全球政治評論　*Review of Global Politics*

第七十七期（2022）No.77 頁 11-17

焦點評析

國家安全概念的再思考：以網路科技在當代美國國家安全戰略中的地位與表現為例

Rethinking the Concept of National Security: Taking the Status and Practice of Cyber Technology in Contemporary U.S. National Security Strategy as a Study Case

張凱銘 *Kai-Ming Chang*
國立臺中科技大學通識教育中心助理教授
Assistant Professor of Center for General Education
National Taichung University of Science and Technology

國家安全（National Security）長期以來皆處於國際關係研究的核心區塊，根據新現實主義（Neo-realism）等主流學派的觀點，由於國際社會一向處於缺乏權威規範的無政府狀態（Anarchy）之中，作為理性行為體的主權國家為求生存無虞，自然傾向於將確保自身安全作為優先考量。[1] 而在歷經兩次世界大戰與漫長冷戰（Cold War）競逐之後，近代國際關係研究對於國家安全議題的探討，多以國防軍事問題為關注焦點，國家的先進戰備、大規模毀滅性武器（Weapon of Mass Destruction, WMD）開發進程、海外駐軍部署態勢、

[1] Kenneth N. Waltz, *Theory of International Politics* (New York: McGraw-Hill, 1979), p. 168.

跨國防務合作等議題，再過往相當長的時間中，幾乎便等同於國家安全研究的主要內容。

然而隨著冷戰於 1980 年代晚期逐漸走向終結，國際關係學界對於安全議題的觀察也逐漸出現轉型趨向，在關注以軍事及外交折衝為主的傳統安全（Traditional Security）問題之餘，對於各類非傳統安全威脅（Non-traditional Security Threats）的討論也日益增加，部分學者注意到過去被視為低階政治（Low Politics）的許多議題，對於國家安全的影響程度在當代世界中迅速升高。雖然國家間的軍力建設與武器發展仍然十分重要，但來自於氣候變遷、國際犯罪、流行疾病與糧食短缺等問題的威脅似乎顯得更為迫切且常見。非傳統安全威脅研究的興起，意味著今日的國家安全較諸往昔有著更為豐富多元的內涵，世界各國的國安戰略規劃必須進行相應調整，方能在複雜而變遷迅速的後冷戰時代中有效確保本國的安全生存並謀求發展利益。就此而言，網路科技近年在美國國家安全戰略中迅速提升的重要性及連動政策表現，或可作為觀察者再思當代國家安全概念的參考案例。

回顧歷史脈絡，網路科技於 1980 年代後漸進融入人類文明各個面向，在行政治理、經濟產業、社會文化乃至各地人民日常生活的食衣住行育樂之中皆扮演起越來越吃重的角色，各國政府也在這一過程中漸進地認識理解發展網路科技、支持資訊產業成長，以及維護網路系統安全的重要性，進而體認網路科技的高度戰略價值，將其納入國家安全戰略規劃之中。以作為全球資訊科技領導強權的美國為例，華府當局早於 1990 年代後便已注意到網路科技的廣泛影響，以及加強國家資安防護的重要性，包括柯林頓（William J. Clinton）政府與其後執政的小布希（George W. Bush）政府皆以聯邦層級的高度頒佈過多項政策指令，力求加速本國科技研發創新進程，以及強化網路科技應用中的法令監管和安全防護措施。若深入檢閱相關政策文件如《國家資訊基礎建設行動議程》（*The National Information Infrastructure: Agenda for Action*）、《保衛美國的網路空間：國家資訊系統防護計畫》（*Defending America's Cyberspace: National Plan for Information Systems Protection*）與《國家網路安

全戰略》（*The National Strategy to Secure Cyberspace*）等，[2] 可發現美國政府在 1990 年代以至 21 世紀初期間，賦予網路科技越來越高的重視，整體上雖仍較傾向於以技術角度看待此議題，但已隱約將其與國家安全戰略進行連結。這一情形至 2009 年後出現轉變，歐巴馬（Barack H. Obama）政府明確將網路科技納入國安戰略規劃當中，透過《網路空間國際戰略》（*International Strategy for Cyberspace*）與《網路空間政策評估：確保可靠而靈活的資通訊基礎設施》（*Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*）等文件的發表，向國內外社會宣示網路科技既是具備高度專業的新興科技領域，也是美國國家安全戰略規劃的重要區塊。[3]

