀為國立臺灣大學海洋所理學博士，現為財團法人國防安全研究院網路安全與決策推演研究所助理研究員。

[14] AFCEA International, “Establishing a Federal Digital Service Academy,” *SIGNAL Magazine*, April 2021, https://www.afcea.org/signal/resources/linkreq.cfm?id=349.

The interwoven US civil-military cyber protection system

Chen-Yi Tu

Assistant Research Fellow

Abstract

The objectives of US cyber strategy is to establish Layered Cyber Deterrence through shaping behavior, denying benefits and imposing costs to reduce the frequency of severe cyber attacks and their damages to US national power and influence. Previous study on the implementation of US cyber strategy usually focused on the formation, integration, and achieving operational capabilities of the United States Cyber Command. The defensive cyber operation, however, receives relatively less attention. Civil-military interweaving is one of the major characteristics of the US cyber defense. Within the current homeland defense framework, the US Department of Defense supports other government units for disaster response, law enforcement and other missions through mechanism of Defense Support to Civil Authorities (DSCA). The US military also supports domestic cyber defense with the same mechanism. Some existing examples of such supports are election security and COVID-19 vaccine development, both span across the public and private sectors. Therefore, building a mechanism such as the DSCA is fundamental for military participation in the cyber defense of critical infrastructure. Moreover, establishing an intelligence sharing mechanism can further enhance the lateral communication and effective use of intelligence.

Keywords: cyber defense, homeland defense, critical infrastructure, whole-of-government approach