2017 年後，隨著抗衡中國成為美國外交核心議程，網路科技在美國國安戰略中的地位更呈現急劇上升的趨勢。川普（Donald J. Trump）政府於 2017 版《國家安全戰略》（*National Security Strategy, NSS*）中，以相當篇幅闡述網路科技對於美國國安防衛與維繫國際領導地位的重要性，隨後更發表了《國家網路戰略》（*National Cyber Strategy, NCS*），深入說明網路科技戰略價值的同時，也指出美國在網路領域正遭遇來自中國等強大競爭對手的挑戰，並據以制定多重因應對策。[4] 美國國務院（U.S. Department of State）更在網路戰略論述的基礎上，進一步制定了《關鍵新興技術國家戰略》（*National Strategy for Critical and Emerging Technology*），羅列人工智慧（Artificial Intelligence）、量子資訊科學（Quantum Information Science）、通訊和網路技術（Communication and Networking Technologies）等二十項關鍵新興技術，強調

---

[2] U.S. Department of Commerce, *The National Information Infrastructure: Agenda for Action*, September 15, 1993；The White House, *Defending America's Cyberspace: National Plan for Information Systems Protection*, January 2000；The White House, *The National Strategy to Secure Cyberspace*, February 2003.

[3] 2009；The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, May 2011；The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, April 2013.

[4] The White House, *National Cyber Strategy*, September 2018.

對於相關技術的掌握攸關美國的國家安全與整體發展前景。[5] 拜登（Joseph R. Biden Jr.）政府的為政思維雖與前任多有扞格，但其提出的國安戰略規劃同樣賦予網路科技高度重視，在《國家安全戰略臨時指南》（*Interim National Security Strategic Guidance*）的論述中，視相關科技為牽動戰略安全與國際權力格局發展趨向的關鍵因素，並力求因應來自中俄等競爭對手的挑戰。[6]

綜觀上述歷程，可發現網路科技於過往數十年間漸由單純的新興專業科技，逐漸為美國政府納為國家安全戰略的一環，其論述要旨可概要歸納為以下兩點：第一，美國政府看待網路科技的角度逐漸轉變，視其為國家安全構成的重要部分，認為若無法維持在此一領域的技術領先優勢，將對本國的國家安全與國際社會地位造成嚴重損害。第二，出於國安考量，美國政府不僅制定了國家層級的網路戰略，更將人工智慧、量子計算等具前瞻性的專門技術逐步納入經略範疇之中。第三，美國政府認為自身在網路科技領域正面臨來自中國等地緣競爭對手的強力挑戰，由於網路科技已成其國家安全的核心組成，相關挑戰遂被美方界定為國安戰略威脅。

透過國家安全角度觀察美國政府近年推動的各項與網路科技相關政策作為，觀察者可發現其施政在完善治理工作的同時，也隱然反映出對國安威脅的因應意涵。根據新現實主義學派的觀點，國家面臨安全挑戰時，在確保生存無虞的理性驅動之下將採取行動平衡對手，常見做法如旨在提升自身實力的內部平衡（Internal Balance）策略、旨在擴大國際聯合的外部平衡（External Balancing）策略，以及透過低強度手段牽制妨礙對手的柔性平衡（Soft Balancing）策略等。[7] 自 2017 年以來，川普與拜登兩任政府的網路施政便在一定程度上展現了平衡策略的具體實踐：

---

[5] U.S. Department of State, *National Strategy for Critical and Emerging Technology*, October 2020.

[6] The White House, *Interim National Security Strategic Guidance*, March 2021.

[7] Kenneth N. Waltz, *Theory of International Politics*, (New York: McGraw-Hill, 1979), pp. 116-128；鄭端耀，〈搶救權力平衡理論〉，收於包宗和主編，《國際關係理論》（臺北：五南圖書，2011 年），頁 69-83。

首先，在內部平衡部分，美國政府的政策目標為提升自身的研發創新與技術防護能力，執行重點包含「完善國內網路基礎設施佈建」、「強化研發創新能力」與「積極應對惡意活動」等三者。在基礎建設方面，川普政府任內陸續發佈的「第 13800 號行政命令」（Executive Order 13800）與「第 13821 號行政命令」（Executive Order 13821），皆以改善國內各地區網路系統設備佈建為目標，要求行政部門汰換過於老舊的軟硬體設施，藉以提升科技應用水準，並有效降低遭遇網路攻擊與數位盜竊損害的風險。在強化研發創新方面，中國近年在網路科技領域的迅速進步使美國政府頗感焦慮，憂心自身的技術領先優勢將逐漸消逝。例如美國人工智慧國家安全委員會（National Security Commission on Artificial Intelligence, NSCAI）在 2021 年初發表的最終評估報告（*Final Report*）中指出，美國須加速推動人工智慧開發應用，否則將在未來數年間遭到中國超越。[8] 而中國在 5G 行動通訊科技方面的成就，更使美方倍感不安。因此，華府當局近年在科技施政中陸續推出擴大研發投資、加強人才培育招募、促進產官學合作、放寬創新監管、鼓勵與友好國家間的技術交流等措施，藉以確保本國在資訊科技領域的地位不受動搖。在應對惡意活動方面，鑑於來自他國與非國家行為體的網路惡意活動日益增加，美國政府近年積極強化網路防護能力，除將網路司令部（Cyber Command）升格為聯合作戰司令部（Unified Combatant Command, UCC）並擴大開發網路戰備外，更以川普總統簽署的「第 13 號國家安全總統備忘錄」（National Security Presidential Memorandum 13, NSPM 13）取代歐巴馬政府任內制訂的「第 20 號總統政策指令」（Presidential Policy Directive 20, PPD20），大幅簡化美軍對外發起網路軍事行動的監管流程，俾提升網路嚇阻與反擊能力。

其次，在外部平衡部分，美國近年以遍佈全球各地的廣闊同盟網絡為基礎，邀集親近國家在網際網路治理、技術研究開發與資安威脅應對等事務上

[8] U.S. National Security Commission on Artificial Intelligence, *Final Repor*t (Washington, D.C.: U.S. National Security Commission on Artificial Intelligence, 2021), pp. 161-163.

加強多邊與雙邊合作。美國與他國在網路事務的多邊合作，以網際網路規範的制定探索工作最具代表性。自歐巴馬政府執政時期以來，美國長期透過「聯合國政府專家工作組」（United Nations Governmental Group of Expert, UNGGE）等平台，與世界各國就網路空間中的國家行為準則設立問題進行磋商，針對將《聯合國憲章》（*Charter of the United Nations*）第 51 條自衛權行使導入網路規範中等敏感議題，積極尋求友好國家的支持。[9] 在雙邊合作方面，美國自 2017 年以來至今，陸續和以色列、英國、澳洲、日本等國家建立網路工作組等雙邊資安合作機制，甚或共同開發配置人工智慧的先進戰備，同時與各國就資訊技術產品出口管制議題進行政策協調。[10]

最後，在柔性平衡方面，美國政府近年積極加強對網路惡意活動的司法偵察工作，同時對外國企業發起的科技產業投資與併購案進行嚴格審查，以防範他國透過數位盜竊和商業手段削弱美國的技術優勢。面對中國近年在資訊領域的強勢崛起，以及習近平政權追求「網路強國」地位等野心，美國商

---

[9] 請參考：Eneken Tikk-Ringas, *Developments in the Field of Information and Telecommunications in the Context of International Security* (Geneva: ICT for Peace Foundation, 2012), pp. 7-9；G7 Summit, "G7 Declaration on Responsible States Behavior in Cyberspace," *https://www.mofa.go.jp/files/000246367.pdf*, April 11, 2017

[10] 請參考：Mark Pomerleau, "Cyber protection teams assigned to THAAD in South Korea," *Fifth Domain*, (June 1, 2017), *https://www.fifthdomain.com/home/2017/06/01/cyber-protection-teams-assigned-to-thaad-in-south-korea/.*；Steven Scheer, "U.S. to Work with Israel, Seek other Ties to Combat Cyber Attacks," *Reuters*, (June 26, 2017), *https://www.reuters.com/article/us-usa-israel-cyber-idUSKBN19H1KE.*；American Institute in Taiwan, "Remarks by AIT Deputy Director Raymond Greene at Opening Ceremony of GCTF on Network Security and Emerging Technologies," *American Institute in Taiwan*, (May 28, 2019), *https://www.ait.org.tw/remarks-by-ait-deputy-director-greene-at-opening-ceremony-of-gctf-on-network-security-and-emerging-technologies/.*；Andrew Greene, "Australian-made Loyal Wingman Air Combat Drone with AI-driven Targeting System Completes First Test Flight," *ABC News*, (March 2, 2021), *https://www.abc.net.au/news/2021-03-02/loyal-wingman-first-flight-australia-boeing/13207388.*

務部工業安全局（Bureau of Industry and Security, BIS）也以涉入人權迫害、損害美國國家安全與外交利益等理由，對華為、海康威視、科大訊飛、雲從科技、中芯國際等具代表性的中國資訊企業列入「實體清單」（Entity List）施加制裁，藉以阻滯中國的資訊科技發展步伐。[11]

經由審視網路科技在當代美國國家安全戰略中的地位變化與實際政策表現，觀察者當可察見國家安全概念在後冷戰時代的顯著轉變。軍事與外交折衝雖仍在國安領域佔據核心地位，但各種新興科技與全球議題，也在現代國家的安全維護上扮演越來越重要的地位，各國政府若無法即時洞察這一趨勢，未能由國家戰略高度通盤籌劃施政方針，勢將對本國的安全防護與利益追求帶來負面影響，在變遷迅速的國際競合中也將落入相對不利的地位。

責任編輯：傅家鈺

[11] 請參考：Bureau of Industry and Security: Entity List, *https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list*.